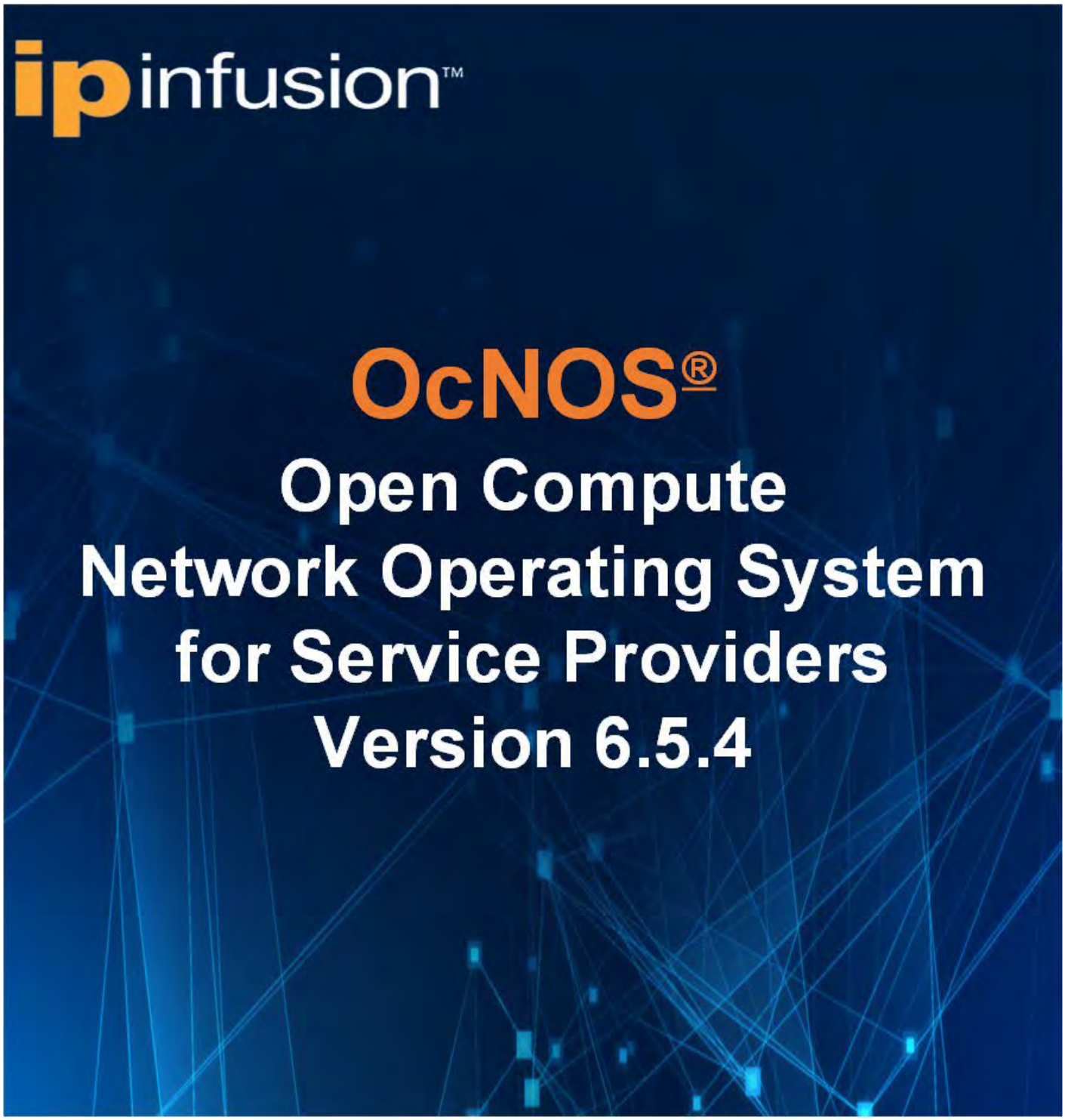


System Management Guide

April 2025

IP Infusion Inc. Proprietary

© 2025 IP Infusion Inc. All Rights Reserved.

This documentation is subject to change without notice. The software described in this document and this documentation are furnished under a license agreement or nondisclosure agreement. The software and documentation may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of IP Infusion Inc.

IP Infusion Inc.

3979 Freedom Circle

Suite 900

Santa Clara, California 95054

http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Trademarks:

IP Infusion and OcNOS are trademarks or registered trademarks of IP Infusion. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Use of certain software included in this equipment is subject to the IP Infusion, Inc. End User License Agreement at http://www.ipinfusion.com/license. By using the equipment, you accept the terms of the End User License Agreement.

Contents

Preface 30
IP Maestro Support 30
Audience 30
Conventions 30
Chapter Organization 30
Related Documentation 30
Feature Availability 31
Migration Guide 31
Support 31
Comments 31

Command Line Interface 32
Overview 32
Command Line Interface Help 32
Command Completion 33
Command Abbreviations 33
Command Line Errors 33
Command Negation 34
Syntax Conventions 34
Variable Placeholders 35
Command Description Format 36
Keyboard Operations 36
Show Command Modifiers 37
String Parameters 40
Command Modes 40
Transaction-based Command-line Interface 42

Authentication Management Configuration 43

CHAPTER 1 AAA Configuration for Console Connection 44
Overview 44
Configuration 44
Glossary 47

CHAPTER 2 Restricted Access to Privilege Mode based on User Role 48
Overview 48
Prerequisites 48
Configuration 48
New CLI Commands 50
Glossary 51

CHAPTER 3 RADIUS Client Configuration 52
Overview 52
RADIUS Authorization Configuration 52
Implementation Examples 56
RADIUS Server Authentication Configuration 56

RADIUS Server Accounting 64
Sample Radius Clients.conf File 65
Sample Radius Users Configuration File 65
Fall Back Option for RADIUS Authentication 66
Configuration 66

CHAPTER 4 TACACS Client Configuration 68
Overview 68
TACACS Server Authentication 68
TACACS Server Accounting 79
TACACS Server Authorization 81
TACACS Server Authentication for User Defined VRF 83
TACACS Server Accounting 92
TACACS Server Authorization 93

CHAPTER 5 Role-Based Access Control. 96
Overview 96
Prerequisites 97
Configuration 97
Implementation Examples 99
New CLI Commands 99
Troubleshooting 105
Abbreviations 105
Glossary 106

Authentication Management Command Reference 107

CHAPTER 1 Authentication, Authorization and Accounting 108
aaa authentication login 109
aaa accounting details 110
aaa authentication login default 111
aaa authorization default 112
aaa authentication login default fallback error 113
aaa group server 114
aaa local authentication attempts max-fail 115
aaa local authentication unlock-timeout 116
debug aaa 117
server 118
show aaa authentication. 119
show aaa authentication login 120
show aaa authorization 121
show aaa groups 122
show aaa accounting 123
show running-config aaa 124

CHAPTER 2 TACACS+ Commands 125
clear tacacs-server counters 126
debug tacacs+ 127
feature tacacs+. 128

show debug tacacs+ . . . 129
show running-config tacacs+ . . . 130
show tacacs-server . . . 131
tacacs-server login host . . . 133
tacacs-server login key . . . 135
tacacs-server login timeout . . . 136

CHAPTER 3 RADIUS Commands . . . 137
clear radius-server . . . 138
debug radius . . . 139
radius-server login host . . . 140
radius-server login host acct-port . . . 142
radius-server login host auth-port . . . 143
radius-server login host key . . . 144
radius-server login key . . . 146
radius-server login timeout . . . 147
show debug radius . . . 148
show radius-server . . . 149
show running-config radius . . . 151

Remote Device Connect Configuration . . . 152

CHAPTER 1 Telnet Configuration . . . 153
Overview . . . 153
Telnet Configuration with IPv4 Address . . . 153
Telent Configuration with IPv6 Address . . . 154

CHAPTER 2 SSH Client Server Configuration . . . 160
Overview . . . 160
SSH Configuration . . . 160
SSH Encryption . . . 163
SSH Key-Based Authentication . . . 168

CHAPTER 3 Max Session and Session Limit Configuration . . . 172
Overview . . . 172
Configuration of SSH Server Session Limit Lesser than Max-Session . . . 173
Configuration of Telnet Session Limit Greater than Max-Session . . . 174
Configuration of SSH Session Limit Greater than Max-Session . . . 175

Remote Device Connect Command Reference . . . 176

CHAPTER 1 Telnet . . . 177
debug telnet server . . . 178
feature telnet . . . 179
show debug telnet-server . . . 180
show running-config telnet server . . . 181
show telnet-server . . . 182
telnet . . . 183
telnet6 . . . 184
telnet server port . . . 185

© 2025 IP Infusion Inc. Proprietary

telnet server session-limit . . . 186

CHAPTER 2 Secure Shell Commands . . . 187
clear ssh host-key . . . 188
clear ssh hosts . . . 189
clear ssh keypair . . . 190
debug ssh server . . . 191
feature ssh . . . 192
show debug ssh-server . . . 193
show running-config ssh server . . . 194
show ssh host-key . . . 195
show ssh server . . . 197
show username . . . 198
ssh . . . 199
ssh6 . . . 200
ssh algorithm encryption . . . 202
ssh keygen host . . . 204
ssh login-attempts . . . 206
ssh server algorithm encryption . . . 207
ssh server algorithm kex . . . 209
ssh server algorithm mac . . . 211
ssh server default algorithm . . . 213
show ssh server algorithm . . . 214
ssh server port . . . 215
ssh server session-limit . . . 216
username sshkey . . . 217
username keypair . . . 218

User Management Configuration . . . 219

CHAPTER 1 Using the Management Interface . . . 220
Overview . . . 220
Management Port . . . 220
In-Band Ports . . . 221

CHAPTER 2 User Configuration . . . 223
Overview . . . 223

CHAPTER 3 Configurable Password Policy . . . 225
Overview . . . 225
New CLI Commands . . . 228
Max Password Age . . . 235
New CLI Commands . . . 237
Removing Users with Expired Passwords . . . 238
Glossary . . . 239

CHAPTER 4 In-band Management over Custom VRF . . . 240
Overview . . . 240
Configuration . . . 240
Implementation Examples . . . 246

Glossary 246

User Management Command Reference 248

CHAPTER 1 User Management 249
clear aaa local user lockout username 250
debug user-mgmt 251
show user-account 252
username 253

DHCP Configuration 255

CHAPTER 1 DHCP Client Configuration 256
Overview 256
DHCP Client Configuration for IPv4 256
DHCP Client Configuration for IPv6 257

CHAPTER 2 DHCP Server Configuration 260
Overview 260
DHCP Server Configuration for IPv4 260
DHCP Server Configuration for IPv6 263

CHAPTER 3 DHCP Server Group 266
Overview 266
Configuration 267
New CLI Commands 280
Abbreviations 284
Glossary 284

CHAPTER 4 DHCP Relay Agent Configuration 285
Overview 285
DHCP Relay for IPv4 285
DHCP Relay for IPv6 Configuration 286
DHCP Relay option 82 287
Physical Interface Configuration with non-default VRF 290
DHCP-Relay with different VRFs 295
DHCP Relay for IPv6 Configuration with different VRFs 297

CHAPTER 5 DHCP Relay Agent Over L3VPN Configuration 299
DHCP Relay Over L3 VPN for IPv4 299

CHAPTER 6 DHCPv6 Prefix Delegation Configuration 308
Overview 308
Configuration 308
DHCP Multiple Prefix Delegation Command 314
Revised CLI Commands 314
Glossary 315

CHAPTER 7 DHCPv6 Relay Prefix Delegation Route Injection Configuration . . 316
Overview 316
Topology 316

DHCP Command Reference 321

CHAPTER 1 Dynamic Host Configuration Protocol Client 322
feature dhcp 323
ip address dhcp 324
ip dhcp client request 325
ipv6 address dhcp 326
ipv6 dhcp address-prefix-length 327
ipv6 dhcp client request 328
ipv6 dhcp client 330
show ipv6 dhcp vendor-opts 332

CHAPTER 2 Dynamic Host Configuration Protocol Relay 333
clear ip dhcp relay option statistics 335
clear ipv6 dhcp pd-route (|vrf NAME) 336
clear ip dhcp relay statistics 337
ip dhcp relay (configure mode) 338
ip dhcp relay (interface mode) 339
ip dhcp relay (L3VPN) 340
ip dhcp relay address 341
ip dhcp relay address global 342
ip dhcp relay information option 343
ip dhcp relay information option always-on 344
ip dhcp relay information source-ip 345
ipv6 dhcp relay (configure mode) 346
ipv6 dhcp relay (interface mode) 347
ipv6 dhcp relay (L3VPN) 348
ipv6 dhcp relay address 349
ipv6 dhcp relay address global 350
ipv6 dhcp relay pd-route-injection 351
ipv6 dhcp relay subscriber-id 352
show ip dhcp relay 353
show ip dhcp relay address 354
show ip dhcp relay option statistics 355
show ip dhcp relay statistics 356
show ipv6 dhcp pd-route 357
show ipv6 dhcp relay 358
show ipv6 dhcp relay address 359
show running-config dhcp 360

CHAPTER 3 DHCPv6 Prefix Delegation Commands 361
ipv6 address 362
ipv6 dhcp prefix-delegation 363
show ipv6 dhcp interface 364

CHAPTER 4 DHCP Server Commands 365
address range low-address A.B.C.D (high-address A.B.C.D|) 366
address range low-address X:X::X:X (high-address X:X::X:X|) 367
boot-file 368

© 2025 IP Infusion Inc. Proprietary

dns-server A.B.C.D . . . 369
dns-server X:X::X:X . . . 370
domain-name . . . 371
host-name . . . 372
ip dhcp server (interface mode) . . . 373
ip dhcp server default-lease-time . . . 374
ip dhcp server max-lease-time . . . 375
ip dhcp server pool . . . 376
ipv6 dhcp server (interface mode) . . . 377
ipv6 dhcp server pool . . . 378
ipv6 dhcp server preference . . . 379
ipv6 dhcp server rapid-commit . . . 380
log-server . . . 381
network A.B.C.D netmask A.B.C.D . . . 382
network X:X::X:X netmask <1-128> . . . 383
ntp-server A.B.C.D . . . 384
ntp-server X:X::X:X . . . 385
prefix high-range X:X::X:X low-range X:X::X:X netmask <1-128> . . . 386
routers A.B.C.D . . . 387
temporary address X:X::X:X . . . 388
tftp-server . . . 389
vendor-options . . . 390

DNS Configuration . . . 391

CHAPTER 1 DNS Configuration . . . 392
Overview . . . 392

CHAPTER 2 DNS Relay Configuration . . . 396
Topology . . . 396
Linux Configuration on the DNS client . . . 396
Linux Configuration on the DNS server . . . 396
OcNOS Configuration . . . 397
Validation . . . 397

DNS Command Reference . . . 399

CHAPTER 1 Domain Name System Commands . . . 400
debug dns client . . . 401
ip domain-list . . . 402
ip domain-lookup . . . 403
ip domain-name . . . 404
ip host . . . 405
ip name-server . . . 406
show hosts . . . 407
show running-config dns . . . 409

CHAPTER 2 Domain Name System Relay Commands . . . 410
ip dns relay (global) . . . 411

ip dns relay (interface) . . . 412
ip dns relay address . . . 413
ip dns relay uplink . . . 414
ipv6 dns relay (global) . . . 415
Ipv6 dns relay (interface) . . . 416
ipv6 dns relay address . . . 417
ipv6 dns relay uplink . . . 418
show ip dns relay . . . 419
show ip dns relay address . . . 421
show ipv6 dns relay . . . 422
show ipv6 dns relay address . . . 423
show running-config dns relay . . . 424

NTP Configuration . . . 425

CHAPTER 1 NTP Client Configuration . . . 426
Overview . . . 426
NTP Modes . . . 426
NTP Client Configuration with IPv4 Address . . . 427
NTP Client Configuration with IPv6 Address . . . 430

CHAPTER 2 NTP Server Configuration . . . 435
Topology . . . 435
Configuration of VRF Management . . . 435
Configuration of User Defined VRF . . . 436
Synchronization of more than one NTP clients with the NTP Master . . . 437
Topology . . . 437
Configuration of VRF Management . . . 438
Configuration of User Defined VRF . . . 439
Synchronization with Authentication . . . 441
Topology . . . 441
Configuration of VRF Management . . . 442
Configuration of User Defined VRF . . . 443
Synchronization of NTP Server and NTP Clients with NTP ACL . . . 445
Topology . . . 446
Configuration of VRF Management . . . 446
Configuration of User Defined VRF . . . 448
Synchronization of NTP Server and NTP Clients with NTP ACL configured as noserve 450
Synchronization of NTP Client with Stratum 2 NTP Master . . . 454
Topology . . . 454
Configuration of Management VRF . . . 455
Configuration of User Defined VRF . . . 456

NTP Command Reference . . . 459

CHAPTER 1 Network Time Protocol . . . 460
clear ntp statistics . . . 461

debug ntp . . . 462
feature ntp . . . 463
ntp acl . . . 464
ntp authenticate . . . 466
ntp authentication-key . . . 467
ntp enable . . . 468
ntp discard . . . 469
ntp logging . . . 470
ntp master . . . 471
ntp master stratum . . . 472
ntp peer . . . 473
ntp request-key . . . 475
ntp server . . . 476
ntp sync-retry . . . 478
ntp trusted-key . . . 479
show ntp authentication-keys . . . 480
show ntp authentication-status . . . 481
show ntp logging-status . . . 482
show ntp peer-status . . . 483
show ntp peers . . . 485
show ntp statistics . . . 486
show ntp trusted-keys . . . 488
show running-config ntp . . . 489

Fault Management System Configuration . . . 490

CHAPTER 1 Fault Management System Configuration . . . 491
Implementation . . . 492
Enabling and Disabling the Fault Management System . . . 492
Alarm Configuration File . . . 492
Auto Generating the Alarm Configuration File . . . 493
Alarm Descriptions . . . 494

CHAPTER 2 Event Manager . . . 497
Overview . . . 497
Configuration . . . 499
Event Manager Commands . . . 500
Glossary . . . 508

Fault Management Sytem Command Reference . . . 510

CHAPTER 1 FMS Command Reference . . . 511
fault-management (enable | disable) . . . 512
fault-management close . . . 513
fault-management flush-db . . . 514
fault-management shelve . . . 515
show alarm active . . . 516
show alarm closed . . . 517

show alarm history . . . 518
show alarm shelved . . . 519
show alarm statistics . . . 520
show alarm transitions . . . 521
show fms status . . . 522
show fms supported-alarm-types . . . 523
show running-config fault-management . . . 524

SNMP Configuration . . . 525

CHAPTER 1 Simple Network Management Protocol . . . 526
Overview . . . 526
Topology . . . 526
Standard SNMP Configurations over User Defined VRF . . . 527
SNMP Trap Server Configuration with IPv6 Address . . . 529
SNMP Informs with IPv6 Address over User Defined VRF . . . 531

SNMP Command Reference . . . 534

CHAPTER 1 Simple Network Management Protocol . . . 535
debug snmp-server . . . 537
show running-config snmp . . . 538
show snmp . . . 539
show snmp community . . . 540
show snmp context . . . 541
show snmp engine-id . . . 542
show snmp group . . . 543
show snmp host . . . 544
show snmp user . . . 545
show snmp view . . . 546
snmp context . . . 547
snmp ent-ipi-iftable . . . 548
snmp-server community . . . 549
snmp-server community-map . . . 550
snmp-server contact . . . 551
snmp-server context . . . 552
snmp-server disable default . . . 553
snmp-server enable snmp . . . 554
snmp-server enable traps . . . 555
snmp-server engineID . . . 557
snmp-server group . . . 558
snmp-server host . . . 560
snmp-server location . . . 562
snmp restart . . . 563
snmp-server smux-port-disable . . . 564
snmp-server tcp-session . . . 565
snmp-server trap-cache 566
snmp-server user . . . 567

snmp-server view 569

Logging Server Configuration 570

CHAPTER 1 Syslog Configuration 571
Overview 571
Syslog Configuration with IPv4 Address 571
Syslog Configuration with IPv6 Address 576

CHAPTER 2 Custom Syslog Port Configuration 579
Overview 579
Custom Syslog Configuration with IPv4 Address 579
Custom Syslog Configuration with IPv6 Address 582
Custom Syslog Configuration with HOSTNAME 584

Logging Server Command Reference 587

CHAPTER 1 Syslog Commands 588
Syslog Severities 589
Log File Rotation 590
clear logging logfile 592
feature rsyslog 593
log syslog 594
logging console 595
logging level 596
logging logfile 598
logging monitor 599
logging remote facility 600
logging remote server 601
logging timestamp 603
show logging 604
show logging last 606
show logging logfile 607
show logging logfile last-index 608
show logging logfile start-seqn end-seqn 609
show logging logfile start-time end-time 610
show running-config logging 611

Monitor and Reporting Server Configuration 612

CHAPTER 1 Configure sFlow for Single Collector 613
Configuration 614

CHAPTER 2 Configure sFlow for Multiple Collectors 615
Overview 615
Prerequisites 615
Configuration 615
CLI Commands 617
Glossary 618

© 2025 IP Infusion Inc. Proprietary

CHAPTER 3 Software Monitoring and Reporting 619
Overview 619

CHAPTER 4 Internet Protocol SLA Configuration 621
Configuration 621
Validation 622

CHAPTER 5 Control Plane Policing Configuration 624

CHAPTER 6 400G PM Alarm 627
Overview 627
Prerequisites 627
Configuration 627
New CLI Commands 633
Abbreviations 639
Glossary 640

CHAPTER 7 IP Flow Information Export 642
Overview 642
Prerequisites 643
Configuration 644
Implementation Examples 647
IPFIX Commands 647
Troubleshooting 659
Glossary 659

Monitor and Reporting Server Command Reference 661

CHAPTER 1 Software Monitoring and Reporting 662
clear cores 663
copy core 664
copy techsupport 665
feature software-watchdog 666
remove file (techsupport) 667
show bootup-parameters 668
show cores 669
show running-config watchdog 670
show software-watchdog status 671
show system log 674
show system login 676
show system reboot-history 677
show system resources 678
show system uptime 680
show techsupport 681
show techsupport status 683
software-watchdog 684
software-watchdog keep-alive-time 686

CHAPTER 2 sFlow Commands 687
clear sflow statistics 688

debug sflow . . . 689
feature sflow . . . 690
sflow agent-ip . . . 691
sflow collector . . . 692
sflow enable . . . 693
sflow poll-interval . . . 694
sflow rate-limit . . . 695
sflow sampling-rate . . . 696
show sflow . . . 697
show sflow interface . . . 699
show sflow statistics . . . 700

CHAPTER 3 Control Plane Policing Commands . . . 701
clear interface cpu counters . . . 702
cpu-queue . . . 703
show interface cpu counters queue-stats . . . 708
show cpu-queue details . . . 709

CHAPTER 4 IP Service Level Agreements Commands . . . 712
clear ip sla statistics . . . 713
frequency . . . 714
icmp-echo . . . 715
ip sla . . . 716
ip sla schedule . . . 717
show ip sla statistics . . . 718
show ip sla summary . . . 720
show running-config ip sla . . . 721
threshold . . . 722
timeout . . . 723

CHAPTER 5 Object Tracking Commands . . . 724
track ip sla reachability . . . 725
delay up down . . . 726
show track . . . 727
show track <1-500> . . . 728
show track summary . . . 729
show running-config track . . . 730

Hardware System Diagnose Configuration . . . 731

CHAPTER 1 Show Tech Support Configurations . . . 732
Overview . . . 732
Tech Support Samples . . . 732

CHAPTER 2 Ethernet Interface Loopback Support . . . 733
Overview . . . 733
Local Loopback . . . 733
Remote Loopback . . . 734
Topology . . . 734
Configurations . . . 735

Validation 736

Hardware System Diagnose Command Reference 745

CHAPTER 1 Chassis Management Module Commands 746
cpu-core-usage 747
debug cmm 749
disk-activity-monitoring interval 750
disk-activity-monitoring threshold 751
locator led 752
show hardware-information 753
show system fru 773
show system-information 774
show system sensor 779
system-load-average 783

CHAPTER 2 Modifying Temperature Sensor Threshold Value 785
Overview 785
Prerequisites 785
CLI Commands 786
temperature threshold 787
emer-max 789
emer-min 790
alrt-max 791
alrt-min 792
crit-max 793
crit-min 794
Glossary 795

CHAPTER 3 Digital Diagnostic Monitoring Commands 796
clear ddm transceiver alarm 797
clear ddm transceiver alarm all 798
ddm monitor 799
ddm monitor all 800
ddm monitor interval 801
debug ddm 802
service unsupported-transceiver 803
show controller details 804
show interface frequency grid 805
show interface transceiver details 807
show supported-transceiver 811
tx-disable 812
wavelength 813

Link Configuration Guide 814

CHAPTER 1 Trigger Failover Configuration 815
Basic Configuration 815
Port-Channel Configuration 816

CHAPTER 2 Link Detection Debounce Timer 820
Log Messages 821

Link Command Reference 823

CHAPTER 1 Trigger Failover Commands 824
clear tfo counter 825
fog 826
fog tfc 827
fog type 828
link-type 829
show tfo 830
tfo 832

QSFP-DD Configuration Guide 833

CHAPTER 1 QSFP-DD Configuration 834
Overview 834
System Description 834
Objectives 834
Topology 834
Loopback 835
PRBS 838
Application 846
Custom Application 849
New CLI Commands 851
Laser Tuning 853
QSFP-DD Monitored Alarms 862
Remote Fault and Local Fault Alarms 869
Signal Integrity 893
Glossary 926
. 926

QSFP-DD Command Reference 927

CHAPTER 1 QSFP-DD Commands 928
application 930
laser channel 934
laser grid 935
laser fine-tune-freq 936
laser output-power 937
loopback 938
prbs 939
qsfp-dd 941
rx-output eq-pre-cursor-target 942
rx-output eq-post-cursor-target 943
rx-output amp-target 944
rx cdr-bypass 945
show qsfp-dd advertisement applications 946

show qsfp-dd advertisement controls . . . 951
show qsfp-dd advertisement diagnostics host . . . 952
show qsfp-dd advertisement diagnostics media . . . 953
show qsfp-dd advertisement diagnostics module . . . 954
show qsfp-dd advertisement durations . . . 955
show qsfp-dd advertisement laser . . . 956
show qsfp-dd advertisement monitors host . . . 957
show qsfp-dd advertisement monitors media . . . 958
show qsfp-dd advertisement monitors module . . . 960
show qsfp-dd advertisement pages . . . 961
show qsfp-dd advertisement si . . . 962
show qsfp-dd si status . . . 964
show qsfp-dd application . . . 966
show qsfp-dd diagnostics host . . . 967
show qsfp-dd diagnostics media . . . 969
show qsfp-dd eeprom . . . 970
show qsfp-dd laser grid . . . 971
show qsfp-dd laser status . . . 973
show qsfp-dd monitors host . . . 974
show qsfp-dd monitors media . . . 976
show qsfp-dd monitors module . . . 978
show qsfp-dd state . . . 979
tx-input eq-target . . . 980
tx cdr-bypass . . . 981

EDFA Configuration Guide . . . 982

CHAPTER 1 Erbium-Doped Fiber Amplifier (EDFA) Configuration . . . 983
Overview . . . 983
System Description . . . 983
Objectives . . . 984
Topology . . . 984

EDFA Command Reference . . . 987

CHAPTER 1 Erbium-doped Fiber Amplifier Commands . . . 988
edfa operating-mode . . . 989
edfa target-gain . . . 990
edfa target-outpwr . . . 991
show edfa operating-mode . . . 992
show interface IFNAME transceiver detail . . . 993
show interface IFNAME transceiver threshold violations . . . 995
show interface IFNAME transceiver . . . 996
show interface transceiver . . . 998
show interface transceiver detail . . . 999
show interface transceiver threshold violations . . . 1000

NetConf Configuration . . . 1001

CHAPTER 1 NetConf Call Home Configuration 1002
User Management VRF Configuration 1002
User Defined VRF Configuration 1002
Validation 1003

CHAPTER 2 NetConf Port Access Control. 1006
Overview 1006
Configuration 1006
Implementation Examples 1021
New CLI Commands 1022
Revised CLI Commands 1026
Abbreviations 1027

NetConf Command Reference 1028

CHAPTER 1 NetConf Call Home Commands 1029
callhome server 1030
debug callhome 1032
feature netconf callhome 1034
management-port 1036
netconf callhome 1038
reconnect 1039
retry-interval 1041
retry-max-attempts 1043
show (xml|) running-config netconf-callhome 1045

CHAPTER 2 NetConf Port Access Commands 1047

Security Management Configuration 1048

CHAPTER 1 Access Control Lists Configurations 1049
Overview 1049
Topology. 1049
IPv4 ACL Configuration 1049
ICMP ACL Configuration 1050
Access List Entry Sequence Numbering 1051
IPv6 ACL Configuration 1052
IPv6 ACL Configuration for 128-Bit Support. 1053
MAC ACL Configuration 1054
Management ACL Overview 1055
ARP ACL Overview 1060
ACL over Loopback 1061
ACL OVER Virtual Terminal (VTY). 1063
Timed ACL Configuration 1065
Topology. 1065
ACL on IRB Interface over MPLS EVPN 1067
Topology. 1067
ACL on IRB Interface over VXLAN EVPN 1078
Topology. 1078

CHAPTER 2 Dynamic ARP Inspection 1091
Overview 1091
Topology 1091

CHAPTER 3 Proxy ARP and Local Proxy ARP 1095
Overview 1095
Local Proxy ARP Overview 1097

CHAPTER 4 DHCP Snooping 1101
Overview 1101
Topology 1101
DHCP Snooping Operation 1104

CHAPTER 5 DHCP Snooping IP Source Guard 1106
Overview 1106
Topology 1106

CHAPTER 6 No IP Unreachable 1112
Overview 1112
Configuration 1113
CLI Commands 1117
Glossary 1118

Security Management Command Reference 1119

CHAPTER 1 Access Control List Commands 1120
arp access-group 1122
arp access-list 1123
arp access-list default 1124
arp access-list remark 1125
arp access-list request 1126
arp access-list resequence 1128
arp access-list response 1129
clear access-list 1131
clear arp access-list 1132
clear ip access-list 1133
clear ipv6 access-list 1134
clear mac access-list 1135
ip access-group 1136
ip access-list 1138
ip access-list default 1139
ip access-list filter 1140
ip access-list icmp 1143
ip access-list remark 1146
ip access-list resequence 1147
ip access-list tcp|udp 1148
ipv6 access-group in 1153
ipv6 access-list 1155
ipv6 access-list default 1157
ipv6 access-list filter 1158

ipv6 access-list icmpv6 . . . 1161
ipv6 access-list remark . . . 1163
ipv6 access-list resequence . . . 1164
ipv6 access-list sctp . . . 1165
ipv6 access-list tcp|udp . . . 1167
mac access-group . . . 1172
mac access-list . . . 1174
mac access-list default . . . 1175
mac access-list filter . . . 1176
mac access-list remark . . . 1178
mac access-list resequence . . . 1179
show access-lists . . . 1180
show arp access-lists . . . 1182
show ip access-lists . . . 1183
show ipv6 access-lists . . . 1185
show mac access-lists . . . 1186
show running-config access-list . . . 1188
show running-config aclmgr . . . 1189
show running-config ipv6 access-list . . . 1190

CHAPTER 2 Access Control List Commands (Standard) . . . 1191
ip access-list standard . . . 1192
ip access-list standard filter . . . 1193
Ipv6 access-list standard . . . 1194
ipv6 access-list standard filter . . . 1195

CHAPTER 3 DHCP Snooping Commands . . . 1196
debug ip dhcp snooping . . . 1197
hardware-profile filter dhcp-snoop . . . 1198
hardware-profile filter dhcp-snoop-ipv6 . . . 1199
ip dhcp packet strict-validation bridge . . . 1200
ip dhcp snooping arp-inspection bridge . . . 1201
ip dhcp snooping arp-inspection vlan . . . 1202
ip dhcp snooping arp-inspection validate . . . 1203
ip dhcp snooping bridge . . . 1204
ip dhcp snooping database . . . 1205
ip dhcp snooping information option bridge . . . 1206
ip dhcp snooping trust . . . 1207
ip dhcp snooping verify mac-address . . . 1208
ip dhcp snooping vlan . . . 1209
renew ip dhcp snooping binding database . . . 1210
show debugging ip dhcp snooping . . . 1211
show ip dhcp snooping arp-inspection statistics bridge . . . 1212
show ip dhcp snooping bridge . . . 1213
show ip dhcp snooping binding bridge . . . 1215

CHAPTER 4 IP Source Guard Commands . . . 1217
hardware-profile filter ipsg . . . 1218

hardware-profile filter ipsg-ipv6 1219
ip verify source dhcp-snooping-vlan 1220

CHAPTER 5 OSPFv3 IPSec Authentication Commands 1221
crypto ipsec transform-set 1222
crypto map 1224
set peer 1225
set session-key 1226
set transform-set 1227
sequence 1228
show crypto ipsec transform-set 1229

Port Breakout Configuration 1230

CHAPTER 1 Port Breakout (100G) on Qumran2 1231
Overview 1231
Limitations 1231
Topology 1231
Port Breakout 4X10g 1232
Port Breakout 4X25g 1234
Port Breakout 2X50g 1235
Un-configure Port Breakout 1237

CHAPTER 2 Port Breakout (100G) on Qumran AX and MX 1239
Port Breakout (100G) for AS5916-54XKS (Qumran-MX) Platform 1239
Overview 1239
Configuration 1239
Unconfigure Port Breakout 1242
Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform 1243
Overview 1243
Configuration 1243
Unconfigure Port Breakout 1245
Port Breakout (100G) for 26XAS7316-26XB (Qumran-AX) Platform 1246
Overview 1246
Configuration 1247
Unconfigure Port Breakout 1248
Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform 1249
Overview 1249
Configuration 1250
Unconfigure Port Breakout 1251

CHAPTER 3 Port Breakout (400G) on Qumran2 1253
Overview 1253
Configuration 1253
EEPROM Details for ZR+ Optics 1255
Port Breakout Unconfiguration 1259
Port Breakout Configuration with serdes 25g 1260
Port Breakout Unconfiguration with serdes 25g 1261

CHAPTER 4 Dynamic Port Breakout (100G) on Qumran AX and MX 1262
Overview 1262
Prerequisites 1262
Limitations 1263
Configuration 1263
Unconfiguration 1270

System Management Command Reference 1273

CHAPTER 1 Basic Commands 1274
banner motd 1276
cli timestamp 1277
clock set 1278
clock timezone 1279
configure terminal 1280
configure terminal force 1281
copy empty-config startup-config 1282
copy running-config startup-config 1283
copy backup-config FILE running-config replace-mode 1284
crypto pki generate rsa common-name ipv4 1285
debug nsm 1286
debug vm-events 1288
disable 1289
do 1290
enable 1291
enable password 1292
end 1293
exec-timeout 1294
exit 1295
help 1296
history 1297
hostname 1298
line console 1299
line vty (all line mode) 1300
line vty (line mode) 1301
logging cli 1302
logout 1303
max-session 1304
ping 1305
ping (interactive) 1308
port breakout 1310
quit 1312
reload 1313
service advanced-vty 1314
service password-encryption 1315
service terminal-length 1316
show clock 1317

show cli 1318
show cli history 1319
show cli list 1320
show cli list all 1321
show cli modes 1323
show crypto csr 1325
show debugging nsm 1326
show debugging vm-events 1327
show logging cli 1328
show nsm client 1329
show process 1330
show running-config 1331
show running-config switch 1332
show startup-config 1334
show tcp 1335
show timezone 1337
show users 1340
show version 1342
sys-reload 1344
sys-shutdown 1345
terminal width 1346
terminal length 1347
terminal monitor 1348
traceroute 1349
watch static-mac-movement 1350
write 1351
write terminal 1352
. 1353

CHAPTER 2 Multi-Line Banner Support 1354
Overview 1354
Multi-Banner Message Commands 1354

CHAPTER 3 Common Management Layer Commands 1357
abort transaction 1359
cancel-commit 1360
cml force-unlock config-datastore 1361
cml lock config-datastore 1362
cml logging 1363
cml notification 1364
cml unlock config-datastore 1365
cmlsh cli-format 1366
cmlsh multiple-config-session 1367
cmlsh notification 1369
cmlsh transaction 1370
cmlsh transaction limit 1371
commit 1372
confirm-commit 1375

commit dry-run . . . 1376
debug cml . . . 1377
module notification . . . 1378
netconf translation openconfig . . . 1379
save cml commit-history WORD . . . 1380
show cml auto-config-sync state . . . 1382
show cml bulk limit cpu state . . . 1383
show cml cli-error status . . . 1384
show cml commit-history state . . . 1385
show cml commit-id rollover state . . . 1386
show cml config-sync detail . . . 1387
show cml database-dump . . . 1388
show cml notification status . . . 1389
show cmlsh multiple-config-session status . . . 1390
show cmlsh notification status . . . 1391
show json/xml commit config WORD . . . 1392
show json/xml commit diff WORD WORD . . . 1393
show max-transaction limit . . . 1395
show module-info . . . 1396
show running-config notification . . . 1398
show system restore failures . . . 1399
show transaction current . . . 1400
show transaction last-aborted . . . 1401
show (xml|json) running-config|candidate-config|startup-config . . . 1402

CHAPTER 4 Remote Management Commands . . . 1405
copy running-config . . . 1406
copy running-config (interactive) . . . 1407
copy startup-config . . . 1408
copy startup-config (interactive) . . . 1409
copy system file . . . 1410
copy system file (interactive) . . . 1411
copy ftp startup-config . . . 1412
copy scp filepath . . . 1413
copy scp startup-config . . . 1414
copy sftp startup-config . . . 1415
copy tftp startup-config . . . 1416
copy http startup-config . . . 1417
copy ftp startup-config (interactive) . . . 1418
copy scp startup-config (interactive) . . . 1419
copy sftp startup-config (interactive) . . . 1420
copy tftp startup-config (interactive) . . . 1421
copy http startup-config (interactive) . . . 1422
copy file startup-config . . . 1423
load-config . . . 1424

CHAPTER 5 Interface Commands . . . 1425
admin-group . . . 1428

bandwidth 1429
bandwidth-measurement static uni-available-bandwidth 1430
bandwidth-measurement static uni-residual-bandwidth 1431
bandwidth-measurement static uni-utilized-bandwidth. 1432
clear hardware-discard-counters 1433
clear interface counters 1434
clear interface cpu counters 1435
clear interface fec 1436
clear ip prefix-list 1437
clear ipv6 neighbors 1438
clear ipv6 prefix-list. 1439
debounce-time 1440
delay-measurement dynamic twamp 1441
delay-measurement a-bit-min-max-delay-threshold 1443
delay-measurement static 1444
delay-measurement a-bit-delay-threshold 1445
description 1446
duplex. 1447
fec. 1448
flowcontrol 1449
hardware-profile port-config 1451
hardware-profile portmode 1452
if-arbiter 1453
interface 1454
ip address A.B.C.D/M. 1455
ip address dhcp 1456
ip forwarding. 1457
ip prefix-list 1458
ip proxy-arp 1460
ip remote-address 1461
ip unnumbered 1462
ip vrf forwarding 1463
ipv6 address 1464
ipv6 forwarding 1465
ipv6 prefix-list 1466
ipv6 unnumbered 1468
link-debounce-time 1469
loopback 1470
loss-measurement dynamic 1471
loss-measurement uni-link-loss 1472
mac-address. 1473
mac-address secondary peer-mlag 1474
monitor speed. 1475
monitor queue-drops 1476
monitor speed threshold 1477
mtu 1478
multicast 1480

show flowcontrol . . . 1481
show hardware-discard-counters . . . 1482
show interface . . . 1484
show interface capabilities . . . 1486
show interface counters . . . 1488
show interface counters drop-stats . . . 1491
show interface counters error-stats . . . 1494
show interface counters (indiscard-stats|outdiscard-stats) . . . 1495
show interface counters protocol . . . 1498
show interface counters queue-drop-stats . . . 1499
show interface counters queue-stats . . . 1500
show interface counters speed . . . 1502
show interface counters summary . . . 1503
show interface fec . . . 1505
show ip forwarding . . . 1507
show ip interface . . . 1508
show ip prefix-list . . . 1510
show ip route . . . 1511
show ip route A.B.C.D/M longer-prefixes . . . 1513
show ip vrf . . . 1522
show ipv6 forwarding . . . 1523
show ipv6 interface brief . . . 1524
show ipv6 route . . . 1526
show ipv6 prefix-list . . . 1528
show hosts . . . 1529
show running-config interface . . . 1531
show running-config interface ip . . . 1533
show running-config interface ipv6 . . . 1534
show running-config ip . . . 1535
show running-config ipv6 . . . 1536
show running-config prefix-list . . . 1537
shutdown . . . 1538
speed . . . 1539
switchport . . . 1542
switchport allowed ethertype . . . 1543
switchport protected . . . 1544
transceiver . . . 1545
tx cdr-bypass . . . 1547
rx cdr-bypass . . . 1548

CHAPTER 6 Time Range Commands . . . 1549
end-time (absolute) . . . 1550
end-time after (relative) . . . 1551
frequency . . . 1552
frequency days (specific days) . . . 1553
start-time (absolute) . . . 1554
start-time after (relative) . . . 1555

start-time now (current) . . . 1556
time-range . . . 1557

CHAPTER 7 VLOG Commands . . . 1558
show vlog all . . . 1559
show vlog clients . . . 1561
show vlog terminals . . . 1562
show vlog virtual-routers . . . 1563

CHAPTER 8 Linux Shell Commands . . . 1564

CHAPTER 9 System Configure Mode Commands . . . 1565
delay-profile interfaces . . . 1566
delay-profile interfaces subcommands . . . 1567
evpn mpls irb . . . 1569
forwarding profile . . . 1570
hardware-profile filter (Qumran1) . . . 1572
hardware-profile filter (Qumran2) . . . 1579
hardware-profile flowcontrol . . . 1590
hardware-profile service-queue . . . 1591
hardware-profile statistics . . . 1592
hardware-profile bgp-flowspec-mode . . . 1595
ip redirects . . . 1596
load-balance enable . . . 1597
show forwarding profile limit . . . 1600
show hardware-profile filters . . . 1601
show nsm forwarding-timer . . . 1607
show queue remapping . . . 1608

CHAPTER 10 Source Interface Commands . . . 1610
ip source-interface . . . 1611
ipv6 source-interface . . . 1612
show ip source-interface detail . . . 1613
show ipv6 source-interface detail . . . 1614
show running-config ip source-interface . . . 1615
show running-config ipv6 source-interface . . . 1616

CHAPTER 11 Smart SFP Commands . . . 1617
ddm raise . . . 1618
show interface controller details . . . 1619
show interface transceiver details . . . 1621
show interface transceiver detail remote . . . 1625
show interface transceiver protocol . . . 1626
show interface transceiver protocol remote . . . 1627
show interface transceiver protocol stats . . . 1628
show interface transceiver remote . . . 1629
show interface transceiver threshold violations remote . . . 1630
xcvr <IFNAME> tx-disable <1-256> remote . . . 1631
xcvr <IFNAME> reset remote . . . 1632
xcvr loopback . . . 1633

CHAPTER 12 Commit Rollback 1634
Overview 1634
Prerequisites 1634
show commit list 1634
commit-rollback 1635
clear cml commit-history (WORD|) 1636
cml commit-history (enable | disable) 1637
cml commit-id rollover (enable | disable) 1638

Index 1640

Preface

This guide describes how to configure OcNOS.

IP Maestro Support

Monitor devices running OcNOS Release 6.3.4-70 and above using IP Maestro software.

Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Related Documentation

For information about installing OcNOS, see the *Installation Guide* for your platform.

Feature Availability

The features described in this document that are available depend upon the OcNOS SKU that you purchased. See the *Feature Matrix* for a description of the OcNOS SKUs.

Migration Guide

Check the *Migration Guide* for configuration changes to make when migrating from one version of OcNOS to another.

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

Command Line Interface

This chapter introduces the OcNOS Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain OcNOS devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running OcNOS or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark “?”. The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword:

```
show ?
  application-priority            Application Priority
  arp                             Internet Protocol (IP)
  bfd                             Bidirectional Forwarding Detection (BFD)
  bgp                             Border Gateway Protocol (BGP)
  bi-lsp                          Bi-directional lsp status and configuration
  bridge                          Bridge group commands
  ce-vlan                         COS Preservation for Customer Edge VLAN
  class-map                       Class map entry
  cli                             Show CLI tree of current mode
  clns                            Connectionless-Mode Network Service (CLNS)
  control-adjacency               Control Adjacency status and configuration
  control-channel                 Control Channel status and configuration
  cspf                            CSPF Information
  customer                        Display Customer spanning-tree
  cvlan                           Display CVLAN information
  debugging                       Debugging functions (see also 'undebug')
  etherchannel                    LACP etherchannel
  ethernet                        Layer-2
...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de?
debugging  Debugging functions (see also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, OcNOS displays help for all matching keywords.

```
> show i? (CLI does not display the question mark).
interface  Interface status and configuration
ip         IP information
isis       ISIS information
```

© 2025 IP Infusion Inc. Proprietary

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip          ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type `n` to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

```
> sh int xe0
```

is an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized command
> show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
                        ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command.

If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent
ication-key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table P-2 describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`
`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`

© 2025 IP Infusion Inc. Proprietary

Table P-2: Syntax conventions (Continued)

Convention	Description	Example
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS|no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table P-3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address
`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647>`
`<0-4294967295>`
	Numeric range

Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

Table P-4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

Table P-5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor

© 2025 IP Infusion Inc. Proprietary

Table P-5: Keyboard operations (Continued)

Key combination	Operation
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  last      Last few lines
  redirect  Redirect output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
...skipping
interface xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
!
interface xe2
 ipv6 address fe80::20d:56ff:fe96:725a/64
!
line con 0
 login
!
end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either “xe2” or “xe4”:

```
# show running-config | begin xe[2-4]

...skipping
```

```
interface xe2
 shutdown
!
interface xe4
 shutdown
!
interface svlan0.1
 no shutdown
!
route-map myroute permit 2
!
route-map mymap1 permit 10
!
route-map rmap1 permit 2
!
line con 0
 login
line vty 0 4
 login
!
end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 613147, bytes 126055987, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet6 fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude (in|out)put
Interface xe0
  Scope: both
  Hardware is Ethernet  Current HW addr: 001b.2139.6c4a
  Physical:001b.2139.6c4a  Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Bandwidth 100m
  DHCP client is disabled.
  inet 10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
  inet6 fe80::21b:21ff:fe39:6c4a/64
    collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Last Modifier

The `last` modifier displays the output of last few number of lines (As per the user input). The last number ranges from 1 to 9999.

For example:

```
#show running-config | last 10
```

String Parameters

The restrictions in Table P-6 apply for all string parameters used in OcNOS commands, unless some other restrictions are noted for a particular command.

Table P-6: String parameter restrictions

Restriction	Description
Input length	1965 characters or less
Restricted special characters	“?”, “,”, “>”, “|”, and “=” The “|” character is allowed only for the `description` command in interface mode.

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-7 lists the command modes common to all protocols.

Table P-7: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family. Configure mode is single user. Only one user at a time can be in configure mode.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as BGP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

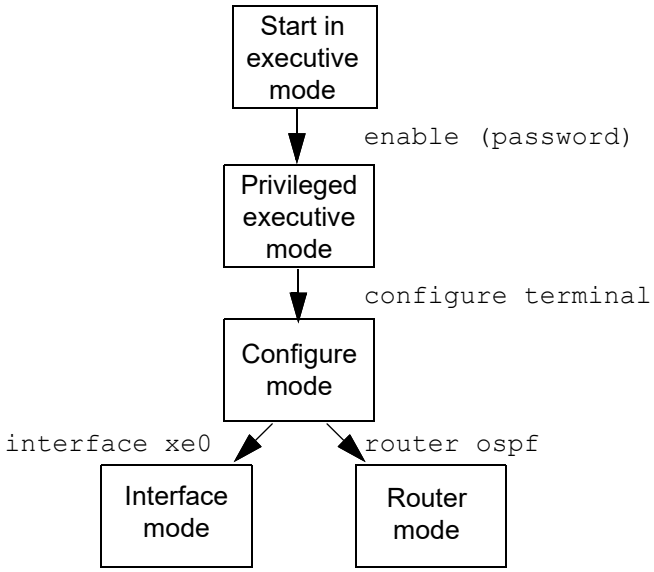


Figure P-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
> enable mypassword
# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)# router ospf
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

Transaction-based Command-line Interface

The OcNOS command line interface is transaction based:

- Any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the show transaction current command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the commit command.
- If a commit fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the commit.
- Discard the candidate configuration with the abort transaction command.
- Check the last aborted transaction with the show transaction last-aborted command.
- Multiple configurations cannot be removed with a single commit. You must remove each configuration followed by a commit.

Note: All commands MUST be executed only in the default CML shell (`cmlsh`). If you log in as root and start `imish`, then the system configurations will go out of sync. The `imish` shell is not supported and should not be started manually.

Authentication Management Configuration

CHAPTER 1 AAA Configuration for Console Connection

Overview

OcNOS uses the Accounting, Authentication, Authorization (AAA) protocol to authenticate the user through RADIUS or TACACS+ remote servers or Local authentication server to gives access to the device. The console port of the OcNOS is accessible (ssh or Telnet) only through the default VRF or VRF management port only. If the user attempts to access the device using the non VRF interface the access is denied.

The AAA authentication from console port via default VRF or VRF management is enhanced to reach the remote authentication servers through the non VRF interface.

Feature Characteristics

TACACS/RADIUS client can reach the OcNOS in both default and management VRF or non VRF interface for authentication.

Following are the features supported:

- Default VRF to reach the remote authentication (TACACS/RADIUS) server in Management VRF
- Management VRF to reach the loopback interface in Default VRF
- The AAA using servers are defined in default and management VRF
- When AAA server is not reachable, the authentication, authorization and accounting is performed via the local authentication server.
- AAA solution is performed based on the configuration only, not on the source of VRF

Configuration

The following configuration uses the TACACS+ remote server for authentication. The same configurations are holds good for RADIUS authentication server.

Perform the following configurations on host.

1. Configure TACACS client using the configuration provided in TACACS Client Configuration or RADIUS Client Configuration section.
2. In the above configuration, configure the TACACS or RADIUS server in both management and default VRF. A sample configuration is provided below:

```
      feature tacacs+ vrf management
      tacacs-server login host 10.12.97.208 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
      feature tacacs+
      tacacs-server login host 40.40.40.1 seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
      tacacs-server login host 30.30.30.1 seq-num 2 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
```

3. Create server group for management VRF using the following CLI. This command changes the configure mode to server group `(config-tacacs)#`.

```
aaa group server tacacs+ TACACS_VRF_MGMT vrf management
```

Note: An AAA server group name configured in a VRF cannot be used to configure another VRF. For example, if the TACACS_VRF_MGMT server group is configured in the VRF management, you cannot configure an AAA server with the same name in any other VRFs.

4. Make the TACAC+S server 10.12.30.86 part of the group TACACS_VRF_MGMT for default VRF.

```
server 10.12.30.86
```

5. Configure the authentication behavior for TACACS+ server with default VRF management, non VRF and fall-back to local authentication server if none configured for management VRF.

```
aaa authentication login default vrf management group TACACS_VRF_MGMT
TACACS_NON_VRF_MGMT local
```

6. Configure AAA behavior for management VRF using the following CLIs.

```
aaa accounting default vrf management group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT
local
aaa authorization default vrf management group TACACS_VRF_MGMT
TACACS_NON_VRF_MGMT local
aaa authentication login default fallback error local non-existent-user vrf
management
```

7. Create a server group for non VRF management using the following CLI. This command changes the configure mode to server group (config-tacacs)#.

```
aaa group server tacacs+ TACACS_NON_VRF_MGMT
 server 40.40.40.1
 server 30.30.30.1
```

8. Configure the authentication behavior for TACACS+ server with console VRF management, non VRF and fall-back to local authentication server if none configured for management VRF.

9. Configure AAA behavior for non management VRF using the following CLIs.

```
aaa authentication login console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa accounting console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa authorization console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa authentication login console fallback error local non-existent-user
```

Note: If both management and default VRF is configured, then the default VRF is used to reach the TACACS/ RADIUS server. If it is not reachable, then the management VRF is used.

Validation

Following is the sample validation show output for TACACS server with default management VRF and non VRF interface.

Following output shows the interface configured for server group.

```
OcNOS# sh tacacs-server groups
        VRF: default
        group tacacs+:
                server: all configured tacacs servers

       group TACACS_NON_VRF_MGMT:
                server 40.40.40.1
```

```
                seq-num 1
                port is 49
                key is ********

                server 30.30.30.1
                seq-num 2
                port is 49
                key is ********
```

Following output shows the TACACS+ server configurations:

```
OcNOS#sh tacacs-server vrf management
        VRF: management
total number of servers:1

Tacacs+ Server                  : 10.12.97.208/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

OcNOS#sh tacacs-server
        VRF: default
total number of servers:2

Tacacs+ Server                  : 40.40.40.1/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 30.30.30.1/49
           Sequence Number      : 2
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.
OcNOS#

OcNOS#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.12.97.208 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb

feature tacacs+
```

```
tacacs-server login host 40.40.40.1  seq-num 1 key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb
tacacs-server login host 30.30.30.1  seq-num 2 key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb
```

Following output shows the AAA configurations:

```
OcNOS#show running-config aaa
aaa group server tacacs+ TACACS_VRF_MGMT vrf management
    server 10.12.97.208

aaa authentication login default vrf management group TACACS_VRF_MGMT
TACACS_NON_VRF_MGMT local
aaa accounting default vrf management group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa authorization default vrf management group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT
local
aaa authentication login default fallback error local non-existent-user vrf management
aaa group server tacacs+ TACACS_NON_VRF_MGMT
    server 40.40.40.1
    server 30.30.30.1

aaa authentication login console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa accounting console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa authorization console group TACACS_VRF_MGMT TACACS_NON_VRF_MGMT local
aaa authentication login console fallback error local non-existent-user
```

Glossary

Key Terms/Acronym	Description
TACACS	Terminal Access Controller Access Control System

CHAPTER 2 Restricted Access to Privilege Mode based on User Role

Overview

The Remote Authentication server is enhanced to provide access to execute mode or privilege level execute mode based on the network user's role. The authentication server can be Remote Authentication Dial-In User Service (RADIUS) or the Terminal Access Controller Access Control System (TACACS) server.

This authorization behavior is enhanced to enable privilege level mode based on the user role specified in the RADIUS/TACACS server. A new CLI `disable default auto-enable` is introduced to implement it. Executing this CLI removes the default access to the privilege execute mode to any user.

Feature Characteristics

Removed the default login behavior of network-admin role and authenticate the user based on difference privilege level defined in the remote authentication

The authentications assumes the following:.

- If no privilege-level is specified in the authentication server, the default user role is "network-user".
- All the user logged into the privilege exec mode by default.
- Executing the `disable default auto-enable` CLI decides the execution mode only for "network-user" role based on the privilege level.
- The user role is determined based on privilege level specified in server configuration user file.

Prerequisites

The following is mandatory before issuing the `disable default auto-enable` CLI:

- Specify the RADIUS/TACACS server to authenticate the remote user login and enable the RADIUS/TACACS authentication.

```
radius-server login host 1.2.7.4 vrf management seq-num 1 key 7 0x67efdb4ad9
d771c3ed8312b2bc74cedb
aaa authentication login default vrf management group radius
```

Configuration

Perform the following configurations on host to disable the privilege execute mode based the user role.

1. Configure RADIUS/TACACS server using the configuration provided in RADIUS Authorization Configuration or TACACS Server Authentication section.
2. In the above configuration after enabling the authentication, execute `disable default auto-enable` CLI to get into network user executive mode based on user role.

```
    (config)#radius-server login host 10.12.97.42 vrf management seq-num 1 key 0
testing123
```

```
OcNOS(config)#aaa authentication login default vrf management group radius
OcNOS(config)#disable default auto-enable
```

Note: By default this command is disabled.

Validation

Without configuring the disable default auto-enable CLI, if you login as remote user, user will be entered into privileged exec-mode.

```
radius-server login host 10.12.97.42 vrf management seq-num 1 key 7 0x67efdb4ad9
d771c3ed8312b2bc74cedb


root@instance-00000759:/home/ZebOS8NG# ssh ipi1@10.12.159.128
ipi1@10.12.159.128's password:
Linux OcNOS 4.19.91-ga6f5ae56f #1 SMP Sun Feb 11 13:19:33 UTC 2025 x86_64
Last login: Thu Feb 14 11:43:28 2019 from 10.12.43.197
OcNOS version UFI_S9500-30XS-XP-6.5.0  02/28/2025 07:28:24
OcNOS#sh users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line   User       Idle       Location/Session  PID     TYPE    Role
(#)    0 con 0    [C]root    0d00h01m          ttyS0   5093    Local  network-admin
(*)  130 vty 0    [C]ipi1    0d00h00m          pts/0   5168    Remote network-user
```

After configuring the `disable default auto-enable` CLI, if you login as remote user with privilege level 0, user will be entered into exec-mode.

```
root@instance-00000759:/home/ZebOS8NG# ssh ipi1@10.12.159.128
ipi1@10.12.159.128's password:
Linux OcNOS 4.19.91-ga6f5ae56f #1 SMP Sun Feb 11 13:19:33 UTC 2024 x86_64
Last login: Thu Feb 14 14:02:48 2019 from 10.12.43.197

OcNOS version UFI_S9500-30XS-XP-6.5.0  02/28/2025 07:28:24
OcNOS>en
OcNOS#sh users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line   User     Idle         Location/Session  PID     TYPE   Role
(#)    0 con 0  [C]root       0d00h00m         ttyS0   5093   Local  network-admin
(*)    130 vty 0[C]ipi1       0d00h00m          pts/0  5207   Remote network-user
```

After configuring the `disable default auto-enable` CLI, if you login as remote user with privilege level 1-15, the user will be entered into privileged execution mode.

```
root@instance-00000759:/home/ZebOS8NG# ssh ipi@10.12.159.128
ipi@10.12.159.128's password:
Linux OcNOS 4.19.91-ga6f5ae56f #1 SMP Sun Feb 11 13:19:33 UTC 2024 x86_64

OcNOS version UFI_S9500-30XS-XP-6.5.0  02/28/2024 07:28:24
OcNOS#sh users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line   User        Idle       Location/Session  PID     TYPE   Role
(#)    0 con 0     [C]root    0d00h01m          ttyS0   5093    Local  network-admin
(*)    130 vty 0   [C]ipi      0d00h00m         pts/0   5239    Remote network-engineer
```

New CLI Commands

The RADIUS authentication introduces the following configuration commands.

disable default auto-enable

Use this command to disable auto-enable feature in remote authentication for user role "network-user".

Use `no` parameter of this command to enable auto-enable feature.

Command Syntax

```
disable default auto-enable
no disable default auto-enable
```

Parameters

None

Default

Disable

Command Mode

Configuration Mode

Applicability

This command was introduced in the OcNOS version 6.5.1.

Example

The following CLI disable auto-enable feature for user role "network-user" in remote authentication.

```
OcNOS(config)#disable default auto-enable
OcNOS(config)#commit
OcNOS(config)#exit
```

Glossary

Key Terms/Acronym	Description
RADIUS	Remote Authentication Dial-In User Service
TACACS	Terminal Access Controller Access Control System server

CHAPTER 3 RADIUS Client Configuration

Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server. A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

The OcNOS device, acting as a RADIUS client, sends the user's credentials to the RADIUS server requesting authentication. The RADIUS server validates the received user's credentials and authenticates it. After the authentication, it authorizes the user's privilege level and shares it with the OcNOS. Thus, the user role is decided based on the received privilege level.

The key points for RADIUS authentication are:

- Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
- The password is encrypted before sending it over the network.
- A maximum of eight RADIUS servers can be configured.

Limitation:

- If the privilege level is not specified in the radius server's user config file, the default role is considered "network-user."
- By default, the Privileged Exec mode is given to all the users

In OcNOS version 6.4.1, the RADIUS is not present on radius server or authentication fails from RADIUS server

To implement the above requirements, the existing CLI `aaa authentication login default fallback error` is used to enable fallback to local authentication server. This is disabled by default.

By default, the fallback to local authentication is applied when the Radius server is unreachable. For other scenarios, enable the fallback using the CLI.

Note: For invalid secret key there is no fallback local authentication.
Console authentication is not supported for Radius.

In OcNOS version 6.4.2, the RADIUS Authorization is supported.

RADIUS Authorization Configuration

Benefits

Based on the privilege level received from the RADIUS server user role is determined.

Prerequisites

RADIUS server process must be up and running.

Configuration

Topology

Following is the RADIUS client and server network topology.

Figure 3-1: RADIUS Server Client Configuration

IPv4 Address

RADIUS server address is configured in IPv4 address format.

RADIUS Client (Host)

`(config)#radius-server login host 10.12.33.211 vrf management seq-num 1 key 0 testing123`	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
`(config)#radius-server login host 1.1.1.2 seq-num 1 key 0 testing123`	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.
`(config)#aaa authentication login default vrf management group radius`	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default.
`(config)#aaa authentication login console group radius`	Enable authentication for radius server . Authorization is also enabled by console
`(config)#aaa authentication login default vrf management group radius local`	Enable authentication for radius server and fallback to local configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login console group radius local`	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default

Specifies privilege level in `radius server` configuration file. The RADIUS client fetch the network operator privilege level from this file. The Privilege level range is between 0-15.

Table P-8: Role/privilege level mapping

Role	Privilege level
Network-admin	15
Network-engineer	14

Table P-8: Role/privilege level mapping

Role	Privilege level
RBAC-customized-role	13
Network-operator	1 to 12
Network-user	0 or any other values (>15 or negative values or any character)

Validation

To verify the RADIUS authorization process, login from the host machine to Host IP with the authenticating user credentials and provide a RADIUS server password.

Execute following show commands to verify the Radius authorization status.

```
OcNOS#sh running-config aaa
aaa authentication login default vrf management group radius
aaa authentication login console group radius
aaa authentication login default vrf management group radius local
aaa authentication login console group radius local

OcNOS#sh running-config radius
radius-server login host 10.12.33.211 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb

radius-server login host 1.1.1.1  seq-num 1 key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb

OcNOS#sh radius-server vrf management
timeout value: 5

Total number of servers:1

VRF: management
Following RADIUS servers are configured:
Radius Server                          : 10.12.33.211 (*)
   Sequence Number                     : 1
   available for authentication on port : 1812
   available for accounting on port     : 1813
   RADIUS shared secret                : ********
   Failed Authentication count         : 3
   Successful Authentication count     : 13
   Failed Connection Request           : 3
   Last Successful authentication      : 2023 November 30, 06:25:07

OcNOS#sh radius-server vrf management
timeout value: 5

Total number of servers:1
```

```
VRF: management
Following RADIUS servers are configured:
Radius Server                           : 1.1.1.1 (*)
   Sequence Number                      : 1
   available for authentication on port : 1812
   available for accounting on port     : 1813
   RADIUS shared secret                 : ********
   Failed Authentication count          : 3
   Successful Authentication count      : 10
   Failed Connection Request            : 0
   Last Successful authentication       : 2023 November 30, 06:28:07


OcNOS#sh users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line        User          Idle         Location/Session  PID   TYPE   Role
(*) 0 con 0 [C]ocnos      0d00h00m     ttyS0             5251  Local  network-admin
130 vty 0   [C]ocnos      0d00h00m     pts/0             5288  Remote network-user
131 vty 1   [C]abc        0d00h00m     pts/1             5340  Remote network-engineer
132 vty 2   [C]ipi        0d00h00m     pts/2             5350  Remote network-operator
```

IPv6 Address

RADIUS server address is configured in IPv6 address.

RADIUS Client (Host)

`OcNOS(config)#radius-server login host 2001:db8:100::2 vrf management seq-num 1 key 0 testing123`	Configure radius server with IPv6 address
`OcNOS(config)#aaa authentication login default vrf management group radius local`	Configure AAA authentication
`(config)#interface eth0`	Navigate to the interface mode
`(config-if)#ipv6 address 2001:db8:100::5/64`	Configure IPv6 address on the eth0 interface
`(config-if)#exit`	Exit interface configure mode
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode

Validation

To verify the RADIUS authorization process, login from the host machine to Host IP with the authenticating user credentials and provide a RADIUS server password.

Execute following show commands to verify the Radius authorization status.

```
#show running-config radius
```

```
radius-server login host 2001:db8:100::2 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb

#show running-config aaa
aaa authentication login default vrf management group radius

#show ipv6 interface eth0 brief
Interface        IPv6-Address                                  Admin-Status
eth0             2001:db8:100::5fe80::218:23ff:fe30:e6ba   [up/up]
```

Implementation Examples

Following is an example for `radius-server` configuration file:

```
ipi Cleartext-Password := "ipi123"
     Management-Privilege-Level := 12
ocnos Cleartext-Password := "ocnos"
     Management-Privilege-Level := 0
abc Cleartext-password :="AC123"
     Management-Privilege-Level := 14
```

RADIUS Server Authentication Configuration

IPv4 Address

Radius server address is configured as IPv4 address.

Topology

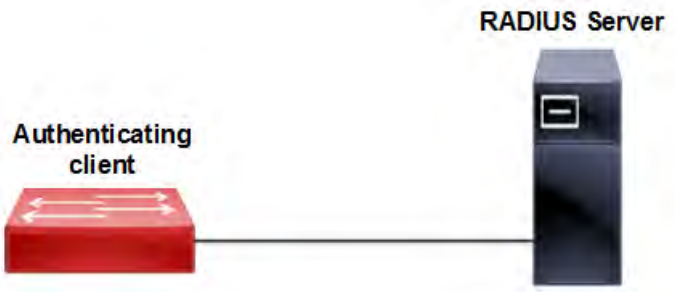


Figure 3-2: RADIUS Server Host Configuration

Host

`#configure terminal`	Enter configure mode.
`(config)#radius-server login key testing101 vrf management`	Specify the global key for radius servers that are not configured with their respective keys for management vrf. This key should match the one present in the config file of tacacs server.
`(config)#radius-server login key testing101`	Specify the global key for radius servers that are not configured with their respective keys for default vrf. This key should match the one present in the config file of tacacs server
`(config)#radius-server login host 10.12.17.13 vrf management seq-num 1 key testing123`	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
`(config)#radius-server login host 10.12.17.13 seq-num 2 key testing123`	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.
`(config)#radius-server login host 10.12.17.11 vrf management seq-num 1 auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 seq-num 1 auth-port 1045`	Specify the radius server ipv4 address to be configured with port number for default vrf. The radius server should be started with same port number
`(config)#radius-server login host 10.12.17.11 vrf management seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 seq-num 1 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for default vrf. The radius server should be started with same port number. The radius server should be started with same port number
`(config)#radius-server login host Radius-Server-1 vrf management seq-num 2 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 2`	Specify the radius server configured with hostname, key authentication port number, accounting port number, for management VRF. The radius server should be started with same port number
`(config)#radius-server login host Radius-Server-1 seq-num 2 key 7 wawyanb123 auth-port 60000  acct-port 60000 timeout 2`	Specify the radius server configured with hostname sequence number, key and port number for default VRF. The radius server should be started with same port number.
`(config)#aaa authentication login default vrf management group radius`	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius`	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.
`(config)#aaa authentication login default vrf management group radius local`	Enable authentication for radius server and fallback to local configured for management VRF. Authorization is also enabled by default
`(config)#aaa authentication login default group radius local`	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf management group radius local none`	Enable authentication for radius server, fallback to local followed by fallback to none, configured for management VRF. Authorization is also enabled by default

(config)#aaa authentication login default radius local none	Enable authentication for radius server, fallback to local followed by fallback to none, configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group radius none	Enable authentication for radius, fallback to none, configured for management VRF. Authorization is also enabled by default
(config)#aaa authentication login default group radius none	Enable authentication for radius, fallback to none, configured for default VRF. Authorization is also enabled by default
(config)#aaa group server radius G1 vrf management	Create aaa radius group G1 for management vrf
(config)#aaa group server radius G1	Create AAA radius group G1 for default VRF
(config-radius)#server 10.12.17.11	Make the radius server 10.12.30.86 a part of this group G1 for default VRF
(config-radius)#server Radius-Server-1	Make Radius-Server-1 a part of this group G1
(config-radius)#exit	Exit radius mode
(config)#commit	Commit the configuration
(config)#aaa group server radius G1	Enter radius mode
(config-radius)#server 10.12.17.11	Make the radius server 10.12.30.86 a part of this group G1 for default vrf
(config-radius)#server Radius-Server-1	Make Radius-Server-1 a part of this group G1
(config-radius)#exit	Exit radius mode.
(config)#commit	Commit the configuration
(config)#aaa authentication login default vrf management group G1	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
(config)#aaa authentication login default group G1	Authenticate the tacacs+ group G1 with aaa authentication for default vrf
(config)#commit	Commit the configuration

Validation

To verify the RADIUS authentication process, use SSH or Telnet from the host machine to Host IP with the authenticating user created, and provide a RADIUS server password and check whether the client validates the user with the corresponding username and password.

```
#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                            : 10.12.17.13
   Sequence Number                       : 1
   available for authentication on port  : 60000
   available for accounting on port      : 60000
   timeout                               : 2
   RADIUS shared secret                  : ********
   Failed Authentication count           : 0
   Successful Authentication count       : 2
   Failed Connection Request             : 2
   Last Successful authentication        : 2000 January 05, 20:55:44
Radius Server                            : 10.12.17.11 (*)
   Sequence Number                       : 2
```

```
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:58:33

#show radius-server
        VRF: default
timeout value: 5

Total number of servers:4

Following RADIUS servers are configured:
Radius Server                           : 192.168.1.1
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 1
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:45:09

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:46:36

#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                           : 10.12.17.13
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
```

```
   Failed Authentication count          : 0
   Successful Authentication count      : 2
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:55:44
Radius Server                           : 10.12.17.11 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:58:33

#show radius-server
        VRF: default
timeout value: 5

Total number of servers:4

Following RADIUS servers are configured:
Radius Server                           : 192.168.1.1
   Sequence Number                      : 1
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 1
   Failed Connection Request            : 2
   Last Successful authentication       : 2000 January 05, 20:45:09

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2

Radius Server                           : 100.0.0.1 (*)
   Sequence Number                      : 2
   available for authentication on port : 60000
   available for accounting on port     : 60000
   timeout                              : 2
   RADIUS shared secret                 : ********
   Failed Authentication count          : 1
   Successful Authentication count      : 1
   Failed Connection Request            : 0
   Last Successful authentication       : 2000 January 05, 20:46:36

#show radius-server vrf all
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
```

```
Radius Server                             : 10.12.17.13
   Sequence Number                        : 1
   available for authentication on port   : 60000
   available for accounting on port       : 60000
   timeout                                : 2
   RADIUS shared secret                   : ********
   Failed Authentication count            : 0
   Successful Authentication count        : 2
   Failed Connection Request              : 2
   Last Successful authentication         : 2000 January 05, 20:55:44
Radius Server                             : 10.12.17.11 (*)
   Sequence Number                        : 2
   available for authentication on port   : 60000
   available for accounting on port       : 60000
   timeout                                : 2
   RADIUS shared secret                   : ********
   Failed Authentication count            : 1
   Successful Authentication count        : 1
   Failed Connection Request              : 0
   Last Successful authentication         : 2000 January 05, 20:58:33

        VRF: default
timeout value: 5

Total number of servers:4

Following RADIUS servers are configured:
Radius Server                             : 192.168.1.1
   Sequence Number                        : 1
   available for authentication on port   : 60000
   available for accounting on port       : 60000
   timeout                                : 2
   RADIUS shared secret                   : ********
   Failed Authentication count            : 0
   Successful Authentication count        : 1
   Failed Connection Request              : 2
   Last Successful authentication         : 2000 January 05, 20:45:09

Radius Server                             : 100.0.0.1 (*)
   Sequence Number                        : 2
   available for authentication on port   : 60000
   available for accounting on port       : 60000
   timeout                                : 2
   RADIUS shared secret                   : ********
   Failed Authentication count            : 1
   Successful Authentication count        : 1
   Failed Connection Request              : 0
   Last Successful authentication         : 2000 January 05, 20:46:36

#show running-config radius
radius-server login key 7 0x6f32ba3f9e05a3db vrf management
radius-server login host 10.12.17.13 vrf management seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb

#show running-config aaa
aaa authentication login default vrf management group radius
aaa group server radius rad1 vrf management
```

```
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1

#show running-config aaa all
aaa authentication login default vrf management group radius
aaa authentication login console local
aaa accounting default vrf management local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default group radius
aaa authentication login console local
aaa accounting default local
no aaa authentication login default fallback error local
no aaa authentication login console fallback error local
no aaa authentication login error-enable
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server radius rad1
    server Radius-Server-1
    server 100.0.0.1
```

IPv6 Address

Radius server address is configured as IPv6 address. Authentication messages are transmitted to radius server from the Router using IPv6 address.

Topology

Figure 3-3 shows the sample configuration of Radius server.

Figure 3-3: RADIUS topology

R1

`#configure terminal`	Enter configure mode.
`(config)#radius-server login host 2001:db8:100::2 vrf management seq-num 1 key 0 testing123`	Configure radius server with IPv6 address
`(config)#aaa authentication login default vrf management group radius`	Configure AAA authentication
`(config)#aaa authentication login error-enable vrf management`	Configure AAA authentication login error-enable
`(config)#interface eth0`	Navigate to the interface mode
`(config-if)#ipv6 address 2001:db8:100::5/64`	Configure IPv6 address on the eth0 interface
`(config-if)#exit`	Exit interface configure mode
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode

Validation

Perform TELNET to the Router R1. Provide the username mentioned in the radius server "users" file as telnet username. Check that R1 sends radius request to the radius server using IPv6 address.

```
#show running-config radius
radius-server login host 2001:db8:100::2 vrf management seq-num 1 key 7
0x67efdb
4ad9d771c3ed8312b2bc74cedb

#show running-config aaa
aaa authentication login default vrf management group radius
aaa authentication login error-enable vrf management

#show ipv6 interface eth0 brief
Interface            IPv6-Address                                  Admin-
Sta
tus
eth0                 2001:db8:100::5
                     fe80::218:23ff:fe30:e6ba                      [up/up]
```

RADIUS Server Accounting

You can configure accounting to measure the resources that another user consumes during access.

User

`#configure terminal`	Enter configure mode.
`(config)#radius-server login host 10.12.17.11 vrf management key 7 seq-num 1 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 seq-num 2 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#aaa accounting default vrf management group radius`	Enable accounting for radius server configured for vrf management
`(config)#aaa accounting default group radius`	Enable accounting for radius server configured for default vrf
`(config)#commit`	Commit the candidate configuration to the running configuration

Validation

```
#show aaa accounting vrf management
                VRF: management
  default: group radius

#show aaa accounting vrf all
                VRF: management
  default: group radius

                VRF: default
  default: group radius

#show aaa accounting
                VRF: default
  default: group radius
#
#show running-config aaa
aaa authentication login default vrf management group radius
aaa accounting default vrf management group radius
aaa group server radius rad1 vrf management
    server Radius-Server-1 vrf management
    server 100.0.0.1 vrf management

aaa authentication login default  group radius
aaa accounting default  group radius
aaa group server radius rad1
    server Radius-Server-1
```

```
    server 100.0.0.1
```

Sample Radius Clients.conf File

```
client 10.12.58.20 {
  secret    = testing123
  shortname = localhost
}
client 192.168.1.2 {
  secret    = testing123
  shortname = localhost
}
client 10.12.37.196 {
  secret    = testing123
}
client 100.0.0.2 {
  secret    = testing123
  shortname = localhost
}

# IPv6 Client
#client ::1 {
#       secret          = testing123
#       shortname       = localhost
#}
#
# All IPv6 Site-local clients
#client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
```

Sample Radius Users Configuration File

```
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com

# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User

# On no match, the user is denied access.

selftest Cleartext-Password := "password"
```

```
testuser1 Cleartext-Password := "user1@101"
testuser2 Cleartext-Password := "user2@202"
testuser3 Cleartext-Password := "user3@303"
```

Fall Back Option for RADIUS Authentication

Currently, the Remote Authentication Dial-In User Service (RADIUS) server authentication fallback to the local authentication server only when the RADIUS server is not reachable.

This behavior is modified to forward the authentication request to the local authentication server when the RADIUS authentication is failed or not reachable.

Feature Characteristics

The RADIUS authentication mechanism is enhanced to fallback to local authentication server when the user

- is not present on RADIUS server or
- authentication fails from RADIUS server

To implement the above requirements, the existing CLI `aaa authentication login default fallback error local non-existent-user vrf management` is used to enable fallback to local authentication server. This is disabled by default.

Note: For invalid secret key there is no fallback local authentication.
Console authentication is not supported for RADIUS.

Benefits

By default, the fallback to local authentication is applied when the RADIUS server is unreachable. For other scenarios, enable the fallback using the CLI.

Configuration

Below is the existing CLI used to enable the fallback local authentication server.

```
aaa authentication login default fallback error local non-existent-user vrf
  management
```

Refer to Chapter 1, *Authentication, Authorization and Accounting* section in the OcNOS System Management Configuration Guide.

Validation

Configure `aaa authentication` console and verify console authentication:

```
OcNOS#con t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#radius-server login host 1.1.1.2 seq-num 1 key 0 kumar
OcNOS(config)#commit
OcNOS(config)#aaa authentication login console group radius
```

```
OcNOS(config)#commit
OcNOS(config)#exit
OcNOS#exit

OcNOS#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line       User          Idle        Location/Session PID    TYPE   Role
(*) 0 con 0 [C]ocnos      0d00h00m    ttyS0           5531   Remote network-admin
```

Enabled RADIUS local fallback and verify the authentication:

```
OcNOS(config)#aaa authentication login console group radius local
OcNOS(config)#commit
OcNOS(config)#exit
OcNOS#exit
OcNOS>exit

OcNOS>enable
OcNOS#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

Line         User          Idle         Location/Session PID   TYPE   Role
(*) 0 con 0  [C]test        0d00h00m     ttyS0           5713  Local  network-engineer
130 vty 0    [C]test        0d00h01m     pts/0           5688  Local  network-engineer
OcNOS#
```

CHAPTER 4 TACACS Client Configuration

Overview

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device. TACACS+ listens at port 49.

TACACS Server Authentication

IPv4 Address Configuration

This section shows a TACACS+ server is configured with an IPv4 address. Authentication messages are transmitted to TACACS+ server from the device using an IPv4 address.

Topology

Figure 4-4 shows the sample configuration of TACACS+ server.

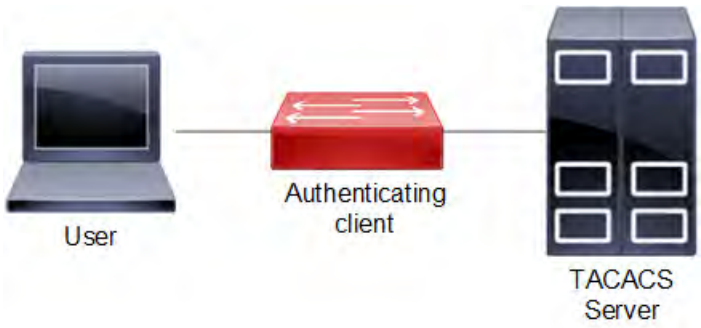


Figure 4-4: TACACS Server Host Configuration

Authenticating Client

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for management vrf
`(config)#feature tacacs+`	Enable the feature TACACS+. for default vrf
`(config)#tacacs-server login key 0 testing101 vrf management`	Specify the global key for tacacs servers that are not configured with their respective keys for management vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login key 0 testing101`	Specify the global key for tacacs servers that are not configured with their respective keys for default vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file

(config)#tacacs-server login host 10.16.19.2 seq-num 3 key 0 testing123	Specify the tacacs server ipv4 address to be configured with shared local key for default vrf The same key should be present on the server config file.
(config)#tacacs-server login host 10.12.30.86 vrf management seq-num 4 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
config)#tacacs-server login host 10.12.30.86 seq-num 2 port 1045	Specify the tacacs server ipv4 address to be configured with the sequence and port number for default vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for management vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host 10.12.17.11 seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for default vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for management vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for default vrf. The tacacs server should be started with same port number
(config)#aaa authentication login default vrf management group tacacs+	Enable authentication for TACACS+ server configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+	Enable authentication for TACACS+ server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group tacacs+ local	Enable authentication for TACACS+ and fall-back to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ local none	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ none	Enable authentication for TACACS+ fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+ none	Enable authentication for TACACS+ fall-back to none , configured for default vrf. Authorization is also enabled by default
(config)#aaa group server tacacs+ G1 vrf management	Create aaa group G1 for management vrf
(config-tacacs)#server 10.12.30.86 vrf management	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacas)#exit	Exit the tacacs-config
(config)#commit	Commit the configuration
(config)#aaa group server tacacs+ G1	Create aaa group G1 for default vrf
(config-tacacs)server 10.12.30.86	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacacs)#exit	Exit the tacacs-config mode

`(config)#commit`	Commit the configuration
`(config)#aaa authentication login default vrf management group G1`	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
`(config)#aaa authentication login default group G1`	Authenticate the tacacs+ group G1 with aaa authentication for default vrf
`(config)#commit`	Commit the configuration

Users are mapped as shown as shown in Table 4-1:

Table 4-1: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 12
RBAC-customized-role	13
Network user	0 or any other values (>15 or negative values or any character)

Validation

```
Leaf1#show tacacs-server vrf management
        VRF: management
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.30.86/1045
           Sequence Number      : 2
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-Server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:
```

```
Leaf1#show tacacs-server
        VRF: default
total number of servers:4

Tacacs+ Server                  : 10.16.19.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.30.86/1045
           Sequence Number      : 2
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-Server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs-server vrf all
        VRF: management
total number of servers:2
Tacacs+ Server                  : Tacacs-Server-1/65535(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222
           Sequence Number      : 7
```

```
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 100.0.0.1/2222
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:


(*) indicates last active.

#show tacacs-server
        VRF: default
total number of servers:2

Tacacs+ Server                 : Tacacs-Server-1/2222
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 100.0.0.1/2222
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs-server vrf management groups G1
        VRF: management

        group G1:
                server Tacacs-Server-1:
                seq-num 7
                port is 65535
                key is ********

                server 10.12.17.11:
                seq-num 8
                port is 65535
                key is ********

#show tacacs-server vrf all groups G1
        VRF: management

        group G1:
                server Tacacs-Server-1:
                seq-num 7
                port is 65535
                key is ********
```

```
                server 10.12.17.11:
                seq-num 8
                port is 65535
                key is ********


        VRF: default

        group G1:
                server Tacacs-Server-1:
                seq-num 7
                port is 2222
                key is ********

                server 100.0.0.1:
                seq-num 8
                port is 2222
                key is ********

#show tacacs-server groups G1
        VRF: default
group G1:
                server Tacacs-Server-1:
                seq-num 7
                port is 2222
                key is ********

                server 100.0.0.1:
                seq-num 8
                port is 2222
                key is ********
#show tacacs vrf management
        VRF: management
total number of servers:2

Tacacs+ Server                 : Tacacs-Server-1/65535(*)
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 1
   Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                 : 10.12.17.11/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs vrf all
        VRF: management
total number of servers:2

Tacacs+ Server                 : Tacacs-Server-1/65535(*)
```

```
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 1
   Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                 : 10.12.17.11/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:


        VRF: default
total number of servers:2

Tacacs+ Server                 : Tacacs-Server-1/2222(*)
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 1
   Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                 : 100.0.0.1/2222
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:


(*) indicates last active.

#show tacacs
        VRF: default
total number of servers:2

Tacacs+ Server                 : Tacacs-Server-1/2222(*)
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 1
   Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                 : 100.0.0.1/2222
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs vrf management
        VRF: management
total number of servers:2
```

```
Tacacs+ Server                  : Tacacs-Server-1/65535(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show tacacs vrf all
        VRF: management
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/65535(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


(*) indicates last active.

#show tacacs
```

```
        VRF: default
total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 1
   Failed Connect Attempts      : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show aaa authentication vrf management
                VRF: management
  default: group G1
  console: local

#show aaa authentication vrf all
                VRF: management
  default: group G1
  console: local

                VRF: default
  default: group tacacs+
  console: local

#show aaa authentication
                VRF: default
  default: group tacacs+
  console: local

# show aaa groups vrf management
                VRF: management
radius
tacacs+
G1

# show aaa groups vrf all
                VRF: management
radius
tacacs+
G1

                VRF: default
radius
tacacs+
G1

#show aaa groups
                VRF: default
```

```
radius
tacacs+
G1

#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535
po
rt 65535
tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port
6
5535

feature tacacs+
tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 2222
tacacs-server login host 100.0.0.1 seq-num 8 key 7 65535 port 2222

#show running-config aaa
aaa authentication login default vrf management group G1
aaa group server tacacs+ G1 vrf management
    server Tacacs-Server-1 vrf management
    server 10.12.17.11 vrf management

aaa authentication login default group tacacs+
aaa group server tacacs+ G1
    server Tacacs-Server-1
    server 100.0.0.1

#show running-config aaa all
aaa authentication login default vrf management group G1
aaa authentication login console local
aaa accounting default vrf management local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server tacacs+ G1 vrf management
    server Tacacs-Server-1 vrf management
    server 10.12.17.11 vrf management

aaa authentication login default group tacacs+
aaa authentication login console local
aaa accounting default local
no aaa authentication login default fallback error local
no aaa authentication login console fallback error local
no aaa authentication login error-enable
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa group server tacacs+ G1
    server Tacacs-Server-1
    server 100.0.0.1
```

IPv6 Address Configuration

This section shows a TACACS+ server is configured with an IPv6 address. Authentication messages are transmitted to TACACS+ server from the device using an IPv6 address.

Topology

Figure 4-5 shows the sample configuration of TACACS+ server.

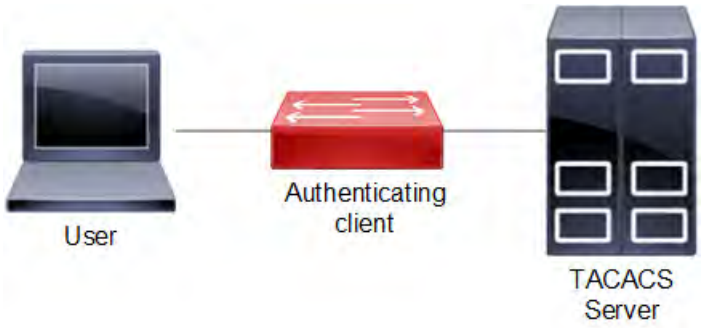


Figure 4-5: TACACS+ server topology

Authenticating Client

`R1#configure terminal`	Enter configure mode.
`R1(config)#tacacs-server login host 2001:db8:100::2 vrf management seq-num 1 key 0 testing123`	Configure TACACS+ server with IPv6 address
`R1(config)# aaa authentication login default vrf management group tacacs+`	Configure AAA authentication
`R1(config)#tacacs-server login host 2001:db8:100::2 vrf management seq-num 1`	Config for IPv6 TACACS server with seq-num
`R1(config)# ip host vrf management Server1 2001:db8:100::2`	Config for assigning hostname to valid IPv6 address
`R1(config)#feature tacacs+ vrf management`	Config for enabling the TACACS+ server
`R1(config)#tacacs-server login host 2002::3 vrf management seq-num 5 key 0 def_abc port 65535 timeout 60`	Config for IPv6 TACACS+ server address with key, port and timeout
`R1(config)#tacacs-server login timeout 60`	Config timeout for TACACS server
`R1(config)#tacacs-server login  key 7 65535`	Config login key for TACACS server
`R1(config)# interface eth0`	Navigate to the interface mode
`R1(config-if)#ipv6 address 2001:db8:100::5/64`	Configure IPv6 address on the eth0 interface
`R1(config-if)# exit`	Exit interface configure mode
`R1(config)#commit`	Commit the configuration
`R1(config)# exit`	Exit configure mode

Validation

Perform TELNET to the Router. Provide the username mentioned in the TACACS+ server "users" file as telnet username. Check that Router sends TACACS request to the TACACS server using IPv6 address.

```
#show running-config tacacas+
tacacs-server login host 2002::3 seq-num 1 key 7 0x6f32ba3f9e05a3db

#sh tacacs-server
        VRF: default
total number of servers:1

Tacacs+ Server                  : 2002::3/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.

#show running-config aaa
aaa authentication login default vrf management group tacacs+
aaa authentication login error-enable vrf management

#show ipv6 interface eth0 brief
Interface            IPv6-Address                                      Admin-Sta
tus
eth0                 2001:db8:100::5
                    fe80::218:23ff:fe30:e6ba                          [up/up]
```

TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for vrf management
`(config)#feature tacacs+`	Enable the feature TACACS+ for default vrf
`(config)#tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 0 testing123`	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
`(config)#tacacs-server login host 10.16.19.2 seq-num 3 key 0 testing123`	Specify the TACACS server IPv4 address to be configured with shared key default vrf. The same key should be present in the server configuration file.
`(config)#aaa accounting default vrf management group tacacs+`	Enable accounting for TACACS server configured for vrf management.
`(config)#aaa accounting default group tacacs+`	Enable accounting for TACACS server configured for default vrf
`(config)#commit`	Commit the configuration

(config)#exit	Exit configure mode
#clear tacacs-server counters vrf management	Clear tacacs server counters for management vrf
#clear tacacs-server counters vrf all	Clear tacacs server counters for management and default vrf
#clear tacacs-server counters	Clear tacacs server counters for default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting vrf management
                     VRF: management
          default: group tacacs+
#

#show aaa accounting vrf all
                     VRF: management
          default: group tacacs+

                     VRF: default
          default: group tacacs+

#show aaa accounting
                     VRF: default
          default: group tacacs+
          #

#show running-config aaa
    aaa authentication login default vrf management group G1
    aaa accounting default vrf management group tacacs+
    aaa group server tacacs+ G1 vrf management
        server Tacacs-Server-1 vrf management
        server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa accounting default group tacacs+
    aaa group server tacacs+ G1
        server Tacacs-Server-1
        server 100.0.0.1
```

Sample TACACS Config File Contents

```
#tacacs configuration file
#set the key

    key = "testing123"
    accounting file = /var/log/tac_acc.log

    user = test1 {
            default service = permit
            login = cleartext "12345"
```

```
}

group = netadmin {
        service = ppp protocol = ip {
        priv-lvl = 1
        }
}

user = test2 {
        default service = permit
        login = cleartext "12345"
        member = netadmin
}

user = test3 {
        default service = permit
        login = cleartext "12345"
        service = ppp protocol = ip {
        priv-lvl = 15
}
}
```

TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in Table 4-1.

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in Table 4-1.

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level <=0 and priv-level > 15 are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is “auto-enabled”. After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configure mode. An error message is displayed upon executing any command which is not allowed.

```
#write
% Access restricted for user %
#configure terminal
% Access restricted for user %
```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```
service = ppp protocol = ip {
        priv-lvl = <0…15>
}
```

Sample TACACS+ Configuration File

```
#tacacs configuration file from “tac_plus version F4.0.3.alpha “
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user “test1”, without any priv-lvl, mapped to role “network-user”
user = test1 {
default service = permit
login = cleartext "12345"
}

#We can create a group of users mapped to a privilege
group = netadmin {
service = ppp protocol = ip {
priv-lvl = 15
}
}

#User “test2” with highest priv-lvl=15, mapped to role “network-admin”
user = test2 {
default service = permit
login = cleartext "12345"
member = netadmin
}

#User “test3” with priv-lvl= 1…13, mapped to role “network-operator”
user = test3 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 10
}
}
#User “test4” with priv-lvl=14, mapped to role “network-engineer” user = test4 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 14
}
}
```

TACACS Server Authentication for User Defined VRF

IPv4 Address Configuration

This section shows a TACACS+ server is configured with an IPv4 address. Authentication messages are transmitted to TACACS+ server from the device using an IPv4 address.

Topology

Figure 4-4 shows the sample configuration of TACACS+ server.

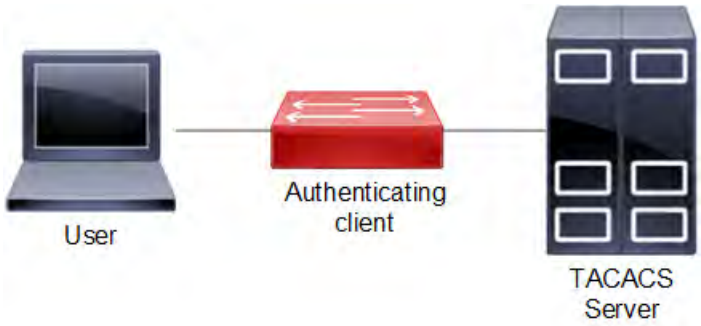


Figure 4-6: TACACS Server Host Configuration

Authenticating Client

`#configure terminal`	Enter configure mode
`(config)#ip vrf vrf1`	Configure the user-defined VRF
`(config)#feature tacacs+ vrf vrf1`	Enable the feature TACACS+ for user-defined vrf
`(config)#tacacs-server login key 0 testing123 vrf vrf1`	Specify the global key for tacacs servers that are not configured with their respective keys for user-defined vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login host 20.20.20.2 vrf vrf1 seq-num 1 key 0 testing123`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file
`(config)#tacacs-server login host 30.30.30.2 vrf vrf1 seq-num 4 port1045`	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
`(config)#tacacs-server login host 40.40.40.2 vrf vrf1 seq-num 8 key 7` 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for user-defined vrf. The tacacs server should be started with same port number.
`(config)#tacacs-server login host Tacacs-Server-1 vrf vrf1 seq-num 7 key 7 65535 port 65535`	Specify the tacacs server configured with host-name sequence number key and port number for user-defined vrf. The tacacs server should be started with same port number
`(config)#aaa authentication login default vrf vrf1 group tacacs+`	Enable authentication for TACACS+ server configured for user-defined vrf. Authorization is also enabled by default
`(config)#aaa authentication login default vrf vrf1 group tacacs+ local`	Enable authentication for TACACS+ and fall-back to local configured for user-defined vrf. Authorization is also enabled by default

`(config)#aaa authentication login default vrf vrf1 group tacacs+ local none`	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for user-defined vrf. `Authorization is also enabled by default`
`(config)#aaa group server tacacs+ G1 vrf vrf1`	Create aaa group G1 for user-defined vrf
`(config-tacacs)#server 20.20.20.2`	Make the tacacs-server 20.20.20.2 a part of this group G1 for user-defined vrf
`(config-tacacs)#server 30.30.30.2`	Make the tacacs-server 30.30.30.2 a part of this group G1 for user-defined vrf
`(config-tacacs)#server 40.40.40.2`	Make the tacacs-server 40.40.40.2 a part of this group G1 for user-defined vrf
`(config-tacacs)#server Tacacs- Server-1`	Make the tacacs-server Tacacs- Server-1a part of this group G1 for user-defined vrf
`(config-tacas)#exit`	Exit the tacacs-config
`(config)#commit`	Commit the configuration
`(config)#aaa authentication login default vrf vrf1 group G1`	Authenticate the tacacs+ group G1 with aaa authentication for user-defined vrf
`(config)#commit`	Commit the configuration

Users are mapped as shown as shown in Table 4-1:

Table 4-2: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 12
RBAC-customized-role	13
Network user	0 or any other values (>15 or negative values or any character)

Validation

```
OcNOS#sh tacacs-server vrf vrf1
        VRF: vrf1
total number of servers:4

Tacacs+ Server                  : 20.20.20.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 30.30.30.2/1045
           Sequence Number      : 4
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:
```

```
Tacacs+ Server                  : Tacacs-server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 40.40.40.2/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

(*) indicates last active.
OcNOS#sh tacacs-server vrf all
        VRF: management
total number of servers:0


        VRF: vrf1
total number of servers:4

Tacacs+ Server                  : 20.20.20.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 30.30.30.2/1045
           Sequence Number      : 4
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 40.40.40.2/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


(*) indicates last active.
OcNOS# sh tacacs-server vrf vrf1 groups G1
        VRF: vrf1
```

```
        group G1:
                server 20.20.20.2:
                seq-num 1
                port is 49
                key is ********

                server 30.30.30.2:
                seq-num 4
                port is 1045

                server Tacacs-server-1:
                seq-num 7
                port is 65535
                key is ********

                server 40.40.40.2:
                seq-num 8
                port is 65535
                key is ********


OcNOS# sh tacacs-server vrf all groups G1
        VRF: management
No such group exists.

        VRF: vrf1

        group G1:
                server 20.20.20.2:
                seq-num 1
                port is 49
                key is ********

                server 30.30.30.2:
                seq-num 4
                port is 1045

                server Tacacs-server-1:
                seq-num 7
                port is 65535
                key is ********

                server 40.40.40.2:
                seq-num 8
                port is 65535
                key is ********



OcNOS#sh tacacs vrf vrf1
        VRF: vrf1
total number of servers:4

Tacacs+ Server                  : 20.20.20.2/49
           Sequence Number      : 1
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
```

```
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 30.30.30.2/1045
           Sequence Number     : 4
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : Tacacs-server-1/65535
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 40.40.40.2/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

(*) indicates last active.
OcNOS# sh tacacs vrf all
        VRF: management
total number of servers:0


        VRF: vrf1
total number of servers:4

Tacacs+ Server                 : 20.20.20.2/49
           Sequence Number     : 1
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 30.30.30.2/1045
           Sequence Number     : 4
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : Tacacs-server-1/65535
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 40.40.40.2/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
```

```
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:


(*) indicates last active.
OcNOS#sh tacacs vrf vrf1
        VRF: vrf1
total number of servers:4

Tacacs+ Server                 : 20.20.20.2/49
           Sequence Number     : 1
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 30.30.30.2/1045
           Sequence Number     : 4
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : Tacacs-server-1/65535
           Sequence Number     : 7
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 40.40.40.2/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

(*) indicates last active.
OcNOS#sh tacacs vrf all
        VRF: management
total number of servers:0


        VRF: vrf1
total number of servers:4

Tacacs+ Server                 : 20.20.20.2/49
           Sequence Number     : 1
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                 : 30.30.30.2/1045
           Sequence Number     : 4
      Failed Auth Attempts     : 0
```

```
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0
 Last Successful authentication:

Tacacs+ Server                  : Tacacs-server-1/65535
           Sequence Number      : 7
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:

Tacacs+ Server                  : 40.40.40.2/65535
           Sequence Number      : 8
      Failed Auth Attempts      : 0
     Success Auth Attempts      : 0
   Failed Connect Attempts      : 0
 Last Successful authentication:


(*) indicates last active.
OcNOS# sh aaa authentication vrf vrf1
                VRF: vrf1
  default: group G1
OcNOS# sh aaa authentication vrf all
                VRF: vrf1
  default: group G1

OcNOS# sh aaa authentication
% AAA Entry not found

OcNOS# sh aaa groups vrf vrf1
                VRF: vrf1
radius
tacacs+
G1
OcNOS# sh aaa groups vrf all
                VRF: management
radius

                VRF: vrf1
radius
tacacs+
G1

OcNOS#sh running-config tacacs+
feature tacacs+ vrf vrf1
tacacs-server login key 7 0x67efdb4ad9d771c3ed8312b2bc74cedb vrf vrf1
tacacs-server login host 20.20.20.2 vrf vrf1 seq-num 1 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb
tacacs-server login host 30.30.30.2 vrf vrf1 seq-num 4 port 1045
tacacs-server login host Tacacs-server-1 vrf vrf1 seq-num 7 key 7
0x67efdb4ad9d771c3ed8312b2bc74cedb po
rt 65535
tacacs-server login host 40.40.40.2 vrf vrf1 seq-num 8 key 7
0x9f4a8983e0216052 port 65535
```

```
OcNOS#sh running-config aaa
aaa group server tacacs+ G1 vrf vrf1
    server 20.20.20.2
    server 30.30.30.2
    server Tacacs-server-1
    server 40.40.40.2

aaa authentication login default vrf vrf1 group G1
aaa accounting default vrf vrf1 group tacacs+
OcNOS#sh running-config aaa all
aaa local authentication attempts max-fail 3
aaa local authentication unlock-timeout 1200
aaa local authentication password expire 0 role network-admin
aaa local authentication password expire 0 role network-engineer
aaa local authentication password expire 0 role network-operator
aaa local authentication password expire 0 role network-user
aaa authentication login default vrf management local
aaa authentication login console local
aaa accounting default vrf management local
aaa accounting console local
no aaa authentication login default fallback error local vrf management
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf management
aaa authentication login default vrf vrf1 group G1
aaa authentication login console local
aaa accounting default vrf vrf1 group tacacs+
aaa accounting console local
no aaa authentication login default fallback error local vrf vrf1
no aaa authentication login console fallback error local
no aaa authentication login error-enable vrf vrf1
aaa group server tacacs+ G1 vrf vrf1
    server 20.20.20.2
    server 30.30.30.2
    server Tacacs-server-1
    server 40.40.40.2
```

IPv6 Address Configuration

This section shows a TACACS+ server is configured with an IPv6 address. Authentication messages are transmitted to TACACS+ server from the device using an IPv6 address.

Topology

Figure 4-5 shows the sample configuration of TACACS+ server.

Figure 4-7: TACACS+ server topology

Authenticating Client

`R1#configure terminal`	Enter configure mode.
`R1(config)# ip vrf vrf1`	Configure the user-defined VRF
`R1(config)#tacacs-server login 2001::2 vrf vrf1 key 0 seq-num 1 testing123`	Configure TACACS+ server with IPv6 address
`R1(config)# aaa authentication login default vrf vrf1 group tacacs+`	Configure AAA authentication
`R1(config)#tacacs-server login 2001:2 vrf vrf1 Hostseq-num 1`	Config for IPv6 TACACS server with seq-num
`R1(config)# ip host vrf vrf1 Server1 2001::2`	Config for assigning hostname to valid IPv6 address
`R1(config)#feature tacacs+ vrf Vrf1`	Config for enabling the TACACS+ server
`R1(config)#tacacs-server login 2002::2 vrf vrf1 seq-num def_abc port 65535 timeout 60`	Config for IPv6 TACACS+ server address with key, port and timeout
`R1(config)#tacacs-server login timeout 60`	Config timeout for TACACS server
`R1(config)#tacacs-server login key 7 65535`	Config login key for TACACS server
`R1(config)# interface eth0`	Navigate to the interface mode
`R1(config-if)#ipv6 address 2001::5/64`	Configure IPv6 address on the eth0 interface
`R1(config-if)# exit`	Exit interface configure mode
`R1(config)#commit`	Commit the configuration
`R1(config)# exit`	Exit configure mode

Validation

Perform TELNET to the Router. Provide the username mentioned in the TACACS+ server "users" file as telnet username. Check that Router sends TACACS request to the TACACS server using IPv6 address.

```
#show running-config tacacas+
tacacs-server login host 2002::5 vrf vrf1 seq-num 1 key 7 0x6f32ba3f9e05a3db

#sh tacacs-server vrf vrf1
VRF: vrf1
 total number of servers:1
```

```
Tacacs+ Server          : 2002::5/49
Sequence Number         : 1
Failed Auth Attempts    : 0
Success Auth Attempts   : 0
Failed Connect Attempts : 0
Last Successful authentication:
(*) indicates last active. #show running-config aaa
aaa authentication login default vrf management group tacacs+ aaa authentication login
error-enable vrf management

#show ipv6 interface eth0 brief
Interface     IPv6-Address               Admin-Sta tus
eth0          2001:db8:100::5
              fe80::218:23ff:fe30:e6ba      [up/up]
```

TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

Authenticating Device

`#configure terminal`	Enter configure mode.
`(config)#feature tacacs+ vrf vrf1`	Enable the feature TACACS+ for user defined vrf
`(config)#tacacs-server login host 10.16.19.2 vrf vrf1 seq-num 1 key 0 testing123`	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
`(config)#aaa accounting default group tacacs+`	Enable accounting for TACACS server configured for default vrf
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode
`#clear tacacs-server counters vrf vrf1`	Clear tacacs server counters for user-defined vrf
`#clear tacacs-server counters vrf all`	Clear tacacs server counters for management and default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting VRF: vrf1
                     VRF: vrf1
          default: group tacacs+
#
```

```
#show aaa accounting vrf all
                    VRF: management
          default:
                 VRF: vrf1
             default: group tacacs+

#show running-config aaa
    aaa authentication login default vrf vrf1 group G1
    aaa accounting default vrf vrf1 group tacacs+
    aaa group server tacacs+ G1 vrf management server Tacacs-Server-1 vrf
    management server 10.12.17.11 vrf management
```

Sample TACACS Config File Contents

```
#tacacs configuration file
#set the key

    key = "testing123"
    accounting file = /var/log/tac_acc.log

    user = test1 {
            default service = permit
            login = cleartext "12345"
    }

    group = netadmin {
            service = ppp protocol = ip {
            priv-lvl = 1
            }
    }

    user = test2 {
            default service = permit
            login = cleartext "12345"
            member = netadmin
    }

    user = test3 {
            default service = permit
            login = cleartext "12345"
            service = ppp protocol = ip {
            priv-lvl = 15
    }
    }
```

TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in Table 4-1.

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in Table 4-1.

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level <=0 and priv-level > 15 are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is “auto-enabled”. After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configure mode. An error message is displayed upon executing any command which is not allowed.

```
#write
% Access restricted for user %
#configure terminal
% Access restricted for user %
```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```
service = ppp protocol = ip {
        priv-lvl = <0…15>
}
```

Sample TACACS+ Configuration File

```
#tacacs configuration file from “tac_plus version F4.0.3.alpha “
#set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user “test1”, without any priv-lvl, mapped to role “network-user”
user = test1 {
default service = permit
login = cleartext "12345"
}

#We can create a group of users mapped to a privilege
group = netadmin {
service = ppp protocol = ip {
priv-lvl = 15
}
}

#User “test2” with highest priv-lvl=15, mapped to role “network-admin”
user = test2 {
default service = permit
login = cleartext "12345"
member = netadmin
}
```

```
#User “test3” with priv-lvl= 1…13, mapped to role “network-operator”
user = test3 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 10
}
}
#User “test4” with priv-lvl=14, mapped to role “network-engineer” user = test4 {
default service = permit
login = cleartext "12345"
service = ppp protocol = ip {
priv-lvl = 14
}
}
```

CHAPTER 5 Role-Based Access Control

Overview

The Role-Based Access Control (RBAC) feature in OcNOS allows the creation of custom user roles locally. This provides administrators with the flexibility to define specific groups of commands that can be allowed or denied for each role. Users can then be assigned to these user roles on a per-switch basis or by utilizing a TACACS+ server.

Feature Characteristics

RBAC offers the capability to restrict or permit users from executing CLI commands in OcNOS and command authorization is entirely handled within OcNOS. With Role-Based Command Authorization, administrators can create the following entities:

- Policy
- User Role
- User Name

Policy

A policy is a collection of rules that determine which commands are permitted or denied. The maximum number of policies that can be configured is 20.

User Role

User roles group users together, allowing restrictions to be applied based on the policies associated with the role. When creating a User Role, a default policy should be specified. This default policy determines whether all commands are permitted or denied by default. One or more policies can be attached to a User Role. The maximum number of roles that can be configured is 14.

User Name

Users can be assigned to predefined user roles or customized roles. Some predefined roles include:

- Network-Administrator
- Network-Operator
- Network-Engineer
- Network-User

Multiple users can be assigned the same User Role.

RBAC user accounts will not be deleted when a corresponding RBAC-role is deleted or when the dynamic-RBAC feature is disabled. If an RBAC-user is authenticated but the associated role is not present, the user privilege will default to network-user privilege, and the role will be displayed as RBAC-customized-role in the `show users` command.

Benefits

RBAC ensures secure and controlled access to CLI commands, streamlining network management.

© 2025 IP Infusion Inc. Proprietary

Prerequisites

Ensure there is a supported OcNOS router with management interface access.

Configuration

Here is the example configurations for the RBAC feature. For TACACS+ configurations, see the TACACS Client Configuration chapter in the System Management guide.

Note: When implemented, users will have visibility into the imposed restrictions through the `show running-config` command. Additionally, both the configured policy and role specifics can be observed using the `show running-config` command.

Example 1:

In the provided example, RBAC is employed to define user roles and policies that restrict command access for enhanced security and control. Here is the configuration steps:

```
OcNOS#show running-config rbac
feature dynamic-rbac
policy p1
 permit "enable"
 permit "configure terminal"
 Permit "snmp-server .*"
role custom
 default deny-all
 add policy p1
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#username test password Test@123
OcNOS(config)#username test role custom
OcNOS(config)#commit
OcNOS#sh user-account
User:ocnos
                roles: network-admin
User:test
                roles: custom
```

- The RBAC feature is enabled with the `feature dynamic-rbac` command.
- A policy named `p1` is created, allowing specific commands such as `enable`, `configure terminal`, and `SNMP-related` commands.
- A custom role called `custom` is established, with a default action to deny all commands (`default deny-all`). The previously defined policy `p1` is added to this role.
- A new user account named `test` is created with the password `Test@123`, and the role custom is assigned to this user.
- The configuration changes are committed using the `commit` command.The output indicates that the user `test` has the custom role, granting specific permissions.

```
root@debian:~# ssh test@10.12.29.130
test@10.12.29.130's password:
Last login: Tue Aug 23 01:06:31 2022 from 10.12.17.153

OcNOS version DELL_S3048-ON-OcNOS-1.3.9.364-ENT_IPBASE-S0-P0  01/21/2022
15:03:56
```

```
OcNOS>en
OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#snmp-server community test vrf management -->Allowed
OcNOS(config)#ntp server 1.1.1.1 vrf management      -->Not Allowed
% Access restricted for user %
```

- The user test logs into the system via SSH and demonstrates RBAC enforcement by successfully executing permitted SNMP-related commands but encountering an access restriction when attempting an unauthorized command (`ntp server`).
- This example showcases RBAC in action, illustrating how user roles and policies can control command access based on predefined configurations.

Example 2:

In the below example, the user `test1` establishes an SSH connection and demonstrates the RBAC setup. As the default action `permits all` commands except SNMP-related ones, the user is able to execute various configurations, except for `snmp-server` configurations:

```
OcNOS#show running-config rbac
feature dynamic-rbac
policy p1
 permit "enable"
 permit "configure terminal"
 permit "snmp-server .*" mode config
policy p2
 permit "enable"
 permit "configure terminal"
 deny "snmp-server .*"
role custom-snmp
 default permit-all
 add policy p2
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#username test1 password Test@1234
OcNOS(config)#username test1 role custom-snmp
OcNOS(config)#commit
OcNOS#sh user-account
User:ocnos
                roles: network-admin
User:test1
                roles: custom-snmp

root@debian:~# ssh test1@10.12.29.130
test1@10.12.29.130's password:

OcNOS version DELL_S3048-ON-OcNOS-1.3.9.364-ENT_IPBASE-S0-P0  01/21/2022
15:03:56
OcNOS>enable
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#ntp server 1.1.1.1 vrf management          --> Allowed
OcNOS(config)#snmp-server community test vrf management  -->Not Allowed
% Access restricted for user %
```

Implementation Examples

RBAC provides a structured and efficient approach to managing and controlling user access to various resources and functionalities within a system. RBAC is particularly beneficial in scenarios with multiple users with varying levels of permissions and responsibilities. Some common use cases for RBAC include:

Network Security: RBAC enhances network security by restricting users to only the resources and commands they need for their roles, reducing the risk of unauthorized access and potential breaches.

Administrative Efficiency: RBAC simplifies user management by categorizing users into predefined roles and streamlining tasks such as provisioning, access updates, and permissions adjustments.

Regulatory Compliance: RBAC ensures compliance with regulations by enforcing proper access controls and maintaining audit trails, helping organizations meet required standards for data security and privacy.

Reduced Human Error: RBAC minimizes the chance of human errors that could lead to network disruptions or security incidents, as users are limited to the specific commands relevant to their roles.

Access Segmentation: In multi-tenant or multi-customer environments, RBAC facilitates access segmentation, ensuring that different groups can only interact with their designated resources, enhancing isolation and privacy.

New CLI Commands

Here is the compilation of the new commands for configuring RBAC feature. For TACACS+ commands, see the TACACS+ Commands chapter in the System Management guide.

add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

Command Syntax

```
add policy POLICY-NAME
no add policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Name of the policy

Default

None

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of a role named 'myRole,' defining its default permissions, adding 'myPolicy1' to the role, and subsequently removing 'myPolicy2' from it.

```
OcNOS(config)#role myRole
OcNOS(config-role)#default permit-all
OcNOS(config-role)#add policy myPolicy1
OcNOS(config-role)#no add policy myPolicy2
OcNOS(config-role)#exit
```

default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Use the no parameter with this command to remove the default rule for a TACACS+ role-based authorization (RBAC) role.

Command Syntax

```
default (permit-all | deny-all)
no default
```

Parameters

permit-all	Permit all commands
deny-all	Deny all commands

Default

Unless this command is explicitly configured, the default rule for a role is deny-all.

Command Mode

RBAC role mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example illustrates the configuration of a role named 'myRole' in OcNOS, and specifying its default permission.

```
OcNOS(config)#role myRole
OcNOS(config-role)#default permit-all
OcNOS(config-role)#exit
```

deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the no form of this command to remove a deny rule from an RBAC policy.

Command Syntax

```
deny RULE-STRING (mode MODE-NAME |)
```

```
no deny RULE-STRING (mode MODE-NAME |)
```

Parameters

RULE-STRING	Command string
MODE-NAME	Command prompt string such as “config-router” or “config-if”. Deny access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below illustrates the configuration of a policy named 'myPolicy' in OcNOS. It includes a deny rule that restricts access to the 'ip address' command, specifically within the configuration interface mode (config-if).

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#deny “ip address” mode config-if
OcNOS(config-policy)#end
```

feature dynamic-rbac

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the no form of this command to disable the RBAC feature.

Command Syntax

```
feature dynamic-rbac
```

```
no feature dynamic-rbac
```

Parameters

None

Default

By default, feature TACACS+ RBAC is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below illustrates the configuration of enabling the TACACS+ RBAC feature.

```
OcNOS#configure terminal
OcNOS(config)#feature dynamic-rbac
```

permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

Command Syntax

```
permit RULE-STRING (mode MODE-NAME |)
no permit RULE-STRING (mode MODE-NAME |)
```

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “config-router” or “config-if”. Permit access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of a policy named '`myPolicy`', permitting access to the '`ip address`' command specifically in the configuration interface mode.

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#permit “ip address” mode config-if
```

policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

Command Syntax

```
policy POLICY-NAME
no policy POLICY-NAME
```

Parameters

`POLICY-NAME`	Policy name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of creating the RBAC policy named `myPolicy`, and the command prompt enters the policy configuration mode.

```
OcNOS#configure terminal
OcNOS(config)#policy myPolicy
OcNOS(config-policy)#exit
```

role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

Command Syntax

```
role ROLE-NAME
no role ROLE-NAME
```

Parameters

`ROLE-NAME`	Role name
	User *cannot* specify one of these roles already defined in OcNOS:
	`network-admin`
	`network-user`
	`network-operator`
	`network-engineer`
	For more about these built-in roles, see username.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples demonstrate the configuration of creating the RBAC role named 'myRole,' with the command prompt entering the role configuration mode.

```
OcNOS#configure terminal
OcNOS(config)#role myRole
OcNOS(config-role)#exit
```

show rbac-policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

Command Syntax

```
show rbac-policy (POLICY-NAME |)
```

Parameters

POLICY-NAME	Policy name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples display the show output of the RBAC policy named 'myPolicy' and its associated configurations.

```
OcNOS#show rbac-policy myPolicy
-----------------------------------------------------------------------
Policy Name     : myPolicy
permit "ip address" mode config-if
```

show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

Command Syntax

```
show rbac-role (ROLE-NAME |)
```

Parameters

ROLE-NAME	Role name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following examples display the show output of the RBAC role named '`myRole`' and its associated configurations.

```
OcNOS#show rbac-role myRole
------------------------------------------------------------------------
Role Name           : myRole
Default rule        : permit-all
Attached Policies   : myPolicy1
                    : myPolicy2

------------------------------------------------------------------------
```

Table P-5-3 explains the output fields.

Table 5-3: show rbac-role fields

Entry	Description
Role Name	Displays the name of the role, in this case, `myRole`.
Default rule	Indicates the default rule associated with the role, which can be `permit-all` or `deny-all`.
Attached Policies	Lists the names of policies that are attached to this role. In the example, `myPolicy1` and `myPolicy2` are attached to `myRole`.

Troubleshooting

For smooth operation, verify accurate sensor path configuration, check encoding method compatibility, and ensure proper router-management system connectivity.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
RBAC	Role Based Access Control
TACACS	Terminal Access Controller Access Control System
TACACS+	Enhanced version of TACACS

Glossary

The following provides definitions for key terms used throughout this document.

Role-Based Access Control (RBAC)	A security paradigm that restricts system access based on roles assigned to users.
User Role	A predefined or customized grouping of permissions assigned to users.
Policy	A set of rules determining which actions are permitted or denied for a specific user role.
Dynamic-RBAC	Dynamic Role-Based Access Control, allowing role assignment during user authentication.

© 2025 IP Infusion Inc. Proprietary

Authentication Management Command Reference

CHAPTER 1 Authentication, Authorization and Accounting

This chapter is a reference for the authentication:

- Authentication identifies users by challenging them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- Authorization provides a method of authorizing commands and services on a per user profile basis.

Note: Authorization will be auto-enabled if user enables the Authentication.

- Accounting collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The authentication feature allows you to verify the identity and, grant access to managing devices. The authentication feature works with the access control protocols as described in these chapters:

- Chapter 3, *RADIUS Commands*
- Chapter 2, *TACACS+ Commands*

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

Note: Per-command authorization needs to be enabled explicitly by the user whereas Session based authorization will be implicitly enabled when user enables authentication.

This chapter describes these commands:

- aaa authentication login
- aaa accounting details
- aaa authentication login default
- aaa authorization default
- aaa authentication login default fallback error
- aaa group server
- aaa local authentication attempts max-fail
- aaa local authentication unlock-timeout
- debug aaa
- disable default auto-enable
- server
- show aaa authentication
- show aaa authentication login
- show aaa authorization
- show aaa groups
- show aaa accounting
- show running-config aaa

© 2025 IP Infusion Inc. Proprietary

aaa authentication login

Use this command to set login authentication behavior.

Use the `no` form of this command to disable either authentication behavior.

Command Syntax

```
aaa authentication login error-enable (vrf management|)
no aaa authentication login error-enable (vrf management|)
```

Parameters

`error-enable`	Display login failure messages
`management`	Management VRF

Default

By default, aaa authentication login is local

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login error-enable vrf management
```

aaa accounting details

Use this command to set a list of server groups to which to redirect accounting logs.

Use the `no` form of this command to only log locally.

Command Syntax

```
aaa accounting default (vrf (NAME|management)|) ((group LINE)|local)
no aaa accounting default (vrf (NAME|management)|) ((group)|local)
```

Parameters

`group`	Server group list for authentication
`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+ server group names
`local`	Use local authentication
`management`	Management VRF
`NAME`	Custom VRF

Default

Default AAA method is local

Default groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#aaa accounting default vrf management group radius
```

aaa authentication login default

Use this command to set the AAA authentication methods.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login default (vrf (NAME|management)|) ((group LINE) | (local
  (|none)) | (none))
no aaa authentication login default (vrf (NAME|management)|) ((group) | (local
  (|none)) | (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication
`management`		Management VRF
`NAME`		Custom VRF

Default

By default, AAA authentication method is local

By default, groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

aaa authorization default

Use this command to enable per-command authorization. By enabling this user should be able to authorize every command executed via configured server.

This authorization will work only when authentication is successful.

Use the no form of this command to disable authorization.

Command Syntax

```
aaa authorization default (vrf (NAME|management)|) ((group LINE)|local)
no aaa authorization default (vrf (NAME|management)|) ((group LINE)|local)
```

Parameters

`group`	Server group list for authentication
`LINE`	Space-separated list of up to 8 configured TACACS+ server group names
`local`	Use local authentication
`management`	Management VRF
`NAME`	Custom VRF

Default

Default AAA method is local

Default groups: TACACS+

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 6.1.0. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#aaa authorization default vrf management group tacacs+
```

aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Command Syntax

```
aaa authentication login default fallback error local (vrf (NAME|management)|)
no aaa authentication login default fallback error local (vrf (NAME|management)|)
```

Parameters

`management`	Management VRF
`NAME`	Custom VRF

Default

By default, AAA authentication is local.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

aaa group server

Use this command to create a server group and enter server group configure mode.

Use the `no` form of this command to remove a server group.

Command Syntax

```
aaa group server (radius|tacacs+) WORD (vrf (NAME|management)|)
no aaa group server (radius|tacacs+) WORD (vrf (NAME|management)|)
```

Parameters

`radius`	RADIUS server group
`tacacs+`	TACACS+ server group
`WORD`	Server group name; maximum 127 characters
`management`	Management VRF
`NAME`	Custom VRF

Default

By default, the AAA group server option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#aaa group server radius maxsmart
(config-radius)#
```

aaa local authentication attempts max-fail

Use this command to set the number of unsuccessful authentication attempts before a user is locked out.

Use the `no` form of this command to disable the lockout feature.

Command Syntax

```
aaa local authentication attempts max-fail <1-25>
no aaa local authentication attempts max-fail
```

Parameters

`<1-25>`	Number of unsuccessful authentication attempts

Default

By default, the maximum number of unsuccessful authentication attempts before a user is locked out is 3.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication attempts max-fail 2
```

aaa local authentication unlock-timeout

Use this command to set timeout value in seconds to unlock local user-account.

Use the no form of this command to set default timeout value in seconds.

Note: This command is applicable only to local user but not for user/s present at the server end to authenticate using TACACS+ or RADIUS.

Command Syntax

```
aaa local authentication unlock-timeout <1-3600>
no aaa local authentication unlock-timeout
```

Parameters

<1-3600>	Timeout in seconds to unlock local user-account. Default value is 1200.

Default

By default, the unlock timeout is 1200 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication unlock-timeout 1800
```

debug aaa

Use this command to display AAA debugging information.

Use the `no` form of this command to stop displaying AAA debugging information.

Command Syntax

```
debug aaa
no debug aaa
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug aaa
```

server

Use this command to add a server to a server group.

Use the `no` form of this command to remove from a server group.

Command Syntax

```
server (A.B.C.D | X:X::X:X | HOSTNAME)
no server (A.B.C.D | X:X::X:X | HOSTNAME)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address

Default

None

Command Modes

RADIUS server group configure mode

TACACS+ server group configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+
(config)#aaa group server tacacs+ TacacsGroup4
(config-tacacs)#server 203.0.113.127
```

show aaa authentication

Use this command to display AAA authentication configuration.

Command Syntax

```
show aaa authentication (|vrf (management|NAME|all))
```

Parameters

None

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#show aaa authentication
                VRF: default
  default: local
  console: local
```

Table 1-4 explains the output fields.

Table 1-4: show aaa authentication fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.
Console	Authentication setting for the console access.

show aaa authentication login

Use this command to display AAA authentication configuration for login default and login console.

Command Syntax

```
show aaa authentication login error-enable vrf (NAME|management)|all))
```

Parameters

`error-enable`	Display setting for login failure messages
`vrf`	Management VRF or all VRFs
`NAME`	Custom VRF

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#show aaa authentication login error-enable
                VRF: default
disabled
```

Table 1-5 explains the output fields.

Table 1-5: show aaa authentication login error-enable fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show aaa authorization

Use this command to display AAA authorization configuration.

Command Syntax

```
show aaa authorization (|vrf(management|all))
```

Parameters

`vrf management`	Authorization configs present in Management VRF
`vrf all`	Authorization configs present in all VRFs

Command Modes

Executive mode

Applicability

This command is introduced in OcNOS version 6.1.0.

Examples

```
#show aaa authorization
 VRF: default
default: group tacacs+
```

show aaa groups

Use this command to display AAA group configuration.

Command Syntax

```
show aaa groups (|vrf (management|NAME|all))
```

Parameters

`vrf`	Management VRF or all VRFs
`NAME`	Custom VRF

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#show aaa groups
VRF: default
radius
```

Table 1-6 explains the output fields.

Table 1-6: show aaa groups fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show aaa accounting

Use this command to display AAA accounting configuration.

Command Syntax

```
show aaa accounting (|vrf (management|NAME|all))
```

Parameters

`vrf`	Management VRF or all VRFs
`NAME`	Custom VRF

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#show aaa accounting
                VRF: default
```

Table 1-7 explains the output fields.

Table 1-7: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.

show running-config aaa

Use this command to display AAA settings in the running configuration.

Command Syntax

```
show running-config aaa (vrf(management|all)|)
```

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show aaa accounting
                VRF: default
  default: local
```

Table 1-8 explains the output fields.

Table 1-8: show aaa accounting fields

Field	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.

CHAPTER 2 TACACS+ Commands

Terminal Access Controller Access-Control System Plus (TACACS+, usually pronounced like tack-axe) is an access control network protocol for network devices.

The differences between RADIUS and TACACS+ can be summarized as follows:

- RADIUS combines authentication and authorization in a user profile, while TACACS+ provides separate authentication.
- RADIUS encrypts only the password in the access-request packet sent from the client to the server. The remainder of the packet is unencrypted. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS is based on an open standard (RFC 2865). TACACS+ is proprietary to Cisco, although it is an open, publicly documented protocol (there is no RFC protocol specification for TACACS+).

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- add policy
- clear tacacs-server counters
- debug tacacs+
- default
- deny
- feature dynamic-rbac
- feature tacacs+
- permit
- policy
- role
- show debug tacacs+
- show rbac-policy
- show rbac-role
- show running-config tacacs+
- show tacacs-server
- tacacs-server login host
- tacacs-server login key
- tacacs-server login timeout

© 2025 IP Infusion Inc. Proprietary

clear tacacs-server counters

Use this command to clear the counter on a specified TACACS server.

Syntax

```
clear tacacs-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

`HOSTNAME`	The name of the server
`X:X::X:X`	IPv6 address of the server
`A.B.C.D`	IPv4 address of the server
`vrf`	VRF of the sever
`management`	The management VRF
`all`	All VRFs

Default

NA

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tacacs-server 10.1.1.1 counters
```

debug tacacs+

Use this command to display TACACS+ debugging information.

Use the `no` form of this command stop displaying TACACS+ debugging information.

Command Syntax

```
debug tacacs+
no debug tacacs+
```

Parameters

None

Default

Disabled.

Command Mode

Executive mode and configure mode.

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug tacacs+
```

feature tacacs+

Use this command to enable the TACACS+ feature.

Use the `no` form of this command to disable the TACACS+ feature.

Command Syntax

```
feature tacacs+ (vrf management|)
no feature tacacs+ (vrf management|)
```

Parameters

`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, feature tacacs+ is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+ vrf management
```

show debug tacacs+

Use this command to display whether TACACS+ debugging is enabled.

Command Syntax

```
show debug tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug tacacs+
TACACS client debugging is on
```

show running-config tacacs+

Use this command to display TACACS+ settings in the running configuration.

Command Syntax

```
show running-config tacacs+
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config tacacs+
feature tacacs+ vrf management
tacacs-server login host 10.16.19.2 vrf management seq-num 1 key 7
0x9f4a8983e0216052
```

Table 2-9 explains the output fields.

Table 2-9: show running-config fields

Entry	Description
TACAS server host	TACACS+ server Domain Name Server (DNS) name.
Seq-num	Sequence number of user authentication attempt with the TACACS+ server.
VRF Management	The management traffic using VPN Routing and Forwarding (VRFs).

show tacacs-server

Use this command to display the TACACS+ server configuration.

Command Syntax

```
show tacacs-server (|vrf (management|all))((WORD)|(groups (GROUP|)|)|(sorted)
```

Parameters

WORD	DNS host name or IP address
groups	TACACS+ server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by TACACS+ server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show tacacs-server
total number of servers:1

Tacacs+ Server                 : 192.168.10.215/49(*)
           Sequence Number     : 1
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 14
   Failed Connect Attempts     : 0
 Last Successful authentication: 2017 December 18, 12:27:13

(*) indicates last active.
```

Table 2-10 explains the output fields.

Table 2-10: show tacacs-server output fields

Field	Description
Sequence Number	Sequence number of user authentication attempt with the TACACS+ server.
Failed Auth Attempts	Number of times user authentication failed with the TACACS+ server. Increments for server key mismatches and password mismatches or wrong password for the user.
Success Auth Attempts	Number of times user authenticated with TACACS+ server. Increments for each successful login.

Table 2-10: show tacacs-server output fields

Field	Description
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server. Increments for server connection failure cases such as server not-reachable, server port mismatches.
Last Successful authentication	Timestamp when user successfully authenticated with the TACACS+ server.

tacacs-server login host

Use this command to set the TACACS+ server host name or IP address.

Use the `no` form of this command to remove an TACACS+ server (if only a host name or IP address is specified as parameter) or to remove all of a TACACS+ server's configuration settings (if any other parameters are also specified).

Command Syntax

```
tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (seq-num
  <1-8> |) (key ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |) (timeout <1-
  60> |)
no tacacs-server login host (HOSTNAME | A.B.C.D | X:X::X:X) (vrf management|)
no tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (key
  ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |) (timeout <1-60> |)
```

Parameters

HOSTNAME	Host name
X:X::X:X	IPv6 address
A.B.C.D	IPv4 address
vrf	Virtual Routing and Forwarding
management	Management VRF
seq-num	Sequence Number / Priority index for tacacs-servers
key	Authentication and encryption key (“shared secret”)
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 512 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
port	TACACS+ server port
<1205-65535>	TACACS+ server port number; the default is 49
timeout	TACACS+ server timeout
<1-60>	Timeout value in seconds; default is 5 seconds

Default

Enable authentication for TACACS+ server configured. Authorization is also enabled by default. The default server port is 49.The default timeout value is 5 seconds.

There is `no` command to enable authorization. Authorization functionality is enabled by default when remote.

authentication is enabled with TACACS+.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login host 203.0.113.31 vrf management
```

tacacs-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and TACACS+ servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax

```
tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
no tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)
```

Parameters

`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 512 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login key 7 jvn05mlQH1 vrf management
```

tacacs-server login timeout

Use this command to set the period to wait for a response from the server before the client declares a timeout failure. The default timeout value is 5 seconds.

You can only give this command when the TACACS+ feature is enabled.

Use the `no` form of this command to set the timeout value to its default value (5 seconds).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
tacacs-server login timeout <1-60> (vrf management|)
no tacacs-server login timeout (vrf management|)
```

Parameters

`<1-60>`	Timeout value in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 1.3.9

Examples

```
#configure terminal
(config)#tacacs-server login timeout 35 vrf management
```

CHAPTER 3 RADIUS Commands

This chapter is a reference for Remote Authentication Dial In User Service (RADIUS) commands, RADIUS provides centralized Authentication, Authorization management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

- clear radius-server
- debug radius
- radius-server login host
- radius-server login host acct-port
- radius-server login host auth-port
- radius-server login host key
- radius-server login key
- radius-server login timeout
- show debug radius
- show radius-server
- show running-config radius

clear radius-server

Use this command to clear Radius Server statistics.

Command Syntax

```
clear radius-server ((HOSTNAME | X:X::X:X | A.B.C.D)|) counters (vrf (management |
  all)|)
```

Parameters

`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`vrf management`	To clear radius server counters for Virtual Routing and Forwarding management
`all`	To clear radius server counters for both management an default vrf
`counters`	To clear radius server counters for default vrf

Default

No default value is specified

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.

Example

```
#clear radius-server counters vrf management
```

debug radius

Use this command to display RADIUS debugging information.

Use the `no` form of this command stop displaying RADIUS debugging information.

Command Syntax

```
debug radius
no debug radius
```

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug radius
```

radius-server login host

Use this command to configure a RADIUS server for both accounting and authentication.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
  (<1-8>)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
  (<1-8>) timeout <1-60>
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
  (<1-8>)(acct-port <0-65535> |) | timeout <1-60> |)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
  (<1-8>)(|(auth-port <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) seq-num
  (<1-8>)(|(key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535> (|(acctport <0-65535>
  (|(timeout <1-60>))))))))


no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) timeout
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of time out period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1
```

radius-server login host acct-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS accounting messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) acct-port <0-65535> |) | timeout <1-60> |)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) acct-port |) | timeout <1-60> |)
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, Radius-server login host acct-port is 1813

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 192.168.2.3 vrf management seq-num 2 acct-
port 23255
```

radius-server login host auth-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS authentication messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(auth-port <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) (auth-port (|(acct-port (|timeout))))
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`seq-num`	seq-num Sequence Number / Priority index for radius-servers
`<1-8>`	sequence number for servers
`auth-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, Radius-server login host acct-port is 1812

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1 auth-
port 23255
```

radius-server login host key

Use this command to set per-server shared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a server shared key.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
  (<1-8>)|) (|(key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535> (|(acct-port <0-
  65535> (|(timeout <1-60>))))))))
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-
  num (<1-8>)|) (key ((0 WORD) | (7 WORD) ) (|(auth-port <0-65535> (|(acct-port
  (|(timeout)))))))
```

Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
seq-num	seq-num Sequence Number / Priority index for radius-servers
<1-8>	sequence number for servers
0	Unencrypted (clear text) shared key
WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management seq-num 1 key 0
testing auth-port 23255
```

radius-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax

```
radius-server login key ((0 WORD) | (7 WORD)) (vrf management|)
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (seq-num
(<1-8>)|) (|(key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535> (|(acctport <0-65535>
  (|(timeout <1-60>))))))))
no radius-server login key ((0 WORD) | (7 WORD)) (vrf management|)
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME)(vrf
  management|)(seqnum(<1-8>)|) (key ((0 WORD) | (7 WORD)) (|(auth-port <0-65535>
  (|(acctport(|(timeout))))))
```

Parameters

`login`	Remote login
`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 63 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login key 7 p2AcxlQA vrf management

#configure terminal
(config)#no radius-server login key 7 p2AcxlQA vrf management
```

radius-server login timeout

Use this command to set the global timeout which is how long the device waits for a response from a RADIUS server before declaring a timeout failure.

Use the `no` form of this command to set the global timeout to its default (1 second).

Note: TELNET client session's default timeout is 60 seconds, so configuring timeout of 60 seconds timeout impacts TELNET client applications, because it cannot be fallback to use the other configured server/group. Hence it is recommended to configure 57 seconds or lesser timeout while using TELNET. This timeout doesn't have an impact on SSH connections.

Command Syntax

```
radius-server login timeout <1-60> (vrf management|)
no radius-server login timeout (vrf management|)
```

Parameters

`login`	Remote login
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Note: The system takes minimum 3 secs to timeout even though the configured timeout value is less than 3 seconds. Hence do not configure timeout value less than 3 secs. The timeout range value is mentioned as 1-60 secs for backward compatibility.

Default

By default, radius-server login timeout is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#radius-server login timeout 15 vrf management

#configure terminal
(config)#no radius-server login timeout 15 vrf management
```

show debug radius

Use this command to display debugging information.

Command Syntax

```
show debug radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug radius
RADIUS client debugging is on
```

show radius-server

Use this command to display the RADIUS server configuration.

Command Syntax

```
show radius-server (|vrf(management|all))((WORD)|(groups (GROUP|))|)|sorted
```

Parameters

WORD	DNS host name or IP address
groups	RADIUS server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by RADIUS server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show radius-server vrf management
        VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:
Radius Server                           : 10.12.12.39
   Sequence Number                      : 1
   available for authentication on port : 1812
   available for accounting on port     : 1813
   RADIUS shared secret                 : ********
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :

Radius Server                           : 1.1.1.1
   Sequence Number                      : 2
   available for authentication on port : 1234
   available for accounting on port     : 1234
   timeout                              : 5
   Failed Authentication count          : 0
   Successful Authentication count      : 0
   Failed Connection Request            : 0
   Last Successful authentication       :
```

Table 3-11 explains the output fields.

Table 3-11: show radius-server fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Timeout Value	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message
Total number of servers	Number of authentication requests received by the authentication server.

show running-config radius

Use this command to display RADIUS configuration settings in the running configuration.

Command Syntax

```
show running-config radius
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config radius
 10.12.12.39 vrf management seq-num 1 key 7 wawyanb123
 1.1.1.1 vrf management seq-num 2 auth-port 1234 acct-po
rt 1234
radius-server login key 7 wawyanb123
```

Remote Device Connect Configuration

CHAPTER 1 Telnet Configuration

Overview

Telnet is a TCP/IP protocol used on the Internet and local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. The Telnet program runs, connects it to a server on the network. A user can then enter commands through the Telnet program and they will be executed as if the user were entering them directly on the server console.Telnet enables users to control the server and communicate with other servers on the network. The default port number for Telnet protocol is 23.Telnet offers users the capability of running programs remotely and facilitates remote administration.

In-band Management Over Default VRF

OcNOS supports Telnet over the default and management VRFs via in-band management interface and OOB management interface, respectively.

By default, Telnet runs on the management VRF.

Telnet Configuration with IPv4 Address

Topology

Figure 1-8: Telnet topology

Enable and Disable the Telnet Server

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#telnet server port 6112 vrf management`	Set Telnet port to 61112
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Telnet Client Session

`#telnet 10.10.10.1 vrf management`	Log into remote machine using IPv4 address

Validation

```
#show telnet server

VRF MANAGEMENT
telnet server enabled port: 23
VRF DEFAULT:
telnet server enabled port: 6112

#show running-config telnet server

feature telnet vrf management
no feature telnet
```

Telent Configuration with IPv6 Address

Telnet is performed with IPv6 IP and verified by logging on remote PC.

Topology

Figure 1-9 shows the sample configuration of Telent.

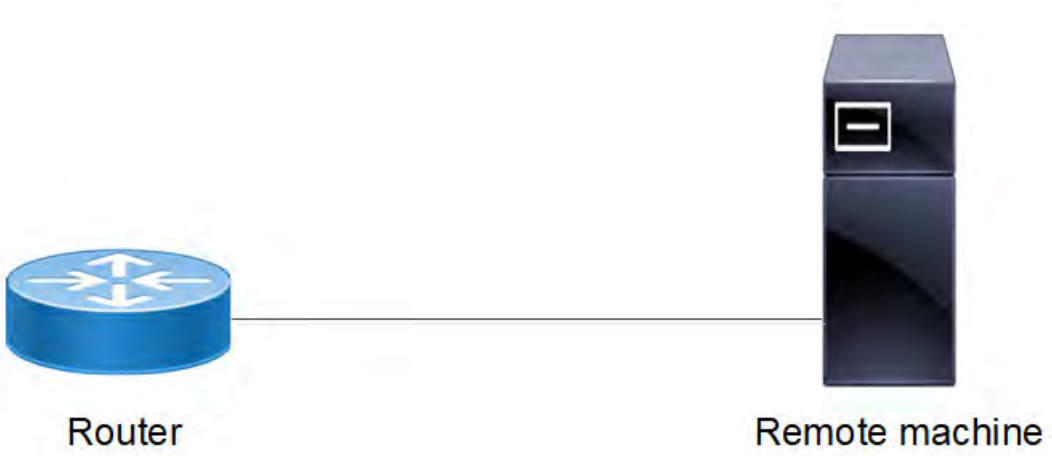


Figure 1-9: Telnet Configuration topology

Basic Configuration

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Telnet feature
`(config)#telnet server port 6112 vrf management`	Set Telnet port to 6112
`(config)#feature telnet vrf management`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Telnet Client Session

`#telnet 2001::1 vrf management`	Log into remote machine using IPv6 address

Validation

```
##show telnet server

VRF MANAGEMENT
telnet server enabled port: 23
```

```
VRF DEFAULT:
telnet server enabled port: 6112

#show running-config telnet server

feature telnet vrf management
no feature telnet
```

In-band Management for User Defined VRF

OcNOS supports Telnet over the user defined vrfs as well along with default and management VRFs via in-band interface.

By default, Telnet runs on the management VRF. If user wants to enable telnet feature over user defined vrfs which can be part of MPLS L3VPN/EVPN, it is possible to enable telnet feature over those user defined vrfs.

User must able to enable telnet feature over multiple user defined vrfs simultaneously with default/non default telnet ports.

Telnet Configuration with IPv4 Address for User Defined VRF

Topology

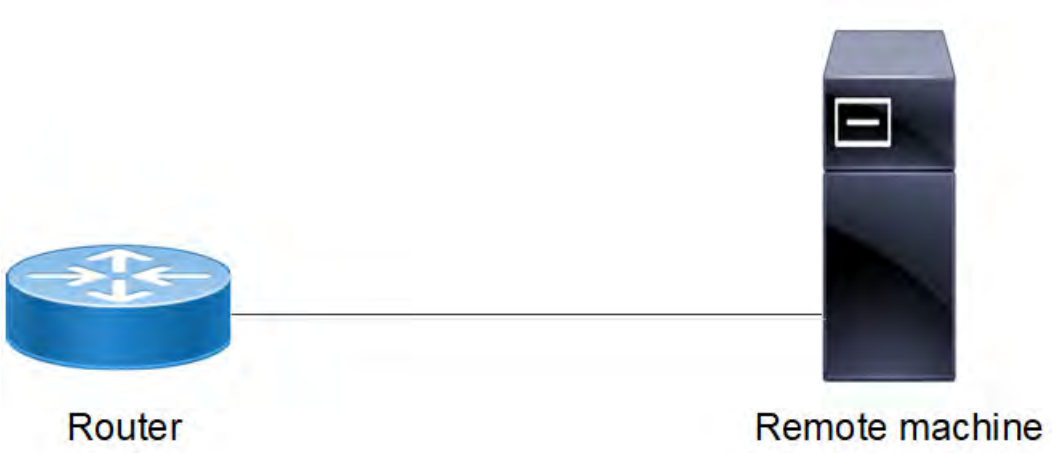


Figure 1-10: Telnet Configuration topology

Enable and Disable the Telnet Server on user defined vrf say vrf name is vrf_test

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf vrf_test`	Disable Telnet feature
`(config)#feature telnet vrf vrf_test`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port on user defined vrf say vrf name is vrf_test

`#configure terminal`	Enter configure mode
`(config)#ip vrf vrf_test`	Configure User defined vrf
`(config)#no feature telnet vrf vrf_test`	Disable Telnet feature
`(config)#telnet server port 6112 vrf vrf_test`	Set Telnet port to 61112
`(config)#feature telnet vrf vrf_test`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Telnet Client Session

`#telnet 10.10.10.1`	Log into remote machine using IPv4 address

Validation

```
#show telnet server

VRF MANAGEMENT
telnet server enabled port: 23 VRF DEFAULT:
telnet server enabled port: 23
VRF vrf_test:
telnet server enabled port: 6112

#show running-config telnet server
feature telnet vrf vrf_test
feature telnet vrf management
feature telnet
```

Telent Configuration with IPv6 Address for User Defined VRF

Telnet is performed with IPv6 IP and verified by logging on remote PC.

Topology

Figure 1-11: Telnet Configuration topology

Basic Configuration

`#configure terminal`	Enter configure mode
`(config)#ip vrf vrf_test`	Configure User defined vrf
`(config)#no feature telnet vrf vrf_test`	Disable Telnet feature
`(config)#feature telnet vrf vrf_test`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Configure the Telnet Server Port

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf vrf_test`	Disable Telnet feature
`(config)#telnet server port 6112 vrf vrf_test`	Set Telnet port to 6112
`(config)#feature telnet vrf vrf_test`	Enable Telnet feature
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Telnet Client Session

`#telnet 2001::1`	Log into remote machine using IPv6 address

© 2025 IP Infusion Inc. Proprietary

Validation

```
#show telnet server
VRF MANAGEMENT
telnet server enabled port: 23 VRF DEFAULT:
telnet server enabled port: 23
VRF vrf_test:
telnet server enabled port: 6112
#show running-config telnet server
feature telnet vrf vrf_test
feature telnet vrf management
feature telnet
```

CHAPTER 2 SSH Client Server Configuration

Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client-server model

TCP port 22 is assigned for contacting SSH servers. This document covers the SSH server configuration to enable SSH service and key generation and SSH client configuration for remote login to server.

Note: For In-Band Management over Custom VRF, refer to In-band Management over Custom VRF.

In-band Management over Default VRF

OcNOS supports SSH over the default and management VRFs via the in-band management interface and out-of-band management interfaces, respectively.

SSH can run on the default and management VRFs simultaneously. By default, it runs on the management VRF.

SSH Configuration

SSH is performed with IPv4 and IPv6 addresses.

IPv4 Address Configuration

Topology

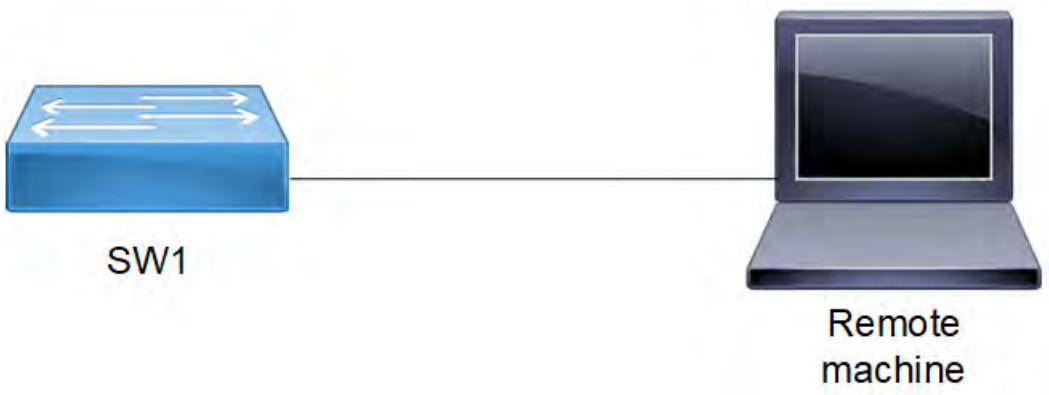


Figure 2-12: SSH sample topology

Basic Configuration

`#configure terminal`	Enter configure mode
`(config)#ssh login-attempts 2 vrf management`	Set the number of login attempts to 2
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Validation

```
#show ssh server
ssh server enabled port: 22
authentication-retries 2

#show running-config ssh server
feature ssh vrf management
ssh login-attempts 2 vrf management
```

SSH Client Session

When the device acts as an SSH client, it supports both SSH IPv4 sessions to log into the remote machine.

`#ssh root@10.10.10.1 vrf management`	Log into remote machine using an IPv4 address

SSH Keys

Use the ssh key command to generate new RSA/DSA keys for the SSH server. By default, the system has RSA/DSA public/private key pair placed in `/etc/ssh/`. If you want to regenerate RSA keys, you must specify the `force` option.

Configuration

`#ssh keygen host rsa vrf management`	Specify the `force` option to regenerate SSH RSA keys. This option overwrites the existing key.

Validation

```
#sh ssh key
****************RSA KEY*******************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj
bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48
************************************
****************DSA KEY*******************
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
```

```
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=
bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
************************************
```

Note: The newly created rsa/dsa key can be verified by logging into the device from a remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

IPv6 Address Configuration

SSH is performed with IPv6 IP and verified by logging in on remote PC.

Topology

Figure 2-13 shows the sample configuration of SSH.

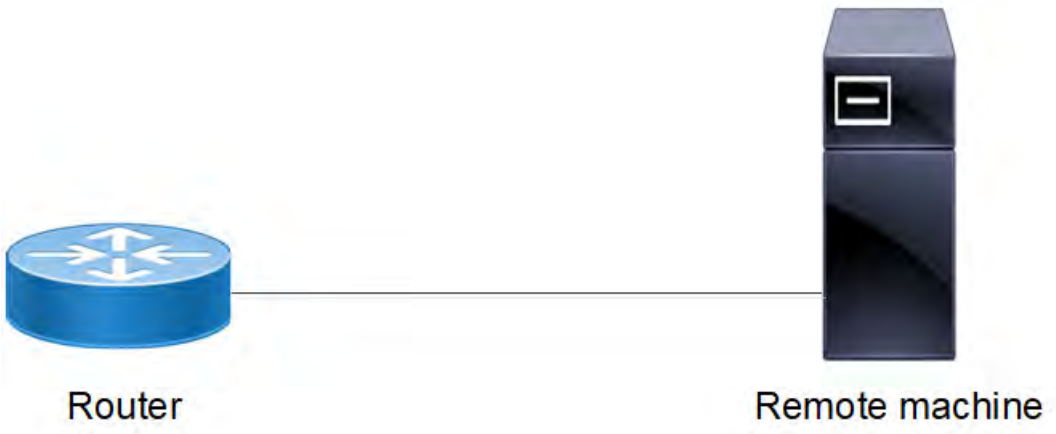


Figure 2-13: SSH Configuration topology

DUT

`#configure terminal`	Enter configure mode
`(config)#ssh login-attempts 2 vrf management`	Set the number of login attempts to 2
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Validation

```
#show ssh server ssh server
ssh server enabled port: 22
authentication-retries 2

#show running-config ssh server
feature ssh vrf management
ssh login-attempts 2 vrf management
```

SSH Client Session

When the device acts as an SSH client, it supports both SSH IPv6 sessions to log into the remote machine.

`#ssh root@2001::1 vrf management`	Log into remote machine using an IPv6 address

SSH Keys

Use the SSH key command to generate new RSA/DSA keys for the SSH server. By default, the system has RSA/DSA public/private key pair placed in `/etc/ssh/`. If you want to regenerate RSA keys, you must specify the force option.

`#ssh keygen host rsa vrf management`	Specify the `force` option to regenerate SSH RSA keys. This option overwrites the existing key.

Validation

```
#sh ssh key ****************RSA KEY********************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/ 1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/ OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj bitcount: 2048 fingerprint:
a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48 ************************************
****************DSA KEY********************
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0 2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA= bitcount: 1024
fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
************************************
```

SSH Encryption

The Secure Shell (SSH) management uses various algorithms in the security mechanisms such as key exchange (KEX), message authentication code (MAC), and encryption (Cipher) for security and flexibility. As part of the security enhancement, additional SSH management algorithms are added into KEX, MAC, and encryption methods.

The security encryption algorithms used in SSH are enhanced to enable the users to use preferable (including weaker algorithms) security mechanisms (for legacy SSH clients) if they want to use them in their network apart from the default cipher algorithms. The default SSH configurations do not use these weaker encryption cipher algorithms due to security priority.

However, OcNOS allows the users to enable or disable the desired algorithms option using the following newly introduced commands.

- ssh server algorithm encryption (Cipher)
- ssh server algorithm kex
- ssh server algorithm mac
- ssh server default algorithm

- show ssh server algorithm

Note:

If the user wishes to modify these defaults, they can reconfigure them with the desired algorithms. For instance, by default, the following algorithms are applied: "`chacha20-poly1305@openssh.com, aes256-gcm@openssh.com, aes128-gcm@openssh.com, aes256-ctr, aes192-ctr, aes128-ctr.`" To remove any of these algorithms, the user must explicitly reconfigure the necessary algorithms, such as using the command: `ssh server algorithm encryption aes256-gcm@openssh.com,aes128-gcm@openssh.com.`

Feature Characteristics

Following are the currently supported encryptions in the SSH session.

- Provides flexibility to user to add or remove the desired SSH encryption algorithms for the following encryption methods.
  - KEX
  - MAC
  - Encryption
- By default, `chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr` ciphers are supported for a new SSH client to connect with the SSH server.
- Allows user to configure multiple algorithms.
- Supports following Strongest Cipher algorithms
  - Strongest Ciphers
    - chacha20-poly1305@openssh.com,
    - aes256-gcm@openssh.com,
    - aes128-gcm@openssh.com,
    - aes256-ctr,aes192-ctr,aes128-ctr
  - MAC algorithms
    - hmac-sha2-512-etm@openssh.com,
    - hmac-sha2-256-etm@openssh.com,
    - hmac-sha2-512,
    - hmac-sha2-256,
  - KEX algorithms
    - curve25519-sha256@libssh.org,
    - diffie-hellman-group18-sha512,
    - diffie-hellman-group16-sha512,
    - ecdh-sha2-nistp521,
    - ecdh-sha2-nistp384,
    - ecdh-sha2-nistp256
    - diffie-hellman-group14-sha256 (uses 2048-bit keys and considered strong)
- Avoid configuring the weaker Cipher algorithms
  - Legacy weaker Cipher

    - aes128-ctr
    - aes192-ctr
    - aes256-ctr
    - aes128-cbc
    - aes192-cbc
    - aes256-cbc (CBC mode is vulnerable to padding Oracle attacks)
    - 3des-cbc
    - blowfish-cbc (Less efficient)
    - arcfour (Based on RC4 which has significant vulnerabilities)
    - hmac-md5 (MD5 can be broken and should not be used)
    - umac-64@openssh.com (Weaker than SHA-2 based MACs)
    - hmac-sha1 (Less secured and weak)
- Extents support to all VRF interfaces including user-defined.
- Allows users with Network Admin or Network Engineer or Network Operator privilege to configure.
- Provides a show CLI command to view the configured SSH algorithms.
- Configured algorithms are persistent even after reload.

Benefits

Enhanced security for remote terminal connections via SSH. It enables users to utilize the legacy SSH clients with the desired algorithms option through the newly introduced commands.

Prerequisites

The SSH process must be enabled.

Configuration

This section provides an example to encrypt an SSH session with cipher algorithm.

Use any one or all of the algorithms to encrypt a default, management or user defined interface SSH session.

- `ssh server algorithm kex KEY_NAME  (vrf|management|Userdefined)`
- `ssh server algorithm mac MAC_NAME  (vrf|management|Userdefined)`
- `ssh server algorithm encryption CIPHER_NAME (vrf|management|Userdefined)`
- `ssh server default algorithm`

Topology

In the below topology, the SSH client from the OcNOS device is initiating an SSH connection to a remote machine.

SSH Sample Topology

Note: Before configuration meet all Prerequisites.

Assign SSH security algorithm to a management Interface

1. Set the SSH server encryption algorithm for the management VRF.
   ```
   (config)#ssh server algorithm encryption aes256-gcm rijndael-cbc aes128-ctr vrf management
   ```
2. Set the SSH server KEX algorithm for the management VRF.
   ```
   (config)#ssh server algorithm kex ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 vrf management
   ```
3. Set the SSH server MAC algorithm for the management vrf.
   ```
   (config)# ssh server algorithm mac hmac-sha2-256-etm hmac-sha1-96 hmac-md5-etm vrf management
   ```
4. Commit the configuration and exit.
   ```
   (config)#commit
   (config)#exit
   ```

Assign SSH security algorithm to a default VRF Interface

1. Set the SSH server encryption algorithm for the default VRF.
   ```
   (config)#ssh server algorithm encryption 3des-cbc aes128-cbc aes192-cbc aes256-cbc
   ```
2. Set the SSH server KEX algorithm for the default VRF**.**
   ```
   (config)#ssh server algorithm kex diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512
   ```
3. Set the SSH server MAC algorithm for the default vrf.
   ```
   (config)# ssh server algorithm mac hmac-md5-etm umac-128
   ```
4. Commit the configuration and exit.
   ```
   (config)#commit
   (config)#exit
   ```

Assign SSH security algorithm to a User Defined Interface

1. Create a user defined VRF interface with the name **vrf1**.
   ```
   (config)#ip vrf vrf1
   (config-vrf)# exit
   ```

2. Set the SSH server encryption algorithm for the user defined **vrf1**.
   ```
   (config)#ssh server algorithm encryption 3des-cbc aes128-cbc aes192-cbc aes256-cbc vrf vrf1
   ```
3. Set the SSH server KEX algorithm for the user defined **vrf1.**
   ```
   ssh server algorithm kex diffie-hellman-group1-sha1 diffie-hellman-group14-sha1
   ```
4. Set the SSH server MAC algorithm for the user defined **vrf1.**
   ```
   (config)#ssh server algorithm mac hmac-md5 hmac-md5-96 vrf vrf1
   ```
5. Commit the configuration and exit.
   ```
   (config)#commit
   (config)#exit
   ```

Validation

Execute the following show command to view the SSH server information.

```
#show running ssh server
feature ssh vrf management
ssh server algorithm mac hmac-sha2-256-etm hmac-sha1-96 hmac-md5-etm vrf management
ssh server algorithm encryption aes256-gcm rijndael-cbc aes128-ctr vrf management
ssh server algorithm kex ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 vrf management

feature ssh
ssh server algorithm mac umac-128 hmac-md5-etm
ssh server algorithm encryption 3des-cbc aes128-cbc aes192-cbc aes256-cbc
ssh server algorithm kex diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512

feature ssh vrf vrf1
ssh server algorithm mac hmac-md5 hmac-md5-96 vrf vrf1
ssh server algorithm encryption 3des-cbc aes128-cbc aes192-cbc aes256-cbc vrf vrf1
ssh server algorithm kex diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256  vrf vrf1
```

Execute the following show command to view the configured SSH algorithms.

```
#show ssh server algorithm
management vrf ssh server algorithm:
    Ciphers aes128-ctr,rijndael-cbc@lysator.liu.se,aes256-gcm@openssh.com,
    KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,
    MACs hmac-sha1-96,hmac-sha2-256-etm@openssh.com,hmac-md5-etm@openssh.com,

default vrf ssh server algorithm:
    Ciphers aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc,
    KexAlgorithms diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,
    MACs umac-128@openssh.com,hmac-md5-etm@openssh.com,

vrf1 vrf ssh server algorithm:
    Ciphers aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc,
```

```
    KexAlgorithms diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-
hellman-group14-sha256,
    MACs hmac-md5,hmac-md5-96
```

SSH Key-Based Authentication

Enable OcNOS device SSH server to perform public key based SSH authentication, to enable machine to machine communication possible without requiring password. Public key based authentication increases the trust between two Linux servers for easy file synchronization or transfer. Public-key authentication with SSH is more secure than password authentication, as it provides much stronger identity checking through keys.

Note: No support for Digital Signature Algorithm (DSA) public key authentication.

Topology

Figure 2-14: SSH Key-based authentication

Public Key Authentication Method

The server has the public key of the user stored; using this the server creates a random value, encrypts it with the public key and sends it to the user. If the user is who is supposed to be, he can decrypt the challenge using the private key and send it back to the server, server uses the public key again to decrypt received message to confirm the identity of the user. SSH is supported in-band (default VRF) and out of band (management VRF). Installed keys are stored in the `~/.ssh/authorized_keys` file.

SSH key based authentication steps:

1. Login to remote machine Linux desktop (ssh client) and generate the key pair using the `ssh-keygen` command.
2. Create the username in OcNOS device (ssh server).
3. Install the public key of remote Linux ssh client in the OcNOS device.
4. Display the installed key in the OcNOS device using the `show running-config` command.
5. Log in from the remote Linux ssh client to the OcNOS device without providing a password.

Useful Commands on Remote Desktop Client

`# ssh-keygen`	To generate key pair on remote Linux machine (ssh client)
`# cd /bob/.ssh/`	To go to the location of saved key pair
`# cat id_rsa.pub`	Command to display the generated public key in remote Linux client

Configuration commands in OcNOS

`(config)#configure terminal`	Enter configure mode.
`(config)#feature ssh vrf management`	Enable the SSH feature on vrf management. To enable in default vrf give the command "feature ssh"
`(config)#username fred`	To create username with default role as network-user. To create user with different role specify role using command "username <username> role <role_name>
`(config)#username fred sshkey ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6y Y6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI /VHVgU2Y0/ ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0 FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1U UxuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyI cwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D 5NnTVh1nroqoozY8i/ qMKfhCFMbysjiDMHU9GclNsNbIF/ DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw1 6Cy3csoTncw0vyXV bob@localhost.localdomain`	Install the public key of remote Linux client in OcNOS device.
`(config)#commit`	Commit the candidate configuration to the running
`(config)#exit`	Exit configure mode.

Validation

The new cipher encryption algorithm takes effect for a new incoming ssh client connection.

```
#show running-config

<skipped other content>
feature ssh vrf management
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
<skipped other content>
```

```
#show running-config ssh server
feature ssh vrf management
```

SSH Key-based Client Session

`#ssh fred@10.10.26.186`	Specify user name and ip address to access the device. Supports IPv4 and IPv6.User should be able to access without password and through key based authentication

Restrictions

- Key generation or installation are not supported for "root" user account in OcNOS device.
- Third party SSH utilities cannot be used for key installation, rather OcNOS CLI is the only way to install public keys.

Sample Use Case

1. Login to remote machine linux desktop (ssh client) and generate the key pair using the `ssh-keygen` command.

```
[bob@localhost ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/bob/.ssh/id_rsa):
/bob/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /bob/.ssh/id_rsa.
Your public key has been saved in /bob/.ssh/id_rsa.pub.
The key fingerprint is:
b2:d0:cc:d2:dd:db:3d:05:c1:33:fc:4a:df:8e:85:af bob@localhost.localdomain
The key's randomart image is:
+--[ RSA 2048]----+
|             o.  |
|              =. |
|              .+ |
|     = . .    ...|
|    o * S .  . +o|
|     o o   o .o.+|
|      .   . . o= |
|              ..o|
|              E. |
+-----------------+
[bob@localhost ~]# cd /bob/.ssh/
[bob@localhost .ssh]# cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
[bob@localhost .ssh]#
```

2. Create username in OcNOS switch device (ssh server)

```
(config)#username fred
```

Note: By default, the user role is `network-user`.

3. Install the public key of remote Linux ssh client in OcNOS device.

```
(config)#username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
```

4. Display the installed key in OcNOS device using the `show running-config` command.

```
#show running-config
<skipped other content>
username fred role network-user
username fred sshkey
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC8XhFiGlZP6yY6qIWUkew884NvqXqMPSOw3fQe5kgpXvX0SbcU15axI/
VHVgU2Y0/
ogAtRUlAk5soRrf5lZ2+rT0zNP37m+Tm5HIEFKZZut0FffGSuXtPKbE+GGlQYHEzC8RSnqQuHlxrlve3lGbB1UU
xuWhMzJfgc2vZ78V2znd2zk4ygiN1jx1sE8UI98WyIcwuq44tzuIaUYAICIfrQJXriQml+QcJ9NER5O8rMS5D5N
nTVh1nroqoozY8i/qMKfhCFMbysjiDMHU9GclNsNbIF/
DQbvWEskFFEvf6fOrzXyvq26NpgaJnZ4pQVzgkOaVw16Cy3csoTncw0vyXV bob@localhost.localdomain
<skipped other content>
```

5. Login from remote Linux ssh client to OcNOS device without providing password

```
[bob@localhost .ssh]# ssh fred@10.10.26.186
```

CHAPTER 3 Max Session and Session Limit Configuration

Overview

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions. Default value for max-session value is 40 in line mode. There is no default value for the telnet-server-limit and ssh-server-limit.

After configuring max-session parameter if user tries to configure SSH/Telnet sessions then the total value of Telnet and SSH session limit should be lesser than the max-session value otherwise error will be thrown.

If already Telnet and SSH session-limits configured, now if user is configuring max-session then there won't be any error but maximum number of sessions will be limited to max-session value.

Topology

The procedures in this section use the topology as mentioned below. Setup consists of one node acting as Telnet server.

Figure 3-15: Telnet topology

Configuration of Telnet Session Limit Lesser than Max-Session

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable Feature Telnet in VRF Managementv
`(config)#telnet server session-limit 12 vrf management`	Configure the Session limit as 12 which is less than Max-Sesssion parameter in line VTY
`(config)#commit`	Perform commit to submit the changes done
`(config)#feature telnet vrf management`	Enable telnet feature in VRF management
`(config)#commit`	Perform commit to submit the changes done
`(config)#exit`	Exit configure mode

Validation

Check that the maximum telnet session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet
```

Configuration of SSH Server Session Limit Lesser than Max-Session

Configure SSH Server Session limit to be lesser than Max-Session.

Topology

Setup consists of one node acting as SSH server.

Figure 3-16: SSH Server topology

Configuration of SSH Server Session Limit Lesser than Max-Session

`#configure terminal`	Enter configure mode
`(config)#no feature ssh vrf management`	Disable feature SSH
`(config)#ssh server session-limit 12 vrf management`	Configure SSH server session-limit to be lesser than Max-Session limit
`(config)#commit`	Perform Commit to submit changes done
`(config)#feature ssh vrf management`	Enable feature SSH
`(config)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the maximum SSH session possible are 12 which is lesser than Max-Session limit parameter value in line VTY.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
```

```
no feature ssh
```

Configuration of Telnet Session Limit Greater than Max-Session

In the below section, configure Telnet Session limit to be greater than Max-Session limit.

Topology

Setup consists of one node acting as Telnet server.

Figure 3-17: Telnet Session Topology

Configuration of Telnet server Session-Limit to be greater than line-VTY max-session

`#configure terminal`	Enter configure mode
`(config)#no feature telnet vrf management`	Disable feature telnet
`(config)#telnet server session-limit 12 vrf management`	Configure Session-limit as 12 for telnet server
`(config)#commit`	Perform commit to submit changes
`(config)#feature telnet vrf management`	Enable Telnet server
`(config)#commit`	Perform commit to submit changes
`(config)#line vty`	Enter line VTY mode
`(config-line)#max-session 10`	Configure max-session as 10
`(config-line)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the total telnet sessions possible is 10 even though telnet server session limit is configured as 12.

```
#show running-config telnet server
telnet server session-limit 12 vrf management
feature telnet vrf management
no feature telnet

#show running-config | grep max-session
 max-session 10
```

Configuration of SSH Session Limit Greater than Max-Session

In the below section, configure SSH Session limit to be greater than Max-Session limit.

Topology

Setup consists of one node acting as SSH server.

Configuration of SSH server Session-Limit to be greater than line-vty max-session

`#configure terminal`	Enter configure mode
`(config)#no feature ssh vrf management`	Disable feature SSH
`(config)#ssh server session-limit 12 vrf management`	Configure Session-limit as 12 for SSH server
`(config)#commit`	Perform commit to submit changes
`(config)#feature ssh vrf management`	Enable SSH server
`(config)#commit`	Perform commit to submit changes
`(config)#line vty`	Enter line VTY mode
`(config-line)#max-session 10`	Configure max-session as 10
`(config-line)#commit`	Perform commit to submit changes
`(config)#exit`	Exit configure mode

Validation

Check that the total SSH sessions possible is 10 even though SSH server session limit is configured as 12.

```
#show running-config ssh server
feature ssh vrf management
ssh server session-limit 12 vrf management
no feature ssh

#show running-config | grep max-session
 max-session 10
```

© 2025 IP Infusion Inc. Proprietary

Remote Device Connect Command Reference

CHAPTER 1 Telnet

This chapter describes telnet commands.

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

- debug telnet server
- feature telnet
- show debug telnet-server
- show running-config telnet server
- show telnet-server
- telnet
- telnet6
- telnet server port
- telnet server session-limit

© 2025 IP Infusion Inc. Proprietary

debug telnet server

Use this command to display telnet debugging information.

Use the `no` form of this command to stop displaying telnet debugging information.

Command Syntax

```
debug telnet server
no debug telnet server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server

telnet server debugging is on
#
```

feature telnet

Use this command to enable the telnet server.

Use the `no` form of this command to disable the telnet server.

Note: Executing `no` form command closes the active telnet session.

Command Syntax

```
feature telnet (vrf management|)
no feature telnet (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

By default, feature telnet is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature telnet vrf management
```

show debug telnet-server

Use this command to display whether telnet debugging is enabled.

Command Syntax

```
show debug telnet-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug telnet-server
telnet server debugging is on
```

show running-config telnet server

Use this command to display telnet settings in the running configuration.

Command Syntax

```
show running-config telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config telnet server

feature telnet vrf management
no feature telnet
```

show telnet-server

Use this command to display the telnet server status.

Command Syntax

```
show telnet server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show telnet server

VRF MANAGEMENT
telnet server enabled port: 23

VRF DEFAULT:
telnet server disabled port: 23
```

telnet

Use this command to open a telnet session to an ipv4 address or host name resolved to ipv4 address.

Command Syntax

```
telnet (A.B.C.D | HOSTNAME) (vrf (NAME|management))
telnet (A.B.C.D | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

A.B.C.D	Destination IPv4 Address to open a telnet session.
HOSTNAME	Destination Hostname to resolve into IPv4 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet 10.12.16.17 2543 vrf management
Trying 10.12.16.17...
```

telnet6

Use this command to open a telnet session to an ipv6 address or host name resolved to ipv6 address.

Command Syntax

```
telnet6 (X:X::X:X| HOSTNAME) (vrf (NAME|management))
telnet6 (X:X::X:X | HOSTNAME) (<1-65535>) (vrf (NAME|management))
```

Parameters

X:X::X:X	Destination IPv6 Address to open a telnet session.
HOSTNAME	Destination Host name to resolve into IPv6 address to open a telnet session.
1-65535	Destination Port to open a telnet session. Default is 23.
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#telnet6 2:2::2:2 2543 vrf management
 Trying 2:2::2:2...
```

telnet server port

Use this command to set the port number on which the telnet server listens for connections. The default port on which the telnet server listens is 23.

You can only give this command when the telnet server is disabled. See the feature telnet command.

Use the `no` form of this command to set the default port number (23).

Command Syntax

```
telnet server (port <1024-65535>) (vrf management|)
no telnet server port (vrf management|)
```

Parameters

`<1024-65535>`	Port number
`management`	Virtual Routing and Forwarding name

Default

By default, telnet server port number is 23

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#telnet server port 1157 vrf management
```

telnet server session-limit

Use this command to limit number of Telnet sessions. Only 40 sessions allowed including Telnet and SSH. User can only give this command when the telnet server is disabled. See the feature telnet command.

Use `no` form of this command to set to default value.

Command Syntax

```
telnet server session-limit <1-40> (vrf management|)
no telnet server session-limit (vrf management|)
```

Parameters

`<1-40>`	Number of sessions
`management`	Virtual Routing and Forwarding name

Default

By default, 40 sessions are allowed.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.2

Examples

```
#configure terminal
(config)#telnet server session-limit 4 vrf management
```

CHAPTER 2 Secure Shell Commands

This chapter describes Secure Shell (SSH) commands.

SSH is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Note: In OcNOS, the default Linux terminal type is "export TERM=xterm"

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear ssh host-key
- clear ssh hosts
- clear ssh keypair
- debug ssh server
- feature ssh
- show debug ssh-server
- show running-config ssh server
- show ssh host-key
- show ssh server
- show username
- ssh
- ssh6
- ssh algorithm encryption
- ssh keygen host
- ssh login-attempts
- ssh server algorithm encryption
- ssh server algorithm kex
- ssh server algorithm mac
- ssh server default algorithm
- show ssh server algorithm
- ssh server port
- ssh server session-limit
- username sshkey
- username keypair

© 2025 IP Infusion Inc. Proprietary

clear ssh host-key

Use this command to clear the host keys.

Command syntax

```
clear ssh host-key  ((dsa|rsa|ecdsa|ed25519)|) (vrf (NAME|management)|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF
`NAME`	Custom VRF

Default

None

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 5.0. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
OcNOS#clear ssh host-key
```

clear ssh hosts

Use this command to clear the `known_hosts` file.

This command clears all trusted relationships established with SSH servers during previous connections. When a client downloads a file from an external server the first time, the client stores the server keys in the `known_hosts` file. After that, other connections to the same server will use the server keys stored in the `known_hosts` file. In other words, a trusted relationship is created when a client accepts the server keys the first time.

An example of when you need to clear a trusted relationship is when SSH server keys are changed.

Command Syntax

```
clear ssh hosts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ssh hosts
```

clear ssh keypair

Use this command to clear RSA/DSA keypair generated for an user. This command can be executed only by networkadmin.

Command Syntax

```
clear ssh keypair user USERNAME
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 4.1.

Examples

```
#clear ssh keypair user test
```

debug ssh server

Use this command to display SSH server debugging information.

Use the `no` form of this command to stop displaying SSH server debugging information.

Command Syntax

```
debug ssh server
no debug ssh server
```

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug ssh server
```

feature ssh

Use this command to enable the SSH server.

Use the `no` form of this command to disable the SSH server.

Command Syntax

```
feature ssh (vrf (NAME|management)|)
no feature ssh (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3

Examples

```
#configure terminal
(config)#feature ssh
```

show debug ssh-server

Use this command to display whether SSH debugging is enabled.

Command Syntax

```
show debug ssh-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debug ssh-server
ssh server debugging is on
```

show running-config ssh server

Use this command to display SSH settings in the running configuration.

Command Syntax

```
show running-config ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config ssh server
feature ssh vrf management
ssh server port 1024 vrf management
ssh login-attempts 2 vrf management
ssh server algorithm encryption 3des-cbc
```

show ssh host-key

Use this command to display the SSH server key.

By default, ssh feature is enabled in "management" vrf. Until and unless the same feature is explicitly enabled in "default" vrf, respective show command output will be empty.

Command syntax

```
show ssh host-key  ((dsa|rsa|ecdsa|ed25519)|) (vrf (NAME|management)|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF
`NAME`	Custom VRF

Default

If no keys are specified, all host keys will be displayed

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#sh ssh host-key
************************************************
dsa public key :

ssh-dss AAAAB3NzaC1kc3MAAACBANgq+TZPkmKOn7ot7PBO9TOCV/
+GPyHCz9Wq39+6veigQ2CWmLNo
uqZb1B05LfeU2MuRz4rtO6mcX81nAygqDLNZaRsirYdWTsJ40HAOZYr9765w+M8TAcKmBYbuWSIkqn
YQ
J1h5bj6UrJ7dW4LgaSxmVmrkXoYrr5gnxfEVgw8HAAAAFQC//
BVHnTWh8Iizbk0mvOyNzqtfMwAAAIBQ
Ca9X0qbL66Js0ul+7LMmLvWkC4Fy1Y/3igZORZ+NsNP4CJIJ1JCLwj7nj/NeUfUuyG1/
dnDVdki4FngL
LjbVa5XrK5VbsEj4sZBfebkLVZKd8h880FqNhfc3iZjCGqdYrWWlRYdNqNvq7zVa6YC7Vvo0sEC5/
rDm
aNygbx0iCAAAAIEAoZHk+5cqaYptqYBPGPMRynpWyWJPJQjoiy+p1BRNk7E/kwInQaqmtFQuM/
YaTOoN
nz5skwQ1dJmdJGq+h7bfmab0atzaaVjkcTjz0rtSBO3JID2G6KqG55yhr03bC8BY+A6g9Qm8TuWZU6
8D
NIZGj28GZSbkIpQgqSD9VUAxEHs=

dsa fingerprint :
```

```
1024 SHA256:Qzd8n4RjsxeW9+AnUP+zc59oPRTl2FBwdwDfVBq0DdQ
**************************************************
**************************************************
rsa public key :

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC706mz0GQvdEaqK/2zUUtCOh/
kEUkZpQ7d8gie4jf1
yV4nV2g1u7oIbdnoBBI0a5bIwbUGDHPUvfTpoJntpryY7G/
QIWuBJVDiu6QteoB4u5byNVbSqA3fljbF
MISYfLxK3i3S07htadDfUIpYTyx/
D5PCf8DDxmdf7UkhOM4Quj8GgGW3PacE2YyJASBq5x7MaWEUiStu
NgtemWqR/DTw+OO8l3gZzHhWBcmHLzo3jdkH/
8ffLGEWqEb78wR4lxckVlja4suFB0GEa7vFLucYO3Tp
GzZARf7iY5A0bB0fi7Zi1yQ3RN7+di28lSNWsFCzZm8vWS7GyLUFn1xttlqJ

rsa fingerprint :

2048 SHA256:YVX+zlrDk8bqzF+HPKpFW0BttbLoiQ5IBDVI/VMYhbs
**************************************************
**************************************************
ecdsa public key :

ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBCN/
XoG
uZGwNfKCE+cuQOULrSHomRSmkDp0u6MsoNIVLhtRe9+r8Ak7G8taE55D7NgugnEDzdLKBmeCZWcww6
4=

ecdsa fingerprint :

256 SHA256:T7KOgXyrU/38EvO6z/apgYDANf+q9YhqCiYoocD5Ajg
**************************************************
**************************************************
ed25519 public key :

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII/jNFIYKbUk/ePbp4wu/
AjhP5gERqn6F+4tH39idbh7

ed25519 fingerprint :

256 SHA256:1MU6iy03eEQBj099GERLjkMCPDoUwkdCwGh8bgYZbeo
**************************************************
#
```

show ssh server

Use this command to display the SSH server status.

Command Syntax

```
show ssh server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show ssh server
VRF MANAGEMENT:
ssh server enabled port: 22
authentication-retries 3
VRF DEFAULT:
ssh server enabled port: 22
authentication-retries 3
#
```

show username

Use this command to display the RSA or DSA key pair for a user.

Command Syntax

```
show username USERNAME keypair
```

Parameters

USERNAME	User identifier

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show username OcNOS keypair
***************RSA KEY*******************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCnWo/3Y7LlVkw/Z43dbVIm+I3o25JlgUTmwa9ll
T35+2gNvDbIPfYAqUKYgrmXKDc9vg7f4SAsmXS+4ZwrrQSTTsHk8PNLA+4lEcufFNl3jpfXTuhphN9
N9
i+uFHGYIIviWZksiRqpMZmDlALyzAIOzyCfG44hlRm3/
pYfhBNhHruvxYVhbP4wHsmrWfcFb+HZCWQGM
CJupxu8bouGd2UW5/BlVy1yuYNIhdo2NHjUI+ameETV+Wroki8+OLVA6eXp5/
KY3Bj9x2+AxOCiKcpU0
axwFSoCbP3+29wrp4JJhl4ssSqM+19+VbUtpuXAM0cR7VQ7mJ0JDZ9tBvK4l8/
bitcount: 2048 fingerprint: 2b:ac:17:a4:ef:1d:79:4e:2d:17:af:72:4c:c7:e4:2f
*************************************
***************DSA KEY*******************
ssh-dss AAAAB3NzaC1kc3MAAACBAP0npAm+Pw8t7OpO+KQ0Vx3ayXavHHVPPAKOo8RTmquE8zUSjn
/XiZ+vP2343RpXu9/
jLwAcCUMfNBZyE8NbmGKxMMk2PqMz10VtfvDOn5LSNurXL4lypZLG2hR2PNva4w
6b4Adpd+E1fEoUncIgOun2i4SO8N5TCMYVyusKjYzDAAAAFQCWeAzeahZeoIzBlnSo87madxfL3QAA
AI
EA4b86l/
nHoWobRoYBrkeOGtjyWLRKk1P2T+rGH+j0rqqJiD0sh2PVfppylliNvqLtYSmXyMCxzEEeFd
HH1cVXgrgQjtUOeCPhF+2We2ummmlCwg4v71Z358FRjsi9VgJ/vQUpOq1hRDhwjJHtEHSA+NkX/
ccW9J
ww8YOoNhCI7DcAAACANuYiP6tKGSU9LeClF1F65Tq1blVHfLp3TSeZYPldqonDoZ1qo3NNvOOH5KN8
Lj
MRtTCN1GaXow1QccS941XFy3efuWXxC00HZ64FhmjCyOYYv2Wsvn4UGCAG3ikiu6M1xjOLl6b53H4m
B3
w7O6bkcjH1GnytwrgR0D/nlsZ/9fs=
bitcount: 1024 fingerprint: c1:0a:e5:e1:a1:78:ae:c2:4a:07:4a:50:07:4b:d5:84
*************************************
```

ssh

Use this command to open an ssh session to a ipv4 address or host name resolved to an ipv4 address.

Command Syntax

```
ssh WORD (vrf (NAME | management))
ssh WORD <1-65535> (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc| aes256-cbc | 3des-cbc)) WORD  (vrf (NAME | management))
ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc | aes256-cbc | 3des-cbc)) WORD <1-65535> (vrf (NAME | management))
```

Parameters

WORD	User and Destination Host name to resolve into IPV4 Address or IPv4 Address to open a ssh session as user@ipv4-address/Hostname
1-65535	Destination Port to open a ssh session. Default is 22
cipher	Specify algorithm to encrypt ssh session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

By default, ssh WORD option is 22

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh cipher aes128-ctr 10.12.16.17 22 vrf management
The authenticity of host '10.12.16.17 (10.12.16.17)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
Are you sure you want to continue connecting (yes/no)?
```

ssh6

Use this command to open an ssh session to an ipv6 address or host name resolved to an ipv6 address.

Command Syntax

```
ssh6 (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
  aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) (vrf (NAME | management))
ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc |
  aes256-cbc | 3des-cbc))  (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME |
  management))
```

Parameters

`X:XX::X:X`	User and Destination IPv6 Address to open a ssh session as user@ipv6-address
`HOSTNAME`	User and Destination Host name to resolve into IPv6 Address to open an ssh session as user@ipv4-address/Hostname
`1-65535`	Destination Port to open a ssh session. Default is 22
`cipher`	Specify algorithm to encrypt ssh session
`aes128-ctr`	Advanced Encryption Standard 128 bit Counter Mode
`aes192-ctr`	Advanced Encryption Standard 192 bit Counter Mode
`aes256-ctr`	Advanced Encryption Standard 256 bit Counter Mode
`aes128-cbc`	Advanced Encryption 128 bit Standard Cipher Block Chaining
`aes192-cbc`	Advanced Encryption Standard 192 bit Cipher Block Chaining
`aes256-cbc`	Advanced Encryption Standard 256 bit Cipher Block Chaining
`3des-cbc`	Triple Data Encryption Standard Cipher Block Chaining
`vrf`	Specify the VPN routing/forwarding instance.
`NAME`	Specify the name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance name.

Default

No default value is specified.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#ssh6 cipher aes128-ctr 2:2::2:2 22 vrf management
The authenticity of host '2:2::2:2 (2:2::2:2)' can't be established.
RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
```

```
Are you sure you want to continue connecting (yes/no)?
```

ssh algorithm encryption

SSH server authorizes connection of only those algorithms that are configured from the list below. If a client tries establishing a connection to the server with the algorithm encryption that are not part of the list, the connection will not established.

SSH server supports the encryption algorithms Advanced Encryption Standard Counter Mode [AES-CTR], Advanced Encryption Standard Cipher Block Chaining [AES-CBC], and Triple Data Encryption Standard [3DES].

and they are as follows:

1. aes128-ctr
2. aes192-ctr
3. aes256-ctr
4. aes128-cbc
5. 3des-cbc
6. aes192-cbc
7. aes256-cbc

Use this command to set an algorithm encryption to establish ssh session.

Use the `no` form of this command to remove an algorithm encryption.

Command Syntax:

```
ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc
  |aes192-cbc | aes256-cbc | 3des-cbc} (vrf (NAME|management)|)
no ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-
  cbc |aes192-cbc | aes256-cbc | 3des-cbc} (vrf (NAME|management)|)
```

Parameters

`aes18-ctr`	AES 128 bit Counter Mode
`aes192-ctr`	AES 192 bit Counter Mode
`aes256-ctr`	AES 256 bit Counter Mode
`aes128-cbc`	AES 128 bit Cipher block chaining
`aes192-cbc`	AES 192 bit Cipher block chaining
`aes256-cbc`	AES 256 bit Cipher block chaining
`3des-cbc`	Triple DES Cipher block chaining
`vrf`	Virtual Routing and Forwarding
`Management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

No default value is specified.

By default, all the ciphers are supported for a new ssh client to connect to the ssh server.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ssh server algorithm encryption aes128-ctr
```

ssh keygen host

Use these commands to create SSH server host, and public keys. These host keys are added in the SSH clients known_hosts file after user's acceptance.

Once entry is added in known_hosts, for the subsequent attempt login to the server will be validated against the host key and if there is key mismatch user will be prompted about the change in server identity.

Command syntax

```
ssh keygen host dsa (vrf (NAME|management)|) (force|)
ssh keygen host rsa (length <1024-4096>|) (vrf (NAME|management)|) (force|)
ssh keygen host ecdsa (length (256|384|521)|) (vrf (NAME|management)|) (force|)
ssh keygen host ed25519 (vrf (NAME|management)|) (force|)
```

Parameters

`dsa`	dsa keys
`rsa`	rsa keys
`ecdsa`	ecdsa keys
`ed25519`	ed25519 keys
`management`	Management VRF
`NAME`	Custom VRF
`force`	Replace the old host-key with newly generated host-key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)

Default

DSA key has length of 1024 bits

RSA key has default length of 2048 bits

ECDSA key has default length of 521 bits

ED25519 key has length of 256 bits

Command Mode

Privilege exec mode

Applicability

This command was introduced in OcNOS version 5.0. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
OcNOS#ssh keygen host rsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa vrf management
OcNOS#
OcNOS#ssh keygen host ecdsa
%% ssh host key exists, use force option to overwrite
OcNOS#
```

```
    OcNOS#ssh keygen host ecdsa force
OcNOS#
```

ssh login-attempts

Use this command to set the number of times SSH client would try to authenticate to establish the SSH session.

Use the `no` form of this command to set the number of authentication attempts to its default (3).

Note: By default, SSH clients may send the keys to authenticate, such a implicit authentication failures would also decrease authentication attempt count. Hence the configured value is not directly proportional to the user's password based authentication attempt.

Command Syntax

```
ssh login-attempts <1-3> (vrf (NAME|management)|)
no ssh login-attempts (vrf (NAME|management)|)
```

Parameters

`<1-3>`	Retries attempts, default is 3 attempts
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

By default, the device attempts to negotiate a connection with the connecting host three times.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3

Examples

```
#configure terminal
(config)#ssh login-attempts 3
```

ssh server algorithm encryption

Use this command to configure Cipher algorithms.

Use `no` parameter to remove the Cipher algorithms.

Command Syntax

```
ssh server algorithm encryption CIPHER_NAME  (vrf (NAME|management)|)
no ssh server algorithm encryption
```

Parameters

`CIPHER_NAME`	Specifies the SSH encryption type as Cipher. • 3des-cbc • aes128-cbc • aes192-cbc • aes256-cbc • rijndael-cbc • aes128-ctr • aes192-ctr • aes256-ctr • aes128-gcm • aes256-gcm • chacha20-poly1305
`vrf management`	Management virtual routing/forwarding instance.
`vrf userdefined`	User defined virtual routing/forwarding instance.

Default

Refer to ssh server default algorithm

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the specific encryption algorithm, execute the following command.

```
OcNOS(config)#ssh server algorithm encryption chacha20-poly1305
OcNOS(config)#ssh server algorithm encryption chacha20-poly1305 vrf management
OcNOS(config)#commit
```

To configure the multiple encryption algorithms, execute the following command.

```
OcNOS(config)#ssh server algorithm encryption 3des-cbc rijndael-cbc aes256-cbc
aes128-gcm
OcNOS(config)#ssh server algorithm encryption 3des-cbc rijndael-cbc aes256-cbc
aes128-gcm vrf management
OcNOS(config)#commit
```

To unconfigure the multiple encryption algorithms, execute the following command.

```
OcNOS(config)#no ssh server algorithm encryption 3des-cbc rijndael-cbc aes256-
cbc aes128-gcm
OcNOS(config)#no ssh server algorithm encryption 3des-cbc rijndael-cbc aes256-
cbc aes128-gcm vrf management
OcNOS(config)#commit
```

ssh server algorithm kex

Use this command to configure KEX algorithms.

Use `no` parameter to remove the KEX algorithms.

Command Syntax

```
ssh server algorithm kex KEY_NAME (vrf |management|userdefined)
no ssh server algorithm kex
```

Parameters

`Kex`	Specifies the SSH encryption type as Key exchange.
`curve25519-sha256`	Specifies the name of the KEX algorithm.
`curve25519-sha256-libssh-org`	
`diffie-hellman-group-exchange-sha1`	
`diffie-hellman-group-exchange-sha256`	
`diffie-hellman-group1-sha1`	
`diffie-hellman-group14-sha1`	
`diffie-hellman-group14-sha256`	
`diffie-hellman-group16-sha512`	
`diffie-hellman-group18-sha512`	
`ecdh-sha2-nistp256`	
`ecdh-sha2-nistp384`	
`ecdh-sha2-nistp521`	
`vrf management`	Management virtual routing or forwarding instance.
`vrf userdefined`	User defined virtual routing or forwarding instance.

Default

Refer to ssh server default algorithm CLI section.

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the specific KEX algorithm, execute the following command.

```
OcNOS(config)#ssh server algorithm kex curve25519-sha256
OcNOS(config)#ssh server algorithm kex curve25519-sha256 vrf management
```

To configure the multiple KEX algorithms, execute the following command.

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#ssh server algorithm kex diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256 ecdh-sha2-nistp256
OcNOS(config)#ssh server algorithm kex diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256 ecdh-sha2-nistp256 vrf management
OcNOS(config)#commit
OcNOS(config)#end
```

To unconfigure the multiple KEX algorithms, execute the following command.

```
OcNOS(config)#no ssh server algorithm kex diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
OcNOS(config)#no ssh server algorithm kex diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256 vrf management
```

ssh server algorithm mac

Use this command to configure MAC algorithms.

Use `no` parameter to remove the MAC algorithms.

Command Syntax

```
ssh server algorithm mac MAC_NAME (vrf |management|userdefined)
no ssh server algorithm mac
```

Parameters

`mac`	Specifies the SSH encryption type as MAC.
`hmac-sha1`	Specifies the name of the MAC algorithm.
`hmac-sha1-96`	
`hmac-sha2-256`	
`hmac-sha2-512`	
`hmac-md5`	
`hmac-md5-96`	
`umac-64@openssh.com`	
`umac-128@openssh.com`	
`hmac-sha1-etm@openssh.com`	
`hmac-sha1-96-etm@openssh.com`	
`hmac-sha2-256-etm@openssh.com`	
`hmac-sha2-512-etm@openssh.com`	
`hmac-md5-etm@openssh.com`	
`hmac-md5-96-etm@openssh.com`	
`umac-64-etm@openssh.com`	
`umac-128-etm@openssh.com`	
`vrf management`	Management virtual routing or forwarding instance.
`vrf userdefined`	User defined virtual routing or forwarding instance.

Default

Refer to ssh server default algorithm CLI section.

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure a specific MAC algorithm, execute the following command.

```
OcNOS(config)#ssh server algorithm mac hmac-sha2-256
OcNOS(config)#ssh server algorithm mac hmac-sha2-256 vrf management
```

To configure multiple MAC algorithms, execute the following command.

```
OcNOS(config)#ssh server algorithm mac hmac-sha2-512 umac-128-etm hmac-md5-96-
etm hmac-sha2-256-etm hmac-sha1-etm
OcNOS(config)#ssh server algorithm mac hmac-sha2-512 umac-128-etm hmac-md5-96-
etm hmac-sha2-256-etm hmac-sha1-etm vrf management
```

To modify the MAC algorithm for user defined VRF, execute the following command.

```
OcNOS(config)#ssh server algorithm mac hmac-md5-96-etm hmac-sha2-256 hmac-
sha2-512-etm vrf VRF1
OcNOS(config)#ssh server algorithm encryption 3des-cbc vrf VRF1
OcNOS(config)#ssh server algorithm kex diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha256 vrf VRF1
```

© 2025 IP Infusion Inc. Proprietary

ssh server default algorithm

Use this command to configure the default strong SSH encryption algorithms. This command reset the existing algorithms.

Use `no` parameter to remove the default strong SSH encryption algorithms.

Command Syntax

```
ssh server default algorithm
```

Parameters

`vrf`	Virtual Routing and Forwarding	
	`NAME`	VRF Name
	`management`	Management VRF

Default

None

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the default strong SSH encryption algorithms.

```
OcNOS#configure terminal
OcNOS#ssh server default algorithm
```

show ssh server algorithm

Use this command to display the current SSH algorithm policy configured.

Use `no` parameter to remove the default encryption algorithms.

Command Syntax

```
show ssh server algorithm
```

Parameters

None

Default

None

Command Mode

Execute Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To view the ssh key configured, execute the following command.

```
OcNOS#show ssh server algorithm

vrf management ssh server algorithm:
KexAlgorithms curve25519-sha256

MACs hmac-sha2-256,hmac-sha2-512,umac-128@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com

Default vrf ssh server algorithm:

KexAlgorithms curve25519-sha256

MACs hmac-sha2-256,hmac-sha2-512,umac-128@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com
```

ssh server port

Use this command to set the port number on which the SSH server listens for connections. The default port on which the SSH server listens is 22.

Use the `no` form of this command to set the default port number (22).

Command Syntax

```
ssh server port <1024-65535> (vrf (NAME|management)|)
no ssh server port (vrf (NAME|management)|)
```

Parameters

`<1024-65535>`	Port number
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

By default, SSH server port is 22.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ssh server port 1720
```

ssh server session-limit

Use this command to limit number of SSH sessions. Only 40 sessions allowed including Telnet and SSH.

Use `no` form of this command to set to default value.

Note: Few Terminal application (Ex: Mobaxterm) where user run SSH Client has limits to use this SSH session limit option.

Command Syntax

```
ssh server session-limit <1-40> (vrf (NAME|management)|)
no ssh server session-limit (vrf (NAME|management)|)
```

Parameters

`<1-40>`	Number of sessions
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

By default, 40 sessions are allowed.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.2. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ssh server session-limit 4 vrf management

(config)#ssh server session-limit 6 vrf NAME
```

username sshkey

Use this command to add public key of the ssh clients to perform pasword-less login into the switch.

Command Syntax

```
username USERNAME sshkey LINE
```

Parameters

`USERNAME`	User identifier
`LINE`	Digital System Algorithm (DSA) key or Rivest, Shamir, and Adelman (RSA) key in OpenSSH format; this key is written to the `authorized_keys` file

Default

By default, SSHKEY is 1024.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#username fred
(config)#username fred sshkey
ssh-rsa AAAAB3NzaC1kc3MAAAEBAIirweZzCdyITqbMWB8Wly9ivGxY1JBVnWTVtcWKi6uc
CPZyw3I6J6/+69LEkPUSAyO+SK8zj0NF2f25FFc2YDMh1KKHi5gK7iXF3/ran54j
nP2byyLeo8rnuVqfEDLaBI1qQaWBcDQvsZc14t5SEJfsOQSfR03PDqPYAisrZRvM
5pWfzo486Rh33J3+17OuARQtZFDP4wA5zZoFxhl4U3RK42JzKNUiYBDrH3lSgfkv
XLWLXz9WcxY6zuKvXFwUpOA9PRXwUsKQqWuyywZQLNavENqFyoQ8oZnNKLCYE0h8
QnUe62NGxb3jQXKLflOL04JFNiii9sACG1Y/ut4ANysAAAAVAJbM7Z4chRgiVahN
iwXFJNkBmWGZAAABAAuF1FlI6xy0L/pBaIlFw34uUL/mh4SR2Di2X52eK70VNj+m
y5eQdRC6cxpaVqpS3Q4xTN+W/kaBbIlX40xJP5lcjMvfn/nqiuIeEodmVIJMWxOD
fh3egeGuSW614Vzd1RGrxpYInIOygMULRcxhmbX+rPliuUIvhg36iH0UR7XBln6h
uyKFvEmaL7bGlRvELjqaj0y6iiCfP1yGBc5vavH5X+jOWqdsJHsCgcIzPF5D1Ybp
w0nZmGsqO+P55mjMuj0O2uI7Ns1sxyirbnGhd+ZZ1u03QDy6MBcUspai8U5CIe6X
WqvXY+yJjpuvlW9GTHowCcGd6Z/e9IC6VE/kNEAAAAEAFIe6kLGTALR0F3AfapYY
/M+bvkmkkhOJUZVdLiwMjcvtJb9fQpPxqXElS3ZvUNIEElUPS/V7KgSsj8eg3FKN
iUGICkTwHIK7RTLC8k4IE6U3V3866JtxW+Znv1DB7uwnbZgoIZuVt3r1+h8O0ah8
UKwDUMJT0fwu9cuuS3G8Ss/gKi1HgByrcxXoK51/r4Bc4QmR2VQ8sXOREv/SHJeY
JGbEX3OxjRgXC7GlpbrdPiL8zs0dPiZ0ovAswsBOYlKYhd7JvfCcvWRjgP5h55aw
GNSmNs3STKufbIqYGeDAISYNYY4F2JzR593KIBnWgyhokyYybyEBh8NwTTO4J5rT
ZA==
```

username keypair

Use this command to generate the key for users.

Command Syntax

```
username USERNAME keypair rsa
username USERNAME keypair dsa
username USERNAME keypair rsa length <1024-4096>
username USERNAME keypair rsa length <1024-4096> force
username USERNAME keypair rsa force
username USERNAME keypair dsa force
```

Parameters

`USERNAME`	User identifier
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`dsa`	Digital System Algorithm (DSA) SSH key
`<1024-4096>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)
`force`	Forces the replacement of an SSH key

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 1024 bits and the default length is 4096.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Execute mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#username fred keypair rsa
```

User Management Configuration

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 Using the Management Interface

Overview

OcNOS provides support for different types of Management Interfaces. The management interface can be the standard out of band (OOB) port, or any in-band port.

To provide segregation between management traffic and data traffic, OcNOS provides a Management VRF. The Management VRF is created by default when OcNOS boots. This VRF cannot be deleted. All ports used as Management Interface needs to be in Management VRF. The management VRF is used for all types of Management applications listed below

- Remote access to router (SSH/Telnet)
- File transfer applications (SFTP/SCP)
- Login Authentication via Radius/Tacacs
- Network management protocols (SNMP, Netconf)

Apart from this, DHCP, DNS, NTP, Syslog, sFlow, and license/software upgrade also uses ports mapped to the management VRF for their operations. Also LLDP can run on any ports mapped to the management VRF.

Note: If the management interface flaps, the device becomes unreachable.

Management Port

The Out of Band (OOB) Management Port in OcNOS is identified as “eth0.” This port is automatically mapped to the Management VRF when OcNOS boots, and will remain in same VRF throughout. It cannot be moved out of this VRF.

The IP address of the management port can be configured statically or via DHCP.

Static IP Configuration

A static IP can be configured on the management port during ONIE installation itself, or after installation using the OcNOS CLIs commands. To configure a static IP during ONIE installation, do the following

```
#onie-stop
#ifconfig eth0 <ip address> netmask <subnet mask> up
```

Please check the Install Guide for details.

The IP address configured during ONIE installation will be applied to the management port and the same will be retained when OcNOS boot up, and the port becomes part of Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address 10.12.44.109/24
```

After getting the OcNOS prompt, this IP address can be changed from the CLI.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address 10.12.44.120/24`	Assign an IPv4 address to the interface
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

If a static IP is not configured during ONIE installation the same can be configured via CLI by following the above steps. Using the OcNOS CLI, DHCP can also be enabled on the Management port.

`#configure terminal`	Enter configure mode
`(config)#interface eth0`	Enter interface mode
`(config-if)#ip address dhcp`	Enable DHCP on interface
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

Obtaining IP Address via DHCP

During onie installation, the management port attempts to acquire IP address via DHCP automatically unless stopped explicitly using the `onie-stop` command. So, if management port is getting IP via DHCP, after OcNOS boots, the management port will continue to use DHCP, even when it is part of the Management VRF.

```
#show running-config interface eth0
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
```

After OcNOS boots, the IP address can be changed to any static IP from the command line as shown earlier.

In-Band Ports

Any front-end ports of the device (in-band ports) can be made part of the management VRF. Once they are part of the management VRF they can also support all management applications such as SSH/Telnet and others as listed in Overview.

Once the ports are part of the management VRF, they should not be used for data traffic and routing or switching purposes. In-band ports can be added or removed from Management VRF as and when required.

`#configure terminal`	Enter configure mode
`(config)#interface xe1/1`	Enter interface mode
`(config-if)#ip vrf forwarding management`	Add in-band port to Management VRF
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit the candidate configuration to the running
`(config)#exit`	Exit configure mode

#configure terminal	Enter configure mode
(config)#interface xe1/1	Enter interface mode
(config-if)# no ip vrf forwarding management	Remove in-band port from Management VRF
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running
(config)#exit	Exit configure mode

Using Ping in Management VRF

To check reachability to any node in the management network, you need to explicitly mention the VRF name as “management.”

In the following example, Node-1 has management interface eth0 and Node-2 has management interfaces eth0 and xe3/1. In order to reach the network 20.20.20.40/24 from Node-1 a static route needs to added.

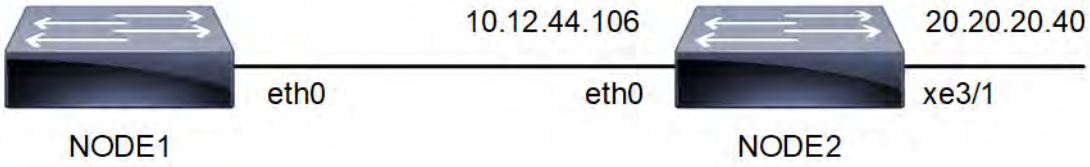


Figure 1-18: Ping in Management VRF topology

#configure terminal	Enter configure mode
(config)# ip route vrf management 20.20.20.0/24 10.12.44.106 eth0	Add static route in management VRF to reach 20.20.20.0/24 network
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

```
Node-1#show ip route vrf management
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
       v - vrf leaked
       * - candidate default

IP Route Table for VRF "management"
C       10.12.44.0/24 is directly connected, eth0
S       20.20.20.0/24 [1/0] via 10.12.44.106, eth0

Gateway of last resort is not set

Node-1#ping 20.20.20.40 vrf management
PING 20.20.20.40 (20.20.20.40) 56(84) bytes of data.
64 bytes from 20.20.20.40: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 20.20.20.40: icmp_seq=2 ttl=64 time=0.476 ms
```

CHAPTER 2 User Configuration

Overview

User management is an authentication feature that provides administrators with the ability to identify and control the users who log into the network.

OcNOS provides 4 different roles for users.

- Network Administrator: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Operator: can make permanent changes to switch configuration. Changes are not persistent across reset/reboot of switch.
- Network User: displays information; cannot modify configuration.

User Configuration

`#configure terminal`	Enter configure mode.
`(config)#username user1 password User12345$`	Create a user “user1” with password User12345$ with default role of network user. Password must be 8-32 characters, username 2-15 characters.
`(config)#username user1 role network-operator password User12345$`	Change the role for user1 to network-operator.
`(config)#username user2 role network-operator password User12345$`	Create a user “user2” with role as network-operator.
`(config)#username user3 role network-admin password User12345$`	Create a user “user3” with role as network-admin.
`(config)#username user4 role network-engineer password User12345$`	Create a user “user4” with role as network-engineer.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode.

Validation

```
#show user-account
User:user1
                roles: network-operator
User:user2
                roles: network-operator
User:user3
                roles: network-admin
User:user4
                roles: network-engineer


#show role
```

```
Role Name                                Info
------------------------------------------------------------------------
network-admin          Network Administrator - Have all permissions
network-engineer       Network Engineer - Can save configuration
network-operator       Network Operator - Can not save configuration
network-user           Network User - Can not change configuration
rbac-customized-role   RBAC User - Can change only  permitted configuration

#show user-account user1
User:user1
                roles: network-operator
```

CHAPTER 3 Configurable Password Policy

Overview

A password is a sequence of characters utilized to confirm a user's identity in the authentication procedure. A strong password helps to protect user accounts and prevents unauthorized access. Strong passwords are the first defense against cyberattacks. Hackers commonly use automated tools to crack passwords. Weak passwords are easily guessed or cracked. Every organization encourages its users to use long passwords combining alphanumeric and special characters. A lengthy password is more complex for hackers, who also need to invest a lot of time to hack the system.

OcNOS manages the user account and its password in its OcNOS configuration, then their password is reflected to LINUX standard user management `db,/etc/passwd and /etc/shadow`.

The password expiration settings in OcNOS and in the standard user management system in LINUX are not always identical. Since the operation of the OcNOS shell is not the same as that of standard shells like bash, similar mechanisms must be implemented in the OcNOS shell to enforce default password changes and set expiration dates.

Feature Characteristics

Setting up strong passwords safeguards sensitive data associated with user accounts, including those of employees and customers, against unauthorized access.

Integrating PAM to OcNOS

Privileged Access Management (PAM) is a third party pluggable security tool that protects organizations from cyberthreats by overseeing, detecting, and thwarting unauthorized privileged access to vital resources.

To satisfy customer requirements, use `pam_pwquality` or `pam_history`, standard PAM modules in LINUX. These are more optimal than implementing a custom password-strength verification system within this system.

When a user sets a password in plain text, it is immediately hashed, and from then on, this hashed password is used for internal management to save settings. The plain text password is not stored anywhere. However, the verification of password strength through PAM is only possible with the plain text password, hence verification can only be conducted while the plain text password is available.

In OcNOS, an actual password change is not performed while the plain text password is held. When a 'commit' operation is executed, it is saved until 'write' operation is executed. However, since PAM cannot verify the strength of a password without setting it, OcNOS temporarily sets the password and while holdd the plain text password to check if the new password meets the password policy and can be changed. If it meets the policy and the password is changed, a process is necessary to revert to the original password.

PAM modules are configured in `/etc/security/pwquality.conf and /etc/pam.d/common_password`. This system internally holds default values based on customer requirements and sets them in these files at system startup. These files are updated if the corresponding configuration values are changed through the CLI and prompts user to update the default password.

To update these default passwords, check if the encrypted password calculated by its username and then prompt the user to update the password. Since the user ‘OcNOS’ shell is ‘`cmlsh`’ and the ‘root’ `shell` is ‘`bash`’, this code is developed independently. For the OcNOS user, it is implemented in `cmlsh_start()` in `cmlsh_main.` For the root user, it is done in `/root/.bash`

Benefits

- Strong passwords protect user accounts and devices from unauthorized access and safeguard sensitive information.
- If the passwords are complex, data is safe from cyber threats and hackers.

Configuration

The OcNOS configuration triggers all user management or password updates including LINUX accounts.

The below configurations allow the user to authenticate the password policy.

Topology

Use the OcNOS interface to configure user accounts, such as creating, disabling passwords and maintain user accounts information.

The image illustrates a method for authenticating and authorizing user account passwords.

Figure 3-19: OcNOS

OcNOS Device

1. Enable the aaa local authentication password-policy

```
OcNOS#configure terminal
OcNOS(config)#aaa local authentication password-policy
OcNOS(config)#commit
```

2. Configure the aaa local authentication password-policy parameter to perform the below actions.

```
OcNOS(config)#aaa local authentication password-policy disable-usercheck
OcNOS(config)#aaa local authentication password-policy history 10
OcNOS(config)#aaa local authentication password-policy lowercase-count 3
OcNOS(config)#aaa local authentication password-policy maxrepeat 2
OcNOS(config)#aaa local authentication password-policy maxsequence 3
OcNOS(config)#aaa local authentication password-policy min-length 10
OcNOS(config)#aaa local authentication password-policy numeric-count 3
OcNOS(config)#aaa local authentication password-policy special-count 3
OcNOS(config)#aaa local authentication password-policy uppercase-count 2
```

Validation 1

Before enabling the local authentication password-policy.

```
# show aaa authentication password-policy

Password policy parameter:

Password policy feature: Disabled
Minimum number of digit: 1
Minimum number of uppercase character: 1
Minimum number of lowercase character: 1
Minimum number of special character: 1
Allowed the number of monotonic character sequences: 5
Username check: Enabled
Allowed the number of same consecutive characters: 1
Minimum length of password: 8
Number of remembered passwords: 5
```

After enabling the `local authentication password-policy`.

```
#show running-config

aaa local authentication password-policy

#show aaa authentication password-policy

Password policy parameter:
Password policy feature: Enabled
Minimum number of digit: 1
Minimum number of uppercase character: 1
Minimum number of lowercase character: 1
Minimum number of special character: 1
Allowed the number of monotonic character sequences: 5
Username check: Enabled
Allowed the number of same consecutive characters: 1
Minimum length of password: 8
Number of remembered passwords: 5
```

Validation 2

```
#show aaa authentication password-policy

Password policy parameter:
Password policy feature: Enabled
Minimum number of digit: 3
Minimum number of uppercase character: 2
Minimum number of lowercase character: 3
Minimum number of special character: 3
Allowed the number of monotonic character sequences: 3
Username check: Disabled
Allowed the number of same consecutive characters: 2
Minimum length of password: 10
Number of remembered passwords: 10
```

Implementation Examples

Set own password policy parameter and enter the password not as per the password-policy.

```
OcNOS(config)#username OcNOS role network-admin password Testing@123
```

BAD PASSWORD: The password contains less than 2 uppercase letters.

%% The password is too weak.

Password-policy logs.

```
OcNOS(config)#username OcNOS role network-admin password T3$$Ting@123
OcNOS(config)#commit
OcNOS(config)#
```

Based on the above configuration set the password in the below format:

- Uppercase characters: 2
- Lowercase characters:3
- Special characters:3
- Numerical characters: 3
- Total Password length: 12

New CLI Commands

The configurable password policy introduces the following configuration commands.

aaa authentication password-policy

Use this command to verify the output for password-policy.

Command Syntax

```
show aaa authentication password-policy
```

Parameters

None

Default

None

Command Mode

Privilege mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
OcNOS# show aaa authentication password-policy

Password policy parameter:
```

```
Password policy feature: Enabled
Minimum number of digit: 1
Minimum number of uppercase character: 1
Minimum number of lowercase character: 1
Minimum number of special character: 1
Allowed the number of monotonic character sequences: 5
Username check: Enabled
Allowed the number of same consecutive characters: 1
Minimum length of password: 8
Number of remembered passwords: 5
```

aaa local authentication password-policy

Use this command to enable/disable the password-policy.

Use `no` parameter of this command to disable.

Command Syntax

```
aaa local authentication password-policy
```

```
no aaa local authentication password-policy
```

Parameters

None

Default

The `aaa local authentication password-policy` is disabled under authentication password policy.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
OcNOS#configure terminal
Ocnos(config)#aaa local authentication password-policy
Ocnos(config)#commit
```

aaa local authentication password-policy numeric-count

Use this command to set the minimum number of digits.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy numeric-count <1-32>
```

```
no aaa local authentication password-policy numeric-count <1-32>
```

Parameters

`<1-32>`	Specifies the numeric count range.

Default

The `aaa local authentication password-policy numeric-count` value is 1.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
config)#aaa local authentication password-policy numeric-count 2
config)#commit
#show aaa authentication password-policy
config)# no aaa local authentication password-policy numeric-count
config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy uppercase-count

Use this command to set the minimum number of uppercase characters.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy uppercase-count <1-32>
```

Parameters

`<1-32>`	Specifies the uppercase characters count range.

Default

The `aaa local authentication password-policy uppercase-count` value is 1.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
config)#aaa local authentication password-policy uppercase-count 2
config)#commit
#show aaa authentication password-policy
config)# no aaa local authentication password-policy uppercase-count
config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy lowercase-count

Use this command to set the minimum number of lowercase character.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy lowercase-count <1-32>
```

Parameters

`<1-32>`	Specifies the minimum number of uppercase characters range.

Default

The `aaa local authentication password-policy uppercase-count` value is 1.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy lowercase-count 2
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy lowercase-count
(config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy special-count

Use this command to set the minimum number of special character.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy special-count <1-32>
```

Parameters

`<1-32>`	Specifies the minimum number of special characters range.

Default

The `aaa local authentication password-policy special-count` value is 1.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy special-count 2
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy special-count
(config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy maxsequence

Use this command to set the number of monotonic character sequence.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy maxsequence <1-32>
```

Parameters

`<1-32>`	Specifies the monotonic character sequences characters range.

Default

The `aaa local authentication password-policy maxsequence` value is 5.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy maxsequence 7
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy maxsequence
(config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy maxrepeat

Use this command to set the same consecutive character.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy maxrepeat <1-32>
```

Parameters

<1-32>	Specifies the same consecutive character range.

Default

The `aaa local authentication password-policy maxrepeat` value is 1.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy maxrepeat 2
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy maxrepeat
(config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy min-length

Use this command to set the minimum length of password.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy min-length <8-32>
```

Parameters

<8-32>	Specifies the minimum password length range.

Default

The `aaa local authentication password-policy min-length` value is 8.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
```

```
(config)#aaa local authentication password-policy min-length 10
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy min-length
(config)# commit
Ocnos#show aaa authentication password-policy
```

aaa local authentication password-policy history

Use this command to set the remembered password.

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy history <1-400>
```

Parameters

`<1-400>`	Specifies the password history range

Default

The `aaa local authentication password-policy history` value is 5.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy history 10
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy history
(config)# commit
#show aaa authentication password-policy
```

aaa local authentication password-policy disable-usercheck

Use this command to set the enable/disable the username check .

Use `no` parameter of this command to get the default value.

Command Syntax

```
aaa local authentication password-policy disable-usercheck
```

Parameters

`<1-400>`	Specifies the password disable range

Default

The `aaa local authentication password-policy usercheck` is enabled under authentication password-policy.

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#aaa local authentication password-policy disable-usercheck
(config)#commit
#show aaa authentication password-policy
(config)# no aaa local authentication password-policy disable-usercheck
(config)# commit
#show aaa authentication password-policy
```

Max Password Age

The maximum age for a user password for OcNOS is 60 days.The password policy setting describes how long users can use their password before it expires. This helps the users periodically change their passwords. When a user's password is updated, the expiry is set according to the user's role. This can be modified or updated per user. Once the expiry is set at the user level, the system will check for user-level expiry.

When a user logs in and `cmlsh` is invoked for the admin user, the admin user is prompted to change the password. A non- admin receives a message to contact the admin to update the password. If the user password has e xpired and it is not updated within the next 30 days, the user account removed from the database.

All these features are enabled and disabled entirely with a CLI. When disabled, `/etc/pam.d/common-password` should be updated not to use both `pam_pwquality` and `pam_pwhistory` modules.

Configuration

The below configurations allow the user to authenticate the maximum password age.

OcNOS Device

1. Enable the aaa local authentication password-policy

   ```
   OcNOS#configure terminal
   OcNOS(config)#aaa local authentication password-policy
   OcNOS(config)#commit
   ```

2. Configure the aaa local authentication password expire for user and role

   ```
   OcNOS(config)#aaa local authentication expire 40 role network-admin
   OcNOS(config)#aaa local authentication expire 45 role network-engineer
   OcNOS(config)#aaa local authentication expire 35 role network-operator
   OcNOS(config)#aaa local authentication expire 50 role network-user
   OcNOS(config)#aaa local authentication expire 50 user Test1
   OcNOS(config)#commit
   ```

Note: The password will not expire, if we select the number of days as 0.

Validation 1

Before enabling the `local authentication password-policy`.

```
# show aaa authentication password-policy

Password policy parameter:
  Minimum number of digit: 1
  Minimum number of uppercase character: 1
  Minimum number of lowercase character: 1
  Minimum number of special character: 1
  Allowed the number of monotonic character sequences: 5
  Username check: Enabled
  Allowed the number of same consecutive characters: 1
  Minimum length of password: 8
  Number of remembered passwords: 5

  network-admin expiration days: Disabled
  network-engineer expiration days: Disabled
  network-operator expiration days: Disabled
  network-user expiration days: Disabled
```

After enable the `local authentication password-policy`.

By default, password expire is enable as well

```
# show aaa authentication password-policy
Password policy parameter:
  Password policy feature: Enabled
  Minimum number of digit: 1
  Minimum number of uppercase character: 1
  Minimum number of lowercase character: 1
  Minimum number of special character: 1
Allowed the number of monotonic character sequences: 5
  Username check: Enabled
  Allowed the number of same consecutive characters: 1
  Minimum length of password: 8
  Number of remembered passwords: 5

  network-admin expiration days: 30
  network-engineer expiration days: 60
  network-operator expiration days: 60
  network-user expiration days: 60
```

After configuring the password expire for role and user.

```
#show aaa authentication password-policy
Password policy parameter:
  Password policy feature: Enabled
  Minimum number of digit: 1
  Minimum number of uppercase character: 1
  Minimum number of lowercase character: 1
  Minimum number of special character: 1
  Allowed the number of monotonic character sequences: 5
  Username check: Enabled
```

```
Allowed the number of same consecutive characters: 1
Minimum length of password: 8
Number of remembered passwords: 5

network-admin expiration days: 40
network-engineer expiration days: 45
network-operator expiration days: 35
network-user expiration days: 50
Test1: will expire in 50 days!!!
```

New CLI Commands

The maximum password policy introduces the following configuration commands.

aaa local authentication password expire role

Use this command to enable or disable the password expire for role.

Use `no` parameter of this command to disable.

Command Syntax

```
aaa local authentication password expire <0-1000> role (network-admin|network-
  engineer|network-operator|network-user)
no aaa local authentication password expire role (network-admin|network-
  engineer|network-operator|network-user)
```

Parameters

`expire <0-1000>`	Specifies the number of days for password expiry for a particular role.
`role network-admin`	Specifies the network administration role for which the configured password expiry days are applicable.
`role network-engineer`	Specifies the network engineer role for which the configured password expiry days are applicable.
`role network-operator`	Specifies the network operator role for which the configured password expiry days are applicable.
`role network-user`	Specifies the network user role for which the configured password expiry days are applicable.

Default

Disabled

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

```
OcNOS#configure terminal
OcNOS(config)#aaa local authentication password expire 50 role network-admin
OcNOS(config)#commit
```

aaa local authentication password expire user

Use this command to enable or disable the password expire for role.

Use no parameter of this command to disable.

Command Syntax

```
aaa local authentication password expire <0-1000> user WORD
no aaa local authentication password expire user WORD
```

Parameters

`expire <0-1000>`	Specifies the number of days for password expiry for a particular user.
`user WORD`	Specifies the user name.

Default

Disabled

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

```
OcNOS#configure terminal
Ocnos(config)#aaa local authentication password expire 50 user user test
Ocnos(config)#commit
```

Removing Users with Expired Passwords

When a user's password is updated, the on set depending on the user's role. This is modified per user. Once the expiry is set, the system will automatically check for expired passwords. When a user logs in and cmlsh is invoked, for the admin user the user will be prompted to change the password. A non- admin user will receive a message to contact the admin to update the password.

If the user is expired and never update password or expiry for next 30 days, that user is removed from the database. All these features are enabled or disabled entirely with a CLI. When disabled, `/etc/pam.d/common-password` needs to be updated but not to use both `pam_pwquality and pam_pwhistory` modules.

Note: When updating a user's level expiry, any days already lapsed are deducted from the new expiry value. If the updated value is greater than the remaining days, it becomes the new remaining days. For example, if a user initially has 20 days and, after 5 days, the expiry is updated to 30 days, the user will have 25 days left (30 - 5). Conversely, if the expiry is updated to 10 days after 5 days have passed, the remaining time is set to 10 days.

Glossary

The following glossary provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
PAM	Privileged Access Management s a third party pluggable security tool that protects organization from cyberthreats by overseeing.

CHAPTER 4 In-band Management over Custom VRF

Overview

OcNOS currently supports system management protocols within the Default and Management Virtual Routing and Forwarding (VRF). However, this configuration is insufficient for customer deployments that require the ability to run these protocols in user-defined VRFs. This document outlines the requirements for expanding OcNOS to support system management protocols in custom VRFs.

Feature Characteristics

- **Support for System Management Protocols in User-Defined VRFs:** Provide the flexibility to run system management protocols over custom VRFs. In large-scale networks, deploying an out-of-band management network is not always practical, making in-band device management over user-defined VRFs necessary to handle the volume of management traffic.
- **Supported Protocols:** SSH, Telnet, TACACS, Syslog, SNMP, NETCONF, and gNMI will operate within user-defined VRFs. Simultaneous support for multiple VRFs for specific protocols, such as Syslog. Support for both default and customizable port values for each protocol.
- **Multi-VRF Protocol Operations:** Management protocols, including SSH and NETCONF, will allow simultaneous operations across multiple VRFs, providing enhanced flexibility in managing network devices.
- **Service Traffic Segmentation:** Management traffic, such as SNMP and Syslog, can be segmented across custom VRFs, allowing for more efficient traffic management and security.

Benefits

- **Scalability and Flexibility:** Enabling system management protocols to operate over custom VRFs allows for ease of managing service provider networks, especially in environments where out-of-band management is impractical.
- **Protocol Customization:** Support for both standard and customizable port values for management protocols provides greater flexibility, allowing customers to tailor the system management configuration to meet their specific network needs.

Configuration

These steps provide a standardized approach to configuring User-Defined VRF on PE routers.

Topology

In this topology, the management traffic from the Linux Server is routed through a specific VRF that is isolated from the traffic on the L3VPN.

PE1 and PE2 are Provider Edge routers in the network. These routers are responsible for managing and routing the traffic between the local network and the wider service provider network.

Both PE routers are connected through L3VPN, which is used to segment and isolate traffic between the two routers over a shared infrastructure. Each customer or service can have its own isolated routing table (VRF).

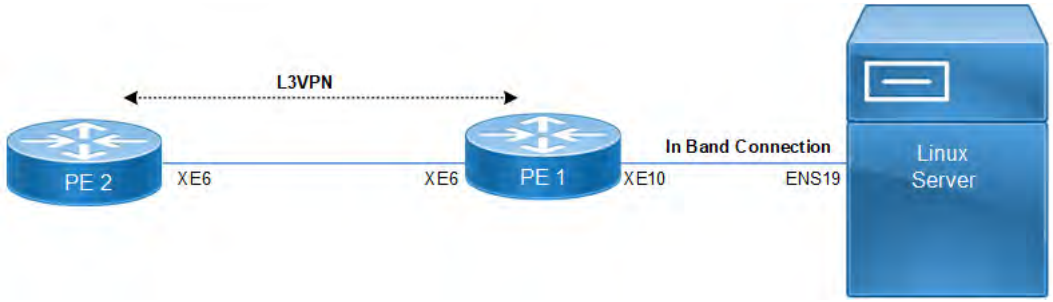
In-Band Connection: The In-Band Connection shown between PE1 and the Linux Server means that both management and normal traffic flow over the same physical network links.

The in-band management traffic is directed over the custom VRF, ensuring it is separated from the service traffic, providing network isolation.

Custom VRF Feature: In this case, the custom VRF is applied to manage the traffic between the Linux Server and the network. This VRF allows traffic related to management tasks to remain separate from other traffic handled by the provider.

VRF helps ensure that different traffic types (such as syslog, or SSH sessions) remain isolated for security and performance reasons.

Multi-VRF Management: Using user-defined VRFs, run management services like Syslog, or SSH on separate VRFs, ensuring that management tasks are not mixed with customer or service traffic.



Custom VRF

Perform the following configuration steps for setting up a custom VRF with routing protocols like BGP, OSPF, and management protocols such as SSH. These can be applied to multiple Provider Edge (PE) routers, or other routers, with adjustments in interface names and IP addresses depending on the specific deployment.

The steps include defining VRFs, configuring interfaces, setting up routing protocols like OSPF and BGP, enabling management features (SSH), and ensuring MPLS support:

1. Enter configuration mode and define the VRF.

```
#configure terminal
(config)# ip vrf vrf1
(config)# rd 100:1
(config)# route-target both 10:10
(config)#exit
```

2. Assign the VRF to the relevant access and loopback interfaces, and configure both IPv4 or IPv6 addresses:

   Access Interface Configuration:

```
#configure terminal
(config)# interface xe10
(config)# ip vrf forwarding vrf1
(config)# ip address 20.20.20.3/24
(config)# ipv6 address 2500::3/64
(config)#exit
```

   Loopback Interface Configuration:

```
#configure terminal
(config)# interface lo.vrf1
(config)# ip vrf forwarding vrf1
(config)# ip address 172.16.1.10/24 secondary
(config)# ipv6 address 2000::10/64
(config)#exit
```

3. On interfaces facing the provider network, configure MPLS and enable LDP:

```
(config)# interface xe6
(config)# ip address 192.168.69.1/24
(config)# ipv6 address 1000::11/64
(config)# label-switching
(config)# enable-ldp ipv4
(config)#exit
```

4. Set up OSPF routing within the network, and ensure to advertise the necessary interfaces:

```
(config)# router ospf 100
(config)# network 1.1.1.1/32 area 0.0.0.0
(config)# network 192.168.69.0/24 area 0.0.0.0
(config)#commit
(config)#exit
#configure terminal
(config)# router ldp
(config)#exit
```

5. Configure BGP for both VPNv4 and VPNv6 address families:

```
#configure terminal
(config)# router bgp 1000
(config)# neighbor 2.2.2.2 remote-as 1000
(config)# neighbor 2.2.2.2 update-source 1.1.1.1
(config)# address-family vpnv4 unicast
(config)# neighbor 2.2.2.2 activate
(config)# exit-address-family
(config)# address-family ipv4 vrf vrf1
(config)# redistribute connected
(config)# exit-address-family
(config)# address-family vpnv6 unicast
(config)# neighbor 2.2.2.2 activate
(config)# exit-address-family
(config)# address-family ipv6 vrf vrf1
(config)# redistribute connected
(config)# exit-address-family
(config)#exit
```

6. Enable SSH (or respective protocols) for VRF Management:

```
#configure terminal
(config)# feature ssh vrf management
(config)# feature ssh vrf
(config)# feature ssh vrf vrf1
(config)#exit

(config)# ssh server port 10000 vrf management
(config)# ssh server port 10000
(config)# ssh server port 10000 vrf vrf1
(config)#exit

(config)# ssh login-attempts 2 vrf management
(config)# ssh login-attempts 2
(config)# ssh login-attempts 2 vrf vrf vrf1
(config)#exit

(config)# ssh server session-limit 10 vrf management
(config)# ssh server session-limit 10
(config)# ssh server session-limit 20 vrf vrf1
(config)#exit
```

```
(config)# ssh server algorithm encryption 3des-cbc  vrf management
(config)# ssh server algorithm encryption 3des-cbc
(config)# ssh server algorithm encryption 3des-cbc  vrf vrf1
(config)#exit
```

Configuration Snapshot:

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
logging console
logging monitor
logging cli
logging level all 7
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
hardware-profile statistics voq-full-color enable
hardware-profile statistics cfm-ccm enable
!
qos enable
!
no ip domain-lookup
ip domain-lookup vrf management
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature ssh vrf vrf1
ssh server port 10000 vrf vrf1
ssh login-attempts 2 vrf vrf1
ssh server algorithm encryption 3des-cbc  vrf vrf1
ssh server session-limit 20 vrf vrf1
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
!
ip vrf management
!
```

```
ip vrf vrf1
 rd 100:1
 route-target both 10:10
!
router ldp
!
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.1/32 secondary
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface lo.vrf1
 ip vrf forwarding vrf1
 ip address 172.16.1.10/24 secondary
 ipv6 address 2000::10/64
!
interface xe6
 speed 10g
 ip address 192.168.69.1/24
 ipv6 address 1000::11/64
 label-switching
 enable-ldp ipv4
!
 ip vrf forwarding vrf1
 ip address 20.20.20.3/24
 ipv6 address 2500::3/64
!
!
router ospf 100
 network 1.1.1.1/32 area 0.0.0.0
 network 192.168.69.0/24 area 0.0.0.0
!
router bgp 1000
 neighbor 2.2.2.2 remote-as 1000
 neighbor 2.2.2.2 update-source 1.1.1.1
 !
 address-family vpnv4 unicast
 neighbor 2.2.2.2 activate
 exit-address-family
 !
 address-family vpnv6 unicast
 neighbor 2.2.2.2 activate
```

```
 exit-address-family
 !
 address-family ipv4 vrf vrf1
 redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf vrf1
 redistribute connected
 exit-address-family
 !
 exit
!
line console 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
!
```

Validation

Validate the VRF and SSH configurations to ensure they support the custom VRF functions as expected.

- **Verify the VRF Configuration:**

```
OcNOS#show running-config vrf vrf1
!
ip vrf vrf1
 rd 100:1
 route-target both 10:10
!
OcNOS#show running-config interface xe10
!
interface xe10
 ip vrf forwarding vrf1
 ip address 20.20.20.3/24
 ipv6 address 2500::3/64
!
OcNOS#show running-config interface lo.vrf1
!
interface lo.vrf1
 ip vrf forwarding vrf1
 ip address 172.16.1.10/24 secondary
 ipv6 address 2000::10/64
!
OcNOS#show running-config interface xe6
interface xe6
 speed 10g
 ip address 192.168.69.1/24
 ipv6 address 1000::11/64
 label-switching
 enable-ldp ipv4
!
```

- **Verify SSH configuration:**

```
OcNOS#show running-config ssh server
feature ssh vrf management
no feature ssh
feature ssh vrf vrf1
ssh server port 10000 vrf vrf1

OcNOS#show ssh server
VRF MANAGEMENT:
ssh server enabled port: 22
authentication-retries: 3
VRF DEFAULT:
ssh server disabled port: 22
authentication-retries: 3
VRF vrf1:
ssh server enabled port: 10000
session-limit: 20
authentication-retries: 2
```

Implementation Examples

- L3VPN or EVPN Tunnel Support: In a service provider network, user-defined VRFs are configured on managed nodes, such as PE and Rout Reflector (RR) nodes. Management nodes connect to a PE node, enabling access to other PE or RR nodes through L3VPN or EVPN tunnels. This architecture supports in-band management of devices over user-defined VRFs.
- Service Traffic Segmentation: Management traffic, such as SNMP and Syslog packets, is segmented across different user-defined VRFs, ensuring separation from other network operations and enhancing security.
- Multi-VRF Support for Protocols: SSH and NETCONF services support connections from multiple VRFs simultaneously, allowing for scalable management across complex networks.

Glossary

The following list provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Virtual Routing and Forwarding (VRF)	A technology that allows multiple instances of a routing table to coexist on the same router. Each VRF operates independently, enabling isolated network paths and address spaces within a single physical infrastructure.
Multiprotocol Label Switching (MPLS)	A method for forwarding packets based on labels rather than network addresses. MPLS is commonly used in conjunction with VRF to route traffic through the network efficiently.
Label Distribution Protocol (LDP)	A protocol used in MPLS networks to establish label-switched paths (LSPs). LDP is responsible for distributing labels between routers to forward packets in an MPLS environment.

Open Shortest Path First (OSPF)	A link-state interior gateway protocol (IGP) used to distribute IP routing information within a single autonomous system. It is commonly used in conjunction with VRFs to handle routing within a VRF instance.
Border Gateway Protocol (BGP)	The protocol used to exchange routing information between different autonomous systems. When combined with VRFs, BGP can handle VPNv4 and VPNv6 routes for isolated routing domains.
Secure Shell (SSH)	A protocol that provides secure access to network devices and systems. In a VRF configuration, SSH can be enabled per VRF, allowing secure management access to routers on a per-VRF basis.

User Management Command Reference

CHAPTER 1 User Management

This chapter is a reference for user management commands.

This chapter includes these commands:

- clear aaa local user lockout username
- debug user-mgmt
- show user-account
- username

clear aaa local user lockout username

Use this command to unlock the locked user due to three times wrong password login attempt.

Command Syntax

```
clear aaa local user lockout username USERNAME
```

Parameters

USERNAME	User name; length 2-15 characters

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear aaa local user lockout username testuser
```

debug user-mgmt

Use this command to display user management debugging information.

Use the `no` form of this command stop displaying user management debugging information.

Command Syntax

```
debug user-mgmt
```

```
no debug user-mgmt
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug user-mgmt
```

```
#config t
(config)#debug user-mgmt
```

show user-account

Use this command to display information about all users or a given user.

Command Syntax

```
show user-account (WORD|)
```

Parameters

WORD	User name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show user-account
User:user1
                roles: network-operator
User:user2
                roles: network-operator
User:user3
                roles: network-operator
```

username

Use this command to add a user or to change a user password.

The `role` parameter maps to privilege levels in the TACACS+ server as shown in Table 1-12

Table 1-12: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or greater then 15

Use the `no` form of this command to remove a user.

Command Syntax

```
username USERNAME
username USERNAME password (encrypted|) PASSWORD
username USERNAME role (network-admin|network-engineer|network-operator|network-user)
username USERNAME role (network-admin|network-engineer|network-operator|network-user) password (encrypted|) PASSWORD
username disable-default
no username disable-default
no username USERNAME
```

Parameters

`USERNAME`	User name; length 2-15 characters
`encrypted`	Encrypted password
`PASSWORD`	Password; length: 8-32 characters. Password must contain at least: - One uppercase letter - One lowercase letter - One digit - One special character (acceptable special characters: `~`!@#$%^&*(){}'[],.\"</\+-_:;) ,` Note: The following characters are not acceptable in passwords: `'=?|>`
`network-admin`	Network administrator role with all access permissions that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch. Only network administrators can manage other users with the enable password, Authentication, Authorization and Accounting, RADIUS Commands, and TACACS+ Commands.

`network-engineer`

Network engineer role with all access permission that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.

`network-operator`

Network operator role with all access permissions that can make temporary changes to the configuration. Changes do not persist after a reset/reboot of the switch.

`network-user` Network user role with access permissions to display the configuration, but cannot change the configuration.

`disable-default`

This option is used to disable the implicit configuration of default user by the system. This command can be executed only by users with "`network-admin`" privileges. When this option is configured, explicit configuration of default user will be rejected. If default-user is explicitly configured using "`username`" CLI, it should be removed using "`no username USERNAME`" before configuring "disable-default".

Default

By default, user name is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#username fred_smith password Fred123$
```

DHCP Configuration

CHAPTER 1 DHCP Client Configuration

Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

DHCP Client Configuration for IPv4

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

Figure 1-20: DHCP sample topology

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#interface eth0`	Enter management interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.

(config if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration.

Validation Commands

```
#show running-config dhcp
    interface xe2
     ip address dhcp
    !
    ip dhcp relay information option

    #sh ip interface brief

    Interface            IP-Address      Admin-Status         Link-Status
    GMPLS Type
    eth0                 10.12.44.20     up                   up
    -
    lo                   127.0.0.1       up                   up
    -
    lo.4                 127.0.0.1       up                   up
    -
    vlan1.1              unassigned      up                   down
    -
    xe1/1                2.2.2.3         up                   up
    -
    xe1/2                unassigned      down                 down
    -
    xe1/3                unassigned      down                 down
    -
    xe1/4                unassigned      up                   down
    -
    xe2                 *40.40.40.40     up                   down
    -
    xe3/1                20.20.30.1      up                   up
    -
```

DHCP Client Configuration for IPv6

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

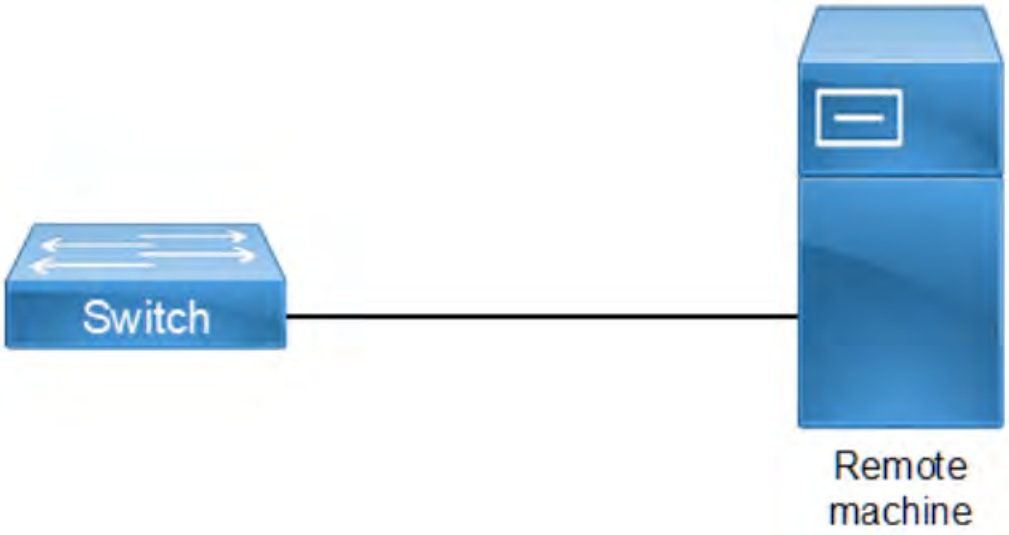


Figure 1-21: DHCP sample topology

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ipv6 dhcp client request dns-nameserver`	The client request for name-server configured in server
`(config-if)#ipv6 dhcp client request domain-search`	The client request for domain names with ip
`(config-if)#ipv6 dhcp client request ntp-server`	The client request for Ntp server details configured in server
`(config-if)#ipv6 dhcp client request rapid-commit`	Enables rapid commit option
`(config-if)#ipv6 dhcp client request vendor-specific-information`	The client request for vendor specific information
`(config-if)#ipv6 dhcp client duid llt`	Set duid type for DHCP Client. Possible values are llt or ll
`(config-if)#ipv6 dhcp client dad-wait-time 300`	Max time that the client process should wait for the duplicate address detection to complete before initiating DHCP requests
`Values range from 1 - 600`	
`(config-if)#ipv6 address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running
`(config)#interface eth0`	Enter management interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.

(config if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running.

Validation Commands

```
OcNOS#show ipv6 interface brief
Interface            IPv6-Address                                    Admin-Sta
tus
ce20                 fe80::eac5:7aff:fe28:a67b                       [up/up]

ce21                 fe80::eac5:7aff:fe28:a67c                       [up/down]

eth0                 fe80::eac5:7aff:fe8e:c365                       [up/up]

                     *3001::1
xe1                  fe80::eac5:7aff:fe28:a66b                       [up/up]


OcNOS#show ipv6 dhcp vendor-opts
Interface name      vendor-opts
===============     ====================
xe1                 0:0:9:bf:0:1:0:c:48:65:6c:6c:6f:20:77:6f:72:6c:64:21


OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe1
 ipv6 dhcp client request dns-nameserver
 ipv6 dhcp client request domain-search
 ipv6 dhcp client request ntp-server
 ipv6 dhcp client request rapid-commit
 ipv6 dhcp client request vendor-specific-information
 ipv6 dhcp client duid llt
 ipv6 dhcp client dad-wait-time 300
 ipv6 address dhcp
!
!
```

CHAPTER 2 DHCP Server Configuration

Overview

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

DHCP Server Configuration for IPv4

Before configuring make sure that DHCP server is ready.

Topology

Figure 2-22: DHCP IPv4 topology

Configuration

DHCP IPv4 Client Interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface (xe1) to be configured and enter the interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config-if)#ip dhcp client request dns-nameserver`	The client requests for the DNS name server.
`(config-if)#ip dhcp client request ntp-server`	The client requests for the NTP server .
`(config-if)#ip dhcp client request host-name`	The client requests for the Name of the client.
`(config-if)#ip dhcp client request log-server`	The client requests for the log server.
`(config if)#exit`	Exit interface mode.

© 2025 IP Infusion Inc. Proprietary

DHCP IPv4 Server Interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe2`	Specify the interface (xe2) to be configured and enter the interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure the IP address to the server interface.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration.

DHCP IPv4 Server Feature

`#configure terminal`	Enter Configure mode.
`(config)#ip vrf vrf1`	Configure IP VRF name.
`(config-vrf)#ip dhcp server max-lease-time 100`	Configure max lease time.
`(config-vrf)#ip dhcp server default-lease-time 100`	Configure default lease time.
`(config-vrf)#ip dhcp server pool test`	Configure DHCP server pool name.
`(dhcp-config)#network 3.3.3.0 netmask 255.255.255.0`	Configure network and netmask.
`(dhcp-config)#address range low-address 3.3.3.1 high-address 3.3.3.4`	Configure address IPv4 range.
`(dhcp-config)#routers 3.3.3.1`	IPv4 DHCP Server option to provide router details to a DHCP client.
`(dhcp-config)#boot-file test`	Configure boot-file name.
`(dhcp-config)#host-name dhcp-server`	Configure host name.
`(dhcp-config)#ntp-server 4.4.4.5`	Configure NTP server.
`(dhcp-config)#log-server 5.5.5.6`	Configure log server.
`(dhcp-config)#dns-server 5.5.5.5`	Configure DNS server.
`(dhcp-config)#tftp-server 5.5.5.6`	Configure TFTP server.
`(dhcp-config)#boot-file test`	Configure boot-file name.

Validation

Client

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe47
 ip address dhcp
ip dhcp client request dns-nameserver
```

```
ip dhcp client request host-name
ip dhcp client request log-server
ip dhcp client request ntp-server
!
!

OcNOS#show ip int br

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
ce54                 unassigned      up                    down
eth0                *10.12.122.114   up                    up
lo                   127.0.0.1       up                    up
lo.management        127.0.0.1       up                    up
xe47                *10.10.10.2      up                    up
xe48                 unassigned      up                    down

OcNOS#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#int xe6
OcNOS(config-if)#ip dhcp client request host-name
OcNOS(config-if)#commit
OcNOS(config-if)#
OcNOS(config-if)#
OcNOS(config-if)#end
dhcp-client#
dhcp-client#
dhcp-client#
dhcp-client#sh hostname
*dhcp-client

* - Hostname learnt by DHCP Client.
dhcp-client#
```

Server

```
OcNOS#show run dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp server max-lease-time 100
ip dhcp server default-lease-time 100
ip dhcp server pool test
 network 10.10.10.0 netmask 255.255.255.0
 address range low-address 10.10.10.1 high-address 10.10.10.5
 host-name dhcp-client
 boot-file test
 tftp-server 5.5.5.6
```

```
 ntp-server 4.4.4.5
 log-server 5.5.5.6
 dns-server 5.5.5.5
interface ge5
 ip dhcp server
```

DHCP Server Configuration for IPv6

Before configuring make sure that DHCP server is ready.

Topology

Figure 2-23: DHCP IPv6 topology

Configuration

DHCP IPv6 Client Interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe47`	Specify the interface (xe47) to be configured and enter the interface mode.
`(config-if)#ipv6 address dhcp`	The client requests for the IPv6 address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config-if)#ipv6 dhcp client request dns-nameserver`	The client requests for the DNS name server.
`(config-if)#ipv6 dhcp client request ntp-server`	The client requests for the NTP server.
`(config-if)#ipv6 dhcp client request domain-search`	The client request for IPv6 domain search.
`(config-if)#ipv6 dhcp client request vendor-specific-information`	The client request for IPv6 vendor-specific-information.
`(config-if)#ipv6 dhcp client request rapid-commit`	The client request to enable rapid-commit.
`(config if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration.

© 2025 IP Infusion Inc. Proprietary

DHCP IPv6 Server Interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe2`	Specify the interface (xe2) to be configured and enter the interface mode.
`(config-if)#ipv6 address dhcp`	The client requests for the IPv6 address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config-if)#ipv6 address 2001::1/64`	Configure the IPv6 address to the server interface.
`(config if)#ipv6 dhcp server`	Configure an interface as a DHCP server starting interface.
`(config if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration.

DHCP IPv6 Server Feature

`#configure terminal`	Enter Configure mode
`(config)#ip vrf vrf1`	Configure IP VRF name
`(config-vrf)#ipv6 dhcp server preference`	Configure IPv6 DHCP server preference
`(config-vrf)#ipv6 dhcp server rapid-commit`	Configure IPv6 DHCP server rapid-commit
`(config-vrf)#ipv6 dhcp server pool test`	Configure IPv6 DHCP server pool name
`(dhcp6-config)#network 2001:: netmask 64`	Configure IPv6 network and netmask
`(dhcp6-config)#address range low-address 2001::1 high-address 2001::124`	Configure IPv6 address range
`(dhcp6-config)#vendor-options 00:00:09:bf:63`	Configure IPv6 vendor option
`(dhcp6-config)#ntp-server 4001::1`	Configure IPv6 NTP server
`(dhcp6-config)#dns-server 3001::1`	Configure IPv6 DNS server
`(dhcp-config)#log-server 5.5.5.6`	Configure log server
`(dhcp6-config)#domain-name abcd`	Configure domain name
`(dhcp-config)#tftp-server 5.5.5.6`	Configure TFTP server
`(dhcp-config)#boot-file test`	Configure boot-file name

Validation

Client

```
OcNOS#sh running-config dhcp
interface eth0
 ip address dhcp
!
interface xe2
 ipv6 dhcp client request dns-nameserver
 ipv6 dhcp client request domain-search
 ipv6 dhcp client request ntp-server
 ipv6 dhcp client request rapid-commit
```

```
 ipv6 dhcp client request vendor-specific-information
 ipv6 address dhcp
!

OcNOS#show ipv6 int br
Interface            IPv6-Address                                    Admin-Sta
tus
ce49                 unassigned                                      [up/down]

eth0                 fe80::e69d:73ff:fe05:8100                       [up/up]

lo                   ::1                                             [up/up]

lo.management        ::1                                             [up/up]

xe45                 unassigned                                      [up/down]

xe46                 unassigned                                      [up/down]

xe47                 *2001::124
                     fe80::e69d:73ff:fe84:8137                       [up/up]

xe48                 unassigned                                      [up/down]
```

Server

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server rapid-commit
ipv6 dhcp server preference
ipv6 dhcp server pool test
 network 2001:: netmask 64
 address range low-address 2001::1 high-address 2001::124
 vendor-options 00:00:09:bf:63
 ntp-server 4001::1
 dns-server 3001::1
 domain-name abcd
interface xe2
 ipv6 dhcp server
!
```

CHAPTER 3 DHCP Server Group

Overview

Dynamic Host Control Protocol (DHCP) Group provides the capability to specify multiple DHCP servers as a group on the DHCP relay agent and to correlate a relay agent interface with the server group. When the interface receives request messages from clients, the relay agent forwards the message to all the DHCP servers of the group. One or multiple DHCP servers in the group process the request and respond with an offer to the client. The client reviews the offer and sends the request message to the chosen server to obtain the network configuration that includes an IP address. The illustration below shows a DHCP client sending a request message to a DHCP relay agent that forwards the message to the three servers in the DHCP server group to get their network configuration. The DHCP client and DHCP relay agent run OcNOS, but the DHCP servers can be OcNOS or Linux devices.

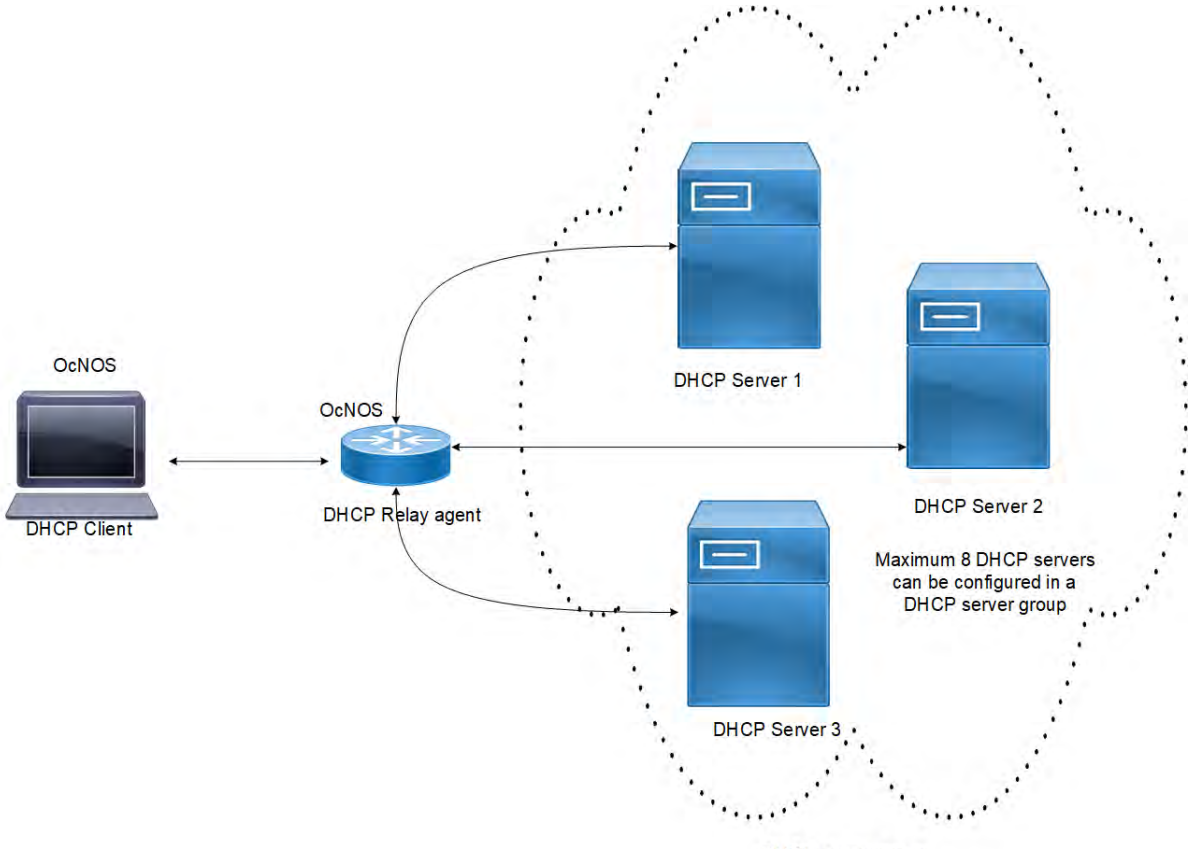


Figure 3-1: DHCP server group

Feature Characteristics

This feature enables the configuration of the DHCP server group and attaches it to a DHCP relay agent through the CLI and the NetConf interface. A DHCP server group can be attached with multiple DHCP relay uplink interfaces, but at a given time, a single DHCP relay uplink interface is allowed to be attached with a single DHCP server group. The attachment of the DHCP relay uplink interface to another DHCP server group dissociates its attachment with the earlier attached DHCP server group.

This feature helps to configure DHCP IPv4 and IPv6 groups and attach server IP addresses to the group. Creating a maximum of 32 IPv4 and 32 IPv6 groups per VRF is allowed, and configuring 8 DHCP servers is permitted for each DHCP server group.

Benefits

The DHCP relay agent forwards the request message from the DHCP client to multiple DHCP servers in the group. Forwarding the request message to multiple DHCP servers increases the reliability of obtaining the network configuration.

Configuration

Before configuring the DHCP client and the DHCP relay agent, make sure that DHCP server is configured and the `dhcpd` service is running in the DHCP server.

Topology

In the below example, DHCP server1 and DHCP server2 (OcNOS or Linux devices) are connected to the DHCP relay agent (an OcNOS device), and the DHCP relay is connected to a DHCP client (an OcNOS device). The DHCP client sends discover message to the DHCP servers through the DHCP relay agent.

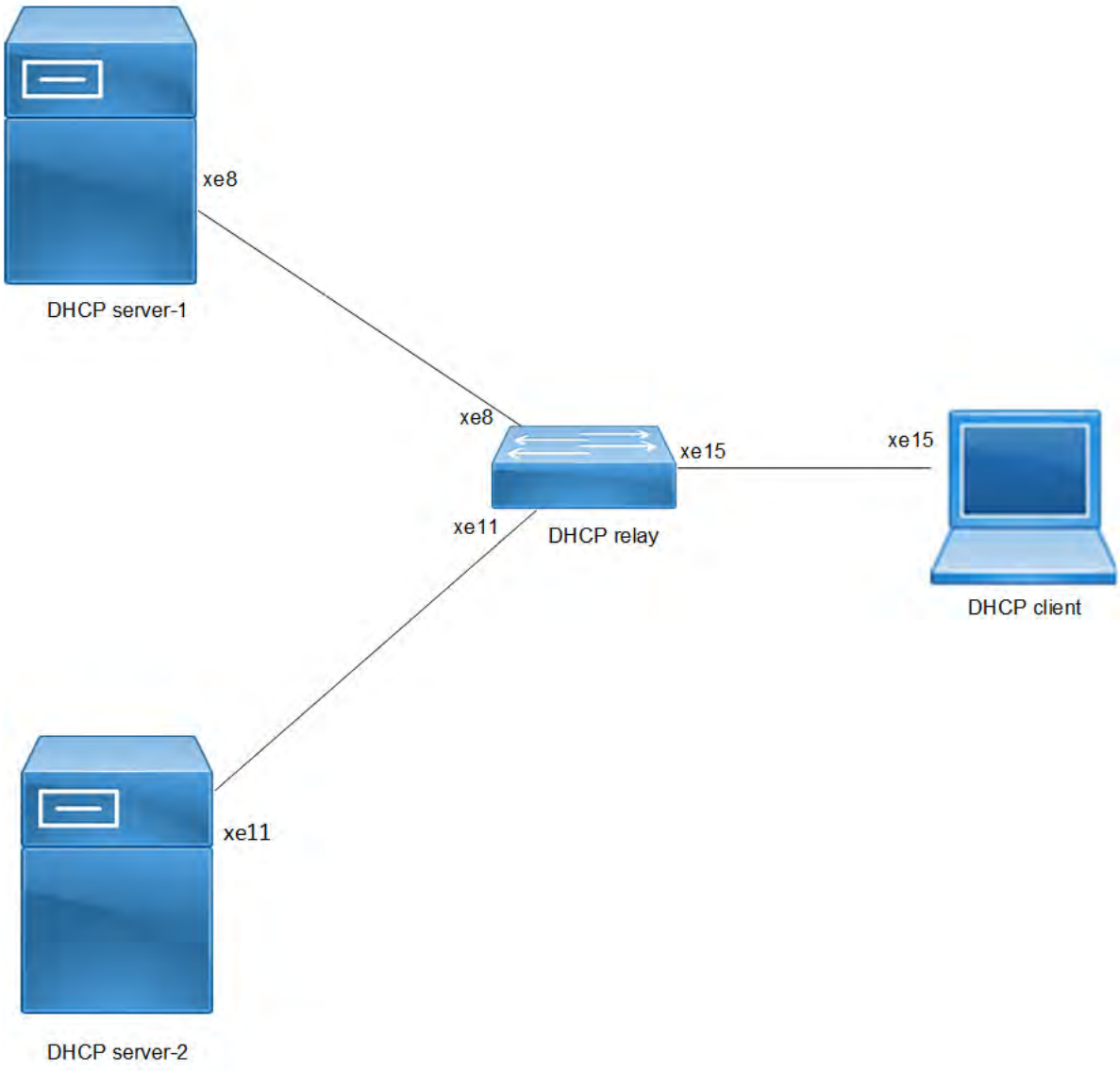


Figure 3-2: DHCP server group topology

DHCP Server-1 Configuration for IPv4

This section shows how to configure the DHCPv4 Server-1.

DHCPv4 Server-1

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)ip dhcp server pool DHCP-Server-1`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp-config)#network 10.10.10.0 netmask 255.255.255.0`	Configure network `10.10.10.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 10.10.10.1 high-address 10.10.10.254`	Configure address range from `10.10.10.1` to `10.10.10.254`.

`OcNOS(dhcp-config)#dns-server 192.2.2.2`	Configure the DNS server `192.2.2.2`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit DHCP config mode.
`OcNOS(config)#ip dhcp server pool DHCP-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp-config)#network 20.20.20.0 netmask 255.255.255.0`	Configure network `20.20.20.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 20.20.20.1 high-address 20.20.20.30`	Configure address range from `20.20.20.1` to `20.20.20.30`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit dhcp config mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ip address 10.10.10.2/24`	Configure IP address on the interface `xe8`.
`OcNOS(config-if)#ip dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip route 20.20.20.0/24 10.10.10.3`	Configure static route of `20.20.20.0/24` by next hop interface `10.10.10.3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv4 Server-1 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp server pool DHCP-Server-1
 network 10.10.10.0 netmask 255.255.255.0
 address range low-address 10.10.10.1 high-address 10.10.10.254
 dns-server 192.2.2.2
ip dhcp server pool DHCP-SER
 network 20.20.20.0 netmask 255.255.255.0
 address range low-address 20.20.20.1 high-address 20.20.20.30
interface xe8
 ip dhcp server
!
OcNOS#
```

DHCP Server-2 Configuration for IPv4

This section shows how to configure the DHCPv4 Server-2.

DHCPv4 Server-2

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ip dhcp server pool DHCP-Server-2`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp-config)#network 40.10.10.0 netmask 255.255.255.0`	Configure network `40.10.10.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 40.10.10.1 high-address 40.10.10.254`	Configure address range from `40.10.10.1` to `40.10.10.254`.
`OcNOS(dhcp-config)#dns-server 192.2.2.2`	Configure DNS server `192.2.2.2`.
`OcNOS(dhcp-config)#ip dhcp server pool DHCP-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp-config)#network 20.20.20.0 netmask 255.255.255.0`	Configure network `20.20.20.0` and netmask `255.255.255.0`.
`OcNOS(dhcp-config)#address range low-address 20.20.20.1 high-address 20.20.20.30`	Configure address range from `20.20.20.1` to `20.20.20.30`.
`OcNOS(dhcp-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ip address 40.10.10.2/24`	Configure IP address `40.10.10.2/24` on the interface `xe11`.
`OcNOS(config-if)#ip dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip route 20.20.20.0/24 40.10.10.3`	Configure static route `20.20.20.0/24` by next hop interface `40.10.10.3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv4 Server-2 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp server pool DHCP-Server-2
 network 40.10.10.0 netmask 255.255.255.0
 address range low-address 40.10.10.1 high-address 40.10.10.254
 dns-server 192.2.2.2
ip dhcp server pool DHCP-SER
 network 20.20.20.0 netmask 255.255.255.0
```

```
 address range low-address 20.20.20.1 high-address 20.20.20.30
interface xe11
 ip dhcp server
!
OcNOS#
```

DHCP Relay Agent Configuration for IPv4

This section shows how to configure the DHCPv4 relay agent.

DHCPv4 Relay Agent

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ip dhcp relay server-group dhcp-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp-relay-group)#server 10.10.10.2`	Configure server `10.10.10.2`.
`OcNOS(dhcp-relay-group)#exit`	Exit DHCP relay group.
`OcNOS(config)#interface xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ip address 20.20.20.2/24`	Configure IPv4 address `20.20.20.2` on the interface `xe15`.
`OcNOS(config-if)#ip dhcp relay`	Relay should be configured on the interface connecting to the client.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ip address 10.10.10.3/24`	Configure IPv4 address `10.10.10.3` on the interface `xe8`.
`OcNOS(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ip dhcp relay server-select dhcp-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ip dhcp relay server-group dhcp-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp-relay-group)#server 40.10.10.2`	Configure IPv4 DHCP server address `40.10.10.2` on the server group.
`OcNOS(dhcp-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp-relay-group)#exit`	Exit DHCP relay group.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ip address 40.10.10.3/24`	Configure IPv4 address `40.10.10.3` on the interface `xe11`.
`OcNOS(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ip dhcp relay server-select dhcp-relay-gp`	Configure relay server-select group name on the device connected to the server.

`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv4 relay agent node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ip dhcp relay server-group dhcp-relay-gp
 server 10.10.10.2
 server 40.10.10.2
interface xe8
 ip dhcp relay uplink
 ip dhcp relay server-select dhcp-relay-gp
!
interface xe11
 ip dhcp relay uplink
 ip dhcp relay server-select dhcp-relay-gp
!
interface xe15
 ip dhcp relay
!
OcNOS#
OcNOS#
OcNOS#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Disabled
  Interface               Uplink/Downlink
  ---------               -------------
  xe8                     Uplink
  xe11                    Uplink
  xe15                    Downlink
  Interface               Group-Name              Server
  ---------               -------------           ------
  xe11                    dhcp-relay-gp     10.10.10.2,40.10.10.2
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED
u
nchanged.
OcNOS#
```

DHCP Client Configuration for IPv4

This section shows how to configure the DHCPv4 Client.

DHCPv4 Client

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#feature dhcp`	Enable the feature DHCP. This will be enabled by default.
`OcNOS(config)#int xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv4 client node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe15
 ip address dhcp

OcNOS#show ip interface brief

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
cd1                  unassigned      up                    down
cd3                  unassigned      up                    down
ce0                  unassigned      up                    down
ce2                  unassigned      up                    down
eth0                *10.12.121.156   up                    up
lo                   127.0.0.1       up                    up
lo.management        127.0.0.1       up                    up
xe4                  unassigned      up                    down
xe5                  unassigned      up                    down
xe6                  unassigned      up                    down
xe7                  unassigned      up                    down
xe8                  unassigned      up                    down
xe9                  unassigned      up                    down
xe10                 unassigned      up                    down
xe11                 unassigned      up                    down
xe12                 unassigned      up                    down
xe13                 unassigned      up                    down
xe14                 unassigned      up                    down
xe15                *20.20.20.1      up                    up
xe16                 unassigned      up                    down
xe17                 unassigned      up                    down
xe18                 unassigned      up                    down
xe19                 unassigned      up                    down
xe20                 unassigned      up                    down
xe21                 unassigned      up                    down
xe22                 unassigned      up                    down
```

```
xe23                 unassigned      up                    down
xe24                 unassigned      up                    down
xe25                 unassigned      up                    down
xe26                 unassigned      up                    down
xe27                 unassigned      up                    down
OcNOS#--
OcNOS#
OcNOS#show ip int xe15 br

'*' - address is assigned by dhcp client

Interface            IP-Address      Admin-Status          Link-Status
xe15                *20.20.20.1      up                    up
OcNOS#
```

DHCP Server-1 Configuration for IPv6

This section shows how to configure the DHCPv6 Server-1.

DHCPv6 Server-1

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp server pool DHCPv6-Server-1`	Configure DHCP server group for server in global mode.
`OcNOS(dhcp6-config)#network 2001:: netmask 64`	Configure network `2001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 2001::1 high-address 2001::124`	Configure address range from `2001::1` to `2001::124`.
`OcNOS(dhcp6-config)#ipv6 dhcp server pool DHCPv6-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp6-config)#network 3001:: netmask 64`	Configure network `3001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 3001::1 high-address 3001::124`	Configure address range from `3001::1` to `3001::124`.
`OcNOS(dhcp6-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ipv6 address 2001::2/64`	Configure IPv6 address `2001::2/64` on the interface `xe8`.
`OcNOS(config-if)#ipv6 dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 route 3001::/64 2001::3`	Configure static route `3001::/64` by next hop interface `2001::3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv6 Server-1 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server pool DHCPv6-Server-1
 network 2001:: netmask 64
 address range low-address 2001::1 high-address 2001::124
ipv6 dhcp server pool DHCPv6-SER
 network 3001:: netmask 64
 address range low-address 3001::1 high-address 3001::124
interface xe8
 ipv6 dhcp server
!
OcNOS#
```

DHCP Server-2 Configuration for IPv6

This section shows how to configure the DHCPv6 Server-2.

DHCPv6 Server-2

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp server pool DHCPv6-Server-2`	Configure dhcp server group for server in global mode.
`OcNOS(dhcp6-config)#network 4001:: netmask 64`	Configure network `4001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 4001::1 high-address 4001::124`	Configure address range from `4001::1` to `4001::124`.
`OcNOS(dhcp6-config)#ipv6 dhcp server pool DHCPv6-SER`	Configure DHCP server group for client in global mode.
`OcNOS(dhcp6-config)#network 3001:: netmask 64`	Configure network `3001::` and netmask `64`.
`OcNOS(dhcp6-config)#address range low-address 3001::1 high-address 3001::124`	Configure address range from `3001::1` to `3001::124`.
`OcNOS(dhcp6-config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-config)#exit`	Exit DHCPv6 config mode.
`OcNOS(config)#interface xe11`	Enter interface mode `xe11`.
`OcNOS(config-if)#ipv6 address 4001::2/64`	Configure IPv6 address on the interface `xe11`.
`OcNOS(config-if)#ipv6 dhcp server`	Server should be configured on the interface while connected to the relay.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.

`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 route 3001::/64 4001::3`	Configure static route `3001::/64` by next hop interface `4001::3`.
`OcNOS(config)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config)#exit`	Exit config mode.

Validation

The below shows the running configuration of the DHCPv6 Server-2 node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp server pool DHCPv6-Server-2
 network 4001:: netmask 64
 address range low-address 4001::1 high-address 4001::124
ipv6 dhcp server pool DHCPv6-SER
 network 3001:: netmask 64
 address range low-address 3001::1 high-address 3001::124
interface xe11
 ipv6 dhcp server
!
OcNOS#
```

DHCP Relay Agent Configuration for IPv6

This section shows how to configure the DHCPv6 relay agent.

DHCPv6 Relay Agent

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#ipv6 dhcp relay server-group dhcpv6-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp6-relay-group)#server 2001::2`	Configure server address `2001::2`.
`OcNOS(dhcp6-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-relay-group)#exit`	Exit DHCPv6 relay group.
`OcNOS(config)#interface xe8`	Enter interface mode `xe8`.
`OcNOS(config-if)#ipv6 address 2001::3/64`	Configure IPv6 address `2001::3/64` on the interface `xe8`.
`OcNOS(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ipv6 dhcp relay server-select dhcpv6-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.

`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#interface xe15`	Enter interface mode.
`OcNOS(config-if)#ipv6 address 3001::2/64`	Configure IPv6 address on the interface `xe15`.
`OcNOS(config-if)#ipv6 dhcp relay`	By default, this will be enabled. This command starts the IPv6 dhcp relay service.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.
`OcNOS(config)#ipv6 dhcp relay server-group dhcpv6-relay-gp`	Configure relay server-group group name in global mode.
`OcNOS(dhcp6-relay-group)#server 4001::2`	Configure server address `4001::2`.
`OcNOS(dhcp6-relay-group)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(dhcp6-relay-group)#exit`	Exit DHCPv6 relay group.
`OcNOS(config)#interface xe11`	Enter interface mode.
`OcNOS(config-if)#ipv6 address 4001::3/64`	Configure IPv6 `4001::3/64` address on the interface `xe11`.
`OcNOS(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`OcNOS(config-if)#ipv6 dhcp relay server-select dhcpv6-relay-gp`	Configure relay server-select group name on the device connected to the server.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv6 relay agent node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
!

ipv6 dhcp relay server-group dhcpv6-relay-gp
 server 2001::2
 server 4001::2
interface xe8
 ipv6 dhcp relay uplink
 ipv6 dhcp relay server-select dhcpv6-relay-gp
!
interface xe11
 ipv6 dhcp relay uplink
 ipv6 dhcp relay server-select dhcpv6-relay-gp
!
interface xe15
 ipv6 dhcp relay
OcNOS#show ipv6 dhcp relay
```

```
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  xe8                      Uplink
  xe11                     Uplink
  xe15                     Downlink
  Interface                Group-Name              Server
  ---------                -------------           ------
  xe11                     dhcpv6-relay-gp     2001::2,4001::2
OcNOS#
```

DHCP Client Configuration for IPv6

This section shows how to configure the DHCPv6 client.

DHCPv6 client

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS (config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`OcNOS(config)#int xe15`	Enter interface mode `xe15`.
`OcNOS(config-if)#ipv6 address dhcp`	The client requests for the IPv6 address to the server. Once it receives the acknowledgment from the server, it assigns the IPv6 address to the interface in which this command is enabled.
`OcNOS(config-if)#commit`	Commit the candidate configuration to the running configuration.
`OcNOS(config-if)#exit`	Exit interface mode.

Validation

The below shows the running configuration of the DHCPv6 client node:

```
OcNOS#show running-config dhcp
interface eth0
 ip address dhcp
!
interface xe15
 ipv6 address dhcp

OcNOS#show ipv6 int br
Interface            IPv6-Address                                    Admin-Sta
tus
cd1                  unassigned                                      [up/down]

cd3                  unassigned                                      [up/down]

ce0                  unassigned                                      [up/down]
```

```
ce2                 unassigned                                  [up/down]

eth0                fe80::d277:ceff:fe9f:4500                   [up/up]

lo                  ::1                                         [up/up]

lo.management       ::1                                         [up/up]

xe4                 unassigned                                  [up/down]

xe5                 unassigned                                  [up/down]

xe6                 unassigned                                  [up/down]

xe7                 unassigned                                  [up/down]

xe8                 unassigned                                  [up/down]

xe9                 unassigned                                  [up/down]

xe10                unassigned                                  [up/down]

xe11                unassigned                                  [up/down]

xe12                unassigned                                  [up/down]

xe13                unassigned                                  [up/down]

xe14                unassigned                                  [up/down]

xe15                *3001::124
                    fe80::d277:ceff:feda:4511                   [up/up]

xe16                unassigned                                  [up/down]

xe17                unassigned                                  [up/down]

xe18                unassigned                                  [up/down]

xe19                unassigned                                  [up/down]

xe20                unassigned                                  [up/down]

xe21                unassigned                                  [up/down]

xe22                unassigned                                  [up/down]

xe23                unassigned                                  [up/down]

xe24                unassigned                                  [up/down]
```

```
xe25                unassigned                                      [up/down]

xe26                unassigned                                      [up/down]

xe27                unassigned                                      [up/down]

OcNOS#show ipv6 int xe15 br
Interface           IPv6-Address                                    Admin-Sta
tus
xe15                *3001::124
                    fe80::d277:ceff:feda:4511                       [up/up]
```

New CLI Commands

ip dhcp relay server-group

Use this command to create the DHCP IPv4 server group. This group lists the servers to which DHCP Relay forwards the DHCP client requests.

Use the `no` form of this command to unconfigure the DHCP IPv4 server group.

Command Syntax

```
ip dhcp relay server-group GROUP_NAME
no ip dhcp relay server-group GROUP_NAME
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum 63 alphanumeric characters).

Command Mode

Configure mode and VRF mode. In the configure mode, the DHCP IPv4 server group is created in the default VRF. In the configure-vrf mode, the DHCP IPv4 server group is created in the user-defined VRF.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below shows the creation of DHCP IPv4 server groups.

```
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ip dhcp relay server-group Group1
OcNOS(dhcp-relay-group)#end
OcNOS#configure terminal
OcNOS(config)#ip dhcp relay server-group Group2
```

ip dhcp relay server-select

Use this command to attach the DHCP IPv4 server group to the DHCP relay uplink interface.

Use the `no` form of this command to remove the DHCP IPv4 server group attached to the DHCP relay interface.

Note: Attach the groups only to the DHCP relay uplink interfaces.

Command Syntax

```
ip dhcp relay server-select GROUP_NAME
no ip dhcp relay server-select
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum 63 alphanumeric characters).

Command Mode

Interface mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows attaching the DHCP IPv4 server group to the DHCP relay uplink interface:

```
OcNOS#configure terminal
OcNOS(config)#interface xe1
OcNOS(config-if)#ip dhcp relay server-select group1
```

ipv6 dhcp relay server-group

Use this command to create the DHCP IPv6 server group. This group lists the servers to which DHCP relay forwards the DHCP client requests.

Use the no form of this command to unconfigure the DHCP IPv6 server group.

Command Syntax

```
ipv6 dhcp relay server-group GROUP_NAME
no ipv6 dhcp relay server-group GROUP_NAME
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum of 63 alphanumeric characters).

Command Mode

Configure mode and VRF mode. In the configure mode, the DHCP IPv6 server group is created in the default VRF. In the configure-vrf mode, the DHCP IPv6 server group is created in the user-defined VRF.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The example below shows the creation of DHCP IPv6 server groups:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
```

```
OcNOS(config-vrf)#ipv6 dhcp relay server-group Group1
OcNOS(dhcp relay server-group)#end
OcNOS#configure terminal
OcNOS(config)#ipv6 dhcp relay server-group Group2
```

ipv6 dhcp relay server-select

Use this command to attach the DHCP IPv6 group to the DHCP relay uplink interface.

Use the `no` form of this command to remove the DHCP IPv6 group attached to the interface.

Note: Attach the groups only to the DHCP relay uplink interfaces.

Command Syntax

```
ipv6 dhcp relay server-select GROUP_NAME
no ipv6 dhcp relay server-select
```

Parameters

`GROUP_NAME`	Name of the DHCP server group (specify a maximum of 63 alphanumeric characters).

Command Mode

Interface mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows how to attach the DHCP IPv6 server group to the DHCP relay uplink interface:

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp relay server-select group1
```

server A.B.C.D

Use this command to add the DHCP IPv4 servers to the DHCP server group.

Use the `no` form of this command to remove the DHCP IPv4 servers from the DHCP server Group.

Note: A maximum of eight servers can be added to a DHCP group.

Command Syntax

```
server A.B.C.D
no server A.B.C.D
```

Parameters

`A.B.C.D`	DHCP IPv4 Relay group server address to be added in the DHCP server group.

Command Mode

DHCP Relay Group Mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows the addition of DHCP IPv4 servers to a DHCP server group:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ip dhcp relay server-group group
OcNOS(dhcp-relay-group)#server 10.12.23.205
OcNOS(dhcp-relay-group)#end
OcNOS#configure terminal
OcNOS(config)#ip dhcp relay server-group group1
OcNOS(dhcp-relay-group)#server 10.12.33.204
```

server X:X::X:X

Use this command to add the DHCP IPv6 servers to the DHCP server group.

Use the `no` form of this command to remove the DHCP IPv6 servers from the DHCP server group.

Note: A maximum of eight servers can be added to a DHCP group.

Command Syntax

```
server X:X::X:X
no server X:X::X:X
```

Parameters

`X:X::X:X`	DHCP IPv6 Relay Group server address to be added in the DHCP server group.

Command Mode

DHCPv6 Relay Group Mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The below example shows the addition of DHCP IPv6 servers to a DHCP server group:

```
OcNOS#configure terminal
OcNOS(config)#ip vrf vrf1
OcNOS(config-vrf)#ipv6 dhcp relay server-group group
OcNOS(dhcp6-relay-group)#server 2003::1
OcNOS(dhcp6-relay-group)#end

OcNOS#configure terminal
OcNOS(config)#ipv6 dhcp relay server-group group1
OcNOS(dhcp-relay-group)#server 2001::1
OcNOS(dhcp6-relay-group)end
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
DHCP	Dynamic Host Configuration Protocol
VRF	Virtual Routing and Forwarding

Glossary

The following provides definitions for key terms used throughout this document:

DHCP Client	A DHCP client is a hardware device or software that uses DHCP to get the network configuration information from a DHCP Server. VRF: VRF creates a logically isolated routing table within a single physical network device. Each VRF instance works as an independent routing instance that enables separate network traffic, maintains different routing tables, and provides network isolation.
DHCP Server	A DHCP server is a hardware device or software that leases a dynamic IP address to the DHCP client.
DHCP relay agent	A DHCP relay forwards the request from a DHCP client to the DHCP server group and takes the response from the DHCP server group to the DHCP client.
VRF	VRF creates a logically isolated routing table within a single physical network device. Each VRF instance works as an independent routing instance that enables separate network traffic, maintains different routing tables, and provides network isolation.

© 2025 IP Infusion Inc. Proprietary

CHAPTER 4 DHCP Relay Agent Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

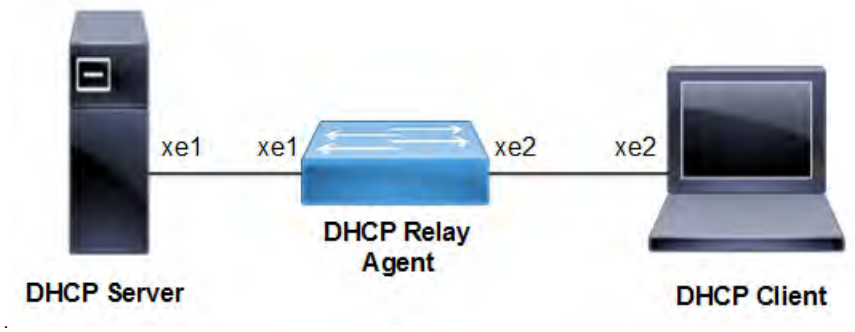


Figure 4-3: DHCP Relay Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config-if)#ip dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running

© 2025 IP Infusion Inc. Proprietary

Validation Commands

```
#show running-config dhcp

ip dhcp relay address 10.10.10.2
interface xe2
 ip dhcp relay
!
interface xe1
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Disabled
  DHCP Servers configured: 10.10.10.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe2                      Downlink
  xe1                      Uplink

#show ip dhcp relay address
 VRF Name: default
  DHCP Servers configured: 10.10.10.2
```

DHCP Relay for IPv6 Configuration

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting to the client.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration

Validation Commands

```
#sh ipv6 dhcp relay address

VRF Name: default
  DHCPv6 Servers configured: 2001::2

#show running-config dhcp

Ipv6 dhcp relay address 2001::2
 interface xe2
 ipv6 dhcp relay
!
interface xe1
 ipv6 dhcp relay uplink
!
```

DHCP Relay option 82

This section contains examples of DHCP Relay option-82 configuration. DHCP option 82 (Agent Information Option) provides additional security when DHCP is used to allocate network addresses. It enables the DHCP relay agent to prevent DHCP client requests from untrusted sources. Service Providers use remote identifier (option 82 sub option 2) for troubleshooting, authentication, and accounting. The DHCP Option 82 Remote ID Format feature adds support for the interpretation of **remote-IDs** that are inserted by end users. On the relay agent, you can configure information option to add option 82 information to DHCP requests from the clients before forwarding the requests to the DHCP server. When configured with option 82 and remote-id, the server will receive the DHCP request packet with Agent Circuit ID and remote-id.

The two examples below, show how to configure the DHCP Relay option 82:

- Configuration of DHCP Relay option 82 on a physical interface with Agent information and remote-id.
- Configuration of DHCP Relay option 82 on a VLAN interface with Agent information and remote-id.

Topology

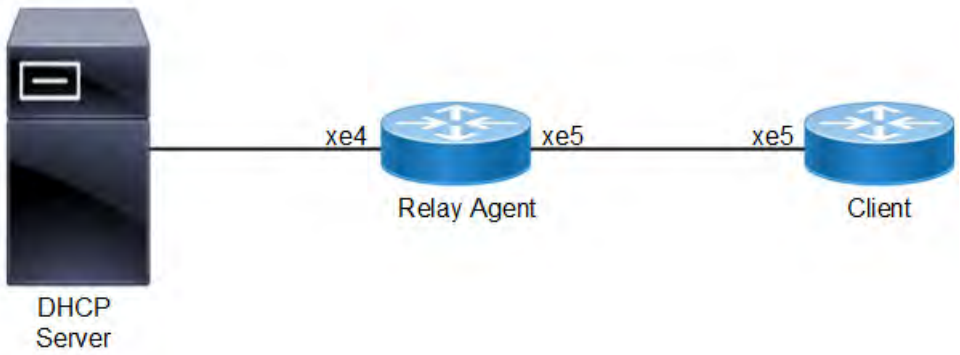


Figure 4-4: DHCP 82 interface topology

Physical Interface Configuration

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for `DHCP OFFER` packets to reach the Relay Agent.

Relay agent

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay
`(config)#ip dhcp relay address 192.168.1.2`	The relay address configured should be server interface address connected to DUT machine
`(config)#ip dhcp relay information option remote-id hostname`	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#ip address 10.10.20.2/24`	Add IP address
`(config-if)#ip dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the candidate configuration to the running
`(config)#interface xe4`	Enter interface mode
`(config-if)#ip address 192.168.1.1/24`	Configure ipv4 address on the interface xe4
`(config-if)#ip dhcp relay uplink`	Configure DHCP relay uplink for the interface connecting to server.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running

Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)#ip address dhcp`	Configure IP address DHCP
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the candidate configuration to the running

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
```

```
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe5                      Downlink
 xe4                       Uplink
```

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
    Option: (255) End
        Option End: 255
    Padding
```

Physical Interface Configuration with non-default VRF

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnet 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent.

Relay agent

#configure terminal	Enter configure mode.
(config)#ip dhcp relay	Enable DHCP Relay.
(config)#ip vrf vrf_dhcp	Configuring non default vrf vrf_dhcp
(config-vrf)#ip dhcp relay information option remote-id hostname	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82 on non default vrf.. String support is also provided for remote-id.
(config-vrf)#ip dhcp relay address 192.168.1.2	Configure DHCP relay address in non default vrf.
(config)#interface xe5	Enter interface mode.
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp.
(config-if)#ip address 10.10.20.2/24	Add IP address.
(config-if)#ip dhcp relay	Configure DHCP relay for the interface connecting to client.
(config-if)#exit	Exit from interface mode
(config)#commit	Commit the candidate configuration to the running
(config)#interface xe4	Enter interface mode
(config-if)#ip vrf forwarding vrf_dhcp	Configure vrf forwarding for vrf_dhcp
(config-if)#ip dhcp relay uplink	Configure DHCP relay uplink for the interface connecting to server.
(config-if)#ip address 192.168.1.4/24	Add IP address.
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running

Client

#configure terminal	Enter configure mode.
(config)#interface xe5	Enter interface mode.
(config-if)#ip vrf forwarding vrf_dhcp	Configure ip vrf forwarding for non default vrf.
(config-if)#ip address dhcp	Configure IP address DHCP.
(config-if)#exit	Exit from interface mode.
(config)#commit	Commit the candidate configuration to the running

Validation

Relay Agent

```
#show running-config dhcp
```

```
!
ip vrf vrf_dhcp
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 192.168.1.2
interface xe5
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf_dhcp
  Option 82: Enabled
  Remote Id: OcNOS
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  xe5                      Downlink
  xe4                      Uplink
```

Client

```
#show ip interface brief | include xe5
xe5            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4e61176c
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
```

```
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 12
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 3
            Agent Circuit ID: 786535
         Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53
    Option: (255) End
        Option End: 255
    Padding
```

```
Sample DHCP configuration for using Remote-id

class "remote-id" {
        match if option agent.remote-id = OcNOS
} # remote-id

subnet 10.10.20.0 netmask 255.255.255.0 {
        pool {
                allow members of                "remote-id";
                default-lease-time               600;
                max-lease-time                    7200;
                range                           10.10.20.3 10.10.10.100;
                option routers                  10.10.20.2;
                option broadcast-address        10.10.20.255;
                option subnet-mask              255.255.255.0;
                option domain-name-servers      4.2.2.2;
}
```

VLAN Interface Configuration

Topology

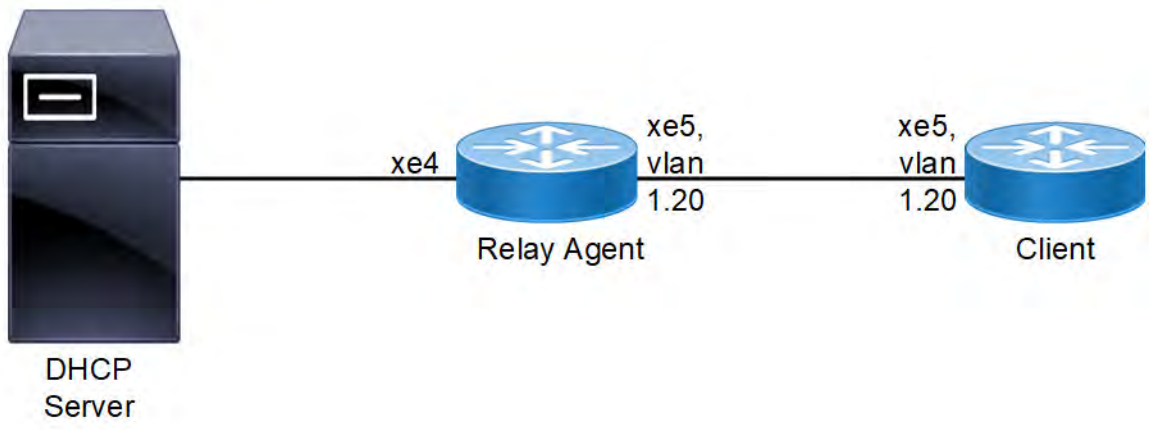


Figure 4-5: DHCP 82 vlan topology

Here, the DHCP Server is running with IP 192.168.1.2 with another pool of subnets 10.10.20.0 configured in the server. Configure a static route to 10.10.20.0 network for DHCP OFFER packets to reach the Relay Agent. In the above topology, vlan 20 is part of interface xe5 in relay Agent and xe5 in Client.

Relay Agent

t

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	Enable DHCP Relay
`(config)#ip dhcp relay information option remote-id hostname`	Enable DHCP Relay information option with both agent circuit id which is sub option 1 of option 82 and remote-id which is sub option 2 of option 82. String support is also provided for remote-id.
`(config)#ip dhcp relay address 192.168.1.2`	Configure DHCP relay address
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge
`(config)#vlan 2-100 bridge 1 state enable`	Enable some VLANs
`(config)#interface xe5`	Enter interface mode
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Configure bridge-group
`(config-if)#switchport mode hybrid`	Configure switchport mode
`(config-if)#switchport hybrid allowed vlan all`	Enable vlan
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the candidate configuration to the running
`(config)#interface vlan1.20`	Enter interface mode for the vlan interface towards client.
`(config-if)#ip address 10.10.20.2/24`	Add IP address
`(config-if)#ip dhcp relay`	Configure DHCP relay on the vlan interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#commit`	Commit the candidate configuration to the running
`(config)#interface xe4`	Enter interface mode
`(config-if)#ip dhcp relay uplink`	Configure DHCP relay uplink for the interface connecting to server.
`(config-if)#ip address 192.168.1.4/24`	Add IP address
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running

Client

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge
`(config)#vlan 2-100 bridge 1 state enable`	Enable VLANs
`(config)#interface xe5`	Enter interface mode.
`(config-if)#switchport`	Configure switchport
`(config-if)#bridge-group 1`	Configure bridge-group
`(config-if)#switchport mode hybrid`	Configure switchport mode
`(config-if)#switchport hybrid allowed vlan add 20 egress-tagged enable`	Enable vlan
`(config-if)#exit`	Exit from interface mode

(config)#commit	Commit the candidate configuration to the running
(config)#interface vlan1.20	Enter interface mode for the vlan interface which connects relay.
(config-if)#ip address dhcp	Configure IP address DHCP
(config-if)#exit	Exit from interface mode
(config)#commit	Commit the candidate configuration to the running

Validation

Relay Agent

```
#show running-config dhcp
!
ip dhcp relay information option remote-id hostname
ip dhcp relay address 192.168.1.2
!
interface vlan1.20
 ip dhcp relay
!
interface xe4
 ip dhcp relay uplink
!


#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: default
  Option 82: Enabled
  Remote Id: ocnos
  DHCP Servers configured: 192.168.1.2
  Interface                Uplink/Downlink
  ---------                -------------
  Vlan1.20                 Downlink
  xe4                      Uplink
```

Client

```
#show ip interface brief |include vlan1.20
vlan1.20            *10.10.20.10     up                    up

Packet captured at DHCP Server

Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x59591459
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
        0... .... .... .... = Broadcast flag: Unicast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
```

```
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 10.10.20.2 (10.10.20.2)
    Client MAC address: b8:6a:97:35:d7:9d (b8:6a:97:35:d7:9d)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
    Option: (53) DHCP Message Type (Discover)
        Length: 1
        DHCP: Discover (1)
    Option: (55) Parameter Request List
        Length: 3
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (28) Broadcast Address
        Parameter Request List Item: (3) Router
    Option: (60) Vendor class identifier
        Length: 39
        Vendor class identifier: onie_vendor:x86_64-accton_as7326_56x-r0
    Option: (82) Agent Information Option
        Length: 17
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 8
            Agent Circuit ID: 766c616e312e3230
        Option 82 Suboption: (2) Agent Remote ID
            Length: 5
            Agent Remote ID: 4f634e4f53

Option: (255) End
    Option End: 255
```

DHCP-Relay with different VRFs

This chapter explains about DHCP Relay package to make Relay talk to different VRFs when Client and Server are running in different VRFs.

DHCP Relay for IPv4 with different VRFs

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

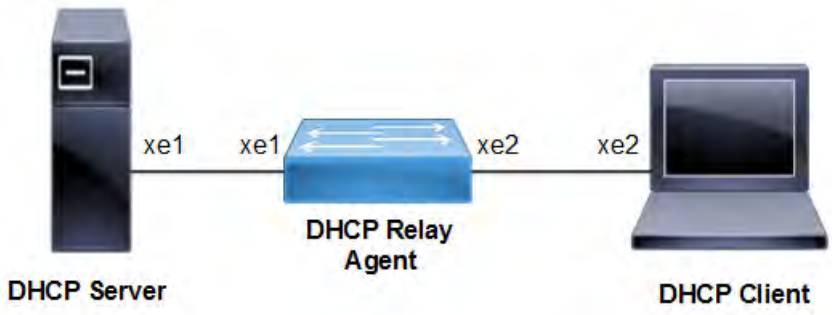


Figure 4-6: DHCP Relay Configuration

DHCP Agent

#configure terminal	Enter configure mode.
(config)#feature dhcp	Enable the feature dhcp. This is enabled in default.
(config)#ipv4 dhcp relay	By default this will be enabled. It starts the ipv4 dhcp relay service.
(config)# ip vrf vrf1	Configure IP VRF
(config)# ip dhcp relay address 10.10.10.2 global	Configure DHCP relay address
(config)#interface xe1	Enter interface mode.
(config-if)#ip address 10.10.10.1/24	Configure ipv4 address on the interface xe1.
(config-if)#ip dhcp relay uplink	Configure relay uplink on the device connecting the server.
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running
(config)#interface xe2	Enter interface mode.
(config)#ip vrf forwarding vrf1	Configure IP VRF forwarding
(config-if)#ip address 20.20.20.1/24	Configure ipv4 address on the interface xe2.
(config-if)#ip dhcp relay	Relay should be configured on the interface connecting to the
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running

Validation Commands

```
#show running-config dhcp
      interface eth0
 ip address dhcp
!
ip vrf vrf1
ip dhcp relay address 10.10.10.2 global
!
interface xe2
ip dhcp relay
!
interface xe1
ip dhcp relay uplink
!

#show ip dhcp relay
DHCP relay service is Enabled. VRF Name: vrf1
Option 82: Disabled
DHCP Servers configured:
10.10.10.2 default
InterfaceUplink/Downlink

xe2 Downlink
VRF Name: default
InterfaceUplink/Downlink
```

```
xe1 Uplink

Incoming DHCPv4 packets which already contain relay agent option are FORWARDED
unchanged.
#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured:
  10.10.10.2        default
Incoming DHCPv4 packets which already contain relay agent option are FORWARDED
unchanged.
```

DHCP Relay for IPv6 Configuration with different VRFs

DHCP Agent

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default, this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ip vrf vrf1`	Configure vrf1
`(config)#ipv6 dhcp relay address 2001::2 global`	The relay address configured should be server interface address which is in default vrf , connected to DUT machine.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface xe2`	Enter interface mode.
`(config-if)# ip vrf forwarding vrf1`	Attach vrf1 under downlink interface
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay`	Relay should be configured on the interface connecting client.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration

Validation Commands

```
#show ipv6 dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured:
  2001::2    default
#show running-config dhcp
interface eth0
 ip address dhcp
!
ip vrf vrf1
ipv6 dhcp relay address 2001::1 global
```

```
interface xe2
ipv6 dhcp relay
!
interface xe1
ipv6 dhcp relay uplink
!

#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  DHCPv6 Servers configured:
  2001::2    default
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  Xe2                      Downlink
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  Xe1                      Uplink
```

CHAPTER 5 DHCP Relay Agent Over L3VPN Configuration

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy. In the L3VPN case, there is a special tunnel which gets created through which all the communication happens. In OcNOS, the interface created is named as tunmpls. This tunnel name is not exposed to the OcNOS control plane.This interface is directly created in the kernel.

DHCP Relay Over L3 VPN for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

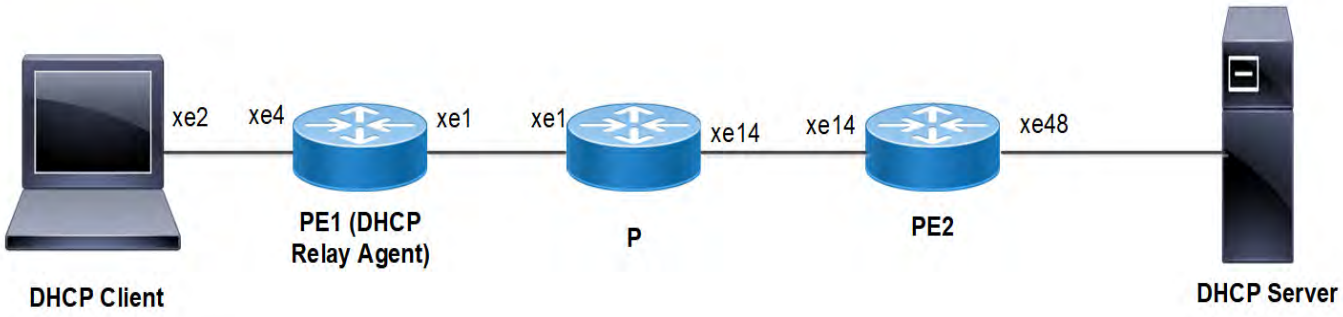


Figure 5-7: DHCP Relay Over L3 VPN Configuration

DHCP Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address dhcp`	Enable DHCP on interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration

PE1 (DHCP Relay Agent)

`#configure terminal`	Enter configure mode.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)#rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)#route-target both 10:10`	Configure a route target for vrf1.
`(config-vrf)#ip dhcp relay address 11.11.0.1`	Configure DHCP server address.
`(config-vrf)#ip dhcp relay uplink l3vpn`	configure IPv4 DHCP Relay over L3VPN.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)#ip address 50.50.50.1/24`	Add IP address.
`(config-if)#ip dhcp relay`	Configure DHCP relay for the interface connecting to client.

© 2025 IP Infusion Inc. Proprietary

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit from interface mode
(config)#interface lo	Enter interface mode
(config-if)#ip address 1.1.1.1/32 secondary	Set an IP address on the interface
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 1.1.1.1	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 10.1.1.1/24	Add IP address.
(config-if)#label-switching	Enable label switching on the interface
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 1.1.1.1/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 1.1.1.1	Configure a fixed Router ID (1.1.1.1)
(config-router)# neighbor 3.3.3.3 remote-as 100	Configuring PE2 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 3.3.3.3 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4
(config-router-af)# neighbor 3.3.3.3 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

P

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 2.2.2.2/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 2.2.2.2`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe14`	Enter interface mode
`(config-if)# ip address 20.1.1.1/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#interface xe1`	Enter interface mode
`(config-if)# ip address 10.1.1.2/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#network 10.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)# commit`	Commit the candidate configuration to the running configuration

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)# rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)# route-target both 10:10`	Configure a route target for vrf1.
`(config)#interface xe48`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)# commit`	Commit the candidate config
`(config-if)#ip address 11.11.0.2/24`	Add IP address.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Set an IP address on the interface

(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 3.3.3.3	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)# ip address 20.1.1.2/24	Add IP address.
(config-if)# label-switching	Enable label switching on the interface
(config-if)# enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# router bgp 100	Enter the Router BGP mode, ASN: 100
(config-router)# bgp router-id 3.3.3.3	Configure a fixed Router ID (3.3.3.3)
(config-router)# neighbor 1.1.1.1 remote-as 100	Configuring PE1 as iBGP neighbor using it's loopback IP
(config-router)# neighbor 1.1.1.1 update-source lo	Source of routing updates as loopback
(config-router)# address-family ipv4 unicast	Entering into IPV4 unicast address family
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the IPV4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family vpnv4 unicast	Entering into address family mode as vpnv4
(config-router-af)# neighbor 1.1.1.1 activate	Activate the neighbor in the vpnv4 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)# redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# commit	Commit the candidate configuration to the running configuration

Validation

PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
ip vrf vrf1
 ip dhcp relay address 11.11.0.1
 ip dhcp relay uplink l3vpn
interface xe4
```

```
 ip dhcp relay

PE1#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Disabled
  DHCP Servers configured: 11.11.0.1

  Interface                Uplink/Downlink
  ---------                -------------
  xe4                      Downlink
  l3vpn                    uplink
```

Incoming DHCPv4 packets which already contain relay agent option are FORWARDED and changed.

```
PE1#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured: 11.11.0.1
```

Incoming DHCPv4 packets which already contain relay agent option are FORWARDED and changed.

DHCP Client

```
#show ip interface brief | include xe2
  xe5    *50.50.50.2  up      up
```

DHCP Relay Over L3 VPN for IPv6

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

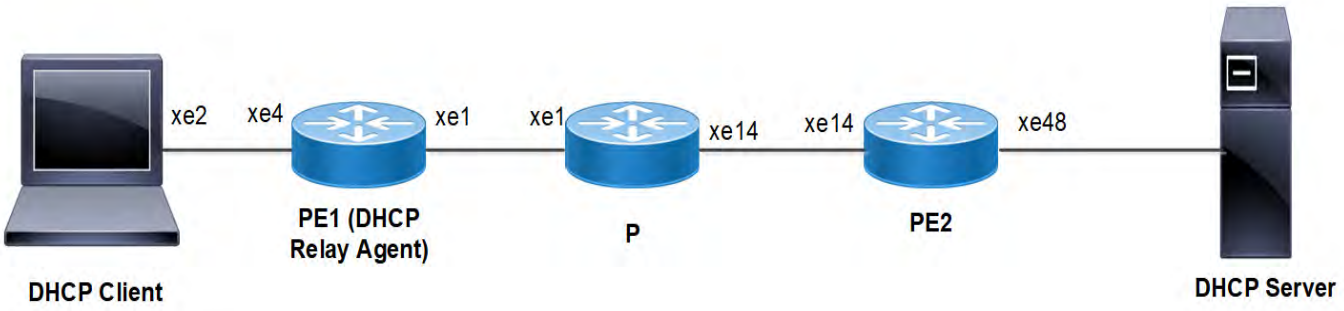


Figure 5-8: DHCP Relay Over L3 VPN Configuration

DHCP Client

`#configure terminal`	Enter configure mode.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ipv6 address dhcp`	Enable DHCP on interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration

PE1 (DHCP Relay Agent)

`#configure terminal`	Enter configure mode.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)#rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)#route-target both 10:10`	Configure a route target for vrf1.
`(config-vrf)#ipv6 dhcp relay address 2002::1`	Configure DHCP server address.
`(config-vrf)#ipv6 dhcp relay uplink l3vpn`	configure IPv6 DHCP Relay over L3VPN.
`(config)#interface xe4`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)# ipv6 address 2001::1/64`	Add IPv6 address.
`(config-if)#ipv6 dhcp relay`	Configure DHCP relay for the interface connecting to client.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 1.1.1.1/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 1.1.1.1`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe1`	Enter interface mode
`(config-if)# ip address 10.1.1.1/24`	Add IP address.
`(config-if)# label-switching`	Enable label switching on the interface
`(config-if)# enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 1.1.1.1/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 10.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)#router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)#bgp router-id 1.1.1.1`	Configure a fixed Router ID (1.1.1.1)
`(config-router)#neighbor 3.3.3.3 remote-as 100`	Configuring PE2 as iBGP neighbor using it's loopback IP
`(config-router)#neighbor 3.3.3.3 update-source lo`	Source of routing updates as loopback
`(config-router)#address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)#address-family vpnv4 unicast`	Entering into address family mode as vpnv4
`(config-router-af)#neighbor 3.3.3.3 activate`	Activate the neighbor in the vpnv4 address family

(config-router-af)#exit	Exiting of Address family mode
(config-router)#address-family vpnv6 unicast	Entering into address family mode as vpnv6
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor in the vpnv6 address family
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)#redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)# address-family ipv6 vrf vrf1	Entering into address family mode as ipv6 vrf vrf1
(config-router-af)#redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)#commit	Commit the candidate configuration to the running configuration

P

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode
(config-if)#ip address 2.2.2.2/32 secondary	Set an IP address on the interface
(config-if)#exit	Exit from interface mode
(config)#router ldp	Enter the Router LDP mode.
(config-router)#router-id 2.2.2.2	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode
(config)#interface xe14	Enter interface mode
(config-if)#ip address 20.1.1.1/24	Add IP address.
(config-if)#label-switching	Enable label switching on the interface
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#interface xe1	Enter interface mode
(config-if)#ip address 10.1.1.2/24	Add IP address.
(config-if)#label-switching	Enable label switching on the interface
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from interface mode
(config)#router ospf 100	Enter the Router OSPF mode.
(config-router)#network 3.3.3.3/32 area 0.0.0.0	Advertise loopback address in OSPF.
(config-router)#network 20.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#network 10.1.1.0/24 area 0.0.0.0	Advertise network address in OSPF.
(config-router)#exit	Exit Router OSPF mode and return to Configure mode.
(config)# commit	Commit the candidate configuration to the running configuration

PE2

`#configure terminal`	Enter configure mode.
`(config)#ip vrf vrf1`	Configuring non default vrf vrf1
`(config-vrf)#rd 10:10`	Assign a route distinguisher to VRF
`(config-vrf)#route-target both 10:10`	Configure a route target for vrf1.
`(config)#interface xe48`	Enter interface mode.
`(config-if)#ip vrf forwarding vrf1`	Configure vrf forwarding for vrf1
`(config-if)#commit`	Commit the candidate config
`(config-if)#ipv6 address 2002::2/64`	Add IPv6 address.
`(config-if)#exit`	Exit from interface mode
`(config)#interface lo`	Enter interface mode
`(config-if)#ip address 3.3.3.3/32 secondary`	Set an IP address on the interface
`(config-if)#exit`	Exit from interface mode
`(config)#router ldp`	Enter the Router LDP mode.
`(config-router)#router-id 3.3.3.3`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode
`(config)#interface xe14`	Enter interface mode
`(config-if)#ip address 20.1.1.2/24`	Add IP address.
`(config-if)#label-switching`	Enable label switching on the interface
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on the interface.
`(config-if)#exit`	Exit from interface mode
`(config)#router ospf 100`	Enter the Router OSPF mode.
`(config-router)#network 3.3.3.3/32 area 0.0.0.0`	Advertise loopback address in OSPF.
`(config-router)#network 20.1.1.0/24 area 0.0.0.0`	Advertise network address in OSPF.
`(config-router)#exit`	Exit Router OSPF mode and return to Configure mode.
`(config)#router bgp 100`	Enter the Router BGP mode, ASN: 100
`(config-router)#bgp router-id 3.3.3.3`	Configure a fixed Router ID (3.3.3.3)
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Configuring PE1 as iBGP neighbor using it's loopback IP
`(config-router)#neighbor 1.1.1.1 update-source lo`	Source of routing updates as loopback
`(config-router)#address-family ipv4 unicast`	Entering into IPV4 unicast address family
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor in the IPV4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)#address-family vpnv4 unicast`	Entering into address family mode as vpnv4
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor in the vpnv4 address family
`(config-router-af)#exit`	Exiting of Address family mode
`(config-router)#address-family vpnv6 unicast`	Entering into address family mode as vpnv6
`(config-router-af)#neighbor 1.1.1.1 activate`	Activate the neighbor in the vpnv6 address family

(config-router-af)#exit	Exiting of Address family mode
(config-router)#address-family ipv4 vrf vrf1	Entering into address family mode as ipv4 vrf vrf1
(config-router-af)#redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)#address-family ipv6 vrf vrf1	Entering into address family mode as ipv6 vrf vrf1
(config-router-af)#redistribute connected	Redistribute connected routes.
(config-router-af)#exit	Exiting of Address family mode
(config-router)#commit	Commit the candidate configuration to the running configuration

Validation

PE1 (DHCP Relay Agent)

```
PE1#show running-config dhcp
ip vrf vrf1
 ipv6 dhcp relay address 2002::1
 ipv6 dhcp relay uplink l3vpn
interface xe4
 ipv6 dhcp relay

PE1#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  DHCPv6 Servers configured: 2002::1
  DHCPv6 IA_PD Route injection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  xe4                      Downlink
  l3vpn                    uplink
PE1#show ip dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2002::1
```

DHCP Client

```
#show ipv6 interface brief | include xe2
  xe5   *2001::200  up     up
```

CHAPTER 6 DHCPv6 Prefix Delegation Configuration

Overview

The prefix delegation feature facilitates the Dynamic Host Control Protocol (DHCP) server capable of assigning prefixes to DHCP clients from a global pool, enabling the Customer Premise Equipment (CPE) to learn the prefix. This feature also supports the DHCP server in assigning multiple prefixes to a single client. The user configures the IPv6 address using the learned prefix on its Local Area Network (LAN) interface with the subnet prefix. The LAN hosts are learning the subnetted prefix through Router Advertisement (RA) messages, an important Neighbor Discovery Protocol (NDP) component, enabling the device to auto-configure the number of IPv6 addresses from 1 to 64.

This feature would enable service providers to assign IP for the CPE that is acting as a router between the service providers' core network and the subscribers' internal network.

Feature Characteristics

- DHCPv6 Identity association for non-temporary addresses (IA_NA) assigns a global IPv6 address on the Wide Area Network (WAN) link. The address comes from a local pool specified in the DHCP Server.
- The Requesting Router (RR) uses the delegated prefix to define the subnet for the LAN based on the prefix received from the DHCP Server.
- The Requesting Router uses the delegated prefix to assign addresses to the LAN devices. The RR can send a Router Advertisement or the devices shall send a Router solicitation.

Benefits

The key benefits are as follows:

- This feature helps the Internet Service Providers (ISPs) to assign the dynamic IPv6 addresses to their customers automatically instead of statically assigning the address.
- This feature adds the capability to get the multiple DHCPv6 prefixes as per the customer requirement.
- This feature allows the centralized management of the IPv6 addresses.

Configuration

This section shows the configuration of the DHCPv6 prefix delegation.

Topology

The requesting router sends the prefix request to the delegating router, which sends the request to the DHCP server. The DHCP server sends the prefix to the requesting router through the delegating router. The IPv6 address is created in the requesting router by combining the prefix learned from the server and the user-defined suffix. The host receives the IPv6 address from the requesting router.

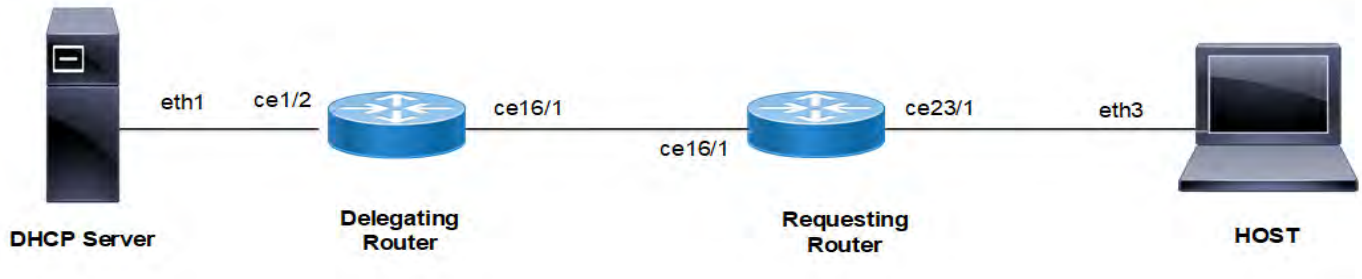


Figure 6-9: DHCPv6 Prefix Delegation Configuration

Configuring DHCP prefixes

Follow the steps to configure the DHCPv6 prefix delegation.

Configure the Delegating Router:

1. Specify the server interface address connected to the delegating router.

```
(config)#ipv6 dhcp relay address 2001:101:0:1::131
```

2. Configure the DHCPv6 up-link interface from the delegating router to the DHCPv6 server using `ipv6 dhcp relay uplink` command.

```
(config)#interface ce1/2
(config-if)#ipv6 address 2001:101:0:1::130/64
(config-if)#ipv6 dhcp relay uplink
```

3. Configure the DHCPv6 down-link interface from the delegating router to the requesting router using `ipv6 dhcp relay` command.

```
(config)#interface ce16/1
(config-if)#ipv6 address 3001:101:0:1::135/64
(config-if)#ipv6 dhcp relay
```

4. Add a static route on the delegating router to reach the host device.

```
(config)#ipv6 route ::/0 3001:101:0:1::
```

Configure the Requesting Router device:

1. In the WAN interface, configure the address prefix length option (`64`). Get the IPv6 address from the server using `ipv6 address dhcp` command. Enable the requesting router to request the prefix by using `ipv6 dhcp prefix-delegation` and configure the number of prefixes using `ipv6 dhcp client max-delegated-prefixes.`

   Note: The default value of simultaneous prefixes delegated to a single client is 8.The minimum of simultaneous prefixes delegated to a single client is 1 and the maximum is 64.

   Note: If the configured `max-delegated-prefix count` is greater than 30, then configure the lease times greater than 180 seconds.

```
(config)#interface ce16/1
(config-if)#ipv6 dhcp address-prefix-len 64
(config-if)#ipv6 address dhcp
(config-if)#ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
(config-if)#ipv6 dhcp client max-delegated-prefixes 10
```

2. In the LAN interface, configure the command `ipv6 address` to create the IPv6 address by using the DHCP prefix learned from the server and user defined suffix.

```
(config)#interface ce23/1
(config-if)#ipv6 address PREFIX_FROM_SERVER ::1:0:0:0:1/64
```

3. Add a static route on the requesting router to reach the host device.

```
(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135
```

Configure the HOST:

1. In the LAN interface, configure the auto-configuration to get the dynamic IPv6 address from the server.

```
(config)#interface eth3
(config-if)#ipv6 address autoconfig max-address 10
(config if)#exit
(config)#commit
```

2. Add a static route on the host to reach the server.

```
(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135
```

Running configurations

The running configuration for the Delegating Router is as follows:

```
#show running-config
!
ipv6 dhcp relay address 2001:101:0:1::131
!
interface ce1/2
 ipv6 address 2001:101:0:1::130/64
 ipv6 dhcp relay uplink
!
interface ce16/1
 ipv6 address 3001:101:0:1::135/64
 ipv6 dhcp relay
 commit
 end
!
```

The running configuration for the Requesting Router is as follows:

```
#show running-config
!
interface ce16/1
 ipv6 dhcp client max-delegated-prefixes 10
 ipv6 address dhcp
 ipv6 dhcp address-prefix-len 64
 ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
!
interface ce23/1
 ipv6 address PREFIX_FROM_SERVER ::1:0:0:0:1/64
 commit
 end
!
```

The running configuration for the HOST is as follows:

```
#show running-config
!
interface eth3
```

```
     ipv6 address autoconfig max-address 10
     commit
     end
    !
```

Validation

Validate the show output after configuration as shown below.

Delegating Router:

```
#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP,
       v - vrf leaked
Timers: Uptime

IP Route Table for VRF "default"
C       ::1/128 via ::, lo, 00:03:20
C       2001:101:0:1::/64 via ::, ce1/2, 00:02:58
D       2001:db9:c0f::/48 [80/0] via fe80::eac5:7aff:fe51:723b, ce16/1, 00:00:44
C       3001:101:0:1::/64 via ::, ce16/1, 00:00:50
C       fe80::/64 via ::, ce16/1, 00:00:50
#show ipv6 dhcp pd-route
VRF : default
  2001:db9:c0a::/48 via 2001:db9:c0b::, ce16/1, (2024-03-07 06:20:43 - 2024-03-07
06:22:13)
  2001:db9:c0b::/48 via 2001:db9:c09::, ce16/1, (2024-03-07 06:20:42 - 2024-03-07
06:22:12)
  2001:db9:c0c::/48 via 2001:db9:c0d::, ce16/1, (2024-03-07 06:20:39 - 2024-03-07
06:22:09)
  2001:db9:c0d::/48 via 2001:db9:c0e::, ce16/1, (2024-03-07 06:20:38 - 2024-03-07
06:22:08)
  2001:db9:c0e::/48 via 2001:db9:c0f::, ce16/1, (2024-03-07 06:20:37 - 2024-03-07
06:22:07)
  2001:db9:c0f::/48 via fe80::eac5:7aff:fe51:723b, ce16/1, (2024-03-07 06:20:36 - 2024-
03-07 06:22:06)
  2001:db9:c05::/48 via 2001:db9:c06::, ce16/1, (2024-03-07 06:20:45 - 2024-03-07
06:22:15)
  2001:db9:c06::/48 via 2001:db9:c0a::, ce16/1, (2024-03-07 06:20:44 - 2024-03-07
06:22:14)
  2001:db9:c08::/48 via 2001:db9:c0c::, ce16/1, (2024-03-07 06:20:40 - 2024-03-07
06:22:10)
  2001:db9:c09::/48 via 2001:db9:c08::, ce16/1, (2024-03-07 06:20:41 - 2024-03-07
06:22:11)
#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 Servers configured:
  2001:101:0:1::131
```

```
  DHCPv6 IA_PD Route injection: Enabled
  DHCPv6 Duplicate Clients detection: Disabled
  Interface                Uplink/Downlink
  ---------                -------------
  ce16/1                   Downlink
  ce1/2                    Uplink
```

Requesting Router:

```
#show ipv6 dhcp interface

ce16/1 is in client mode
        prefix name: PREFIX_FROM_SERVER
        learned prefix: 2001:db9:c05::/48
        preferred lifetime 0, valid lifetime 60
        interfaces using the learned prefix
                ce23/1    2001:db9:c0f:1::1
                ce23/1    2001:db9:c0e:1::1
                ce23/1    2001:db9:c0d:1::1
                ce23/1    2001:db9:c0c:1::1
                ce23/1    2001:db9:c08:1::1
                ce23/1    2001:db9:c09:1::1
                ce23/1    2001:db9:c0b:1::1
                ce23/1    2001:db9:c0a:1::1
                ce23/1    2001:db9:c06:1::1
                ce23/1    2001:db9:c05:1::1

#show interface ce23/1
Interface ce23/1
  Flexport: Non Control Port (Active)
  Hardware is ETH  Current HW addr: e8c5.7a51.722e
  Physical:e8c5.7a51.722e  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is Router
  Protected Mode is Promiscuous
  Interface index: 10017
  Metric 1 mtu 1500 duplex-full  link-speed 10g
  Debounce timer: disable
  ARP ageing timeout 1500
  <UP,BROADCAST,RUNNING,ALLMULTI,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  Bandwidth 10g
  Maximum reservable bandwidth 10g
    Available b/w at priority 0 is 10g
    Available b/w at priority 1 is 10g
    Available b/w at priority 2 is 10g
    Available b/w at priority 3 is 10g
```

```
    Available b/w at priority 4 is 10g
    Available b/w at priority 5 is 10g
    Available b/w at priority 6 is 10g
    Available b/w at priority 7 is 10g
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  inet6 2001:db9:c05:1::1/64
  inet6 2001:db9:c06:1::1/64
  inet6 2001:db9:c08:1::1/64
  inet6 2001:db9:c09:1::1/64
  inet6 2001:db9:c0a:1::1/64
  inet6 2001:db9:c0b:1::1/64
  inet6 2001:db9:c0c:1::1/64
  inet6 2001:db9:c0d:1::1/64
  inet6 2001:db9:c0e:1::1/64
  inet6 2001:db9:c0f:1::1/64
  inet6 fe80::eac5:7aff:fe51:722e/64
  ND router advertisements are sent approximately every 561 seconds
  ND next router advertisement due in 517 seconds.
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
  5 minute input rate 82 bits/sec, 0 packets/sec
  5 minute output rate 191 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 25 broadcast packets 0
    input packets 25 bytes 2862
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 0 multicast packets 38 broadcast packets 0
    output packets 38 bytes 5540
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

HOST:

```
#show ipv6 interface eth3 brief
Interface            IPv6-Address                                          Admin-Status
eth3                 2001:db9:c05:1:923c:b3ff:fe90:9fa9
                     2001:db9:c06:1:923c:b3ff:fe90:9fa9
                     2001:db9:c08:1:923c:b3ff:fe90:9fa9
                     2001:db9:c09:1:923c:b3ff:fe90:9fa9
                     2001:db9:c0a:1:923c:b3ff:fe90:9fa9
                     2001:db9:c0b:1:923c:b3ff:fe90:9fa9
                     2001:db9:c0c:1:923c:b3ff:fe90:9fa9
```

```
                    2001:db9:c0d:1:923c:b3ff:fe90:9fa9
                    2001:db9:c0e:1:923c:b3ff:fe90:9fa9
                    2001:db9:c0f:1:923c:b3ff:fe90:9fa9
                    fe80::923c:b3ff:fe90:9fa9                          [up/up]
```

DHCP Multiple Prefix Delegation Command

The DHCPv6 Prefix Delegation introduces the following configuration command.

ipv6 dhcp client max-delegated-prefixes

Use this command to configure multiple DHCPv6 prefix delegation for a single client.

Command Syntax

```
ipv6 dhcp client max-delegated-prefixes <1-64>
```

Parameters

`max-delegated-prefixes <1-64>`	Specifies the number of prefixes need for a DHCP client. Default number of DHCP prefixes are 8.

Default

None

Command Mode

Interface mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

This example shows how to configure multiple DHCPv6 prefix delegation for a single client:

```
RR#configure terminal
RR#(config)#interface ce16/1
RR#(config-if)#ipv6 dhcp address-prefix-len 64
RR#(config-if)#ipv6 address dhcp
RR#(config-if)#ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER
RR#(config-if)#ipv6 dhcp client max-delegated-prefixes 10
RR#(config-if)#exit
RR#(config)#commit
```

Revised CLI Commands

The following command is revised:

ipv6 address autoconfig

The existing syntax now includes the newly added parameter `(max-address <1-64>|)`. For more details, refer to ipv6 dhcp prefix-delegation command in the DHCPv6 Prefix Delegation Commands chapter in the *System Management Guide*.

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Border Network Gateway (BNG)	Border Network Gateway is a critical component in the telecommunication network that serves as the entry and exit point between the ISP and the global network.
Customer Premises Equipment (CPE)	Customer Premises Equipment is a networking device located on the customer premises. It is present on the edge of the service provider network, which connects the customer devices to the service provider network.
Delegating Router (DR)	Delegating Router is a network device that delegates the IPv6 address prefixes to the downstream devices.
Identity association for non-temporary addresses (IA_NA)	Identity association for non-temporary addresses is a unique identifier associated with a set of IPv6 addresses assigned to client devices permanently or for a long time.
Local Area Network (LAN)	Local Area Network is a network of devices in a small area that may include a building or home.
Neighbor Discovery Protocol (NDP)	Neighbor Discovery Protocol is a crucial protocol in the IPv6 networks, helping establish the communication and auto-configuration to run the devices in the local network segment seamlessly.
Neighbor Discovery Router Advertisement (NDRA)	Neighbor Discovery Router Advertisement facilitates a network device to advertise the routing information with the neighboring device so that the neighboring devices take the forwarding decision in dynamic routing.
Router Advertisement (RA)	Router Advertisement is a critical component in the IPv6 network. The router sends a message to the devices connected to the LAN to communicate its presence and share the configurations with the LAN host.
Requesting Router (RR)	Requesting Router is a network device that requests the IPv6 address prefixes to the DHCP server to share it with the downstream devices.
Router Solicitation (RS)	Router Solicitation is a component of the neighbor discovery protocol in the IPv6 network where the host sends a message to discover routers in the local area. When a router receives RS, it responds to the host with RA, which includes the configuration.
Wide Area Network (WAN)	Wide Area Network refers to large network that includes multiple LANs and spans over a large geographical area.

CHAPTER 7 DHCPv6 Relay Prefix Delegation Route Injection Configuration

Overview

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can then configure an IPv6 address on its LAN interface using the prefix it received. It will then send router advertisements including the prefix, allowing other devices to auto-configure their own IPv6 addresses.

If the network topology where Prefix Delegation is running has a Relay agent, then a route needs to be injected in Delegating Router, so that the traffic from the DHCP server-side shall be forwarded towards the Requesting Router.

Note:

- Auto-injected routes cannot be leaked between VRFs.
- To ensure smooth auto injection of routes, the operator must ensure that unicast DHCP Renew packets are routed through the Delegating Router.

Topology

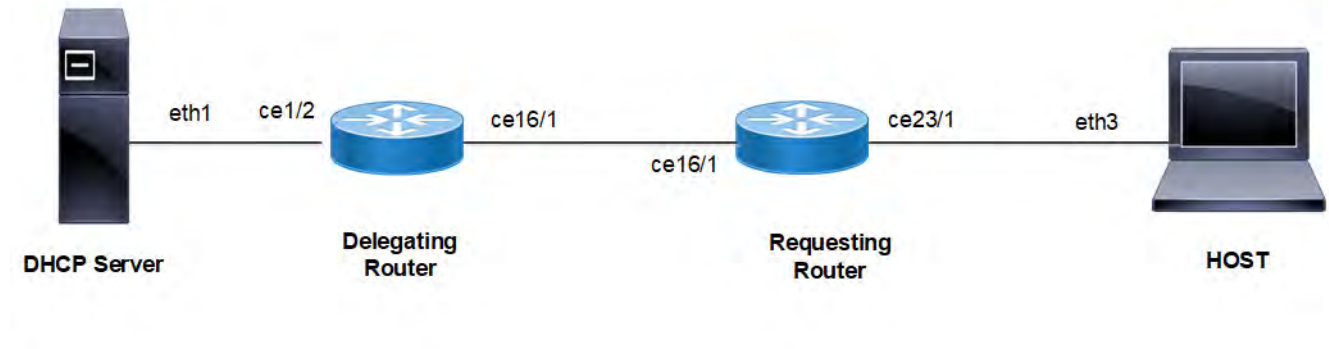


Figure 7-10: DHCPv6 Relay Delegating Configuration

DHCP Relay - Delegating Router (DR)

`#configure terminal`	Enter configure mode.
`(config)#feature dhcp`	Enable the feature DHCP. This is enabled by default.
`(config)#ipv6 dhcp relay`	By default, this will be enabled. It starts the IPv6 DHCP relay service.
`(config)#ipv6 dhcp relay address 2001:101:0:1::131`	The relay address configured should be server interface address connected to Delegating Router.
`(config)#interface ce1/2`	Enter interface mode.
`(config-if)#ipv6 address 2001:101:0:1::130/64`	Configure IPv6 address on the interface ce1/2
`(config-if)#ipv6 dhcp relay uplink`	Configure relay uplink on the device connecting the server.
`(config-if)#exit`	Exit interface mode.

(config)#commit	Commit the candidate configuration to the running
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 address 3001:101:0:1::135/64	Configure IPv6 address on the interface ce16/1
(config-if)#ipv6 dhcp relay	Relay should be configured on the interface connecting to the client.
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running
(config)#ipv6 dhcp relay pd-route-injection	Configure to enable auto route injection.

Requesting Router (RR)

#configure terminal	Enter configure mode.
(config)#interface ce16/1	Enter interface mode.
(config-if)#ipv6 address dhcp	Configure IPv6 address DHCP.
(config-if)#ipv6 dhcp prefix-delegation PREFIX_FROM_SERVER	Configure IPv6 DHCP prefix-delegation
(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface ce23/1	Enter interface mode.
(config-if)#ipv6 address PREFIX_FROM_SERVER ::1:0:0:0:1/64	Configure IPv6 address from the prefix learnt
(config-if)#ipv6 nd ra-interval 4	Configure ra-interval
(config-if)#exit	Exit interface mode.
(config)#ipv6 route 2001:101:0:1::/64 3001:101:0:1::135	Configure static route towards server
(config)#commit	Commit the candidate configuration to the running configuration

HOST

#configure terminal	Enter configure mode.
(config)#interface ce23/1	Enter interface mode.
(config-if)#ipv6 address autoconfig	Configure IPv6 autoconfig
(config if)#exit	Exit interface mode.
(config)#ipv6 route 2001:101:0:1::/64 fe80::ce37:abff:fec9:7426 ce23/1	Configure static route towards server
(config)#commit	Commit the candidate configuration to the running

Linux Host

IPV6_AUTOCONF=yes	IPv6 autoconfig should be set to yes in interface config file.

DHCP Server

`ifconfig eth1 inet6 add 2001:101:0:1::131/64`	Configure IPv6 address on client facing interface
`dhcpd -d -6 -cf /etc/dhcp/dhcpd6.conf eth1`	Start server
`ipv6 route 1212:501:102:1::/64 2001:101:0:1::130`	Configure static route towards Requesting Router

Sample dhcpd6.conf file

```
#
#DHCPv6 Server Configuration file.
#see /usr/share/doc/dhcp*/dhcpd6.conf.sample
#see dhcpd.conf(5) man page
#
preferred-lifetime 400;
default-lease-time 600;

subnet6 2001:101:0:1::/64 {
range6 2001:101:0:1::129 2001:101:0:1::254;
}
subnet6 3001:101:0:1::/64 {
range6 3001:101:0:1::129 3001:101:0:1::254;
prefix6 1212:501:101:: 1212:501:102:: /48;
option dhcp6.name-servers fec0:0:0:1::1;
option dhcp6.domain-search "domain.example";
}
```

Validation

Delegation Router (DR)

```
DR#sh ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: default
  DHCPv6 Servers configured: 2001:101:0:1::131
  DHCPv6 IA_PD Route injection: Enabled
  Interface                Uplink/Downlink
  ---------                -------------
  ce1/2                      Downlink
  ce16/1                     Uplink

DR#sh ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, D- DHCP, R - RIP,
       O - OSPF, IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, E - EVPN  N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, i - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 19:24:04
D      1212:501:102::/48 [80/0] via fe80::eac5:7aff:fe64:4a20, ce16/1, 00:00:01
```

```
C      2001:101:0:1::/64 via ::, xe4, 03:42:58
C      3001:101:0:1::/64 via ::, xe2, 02:51:04
C      4001:101:0:1::/64 via ::, xe5, 03:14:41
C      fe80::/64 via ::, xe9, 00:41:39

#sh ipv6 dhcp pd-route
VRF : default
  1212:501:102::/48 via fe80::eac5:7aff:fe64:4a20, ce16/1, (2019-05-30 14:02:50 - 2
019-05-30 14:04:50)
```

Requesting Router (RR)

```
RR#show ipv6 dhcp interface

ce16/1 is in client mode
prefix name: PREFIX_FROM_SERVER1
learned prefix: 1212:501:102::/48
preferred lifetime 600, valid lifetime 600
interfaces using the learned prefix
ce23/1    1212:501:102:1::1

RR#sh ipv6 interface ce23/1 brief
Interface            IPv6-Address                                    Admin-Status
Ce23/1               *1212:501:102:1::1
                     fe80::ce37:abff:fec9:7426                       [up/up]

RR#show int ce23/1
Interface ce23/1
Scope: both
Flexport: Breakout Control Port (Active): Break Out Enabled
Hardware is ETH  Current HW addr: cc37.abc9.7426
Physical:cc37.abc9.743f  Logical:(not set)
Port Mode is Router
Interface index: 10025
Metric 1 mtu 1500 duplex-full link-speed 1g
Debounce timer: disable
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
Last Flapped: 2021 Mar 02 09:44:05 (00:03:55 ago)
Statistics last cleared: 2021 Mar 02 09:44:05 (00:03:55 ago)
inet6 1212:501:102:1::1/64
inet6 fe80::ce37:abff:fec9:7426/64
ND router advertisements are sent approximately every 571 seconds
ND next router advertisement due in 434 seconds.
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
5 minute input rate 2 bits/sec, 0 packets/sec
5 minute output rate 23 bits/sec, 0 packets/sec
```

HOST

```
[root@localhost ~]#ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:07:E9:A5:23:4C
inet6 addr: 1212:501:102:1:207:e9ff:fea5:234c/64 Scope:Global
inet6 addr: fe80::207:e9ff:fea5:234c/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:196985 errors:0 dropped:0 overruns:0 frame:0
TX packets:5733 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:23542362 (22.4 MiB)  TX bytes:710558 (693.9 KiB)

N4#show ipv6 interface xe7 brief
Interface            IPv6-Address                                    Admin-Status
ce23/1               *1212:501:102:1:6821:5fff:fe55:4a27
                     fe80::6a21:5fff:fe55:4a27                       [up/up]
```

DHCP Command Reference

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 Dynamic Host Configuration Protocol Client

This chapter describes the Dynamic Host Configuration Protocol (DHCP) client commands.

DHCP is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

This chapter contains these commands:

- feature dhcp
- ip address dhcp
- ip dhcp client request
- ipv6 address dhcp
- ipv6 dhcp address-prefix-length
- ipv6 dhcp client request
- ipv6 dhcp client
- show ipv6 dhcp vendor-opts

feature dhcp

Use this command to enable the DHCP client and DHCP relay on the device.

Use the `no` form of this command to disable the DHCP client and DHCP relay and delete any DHCP-related configuration.

Command Syntax

```
feature dhcp
no feature dhcp
```

Parameters

None

Default

By default, feature dhcp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#feature dhcp
```

ip address dhcp

Use this command to get an IP address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the ip dhcp client request command before giving this command to request additional options.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip address dhcp
(config-if)#
```

ip dhcp client request

Use this command to add an option to a DHCP request.

Use the `no` form of this command to remove an option from a DHCP request.

Command Syntax

```
ip dhcp client request dns-nameserver
ip dhcp client request host-name
ip dhcp client request log-server
ip dhcp client request ntp-server
no ip dhcp client request dns-nameserver
no ip dhcp client request host-name
no ip dhcp client request log-server
no ip dhcp client request ntp-server
```

Parameters

`dns-nameserver`	List of DNS name servers (DHCP option 6)
`host-name`	Name of the client (DHCP option 12)
`ntp-server`	List of NTP servers (DHCP option 42)
`log-server`	List of log servers (DHCP option 7)

Default

By default, ip dhcp client request is enabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip dhcp client request ntp-server
```

ipv6 address dhcp

Use this command to get an IPV6 address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the ipv6 dhcp client request command before giving this command to request additional options.

Command Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 address dhcp
(config-if)#
```

ipv6 dhcp address-prefix-length

Use this command to configure the prefix-length for dynamically allocated ipv6 address.

Use the `no` form of this command to unconfigure the prefix-length.

Command Syntax

```
ipv6 dhcp address-prefix-length <1-128>
no ipv6 dhcp address-prefix-length
```

Parameters

`<1-128>`	IPv6 address prefix length

Default

Default ipv6 address prefix length is 128

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.2.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp address-prefix-length 64
(config-if)
```

ipv6 dhcp client request

Use this command to add an option to a DHCPv6 request.

Use the `no` form of this command to remove an option from a DHCPv6 request.

Note:

- Vendor-specific options allow a specific vendor to define a set of DHCP options that really make sense for their device or operating system.
- By default DHCPv6 uses four messages exchange (Solicit, Advertise, Request, and Reply) to obtain configuration parameters from a server. But when rapid-commit is specified, `dhcp6-client` will include a rapid-commit option in solicit messages and wait for an immediate reply instead of advertisements.The Rapid Commit option is used to signal the use of the two message exchange for address assignment.

Command Syntax

```
ipv6 dhcp client request dns-nameserver
ipv6 dhcp client request ntp-server
ipv6 dhcp client request domain-search
ipv6 dhcp client request vendor-specific-information
ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request rapid-commit
no ipv6 dhcp client request vendor-specific-information
no ipv6 dhcp client request domain-search
no ipv6 dhcp client request ntp-server
no ipv6 dhcp client request dns-nameserver
```

Parameters

`dns-nameserver`	List of DNS name servers
`ntp-server`	Request for IPv6 NTP server
`domain-search`	Request for IPv6 domain search
`vendor-specific-information`	Request for IPv6 vendor-specific-information
`rapid-commit`	Request to enable rapid-commit

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS version 5.0

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client request dns-nameserver
(config-if)#

(config)#interface eth0
(config-if)#ipv6 dhcp client request ntp-server
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request domain-search
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request vendor-specific-information
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client request rapid-commit
(config-if)#exit
```

ipv6 dhcp client

Use this command to configure DHCP client options to a DHCPv6 request.

Use the `no` form of this command to remove client options from a DHCPv6 request.

Note:

- `ipv6 dhcp client information-request` is used to get only stateless configuration parameters (i.e., without address).
- DAD-wait-time value is the maximum time (in seconds) that the client should wait for the duplicate address detection (DAD) to complete on an interface.
- DUID option override the default when selecting the type of DUID to use. By default, DHCPv6 dhclient creates an identifier based on the link-layer address (DUID-LL) if it is running in stateless mode (with -S, not requesting an address), or it creates an identifier based on the link-layer address plus a timestamp (DUID-LLT) if it is running in stateful mode (without -S, requesting an address).

Command Syntax

```
ipv6 dhcp client information-request
ipv6 dhcp client dad-wait-time <1-600>
ipv6 dhcp client duid (ll | llt)
no ipv6 dhcp client duid
no ipv6 dhcp client dad-wait-time
no ipv6 dhcp client information-request
```

Parameters

`information-request`	Request to enable information-request
`<1-600>`	DAD wait-time in seconds
`ll`	Link-layer address
`llt`	Link-layer address plus timestamp

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3 and modified in OcNOS version 5.0

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 dhcp client information-request
(config-if)#exit
```

```
(config)#interface eth0
(config-if)#ipv6 dhcp client dad-wait-time 20
(config-if)#exit

(config)#interface eth0
(config-if)#ipv6 dhcp client duid ll
(config-if)#exit
```

show ipv6 dhcp vendor-opts

Use this command to display vendor-specific-information option value given by DHCP server.

Command Syntax

```
show ipv6 dhcp vendor-opts
```

Parameters

None

Command Mode

Executive mode

Applicability

This command is introduced in OcNOS version 5.0

Examples

```
#sh ipv6 dhcp vendor-opts
ifName              vendor-opts
==========          ====================
xe5                 IP Infusion Inc
#
```

CHAPTER 2 Dynamic Host Configuration Protocol Relay

This chapter describes the Dynamic Host Configuration Protocol (DHCP) relay commands.

In small networks with only one IP subnet, DHCP clients communicate directly with DHCP servers. When DHCP clients and associated servers do not reside on the same subnet, a DHCP relay agent can be used to forward DHCP client messages to DHCP server.

The DHCP client broadcasts on the local link, the relay agents receives the broadcast DHCP messages, and then generate a new DHCP message to send out on another interface.

The relay agent sets the gateway IP address (`giaddr` field of the DHCP packet) and, if configured, adds the relay agent information option (option 82) in the packet and forwards it to the DHCP server. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

This chapter contains these commands:

- clear ip dhcp relay option statistics
- clear ipv6 dhcp pd-route (|vrf NAME)
- clear ip dhcp relay statistics
- ip dhcp relay (configure mode)
- ip dhcp relay (interface mode)
- ip dhcp relay (L3VPN)
- ip dhcp relay address
- ip dhcp relay address global
- ip dhcp relay information option
- ip dhcp relay information option always-on
- ip dhcp relay information source-ip
- ip dhcp relay server-group
- ip dhcp relay server-select
- ipv6 dhcp relay (configure mode)
- ipv6 dhcp relay (interface mode)
- ipv6 dhcp relay (L3VPN)
- ipv6 dhcp relay address
- ipv6 dhcp relay address global
- ipv6 dhcp relay pd-route-injection
- ipv6 dhcp relay server-group
- ipv6 dhcp relay server-select
- ipv6 dhcp relay subscriber-id
- ipv6 dhcp relay (L3VPN)
- server A.B.C.D
- server X:X::X:X
- show ip dhcp relay
- show ip dhcp relay address
- show ip dhcp relay option statistics

- show ip dhcp relay statistics
- show ipv6 dhcp pd-route
- show ipv6 dhcp relay
- show ipv6 dhcp relay address
- show running-config dhcp

clear ip dhcp relay option statistics

Use this command to clear ipv4 relay option statistics.

command syntax

```
clear ip dhcp relay option statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
#clear ip dhcp relay option statistics
```

clear ipv6 dhcp pd-route (|vrf NAME)

Use this command to clear the routes in RIBD module learnt as part of Route injection feature.

Command Syntax

```
clear ipv6 dhcp pd-route (|vrf NAME)
```

Parameters

NAME	Name of the VRF

Default

No default value

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#clear ipv6 dhcp pd-route vrf vrf1
```

clear ip dhcp relay statistics

Use this command to clear ipv4 relay statistics.

Command syntax

```
clear ip dhcp relay statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
#clear ip dhcp relay statistics
```

ip dhcp relay (configure mode)

Use this command to enable the DHCP relay agent. The DHCP relay starts forwarding packets to the DHCP server address once configured.

Use the `no` form of this command to disable the DHCP relay agent.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

By default, this feature is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip dhcp relay

#configure terminal
(config)#no ip dhcp relay
```

ip dhcp relay (interface mode)

Use this command to configure an interface as a DHCP client-facing port.

Use the `no` form of this command to remove an interface as a DHCP client-facing port.

Command Syntax

```
ip dhcp relay
no ip dhcp relay
```

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ip dhcp relay
```

ip dhcp relay (L3VPN)

Use this command to specify IPv4 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv4 DHCP relay.

Command Syntax

```
ip dhcp relay (uplink|downlink) (l3vpn)
no ip dhcp relay (uplink|downlink) (l3vpn)
```

Parameters

`uplink`	DHCP Relay uplink interface
`downlink`	DHCP Relay downlink interface
`l3vpn`	L3VPN interface

Default

No default value is specified.

Command Mode

Configure and VRF mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ip dhcp relay uplink l3vpn
```

ip dhcp relay address

Use this command to set an IPv4 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove the IP address of a DHCP server.

User must enable the DHCP relay feature with the ip dhcp relay (configure mode) command to configure server address.

Command Syntax

```
ip dhcp relay address A.B.C.D
no ip dhcp relay address A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127

#configure terminal
(config)#ip dhcp relay address 198.51.100.127
```

ip dhcp relay address global

When the IPv4 DHCP server resides in a different VPN or global space that is different from the VPN, then use this command to specify the name of the VRF or global space in which the DHCP server resides.

Use the no form of this command to remove the VRF in which IPv4 DHCP server resides.

Command Syntax

```
ip dhcp relay address A.B.C.D global (|VRF-NAME)
no ip dhcp relay address A.B.C.D global
```

Parameters

A.B.C.D	IPv4 address of the DHCP server
VRF-NAME	Name of VRF where the DHCP server is present

Default

If no input given, default VRF is the default Value.

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay address 198.51.100.127 global

#configure terminal
(config)#ip dhcp relay address 198.51.100.127 global vrf1
```

ip dhcp relay information option

Use this command to enable the device to insert and remove option 82 information in DHCP packets forwarded by the relay agent.

The option 82 suboption remote-id can be configured either as hostname or any string provided by the User.

Use the `no` form of this command to disable inserting and removing option-82 information.

Command Syntax

```
ip dhcp relay information option (|remote-id (hostname|WORD))
no ip dhcp relay information option (|remote-id)
```

Parameters

`remote-id`	Remote host Identifier, can either be the System's hostname or a user-specified string.
`WORD`	Specify a string as remote-id (Maximum 255 alphanumeric characters).

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option remote-id hostname

#configure terminal
(config)#ip dhcp relay information option

#configure terminal
(config)#no ip dhcp relay information option
```

ip dhcp relay information option always-on

Use this command to enable the device to insert options 82 information in DHCP packets forwarded by the relay-agent and keep them while forwarding to client.

Use the `no` form of this command to disable the option-82 always-on information.

Command Syntax

```
ip dhcp relay information option always-on
no ip dhcp relay information option always-on
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option always-on

#configure terminal
(config)#ip dhcp relay information option always-on

#configure terminal
(config)#no ip dhcp relay information option always-on
```

ip dhcp relay information source-ip

Use this command to enable DHCP relay option 82 link selection.

Use the no form of this command to disable DHCP relay option 82 link selection.

Command Syntax

```
ip dhcp relay information source-ip A.B.C.D
no ip dhcp relay information source-ip
```

Parameters

A.B.C.D	IPv4 address

Default

No default value is specified.

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3.6.

Example

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp relay information option source-ip 2.2.2.2

#configure terminal
(config)#ip dhcp relay information option source-ip 3.3.3.3
```

ipv6 dhcp relay (configure mode)

Use this command to enable the DHCP IPv6 relay agent.

Use the `no` form of this command to disable the DHCP IPv6 relay agent.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 dhcp relay

#configure terminal
(config)#no ipv6 dhcp relay
```

ipv6 dhcp relay (interface mode)

Use this command to configure an interface as a DHCPv6 client-facing port.

Use the `no` form of this command to remove an interface as a DHCPv6 client-facing port.

Command Syntax

```
ipv6 dhcp relay
no ipv6 dhcp relay
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 dhcp relay
```

ipv6 dhcp relay (L3VPN)

Use this command to specify IPv6 DHCP relay to use tunnel interfaces as Uplink/Downlink.

Use the `no` form of this command to remove the usage of tunnel interfaces in IPv6 DHCP relay.

Command Syntax

```
ipv6 dhcp relay (uplink|downlink) (l3vpn)
no ipv6 dhcp relay (uplink|downlink) (l3vpn)
```

Parameters

`uplink`	DHCP Relay uplink interface
`downlink`	DHCP Relay downlink interface
`l3vpn`	L3VPN interface

Default

No default value is specified.

Command Mode

Configure and VRF mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay uplink l3vpn
(config-vrf)#end

#configure terminal
(config)#ipv6 dhcp relay uplink l3vpn
```

ipv6 dhcp relay address

Use this command to set an IPv6 address of a DHCP server to which a DHCP relay agent forwards client requests.

Use the `no` form of this command to remove an IPv6 address of a DHCP server.

User must enable the IPv6 DHCP relay feature with the ipv6 dhcp relay (configure mode) command to configure server address.

Command Syntax

```
ipv6 dhcp relay address X:X::X:X
no ipv6 dhcp relay address X:X::X:X
```

Parameters

`X:X::X:X`	IPv6 address of the DHCP server

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced before OcNOS version 1.3 and was changed in OcNOS version 1.3.8.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F

#configure terminal
(config)#ipv6 dhcp relay address 2001:db8::7F
```

ipv6 dhcp relay address global

When the IPv6 DHCP server resides in a different VPN or global space that is different from the VPN, then use this command to specify the name of the VRF or global space in which the DHCP server resides.

Use the no form of this command to remove the VRF in which IPv6 DHCP server resides.

Command Syntax

```
ipv6 dhcp relay address X:X::X:X global (|VRF-NAME)
no ipv6 dhcp relay address X:X::X:X global
```

Parameters

`X:X::X:X`	IPv6 address of the DHCP server
`VRF-NAME`	Name of VRF where the DHCP server is present

Default

If no input given, default VRF is the default Value.

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp relay address 2001:db8::7F global

#configure terminal
(config)#ipv6 dhcp relay address 2001:db8::7F global vrf1
```

ipv6 dhcp relay pd-route-injection

Use this command to enable the Route Injection of the delegated prefixes in DHCP Relay.

Use the no form of this command to disable Route Injection.

Command Syntax

```
ipv6 dhcp relay pd-route-injection
no ipv6 dhcp relay pd-route-injection
```

Parameters

None

Default

By default this feature is disabled.

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#configure terminal
(config)# ip vrf vrf1
(config-vrf)# ipv6 dhcp relay pd-route-injection

#configure terminal
(config)#ipv6 dhcp relay pd-route-injection
```

ipv6 dhcp relay subscriber-id

Use this command to configure subscriber-ID for IPv6 DHCP relay.

Use `no` form of this command to disable subscriber-id.

Command Syntax

```
ipv6 dhcp relay information option subscriber-id WORD
no ipv6 dhcp relay information option subscriber-id
```

Parameters

`WORD`	Subscriber ID

Default

No default value is specified.

Command Mode

Configuration mode and VRF mode

Applicability

This command is introduced in OcNOS version 5.0

Examples

```
#configure terminal
(config)#ipv6 dhcp relay information option subscriber-id test
(config)#exit
```

show ip dhcp relay

Use this command to display DHCP relay status including DHCP server addresses configured on interfaces.

Command Syntax

```
show ip dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay
DHCP relay service is Enabled.
VRF Name: vrf1
  Option 82: Enabled
  Remote Id: ocnos-device
  Link selection Source-IP: 1.4.5.6
  DHCP Servers configured: 9.9.9.9 8.8.8.8
  Interface                Uplink/Downlink
  ---------                -------------
  ge10                     Uplink
  ge28                     Downlink
VRF Name: default
  Option 82: Enabled
  Remote Id: OcNOS
  Link selection Source-IP: 1.2.3.4
  DHCP Servers configured: 1.1.1.1 2.2.2.2
  Interface                Uplink/Downlink
  ---------                -------------
  ge11                     Uplink
  ge27                     Downlink
```

show ip dhcp relay address

Use this command to display DHCP relay addresses.

Command Syntax

```
show ip dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ip dhcp relay address
VRF Name: vrf1
  DHCP Servers configured: 9.9.9.9 8.8.8.8
VRF Name: default
  DHCP Servers configured: 1.1.1.1 2.2.2.2
```

show ip dhcp relay option statistics

Use this command to display IPv4 DHCP Relay Agent Option(Option82) packet statistics

command syntax

```
show ip dhcp relay option statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
#sh ip dhcp relay option statistics
VRF Name: default
Remote ID : OcNOS
Circuit ID : ge5
Number of packets forwarded without agent options  : 0
Dropped pkts due to bad relay agent information option : 0
Dropped pkts due to no RAI option match found : 0
Circuit ID option is not matching with known circuit ID : 0
Circuit ID option in matching RAI option was missing : 0
#
```

show ip dhcp relay statistics

Use this command to display IPv4 DHCP relayed packet statistics.

Note: DHCPv6 relay statistics is not supported

command syntax

```
show ip dhcp relay statistics
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 1.3.9.

Examples

```
#sh ip dhcp relay statistics
VRF Name: default
Packets sent with a bogus giaddr : 0
Packets relayed from client to server : 12
Errors sending packets to servers : 0
Packets relayed from server to client : 1
Errors sending packets to clients : 0
#
```

show ipv6 dhcp pd-route

Use this command to display the routes and their properties installed as part of the Route Injection feature

Command Syntax

```
show ipv6 dhcp pd-route
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#show ipv6 dhcp pd-route
VRF : vrf1
  4002:db8:1bff::/48 via xe9 (2019-02-14 10:50:18 - 2019-02-14 10:51:58)
```

show ipv6 dhcp relay

Use this command to display DHCP IPv6 relay status including DHCP IPv6 server addresses configured on interfaces.

Command Syntax

```
show ipv6 dhcp relay
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay
IPv6 DHCP relay service is Enabled.
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge35                     Uplink
  xe50                     Downlink
VRF Name: default
  DHCPv6 Servers configured: 3001::1
  Interface                Uplink/Downlink
  ---------                -------------
  ge34                     Uplink
  xe49                     Downlink
```

show ipv6 dhcp relay address

Use this command to display DHCP IPv6 relay addresses.

Command Syntax

```
show ipv6 dhcp relay address
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show ipv6 dhcp relay address
VRF Name: vrf1
  DHCPv6 Servers configured: 2001::1
VRF Name: default
  DHCPv6 Servers configured: 3001::1
```

show running-config dhcp

Use this command to display DHCP settings in the running configuration.

Command Syntax

```
show running-config dhcp
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 1.3.8.

Examples

```
#show running-config dhcp
ip vrf vrf1
 ip dhcp relay information option remote-id hostname
 ip dhcp relay address 1.1.1.2

ip dhcp relay information option remote-id hostname
ip dhcp relay information source-ip 5.4.3.2
ip dhcp relay address 1.1.1.1
```

CHAPTER 3 DHCPv6 Prefix Delegation Commands

This chapter describes the Dynamic Host Configuration Protocol (DHCP) v6 Prefix delegation commands.

The prefix delegation feature lets a DHCP server assign prefixes chosen from a global pool to DHCP clients. The DHCP client can configure an IPv6 address on its LAN interface using the prefix it received. Then it send router advertisements including the prefix, allowing other devices to auto configure their own IPv6 addresses.

Enable OcNOS device DHCP Client to receive the prefixes from external DHCP Server and enable IPv6 address autoconfiguration of LAN interfaces and the respective host machines.

This feature enables the service providers to assign IP for the Customer Premise Equipment acting as a router between the service providers core network and subscribers internal network.

This chapter contains these commands:

- ipv6 address
- ipv6 dhcp client max-delegated-prefixes
- ipv6 dhcp prefix-delegation
- show ipv6 dhcp interface

ipv6 address

Use this command to configure the global IPv6 address using the learned prefix and user provided suffix.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
ipv6 address PREFIX-NAME X:X::X:X/M
no ipv6 address PREFIX-NAME X:X::X:X/M
```

Parameters

`PREFIX-NAME`	Name of the prefix which stores the address-prefix learned using prefix delegation enabled in the client interface
`X:X::X:X/M`	Suffix address consists subnet id and host address. This value must start with '::', and end with a /64 bit prefix.

Default

DHCPv6 IA_PD option is not requested by default.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 address dhcp
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#

(config)#interface xe3
(config-if)#ipv6 address prefix_xe1 ::1:0:0:0:1/64
(config-if)#
```

ipv6 dhcp prefix-delegation

Use this command to enable the DHCPv6 client to request the prefix (IA_PD) for the interface.

Prefixes delegated by the DHCP server are stored in the general prefix called `PREFIX-NAME`.

Use the no form of command to remove the IA_PD option from the DHCPv6 client request. This command also deletes the learned prefix if it exists.

Command Syntax

```
ipv6 dhcp prefix-delegation PREFIX-NAME
no ipv6 dhcp prefix-delegation
```

Parameters

`PREFIX-NAME`	Name of the learned prefix (maximum length 255 characters).

Default

DHCPv6 Prefix delegation client is not enabled by default.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ipv6 dhcp prefix-delegation prefix_xe1
(config-if)#
```

show ipv6 dhcp interface

Use this command to display the DHCPv6 prefix delegation information in the Requesting Router device.

Command Syntax

```
show ipv6 dhcp interface
```

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced in OcNOS version 4.2.

Examples

```
#show ipv6 dhcp interface
      xe1 is in client mode
      prefix name: prefix_xe1
      learned prefix: 1212:501:102::/48
      preferred lifetime 600, valid lifetime 600
      interfaces using the learned prefix
      xe3    1212:501:102:1::1
```

CHAPTER 4 DHCP Server Commands

This chapter describes the Dynamic Host Configuration Protocol (DHCP) server commands.

A DHCP server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. A DHCP server relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients.

This chapter contains these commands:

- address range low-address A.B.C.D (high-address A.B.C.D|)
- address range low-address X:X::X:X (high-address X:X::X:X|)
- boot-file
- dns-server A.B.C.D
- dns-server X:X::X:X
- domain-name
- host-name
- ip dhcp server (interface mode)
- ip dhcp server default-lease-time
- ip dhcp server max-lease-time
- ip dhcp server pool
- ipv6 dhcp server (interface mode)
- ipv6 dhcp server pool
- ipv6 dhcp server preference
- ipv6 dhcp server rapid-commit
- log-server
- network A.B.C.D netmask A.B.C.D
- network X:X::X:X netmask <1-128>
- ntp-server A.B.C.D
- ntp-server X:X::X:X
- prefix high-range X:X::X:X low-range X:X::X:X netmask <1-128>
- routers A.B.C.D
- temporary address X:X::X:X
- tftp-server
- vendor-options

© 2025 IP Infusion Inc. Proprietary

address range low-address A.B.C.D (high-address A.B.C.D|)

Use this command to create an address-range in the IPv4 DHCP server pool.

Use the `no` form of this command to delete an address-range from the IPv4 DHCP server pool.

Command Syntax

```
address range low-address A.B.C.D (high-address A.B.C.D|)
no address range low-address A.B.C.D (high-address A.B.C.D|)
```

Parameters

`A.B.C.D`	The low range of the IPv4 addresses that the DHCP server should assign to DHCP clients.
`A.B.C.D`	The high range of the IPv4 addresses that the DHCP server should assign to DHCP clients.

Default

No default value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#address range low-address 3.3.3.1 high-address 3.3.3.4

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#address range low-address 3.3.3.1 high-address 3.3.3.4
```

address range low-address X:X::X:X (high-address X:X::X:X|)

Use this command to create an address-range in the IPv6 DHCP server pool.

Use the `no` form of this command to delete an address-range from the IPv6 DHCP server pool.

Command Syntax

```
address range low-address X:X::X:X (high-address X:X::X:X|)
no address range low-address X:X::X:X (high-address X:X::X:X|)
```

Parameters

`X:X::X:X`	The low range of the IPv6 addresses that the DHCP server should assign to DHCP clients.
`X:X::X:X`	The high range of the IPv6 addresses that the DHCP server should assign to DHCP clients.

Default

No default value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#address range low-address 2001::1 high-address 2001::124

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#address range low-address 2001::1 high-address 2001::124
```

boot-file

Use this command to specify a boot file in the IPv4 DHCP server pool.

Use the `no` form of this command to delete a boot file from the IPv4 DHCP server pool.

Command Syntax

```
boot-file BOOTFILE
no boot-file BOOTFILE
```

Parameters

`BOOTFILE`	Name of the boot file (maximum 63 alphanumeric characters)

Default

No default Value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#boot-file ocnos-boot-file

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#boot-file ocnos-boot-file
```

dns-server A.B.C.D

Use this command to specify a DNS name server in the IPv4 DHCP server pool. Multiple name servers can be added to the pool.

Use the `no` form of this command to delete a DNS name server details from the IPv4 DHCP server pool.

Command Syntax

```
dns-server A.B.C.D
no dns-server A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 DNS name server address

Default

No default value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#dns-server 10.12.3.23

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#dns-server 10.12.3.23
```

dns-server X:X::X:X

Use this command to specify a DNS name server in the IPv6 DHCP server pool. Multiple DNS name servers can be added to the pool.

Use the `no` form of this command to delete a DNS name server from the IPv6 DHCP server pool.

Command Syntax

```
dns-server X:X::X:X
no dns-server X:X::X:X
```

Parameters

`X:X::X:X`	DNS IPv6 name server address

Default

No default value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#dns-server 2001::2

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#dns-server 2001::2
```

domain-name

Use this command to set the domain name in the IPv6 DHCP server pool.

Use the `no` form of this command to delete the domain name from the IPv6 DHCP server pool.

Command Syntax

```
domain-name NAME
no domain-name NAME
```

Parameters

`NAME`	Name of the domain (maximum 63 alphanumeric characters)

Default

No default Value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#domain-name ipinfusion.com

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#domain-name ipinfusion.com
```

host-name

Use this command to set a host name in the IPv4 DHCP server pool.

Use the `no` form of this command to delete the host name from the IPv4 DHCP server pool.

Command Syntax

```
host-name NAME
no host-name NAME
```

Parameters

`NAME`	Name of the host (maximum 63 alphanumeric characters)

Default

No default value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#host-name dhcp-server

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#host-name dhcp-server
```

ip dhcp server (interface mode)

Use this command to configure an interface as a DHCP server starting interface.

Use the `no` form of this command to remove an interface as a DHCP server starting interface.

Command Syntax

```
ip dhcp server
no ip dhcp server
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ip dhcp server
```

ip dhcp server default-lease-time

Use this command to set the default lease time for the DHCP server to be shared with the DHCP client.

Use the `no` form of this command to delete the IPv4 default lease time configuration.

Command Syntax

```
ip dhcp server default-lease-time SECONDS
no ip dhcp server default-lease-time
```

Parameters

`SECONDS`	Default lease time in seconds. Default is 86400 seconds.

Default

Default value is 86400 seconds

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server default-lease-time 500

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server default-lease-time 400
```

ip dhcp server max-lease-time

Use this command to set the maximum lease time for the DHCP server to be shared with the DHCP client.

Use the `no` form of this command to delete the IPv4 maximum lease time configuration.

Command Syntax

```
ip dhcp server max-lease-time SECONDS
no ip dhcp server max-lease-time
```

Parameters

`SECONDS`	Maximum lease time in seconds. Default is 86400 seconds.

Default

Default value is 86400 seconds

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server max-lease-time 500

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server max-lease-time 400
```

ip dhcp server pool

Use this command to create a IPv4 DHCP server pool.

Use the `no` form of this command to delete a IPv4 DHCP server pool.

Command Syntax

```
ip dhcp server pool NAME
no ip dhcp server pool NAME
```

Parameters

`NAME`	Name of the pool (maximum 63 alphanumeric characters)

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
```

ipv6 dhcp server (interface mode)

Use this command to set an interface as a DHCPv6 server starting interface.

Use the `no` form of this command to remove an interface as a DHCPv6 server starting interface.

Command Syntax

```
ipv6 dhcp server
no ipv6 dhcp server
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ipv6 dhcp server
```

ipv6 dhcp server pool

Use this command to create a IPv6 DHCP server pool.

Use the `no` form of this command to delete a IPv6 DHCP server pool.

Command Syntax

```
ipv6 dhcp server pool NAME
no ipv6 dhcp server pool NAME
```

Parameters

`NAME`	Name of the pool (maximum 63 alphanumeric characters)

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool test-pool

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool test-pool
```

ipv6 dhcp server preference

Use this command to make a DHCPv6 server preferred.

Use the `no` form of this command to disable a server preference.

Command Syntax

```
ipv6 dhcp server preference
no ipv6 dhcp server preference
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server preference

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server preference
```

ipv6 dhcp server rapid-commit

Use this command to enable the DHCP client to obtain configuration parameters from the server through a rapid two message exchange (solicit and reply).

Use the `no` form of this command to disable the IPv6 DHCP server rapid-commit option.

Command Syntax

```
ipv6 dhcp server rapid-commit
no ipv6 dhcp server rapid-commit
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server rapid-commit

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server rapid-commit
```

log-server

Use this command to specify a log server in the IPv4 DHCP server pool. Multiple log servers can be added to the pool.

Use the `no` form of this command to delete a log server from the IPv4 DHCP server pool.

Command Syntax

```
log-server A.B.C.D
no log-server A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 log server address

Default

No default value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#log-server 10.12.43.97

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#log-server 10.12.43.97
```

network A.B.C.D netmask A.B.C.D

Use this command to specify a network and netmask in the IPv4 DHCP server pool.

Use the `no` form of this command to delete the network and netmask from the IPv4 DHCP server pool.

Command Syntax

```
network A.B.C.D netmask A.B.C.D
no network A.B.C.D netmask A.B.C.D
```

Parameters

`A.B.C.D`	Network part of the subnet to use to assign IPv4 addresses to hosts
`A.B.C.D`	Mask part of the subnet to use to assign IPv4 addresses to host

Default

No default value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#network 3.3.3.0 netmask 255.255.255.0

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#network 3.3.3.0 netmask 255.255.255.0
```

network X:X::X:X netmask <1-128>

Use this command to specify a network and netmask in the IPv6 DHCP server pool.

Use the `no` form of this command to delete the network and netmask from the IPv6 DHCP server pool.

Command Syntax

```
network X:X::X:X netmask <1-128>
no network X:X::X:X netmask <1-128>
```

Parameters

`X:X:X:X`	Network part of the subnet to use to assign IPv6 addresses to hosts
`<1-128>`	Mask part of the subnet to use to assign IPv6 addresses to host

Default

No default value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#network 2001:: netmask 64

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#network 2001:: netmask 64
```

ntp-server A.B.C.D

Use this command to specify an NTP server in the IPv4 DHCP server pool. Multiple NTP servers can be added to the pool.

Use the `no` form of this command to delete an NTP server from the IPv4 DHCP server pool.

Command Syntax

```
ntp-server A.B.C.D
no ntp-server A.B.C.D
```

Parameters

`A.B.C.D`	NTP IPv4 server address

Default

No default Value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#ntp-server 10.12.43.97

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#ntp-server 10.12.43.97
```

© 2025 IP Infusion Inc. Proprietary

ntp-server X:X::X:X

Use this command to specify an NTP server in the IPv6 DHCP server pool. Multiple NTP servers can be added to the pool.

Use the `no` form of this command to delete an NTP server from the IPv6 DHCP server pool.

Command Syntax

```
ntp-server X:X::X:X
no ntp-server X:X::X:X
```

Parameters

`X:X::X:X`	NTP IPv6 server address

Default

No default Value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#ntp-server 2001::2

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#ntp-server 2001::2
```

prefix high-range X:X::X:X low-range X:X::X:X netmask <1-128>

Use this command to add the DHCPv6 prefix range in the IPv6 DHCP server pool used for prefix delegation.

Use the `no` form of this command to delete the prefix-range from the IPv6 DHCP server pool.

Command Syntax

```
prefix high-range X:X::X:X low-range X:X::X:X netmask <1-128>
no prefix high-range X:X::X:X low-range X:X::X:X netmask <1-128>
```

Parameters

`X:X::X:X`	IPv6 prefix high range value
`X:X::X:X`	IPv6 prefix low range value
`<1-128>`	Network mask

Default

No default value is specified

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#prefix high-range 3001:db8:1234:: low-range 3001:db8:1c0f:: netmask 48

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#prefix high-range 3001:db8:1234:: low-range 3001:db8:1c0f:: netmask 48
```

routers A.B.C.D

Use this command to specify the routers in the IPv4 DHCP server pool.

Use the `no` form of this command to delete an routers from the IPv4 DHCP server pool.

Command Syntax

```
routers A.B.C.D
no routers A.B.C.D
```

Parameters

`A.B.C.D`	NTP IPv4 server address

Default

None

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#routers 10.12.43.97

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test--pool
(dhcp-config)#routers 10.12.43.97
```

temporary address X:X::X:X

Use this command to add an IPv6 temporary address to the IPv6 DHCP server pool.

Use the `no` form of this command to delete an IPv6 temporary address from the IPv6 DHCP server pool.

Command Syntax

```
temporary address X:X::X:X
no temporary address
```

Parameters

`X:X::X:X`	IPv6 DHCP Temporary address

Default

No default value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#temporary address 2001::

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#temporary address 2001::
```

tftp-server

Use this command to specify a TFTP server in the IPv4 DHCP server pool.

Use the `no` form of this command to delete a TFTP server from the IPv4 DHCP server pool.

Command Syntax

```
tftp-server A.B.C.D
no tftp-server A.B.C.D
```

Parameters

`A.B.C.D`	TFTP IPv4 server address

Default

No default Value is specified

Command Mode

DHCP configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ip dhcp server pool test-pool
(dhcp-config)#tftp-server 10.12.43.97

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ip dhcp server pool test-pool
(dhcp-config)#tftp-server 10.12.43.97
```

vendor-options

Use this command to specify vendor options in the IPv6 DHCP server pool.

Use the `no` form of this command to delete the vendor options from the IPv6 DHCP server pool.

Command Syntax

```
vendor-options VENDOR-OPTS
no vendor-options VENDOR-OPTS
```

Parameters

`VENDOR-OPTS`	Vendor option details

Default

No default Value is specified

Command Mode

DHCP6 configure mode

Applicability

This command was introduced in OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#vendor-options 00:00:09:bf:63

#configure terminal
(config)#ip vrf vrf1
(config-vrf)#ipv6 dhcp server pool ipv6_pool
(dhcp6-config)#vendor-options 00:00:09:bf:63
```

DNS Configuration

CHAPTER 1 DNS Configuration

Overview

The Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. When a domain name is used, DNS service translates the name into the corresponding IP address. If one DNS server does not know how to translate a particular domain name, it gathers information from other Domain Name Systems to obtain the correct IP address.

Support for In-band Management over default VRF

OcNOS offers support for DNS over default, management VRFs, and custom VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on management VRF.

Topology

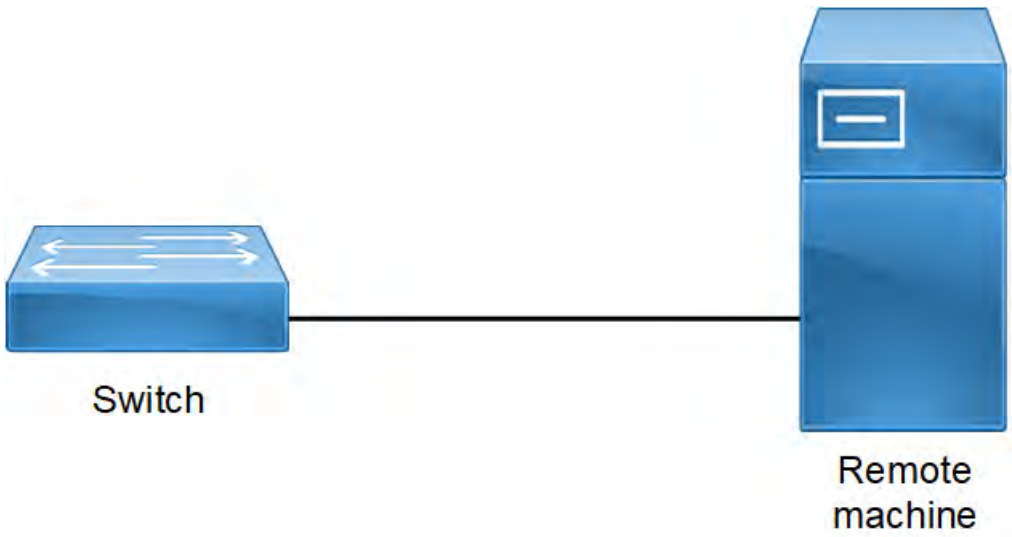


Figure 1-11: DNS sample topology

VRF Management Configuration-IPv4

`#configure terminal`	Enter Configure mode.
`(config)#ip name-server vrf management 10.12.17.11`	This add a IPv4 Name Server to the DNS.
`(config)#ip name-server vrf management 10.1.1.2`	This add a IPv4 Name Server to the DNS.
`(config)#ip host vrf management BINGO 10.1.1.1`	This will add IPv4 host to the DNS

(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode.

Validation Commands

```
#show hosts vrf management
         VRF: default

 DNS lookup is disabled
 Default domain is empty
 DNS domain list is empty

 Name Servers        : 10.12.17.11 10.1.1.2
Host                                                                    Address

----                                                                    -------

BINGO                                                                   10.1.1.1


 * - Values assigned by DHCP Client.
```

VRF Management Configuration-IPv6

#configure terminal	Enter Configure mode.
(config)#ip name-server vrf management 3001::1	This add a IPv6 Name Server to the DNS.
(config)#ip host vrf management bingo 5001::1	This will add IPv6 host to the DNS
(config)#commit	Commit the Candidate configuration to the running configuration
(config)#exit	Exit configure mode.

Validation Commands

```
OcNOS#show hosts vrf management
       VRF: management

DNS lookup is enabled
 Default domain is empty
 DNS domain list is empty

 Name Servers        : 3001::1
Host                                                                    Address
----                                                                    -------
bingo                                                                   5001::1

 * - Values assigned by DHCP Client.
OcNOS#
```

User Defined VRF Configuration-IPv4

#configure terminal	Enter configure mode
(config)# ip vrf vrf1	Configuring user defined vrf in global
(config)#commit	Commit the candidate configuration to the running configuration
#configure terminal	Enter Configure mode
(config)#ip domain-lookup vrf vrf1	This command is to enable DNS for user-defined vrf
(config)#ip name-server vrf vrf1 10.12.17.11	This add a IPv4 Name Server to the DNS
(config)#ip name-server vrf vrf1 10.1.1.2	This add a IPv4 Name Server to the DNS
(config)#ip host vrf vrf1 BINGO 10.1.1.1	This will add IPv4 host to the DNS
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

Validation Commands

```
#show hosts vrf vrf1
VRF: vrf1
DNS lookup is enabled
 Default domain is empty
 DNS domain list is empty
Name Servers: 10.12.17.11 10.1.1.2
HostAddress
BINGO10.1.1.1
* - Values assigned by DHCP Client.
```

User Defined VRF Configuration-IPv6

#configure terminal	Enter Configure mode
(config)#ip name-server vrf vrf1 3001::1	This add a IPv6 Name Server to the DNS
(config)#ip host vrf vrf1 bingo 5001::1	This will add IPv6 host to the DNS
(config)#commit	Commit the Candidate configuration to the running configuration
(config)#exit	Exit configure mode

Validation Commands

```
OcNOS#show hosts vrf vrf1
VRF: vrf1

DNS lookup is disabled
 Default domain is empty
 DNS domain list is empty

Name Servers: 3001::1
HostAddress
```

```
-----------
bingo5001::1
* - Values assigned by DHCP Client.
```

CHAPTER 2 DNS Relay Configuration

DNS relay is used to forward DNS request and reply packets between the DNS client and DNS server. In the network where DNS relay is used, the DNS client sends DNS request packets to the DNS relay. The DNS relay forwards request packets to the DNS server and sends reply packets to the DNS client, and domain resolution is realized.

Topology

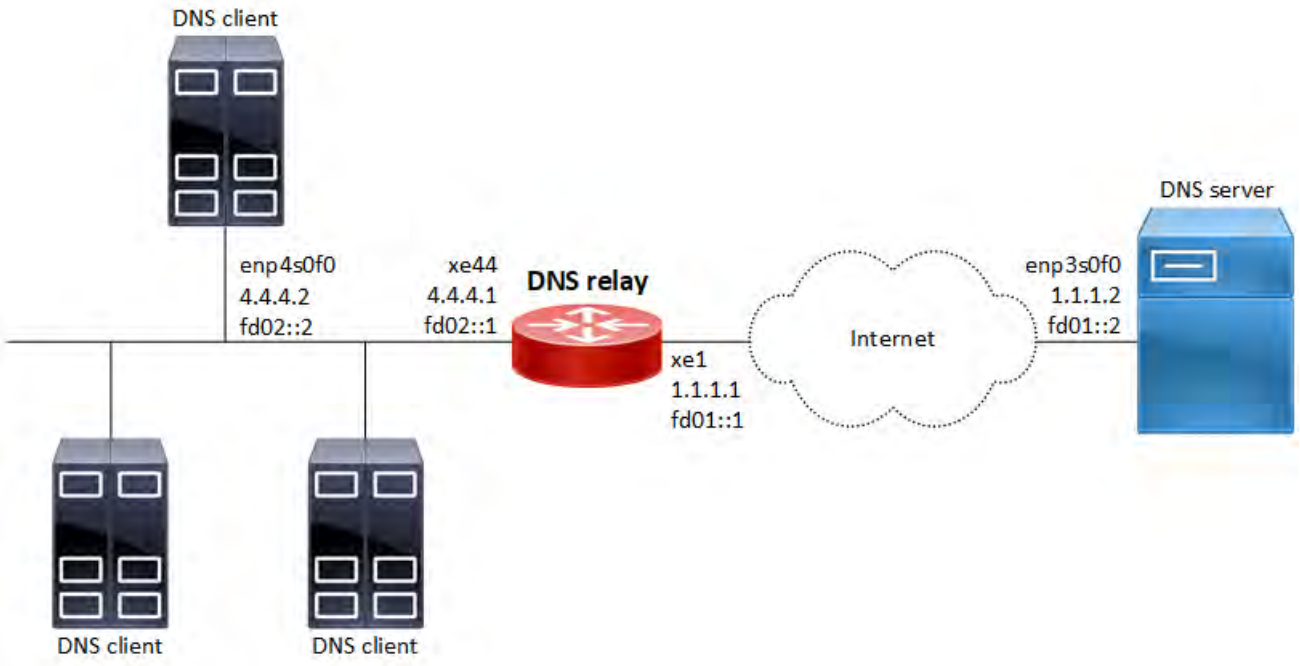


Figure 2-12: DNS relay configuration

Linux Configuration on the DNS client

```
1. sudo ifconfig enp4s0f0 4.4.4.2/24
2. sudo ifconfig enp4s0f0 inet6 add fd02::2/16
3. echo nameserver fd02::1 >> /etc/resolv.conf
4. echo nameserver 4.4.4.1 >> /etc/resolv.conf
```

Linux Configuration on the DNS server

1. `sudo ifconfig enp3s0f0 1.1.1.2/24`
2. `sudo ifconfig enp3s0f0 inet6 add fd01::2/16`
3. Install and configure BIND9:

a. `apt-get -y update && apt install -y bind9`

b. Configure 'forwarders' section in the `/etc/bind/named.conf.options` file like this:

```
forwarders  { 8.8.8.8;  2001:4860:4860::8888; };
```

OcNOS Configuration

`#configure terminal`	Enter configure mode
`(config)#ip dns relay address 1.1.1.2`	Set the IPv4 address of a DNS server
`(config)#ipv6 dns relay address fd01::2`	Set the IPv6 address of a DNS server
`(config)#commit`	Commit the configuration
`(config)#interface xe44`	Enter interface mode (interface connected to client)
`(config-if)#ip address 4.4.4.1/24`	Assign an IPv4 address to the interface
`(config-if)#ip dns relay`	Set the interface as a DNS relay client-facing IPv4 port
`(config-if)#ipv6 address fd02::1/16`	Assign an IPv6 address to the interface
`(config-if)#ipv6 dns relay`	Set the interface as a DNS relay client-facing IPv6 port
`(config-if)#commit`	Commit the configuration
`(config)#interface xe1`	Enter interface mode (interface connected to server)
`(config-if)#ip address 1.1.1.1/24`	Assign an IPv4 address to the interface
`(config-if)#ip dns relay uplink`	Set the interface as a DNS relay server-facing IPv4 port
`(config-if)#ipv6 address fd01::1/16`	Assign an IPv6 address to the interface
`(config-if)#ipv6 dns relay uplink`	Set the interface as a DNS relay server-facing IPv6 port
`(config-if)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode

Validation

```
#sh run dns relay
!
ip dns relay address 1.1.1.2
!
ipv6 dns relay address fd01::2
!
interface xe1
 ip dns relay uplink
 ipv6 dns relay uplink
!
interface xe44
 ip dns relay
 ipv6 dns relay
!
#show running-config interface xe1
!
interface xe1
```

```
 ip address 1.1.1.1/24
 ipv6 address fd01::1/16
 ip dns relay uplink
 ipv6 dns relay uplink
!
#show running-config interface xe44
!
interface xe44
 ip address 4.4.4.1/24
 ipv6 address fd02::1/16
 ip dns relay
 ipv6 dns relay
!
```

Verify DNS Query result on DNS client machine:

```
[root@localhost ~]# host google.com
google.com has address 172.217.160.238
google.com has IPv6 address 2404:6800:4002:804::200e
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
```

© 2025 IP Infusion Inc. Proprietary

DNS Command Reference

CHAPTER 1 Domain Name System Commands

This chapter describes Domain Name System (DNS) commands. DNS translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol (IP).

Note: The commands below are supported only on the “management” VRF.

The chapter contains these commands:

- debug dns client
- ip domain-list
- ip domain-lookup
- ip domain-name
- ip host
- ip name-server
- show hosts
- show running-config dns

debug dns client

Use this command to display DNS debugging messages.

Use the `no` form of this command to stop displaying DNS debugging messages.

Command Syntax

```
debug dns client
no debug dns client
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug dns client
```

ip domain-list

Use this command to define a list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.

The `ip domain-list` command is similar to the ip domain-name command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If there is no domain list, the default domain name specified with the `ip domain-name` command is used. If there is a domain list, the default domain name is not used.

Use the `no` form of this command to remove a domain.

Command Syntax

```
ip domain-list (vrf (NAME|management)|) DOMAIN-NAME
no ip domain-list (vrf (NAME|management)|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain string (e.g. company.com)(Max Size 63)
`NAME`	Custom VRF

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ip domain-list mySite.com
```

ip domain-lookup

Use this command to enable DNS host name-to-address translation.

Use the `no` form of this command to disable DNS.

Command Syntax

```
ip domain-lookup (vrf management|)
no ip domain-lookup (vrf management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip domain-lookup
```

ip domain-name

Use this command to set the default domain name used to complete unqualified host names (names without a dotted-decimal domain name).

The ip domain-list command is similar to the `ip domain-name` command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If a domain list has been created with ip domain-list, the default domain name is not used. If there is no domain list, the default domain name is used.

Use the `no` form of this command to disable DNS.

Command Syntax

```
ip domain-name (vrf (NAME|management)|) DOMAIN-NAME
no ip domain-name (vrf (NAME|management)|) DOMAIN-NAME
```

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain string (e.g. company.com)(Max Size 63)
`NAME`	Custom VRF

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ip domain-name company.com
```

ip host

Use this command to define static a hostname-to-address mapping in DNS. You can specify one mapping in a command.

Use the `no` form of this command remove a hostname-to-address mapping.

Note: When the command `ip host <hostname> <ip>` is enabled for a particular VRF and that hostname is utilized by any feature, changing the associated IP later will lead to issues. If we decide to update the IP address, the old IP tied to the hostname will continue to be used until we disable and then re-enable the feature.

Command Syntax

```
ip host (vrf (NAME|management)|) WORD (X:X::X:X | A.B.C.D)
no ip host (vrf (NAME|management)|) WORD (X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`WORD`	Host name, such as company.com
`X:X::X:X`	IPv6 address of the host
`A.B.C.D`	IPv4 address of the host
`NAME`	Custom VRF

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ip host company.com 192.0.2.1
```

ip name-server

Use this command to add a DNS server address that is used to translate hostnames to IP addresses.

Use the `no` form of this command to remove a DNS server address.

Note: If the hostname resolution takes time even after adding proper name-servers, check the list of name-servers added. Non-responsive name-servers take a long time to resolve the hostnames and result in utilities timeout and "*Failed to resolve hostname*" error. Ensure that the non-reachable/non-DNS name-servers are removed from the configured list.

Command Syntax

```
ip name-server (vrf (NAME|management)|) (X:X::X:X | A.B.C.D)
no ip name-server (vrf (NAME|management)|)(X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`A.B.C.D`	IPv4 address of the host
`X:X::X:X`	IPv6 address of the host
`NAME`	Custom VRF

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ip name-server 123.70.0.23
```

show hosts

Use this command to display the DNS name servers and domain names.

Command Syntax

```
show hosts (vrf (NAME|management)|)
```

Parameters

`vrf`	management or all VRFs
`NAME`	Custom VRF

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Example

The following is a sample output of this command displaying two name servers: 10.10.0.2 and 10.10.0.88.

```
#show hosts
       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 1-1 explains the output fields.

Table 1-1: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF.
DNS lookup is enabled	DNS feature enabled or disabled.
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 1-1: show hosts fields

Entry	Description
Host	Static hostname-to-address mappings in DNS.
Test	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	Name-server indicates it has been learned dynamically.

show running-config dns

Use this command to show the DNS settings of the running configuration.

Command Syntax

```
show running-config dns (vrf management|)
```

Parameters

`vrf`	management

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config dns
ip domain-lookup vrf management
ip domain-name vrf management .com
ip domain-list vrf management .in
ip domain-list vrf management .ac
ip name-server vrf management 10.12.3.23
ip host vrf management test 10.12.12.67 10::23
```

CHAPTER 2 Domain Name System Relay Commands

This chapter describes the DNS relay commands:

- ip dns relay (global)
- ip dns relay (interface)
- ip dns relay address
- ip dns relay uplink
- ipv6 dns relay (global)
- lpv6 dns relay (interface)
- ipv6 dns relay address
- ipv6 dns relay uplink
- show ip dns relay
- show ip dns relay address
- show ipv6 dns relay
- show ipv6 dns relay address
- show running-config dns relay

ip dns relay (global)

Use this command to globally enable the IPv4 DNS relay agent.

Use the `no` form of this command to globally disable the IPv4 DNS relay agent.

Command Syntax

```
ip dns relay
no ip dns relay
```

Parameters

None

Default

By default, IPv4 DNS relay agent is enabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#ip dns relay

(config)#no ip dns relay
```

ip dns relay (interface)

Use this command to configure an IPv4 interface as a DNS relay client-facing port.

Use the `no` form of this command to remove an IPv4 interface as a DNS relay client-facing port.

Command Syntax

```
ip dns relay
no ip dns relay
```

Parameters

None

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#int xe44
(config-if)#ip address 4.4.4.1/24
(config-if)#ip dns relay

(config)#int xe44
(config-if)#ip vrf forwarding vrf1
(config-if)#ip address 4.4.4.1/24
(config-if)#ip dns relay
```

ip dns relay address

Use this command to set the IP address of a DNS server.

Use the `no` form of this command to remove the IP address of a DNS server.

Command Syntax

```
ip dns relay address A.B.C.D
no ip dns relay address A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address of the DNS server

Default

N/A

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#ip dns relay address 1.1.1.2
#
(config)#ip vrf vrf1
(config-vrf)#ip dns relay address 1.1.1.2
```

ip dns relay uplink

Use this command to configure an IPv4 interface as a DNS relay server-facing port.

Use the `no` form of this command to remove an IPv4 interface as a DNS relay server-facing port.

Command Syntax

```
ip dns relay uplink
no ip dns relay uplink
```

Parameters

None

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#int xe44
(config-if)#ip address 4.4.4.1/24
(config-if)#ip dns relay uplink
```

ipv6 dns relay (global)

Use this command to globally enable the IPv6 DNS relay agent.

Use the `no` form of this command to globally disable the IPv6 DNS relay agent.

Command Syntax

```
ipv6 dns relay
no ipv6 dns relay
```

Parameters

None

Default

By default, the IPv6 DNS relay agent is enabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#ipv6 dns relay

#(config)#no ipv6 dns relay
```

Ipv6 dns relay (interface)

Use this command to configure an IPv6 interface as a DNS relay client-facing port.

Use the `no` form of this command to remove an IPv6 interface as a DNS relay client-facing port.

Command Syntax

```
ipv6 dns relay
no ipv6 dns relay
```

Parameters

None

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#int xe44
(config-if)#ipv6 address fd02::1/16
(config-if)#ipv6 dns relay

(config)#int xe44
(config-if)#ip vrf forwarding vrf1
(config-if)#ipv6 address fd02::1/16
(config-if)#ipv6 dns relay
```

ipv6 dns relay address

Use this command to set the IPv6 address of a DNS server.

Use the `no` form of this command to remove the IPv6 address of a DNS server.

Command Syntax

```
ipv6 dns relay address X:X::X:X
no ipv6 dns relay address X:X::X:X
```

Parameters

`X:X::X:X`	IPv6 address of the DNS server

Default

N/A

Command Mode

Configure mode

VRF mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#ipv6 dns relay address 2001:4860:4860::8888

(config)#ip vrf vrf1
(config-vrf)#ip dns relay address 2001:4860:4860::8888
```

ipv6 dns relay uplink

Use this command to configure an IPv6 interface as a DNS relay server-facing port.

Use the `no` form of this command to remove an IPv6 interface as a DNS relay server-facing port.

Command Syntax

```
ipv6 dns relay uplink
no ipv6 dns relay uplink
```

Parameters

None

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#int xe44
(config-if)#ipv6 address fd02::1/16
(config-if)#ipv6 dns relay uplink
```

show ip dns relay

Use this command to display the IPv4 DNS relay configuration including VRF name, DNS servers, and client/user facing interfaces.

Command Syntax

```
show ip dns relay
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ip dns relay
  DNS feature status:            Enabled
  DNS relay service status:      Enabled
  VRF Name: vrf1
    Status     : Running
    DNS Servers: 1.1.1.2
    Interfaces :
      Name         Type            State   Address
      -------------------------------- ----------
      xe1          Uplink          UP      1.1.1.1
      xe32         Downlink        UP      2.2.2.1
      xe33         Downlink        UP      3.3.3.1
      xe44         Downlink        UP      4.4.4.1
  VRF Name: management
    Status     : Running
    DNS Servers: 8.8.8.8
    Interfaces :
      Name         Type            State   Address
      -------------------------------- ----------
      eth0         Downlink        UP      172.29.4.139
```

Table 2-2 explains the fields in the output.

Table 2-2: show ip dns relay fields

Field	Description
DNS feature status	Whether DNS relay is enabled
DNS relay service status	Whether DNS relay is enabled

Table 2-2: show ip dns relay fields (Continued)

Field	Description
VRF Name	Name of the VRF
Status	Not-running, Running, or Failed
DNS Servers	IPv4 address of the DNS server
Name	DNS server facing interface
Type	Whether an uplink or a downlink
State	Whether the interface is up of down
Address	IPv4 address of the interface

show ip dns relay address

Use this command to display the IPv4 DNS relay configuration including VRF name and DNS servers.

Command Syntax

```
show ip dns relay address
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ip dns relay address
  DNS feature status:            Enabled
  DNS relay service status:      Enabled
  VRF Name: vrf1
    Status     : Running
    DNS Servers: 1.1.1.2
  VRF Name: management
    Status     : Running
    DNS Servers: 8.8.8.8
```

Table 2-3 explains the fields in the output.

Table 2-3: show ip dns relay address fields

Field	Description
DNS feature status	Whether DNS relay is enabled
DNS relay service status	Whether DNS relay is enabled
VRF Name	Name of the VRF
Status	Not-running, Running, or Failed
DNS Servers	IPv4 address of the DNS server

show ipv6 dns relay

Use this command to display IPv6 DNS relay configuration including VRF name, DNS servers, and client/user facing interfaces.

Command Syntax

```
show ipv6 dns relay
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ipv6 dns relay
  DNS feature status:            Enabled
  DNS relay IPv6 service status: Enabled
  VRF Name: vrf1
    Status     : Not-running
    DNS Servers: fd01::2
    Interfaces :
      Name         Type            State   Address
      ------------------------------ ----------
      xe44         Downlink        UP      fd02::1
```

Table 2-4 explains the fields in the output.

Table 2-4: show ipv6 dns relay fields

Field	Description
DNS feature status	Whether DNS relay is enabled
DNS relay IPv6 service status	Whether DNS relay is enabled
VRF Name	Name of the VRF
Status	Not-running, Running, or Failed
DNS Servers	IPv6 address of the DNS server
Name	DNS server facing interface
Type	Whether an uplink or a downlink
State	Whether the interface is up of down
Address	IPv6 address of the interface

show ipv6 dns relay address

Use this command to display the IPv6 DNS relay configuration including the VRF name and DNS servers.

Command Syntax

```
show ipv6 dns relay address
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ipv6 dns relay
  DNS feature status:            Enabled
  DNS relay IPv6 service status: Enabled
  VRF Name: vrf1
    Status     : Not-running
    DNS Servers: fd01::2
```

Table 2-5 explains the fields in the output.

Table 2-5: show ipv6 dns relay address fields

Field	Description
DNS feature status	Whether DNS relay is enabled
DNS relay IPv6 service status	Whether DNS relay is enabled
VRF Name	Name of the VRF
Status	Not-running, Running, or Failed
DNS Servers	IPv6 address of the DNS server

show running-config dns relay

Use this command to display DNS relay settings in the running configuration.

Command Syntax

```
show running-config dns relay
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show running-config dns relay
no ipv6 dns relay
!
ip vrf vrf1
 ip dns relay address 1.1.1.2
 ipv6 dns relay address fd01::2
!
ip vrf management
 ip dns relay address 8.8.8.8
!
interface eth0
 ip dns relay
!
interface xe1
 ip dns relay uplink
!
interface xe32
 ip dns relay
!
interface xe33
 ip dns relay
!
interface xe44
 ip dns relay
 ipv6 dns relay
!
```

NTP Configuration

CHAPTER 1 NTP Client Configuration

Overview

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

Support for Default VRF via In-band Management

OcNOS now offers support for NTP over default, management VRFs, and User defined VRFs via in-band management interface & OOB management interface, respectively.

The feature can either be running on the default or management VRF. By default, it runs on the management VRF.

NTP Modes

The following describes the various NTP node types.

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the others, and each device can also provide time synchronization to the others.

Authentication

For additional security, you can configure your NTP servers and clients to use authentication. Routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the ntp authentication-key vrf management command. A unique number identifies each NTP key. This number is the first argument to the ntp authentication-key vrf management command.

3. 3.Use the ntp trusted-key vrf management command to tell the router which keys are valid for authentication. If a key is trusted, the system will be ready to synchronize to a system that uses this key in its NTP packets. The trusted key should already be configured and authenticated.

NTP Client Configuration with IPv4 Address

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server

After configuring the NTP servers, wait a few minutes before you verify that clock synchronization is successful. When the clock synchronization has actually happened, there will be an '*' symbol along with the interface while you give the "`show ntp peers`" command.

Topology

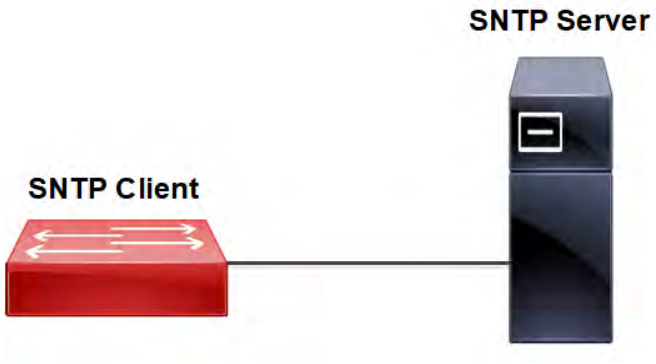


Figure 1-13: SNTP Client and Server

NTP Client for User Management

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp enable vrf management`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

    #show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
```

```
- - peer mode(passive), = - polled in client mode
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

NTP Client for User Defined VRF

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf vrf1`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp enable vrf vrf1`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 192.168.2.2 vrf vrf1`	Configure ntp server ip address.
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

    #show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the `maxpoll` option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the `minpoll` option.

The client will retry between `minpoll` and `maxpoll` range configured for synchronization with the server.

Client for Management VRF

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp server 10.1.1.1 maxpoll 7 minpoll 5 vrf management`	Configure `minpoll` and `maxpoll` range for ntp server.
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

#show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

Client for User Defined VRF

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf vrf1`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp server 192.168.2.2 maxpoll 7 minpoll 5 vrf vrf1`	Configure minpoll and maxpoll range for ntp server.
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

#show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active),
    - - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf vrf1`	Enable feature on default or management VRF. By default this feature runs on management VRF..
`(config)#ntp server 192.168.2.2 vrf vrf1`	Configure ntp server ip address.
`(config)#ntp authenticate vrf vrf1`	Enable NTP Authenticate. NTP authentication is disabled by default.
`(config)#ntp authentication-key 1 md5 cisco vrf vrf1`	Configure ntp authentication key along with md5 value.
`(config)# ntp request-key 1 vrf vrf1`	Configure reuest-key
`(config)#ntp trusted-key 1 vrf vrf1`	Configure trusted key <1-65535>
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp authentication-status
    Authentication enabled

#show ntp authentication-keys
    --------------------------
     Auth Key       MD5 String
    --------------------------
    1234               SWWX

#show ntp trusted-keys
    Trusted Keys:
    1234
```

NTP Client Configuration with IPv6 Address

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server.

Topology

Figure 1-14 shows the sample configuration of NTP Client.

Figure 1-14: NTP Client topology

NTP Client VRF Management

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)# ntp enable vrf management`	This feature enables NTP. This will be enabled in default.
`(config)#ntp server 2001::1 vrf management`	Configure NTP server IP address.
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode.

Validation

```
#show ntp peers
     ================================================
     Peer IP Address Serv/Peer
     ================================================
     2001::1 Server (configured)
     #show ntp peer-status
     Total peers : 1
     * - selected for sync, + - peer mode(active),
     - - peer mode(passive), = - polled in client mode
         Remote  refid     st when             poll reach delay   offset        jitter
==============================================================================
        *2001::1         LOCAL(0) 7 u   14   32   37    0.194       -4.870       3.314
```

NTP Client User Defined VRF

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf vrf1`	Configure feature on default or management VRF. By default this feature runs on management VRF.

(config)# ntp enable vrf vrf1	This feature enables NTP. This will be enabled in default.
(config)#ntp server 2001::1 vrf vrf1	Configure NTP server IP address.
(config)#commit	Commit the configuration
(config)#exit	Exit from the Configure Mode.

Validation

```
#show ntp peers
     ================================================
     Peer IP Address Serv/Peer
     ================================================
     2001::1 Server (configured)
     #show ntp peer-status
     Total peers : 1
     * - selected for sync, + - peer mode(active),
     - - peer mode(passive), = - polled in client mode
         Remote  refid     st when             poll reach delay   offset        jitter
==============================================================================
        *2001::1         LOCAL(0) 7 u   14  32  37    0.194       -4.870       3.314
```

Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the maxpoll option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the minpoll option. The client will retry between minpoll and maxpoll range configured for synchronization with the server.

Client for VRF Management

#configure terminal	Enter configure mode
(config)#feature ntp vrf management	Configure feature on default or management VRF. By default this feature runs on management VRF
(config)#ntp server 2001::1 maxpoll 7 minpoll 5 vrf management	Configure minpoll and maxpoll range for NTP server
(config)#commit	Commit the configuration
(config)#exit	Exit from the Configure Mode

Validation

```
#show ntp peers
     ================================================
     Peer IP Address Serv/Peer
     ================================================
```

```
        2001::1 Server (configured)
        #show ntp peer-status
        Total peers : 1
        * - selected for sync, + - peer mode(active),
        - - peer mode(passive), = - polled in client mode
            Remote  refid     st when poll reach delay   offset        jitter
    ==============================================================================
           *2001::1  LOCAL(0) 7  u   14  32  37    0.194       -4.870       3.314
```

Client for User Defined VRF

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf vrf1`	Configure feature on default or management VRF. By default this feature runs on management VRF
`(config)#ntp server 2001::1 maxpoll 7 minpoll 5 vrf vrf1`	Configure minpoll and maxpoll range for NTP server
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit from the Configure Mode

Validation

```
    #show ntp peers
         ================================================
         Peer IP Address Serv/Peer
         ================================================
         2001::1 Server (configured)
         #show ntp peer-status
         Total peers : 1
         * - selected for sync, + - peer mode(active),
         - - peer mode(passive), = - polled in client mode
             Remote  refid     st when poll reach delay   offset        jitter
    ==============================================================================
           *2001::1  LOCAL(0) 7  u   14  32  37    0.194       -4.870       3.314
```

NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client for VRF Management

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf management`	Enable feature on default or management VRF. By default this feature runs on management VRF..
`(config)#ntp server 2001::1 vrf management`	Configure NTP server IP address.
`(config)#ntp authenticate vrf management`	Enable NTP Authenticate. NTP authentication is disabled by default.
`(config)#ntp authentication-key 1234 md5 text vrf management`	Configure NTP authentication key along with MD5 value.

(config)#ntp trusted-key 1234 vrf management	Configure trusted key
(config)#commit	Commit the configuration
(config)#exit	Exit from the Configure Mode.

Validation

```
#show ntp authentication-status
 Authentication enabled

#show ntp authentication-keys
 --------------------------- Auth Key   MD5 String --------------------------
                    1234       SWWX

 #show ntp trusted-keys
 Trusted Keys: 1234
```

Client for User Defined VRF

#configure terminal	Enter configure mode
(config)#feature ntp vrf vrf1	Enable feature on default or management VRF. By default this feature runs on management VRF..
(config)#ntp server 2001::1 vrf vrf1	Configure NTP server IP address.
(config)#ntp authenticate vrf vrf1	Enable NTP Authenticate. NTP authentication is disabled by default.
(config)#ntp authentication-key 1 md5 cisco vrf vrf1	Configure NTP authentication key along with MD5 value.
(config)# ntp request-key 1 vrf vrf1	Configure request key
(config)#ntp trusted-key 1 vrf vrf1	Configure trusted key
(config)#commit	Commit the configuration
(config)#exit	Exit from the Configure Mode.

Validation

```
#show ntp authentication-status
 Authentication enabled

#show ntp authentication-keys
 --------------------------- Auth Key   MD5 String --------------------------
                    1234       SWWX

 #show ntp trusted-keys
 Trusted Keys: 1234
```

CHAPTER 2 NTP Server Configuration

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server, and then distributes this time across the network.

Above explained NTP Server and Client functionality will be supported in OcNOS. NTP Access restrictions can be configured to allow Client devices to access NTP Server.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of two nodes. One node acting as NTP Master and the other node acting as NTP Client.

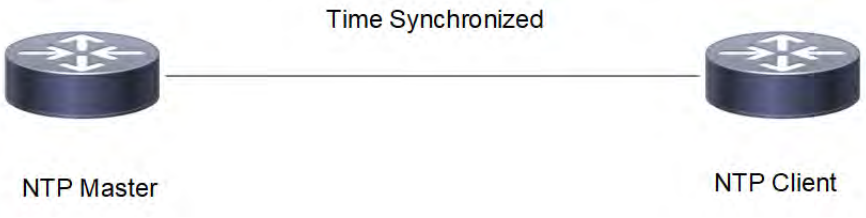


Figure 2-15: Synchronization of NTP Master and NTP Client

Configuration of VRF Management

NTP Master

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf management`	Enable feature ntp
`(config)#ntp enable vrf management`	Enable ntp
`(config)#ntp master vrf management`	Configure the node as NTP master
`(config)#ntp master stratum 1 vrf management`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)#ntp allow 10.12.20.6 vrf management`	Configure ntp client address in the ntp allow list
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Enable feature ntp.
`(config)#ntp enable vrf management`	Enable ntp
`(config)#ntp server 10.12.20.5 vrf management`	Configure ntp server address for the sync to happen
`(config)#commit`	Commit the candidate configuration to the running
`(config)#exit`	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   59   64  377    0.000    0.000   0.000
```

Check the ntp client synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u    4   16  377    0.137   -0.030   0.004
```

Configuration of User Defined VRF

NTP Master

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf vrf1`	Enable feature ntp
`(config)#ntp enable vrf vrf1`	Enable ntp
`(config)#ntp master vrf vrf1`	Configure the node as NTP master
`(config)#ntp master stratum 1 vrf vrf1`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)#ntp allow 192.168.2.0 mask 255.255.255.0 vrf vrf1`	Configure ipv4 ntp client address in the ntp allow list
`(config) ntp allow 2001:: mask 64 vrf vrf1`	Configure ipv6 ntp client address in the ntp allow list
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode

NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf vrf1`	Enable feature ntp.
`(config)#ntp enable vrf vrf1`	Enable ntp
`(config)#ntp server 192.168.2.2 vrf vrf1`	Configure ntp server address for the sync to happen
`(config)#ntp server 2001::2 vrf vrf1`	
`(config)#commit`	Commit the candidate configuration to the running
`(config)#exit`	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
ntpmaster#sh ntp peer-status
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   60   64  377    0.000    0.000   0.000
```

Check the ntp client synchronization status as mentioned below:

```
Ntpclient1#sh ntp peer-status
Total peers : 2
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.2.2     LOCAL(0)         2 u   23   64  377    0.429    0.006   0.042
+2001::2         LOCAL(0)         2 u   35   64  377    0.440   -0.007   0.033
```

Synchronization of more than one NTP clients with the NTP Master

In the below section, check the Synchronization of more than one NTP clients with the NTP Master using Subnet definition on the NTP Master.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of three nodes. One node acting as NTP Master and the other two nodes acting as NTP Clients.

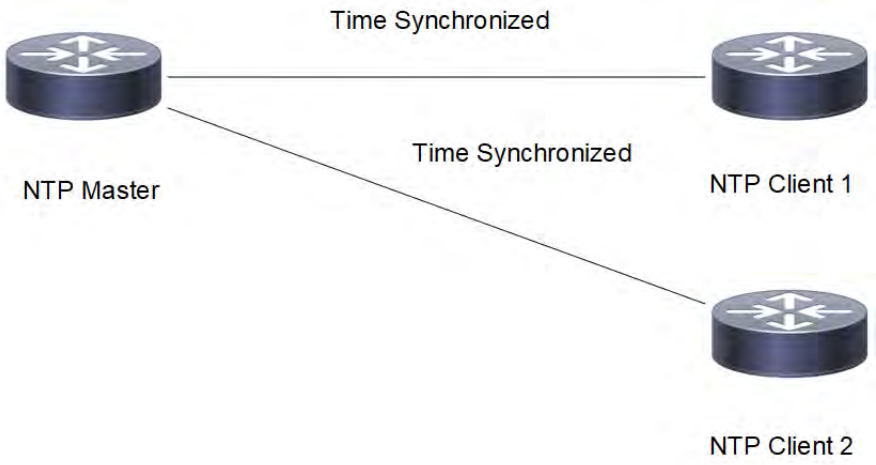


Figure 2-16: Synchronization of more than one NTP clients with NTP Master using subnet definition

Configuration of VRF Management

NTP Master

`#configure terminal`	Enter configure mode
`(config)# feature ntp vrf management`	Enable feature ntp
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp master vrf management`	Configure the node as NTP master
`(config)# ntp master stratum 1 vrf management`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 vrf management`	Configure the mask in the ntp allow list
`(config)#commit`	Commit the candidate configuration to the running
`(config)# exit`	Exit configure mode

NTP Client1

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf management`	Enable feature ntp.
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp server 10.12.20.5 vrf management`	Configure ntp server address for the sync to happen
`(config)#commit`	Commit the candidate configuration to the running
`(config)# exit`	Exit Configure mode

NTP Client2

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf management`	Enable feature ntp.
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp server 10.12.20.5 vrf management`	Configure ntp server address for the sync to happen
`(config)#commit`	Commit the candidate configuration to the running
`(config)# exit`	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   59   64  377    0.000    0.000   0.000

Check the ntp client1 synchronization status as mentioned below :
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u    8   32  377    0.153   -0.053   0.020
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   14   16  377    0.150   -0.686   0.034
```

Configuration of User Defined VRF

NTP Master

`#configure terminal`	Enter configure mode
`(config)# feature ntp vrf vrf1`	Enable feature ntp

(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp master vrf vrf1	Configure the node as NTP master
(config)# ntp master stratum 1 vrf vrf1	Configure the ntp stratum level as 1 indicating that it is using local clock
(config)# ntp allow 192.168.2.0 mask 255.255.255.0 vrf vrf1	Configure the mask in the ntp allow list for ipv4
(config)# ntp allow 192.168.3.0 mask 255.255.255.0 vrf vrf1	Configure the mask in the ntp allow list for ipv4
(config)# ntp allow 2001:: mask 64 vrf vrf1	Configure the mask in the ntp allow list for ipv6
(config)# ntp allow 5001:: mask 64 vrf vrf1	Configure the mask in the ntp allow list for ipv6
(config)#commit	Commit the candidate configuration to the running
(config)# exit	Exit configure mode

NTP Client1

#configure terminal	Enter configure mode.
(config)# feature ntp vrf vrf1	Enable feature ntp.
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp server 192.168.2.2 vrf vrf1	Configure ipv4 ntp server address for the sync to happen
(config)# ntp server 2001::2 vrf vrf1	Configure ipv6 ntp server address for the sync to happen
(config)#commit	Commit the candidate configuration to the running
(config)# exit	Exit Configure mode

NTP Client2

#configure terminal	Enter configure mode.
(config)# feature ntp vrf vrf1	Enable feature ntp.
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp server 192.168.3.2 vrf vrf1	Configure ipv4 ntp server address for the sync to happen
(config)# ntp server 5001::2 vrf vrf1	Configure ipv6 ntp server address for the sync to happen
(config)#commit	Commit the candidate configuration to the running
(config)# exit	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
ntpmaster#show ntp peer-status
 remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   46   64  377    0.000    0.000   0.000
```

Check the ntp client1 synchronization status as mentioned below:

```
ntpclient-7012#show ntp peer-status
Total peers : 2
```

```
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.2.2     LOCAL(0)         2 u   54   64  377    0.410    0.088   0.026
+2001::2         LOCAL(0)         2 u   54   64  377    0.453    0.019   0.206
```

Check the ntp client2 synchronization status as mentioned below:

ntpclient-7025#show ntp peer-status

```
Total peers : 2
* - selected for sync, + -  peer mode(active),qw
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.3.2     LOCAL(0)         2 u   30   64  377    0.476   -0.021   0.033
  +5001::2         LOCAL(0)         2 u   34   64  377    0.451   -0.060   0.040
```

Synchronization with Authentication

In the below section, check the synchronization of NTP Master and NTP Client with Authentication.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of three nodes. One node acting as NTP Master and the other two nodes acting as NTP Clients.

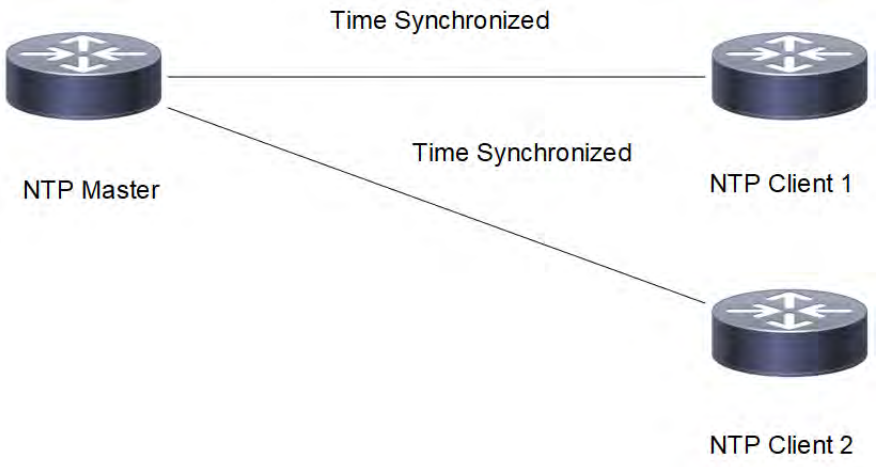


Figure 2-17: Synchronization of NTP Master and NTP Clients using authentication

Configuration of VRF Management

NTP Master

`#configure terminal`	Enter configure mode
`(config)# feature ntp vrf management`	Enable feature ntp
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp master vrf management`	Configure the node as NTP master
`(config)# ntp master stratum 1 vrf management`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)# ntp authenticate vrf management`	Configure ntp server for authentication
`(config)# ntp authentication-key 65 md5 test123 vrf management`	Configure ntp authentication key with password
`(config)# ntp trusted-key 65 vrf management`	Configure ntp trusted key
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 vrf management`	Configure the mask in the ntp allow list
`(config)#commit`	Commit the configuration
`(config)# exit`	Exit configure mode

NTP Client1

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf management`	Enable feature ntp.
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp authenticate vrf management`	Configure ntp client for authentication
`(config)# ntp authentication-key 65 md5 test123 vrf management`	Configure ntp authentication key with password
`(config)# ntp trusted-key 65 vrf management`	Configure ntp trusted key
`(config)# ntp server 10.12.20.5 key 65 vrf management`	Configure ntp server address for the sync to happen with authentication key
`(config)#commit`	Commit the configuration
`(config)# exit`	Exit Configure mode

NTP Client2

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf management`	Enable feature ntp.
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp authenticate vrf management`	Configure ntp client for authentication
`(config)# ntp authentication-key 65 md5 test123 vrf management`	Configure ntp authentication key with password
`(config)# ntp trusted-key 65 vrf management`	Configure ntp trusted key

(config)# ntp server 10.12.20.5 key 65 vrf management	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)# exit	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   64   64  377    0.000    0.000   0.000
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   12   64  377    0.185    0.002   0.006

Check the ntp client2 synchronization status as mentioned below :
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   16   32  377    0.175   -0.360   0.226
```

Configuration of User Defined VRF

NTP Master

#configure terminal	Enter configure mode
(config)# feature ntp vrf vrf1	Enable feature ntp
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp master vrf vrf1	Configure the node as NTP master
(config)# ntp master stratum 1 vrf vrf1	Configure the ntp stratum level as 1 indicating that it is using local clock
(config)# ntp authenticate vrf vrf1	Configure ntp server for authentication
(config)# ntp authentication-key 1 md5 cisco 7 vrf vrf1	Configure ntp authentication key with password

(config)# ntp trusted-key 1 vrf vrf1	Configure ntp trusted key
(config)# ntp request-key 1 vrf vrf1	Configure request key
(config)# ntp allow 192.168.2.0 mask 255.255.255.0 vrf vrf1	Configure the mask in the ntp allow list for ipv4
(config)# ntp allow 2001:: mask 64 vrf vrf1	Configure the mask in the ntp a6llow list for ipv6
(config)# ntp allow 192.168.3.0 mask 255.255.255.0 vrf vrf1	Configure the mask in the ntp allow list for ipv4
(config)# ntp allow 5001:: mask 64 vrf vrf1	Configure the mask in the ntp allow list for ipv6
(config)#commit	Commit the configuration
(config)# exit	Exit configure mode

NTP Client1

#configure terminal	Enter configure mode.
(config)# feature ntp vrf vrf1	Enable feature ntp.
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp authenticate vrf vrf1	Configure ntp client for authentication
(config)# ntp authentication-key 1 md5 cisco vrf vrf1	Configure ntp authentication key with password
(config)# ntp request-key 1 vrf vrf1	Configure request key
(config)# ntp trusted-key 1 vrf vrf1	Configure ntp trusted key
(config)# ntp server 192.168.2.2 key 1 vrf vrf1	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)# exit	Exit Configure mode

NTP Client2

#configure terminal	Enter configure mode.
(config)# feature ntp vrf vrf1	Enable feature ntp.
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp authenticate vrf vrf1	Configure ntp client for authentication
(config)# ntp authentication-key 1 md5 cisco vrf vrf1	Configure ntp authentication key with password
(config)# ntp request-key 1 vrf vrf1	Configure request key
(config)# ntp trusted-key 1 vrf vrf1	Configure ntp trusted key
(config)# ntp server 192.168.3.2 key 1 vrf vrf1	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)# exit	Exit Configure mode

Validation

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach    delay    offset  jitter
   ==============================================================================
   *127.127.1.0     .LOCL.           1 l   50   64  377    0.000    0.000   0.000
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 2
  * - selected for sync, + -  peer mode(active),
  - - peer mode(passive), = - polled in client mode,
  x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
  ==============================================================================
  *192.168.2.2     LOCAL(0)         2 u   43   64  377    0.407   -0.018   0.034
  +2001::2         LOCAL(0)         2 u   22   64  377    0.432   -0.031   0.063
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 2
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
+192.168.3.2     LOCAL(0)         2 u   51   64  377    0.443    0.007   0.032
*5001::2         LOCAL(0)         2 u   49   64  377    0.471   -0.034   0.065
```

Synchronization of NTP Server and NTP Clients with NTP ACL

The command `nomodify ntp acl` signifies NTP Clients must be denied ntpq(1) and ntpdc(1) queries which attempt to modify the state of the server (i.e., run time reconfiguration).Queries which return information shall be permitted.

The command `noquery ntp acl` signifies Deny ntpq(1) and ntpdc(1) queries by NTP Clients. But Time service shall not be affected.

The command `nopeer ntp acl` signifies NTP Clients shall be denied access if unauthenticated packets which would result in mobilizing a new association is sent.

The command `notrap ntp acl` signifies NTP Clients shall be declined to provide mode 6 control message trap service to matching hosts. The trap service is a sub-system of the ntpq(1) control message protocol which is intended for use by remote event logging programs.

The command `KoD ntp acl` signifies When an access violation happens by NTP Clients, the server must send the KoD (kiss-o'-death) packets. KoD packets are rate limited to no more than one per second. If another KoD packet occurs within one second after the last one, the packet is dropped.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of three nodes. One node acting as NTP Master and the other two nodes acting as NTP Clients.

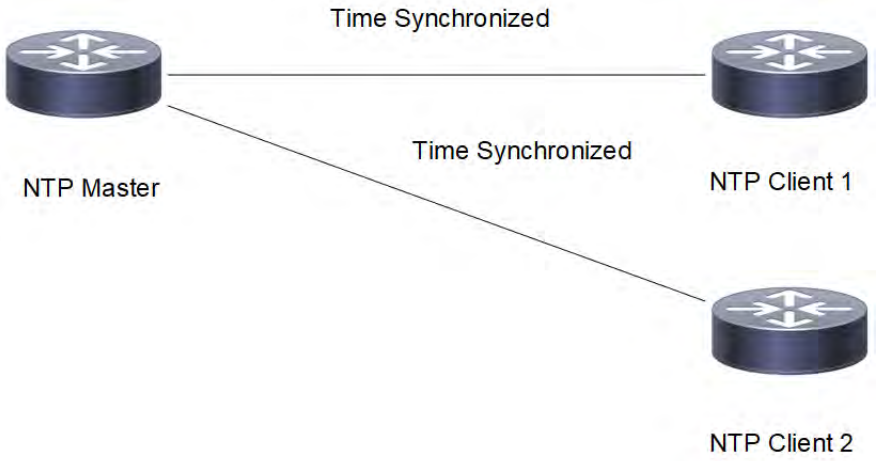


Figure 2-18: Synchronization of NTP Master and NTP Clients with NTP ACL

Configuration of VRF Management

NTP Master

`#configure terminal`	Enter configure mode
`(config)# feature ntp vrf management`	Enable feature ntp
`(config)# ntp enable vrf management`	Enable ntp
`(config)# ntp master vrf management`	Configure the node as NTP master
`(config)# ntp master stratum 1 vrf management`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)# ntp authenticate vrf management`	Configure ntp server for authentication
`(config)# ntp authentication-key 65 md5 test123 vrf management`	Configure ntp authentication key with password
`(config)# ntp trusted-key 65 vrf management`	Configure ntp trusted key
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 nomodify  vrf management`	Configure the ntp acl nomodify in the ntp allow list
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 noquery  vrf management`	Configure the ntp acl noquery in the ntp allow list
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 nopeer  vrf management`	Configure the ntp acl nopeer in the ntp allow list
`(config)# ntp allow 10.12.20.6 mask 255.255.255.0 notrap  vrf management`	Configure the ntp acl notrap in the ntp allow list

© 2025 IP Infusion Inc. Proprietary

(config)# ntp allow 10.12.20.6 mask 255.255.255.0 kod vrf management	Configure the ntp acl KoD in the ntp allow list
(config)#commit	Commit the configuration
(config)# exit	Exit configure mode

NTP Client1

#configure terminal	Enter configure mode.
(config)# feature ntp vrf management	Enable feature ntp.
(config)# ntp enable vrf management	Enable ntp
(config)# ntp authenticate vrf management	Configure ntp client for authentication
(config)# ntp authentication-key 65 md5 test123 vrf management	Configure ntp authentication key with password
(config)# ntp trusted-key 65 vrf management	Configure ntp trusted key
(config)# ntp server 10.12.20.5 key 65 vrf management	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)# exit	Exit Configure mode

NTP Client2

#configure terminal	Enter configure mode.
(config)# feature ntp vrf management	Enable feature ntp.
(config)# ntp enable vrf management	Enable ntp
(config)# ntp authenticate vrf management	Configure ntp client for authentication
(config)# ntp authentication-key 65 md5 test123 vrf management	Configure ntp authentication key with password
(config)# ntp trusted-key 65 vrf management	Configure ntp trusted key
(config)# ntp server 10.12.20.5 key 65 vrf management	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)# exit	Exit Configure mode

Validation

```
Normal Time synchronization is not affected.
```

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   40   64  377    0.000    0.000   0.000
VTEP1#
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
```

```
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   13   16  377    0.180    0.019   0.013
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   15   16  377    0.185   -0.018   0.017
```

Configuration of User Defined VRF

NTP Master

`#configure terminal`	Enter configure mode
`(config)# feature ntp vrf vrf1`	Enable feature ntp
`(config)# ntp enable vrf vrf1`	Enable ntp
`(config)# ntp master vrf vrf1`	Configure the node as NTP master
`(config)# ntp master stratum 1 vrf vrf1`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)# ntp authenticate vrf vrf1`	Configure ntp server for authentication
`(config)# ntp authentication-key 1 md5 cisco vrf vrf1`	Configure ntp authentication key with password
`(config)# ntp trusted-key 1 vrf vrf1`	Configure ntp trusted key
`(config)# ntp request-key 1 vrf vrf1`	Configure ntp request key
`(config)# ntp allow 192.168.2.0 mask 255.255.255.0 nomodify vrf vrf1`	Configure the ntp acl nomodify in the ntp allow list
`(config)# ntp allow 192.168.2.0  mask 255.255.255.0 noquery vrf vrf1`	Configure the ntp acl noquery in the ntp allow list
`(config)# ntp allow 192.168.2.0  mask 255.255.255.0 nopeer vrf vrf1`	Configure the ntp acl nopeer in the ntp allow list
`(config)# ntp allow 192.168.2.0  mask 255.255.255.0 notrap vrf vrf1`	Configure the ntp acl notrap in the ntp allow list
`(config)# ntp allow 10.12.20.6+-192.168.2.0 mask 255.255.255.0 kod vrf vrf1`	Configure the ntp acl KoD in the ntp allow list
`(config)#commit`	Commit the configuration
`(config)# exit`	Exit configure mode

NTP Client1

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf vrf1`	Enable feature ntp.
`(config)# ntp enable vrf vrf1`	Enable ntp
`(config)# ntp authenticate vrf vrf1`	Configure ntp client for authentication
`(config)# ntp authentication-key 1 md5 cisco vrf vrf1`	Configure ntp authentication key with password
`(config)# ntp trusted-key 1 vrf vrf1`	Configure ntp trusted key
`(config)# ntp request-key 1 vrf vrf1`	Configure ntp trusted key
`(config)# ntp server 192.168.2.2 key 1 vrf vrf1`	Configure ntp server address for the sync to happen with authentication key
`(config)#commit`	Commit the configuration
`(config)# exit`	Exit Configure mode

NTP Client2

`#configure terminal`	Enter configure mode.
`(config)# feature ntp vrf vrf1`	Enable feature ntp.
`(config)# ntp enable vrf vrf1`	Enable ntp
`(config)# ntp authenticate vrf vrf1`	Configure ntp client for authentication
`(config)# ntp authentication-key 1 md5 cisco vrf vrf1`	Configure ntp authentication key with password
`(config)# ntp trusted-key 1 vrf vrf1`	Configure ntp trusted key
`(config)# ntp request-key 1 vrf vrf1`	Configure ntp trusted key
`(config)# ntp server 192.168.3.2 key 1 vrf vrf1`	Configure ntp server address for the sync to happen with authentication key
`(config)#commit`	Commit the configuration
`(config)# exit`	Exit Configure mode

Validation

```
Normal Time synchronization is not affected.
```

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   40   64  377    0.000    0.000   0.000
VTEP1#
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
```

```
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   13   16  377    0.180    0.019   0.013
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      LOCAL(0)         2 u   15   16  377    0.185   -0.018   0.017
```

Synchronization of NTP Server and NTP Clients with NTP ACL configured as noserve

The command `noserve ntp acl` signifies NTP Clients shall be denied all packets except ntpq(1) and ntpdc(1) queries.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of three nodes. One node acting as NTP Master and the other two nodes acting as NTP Clients.

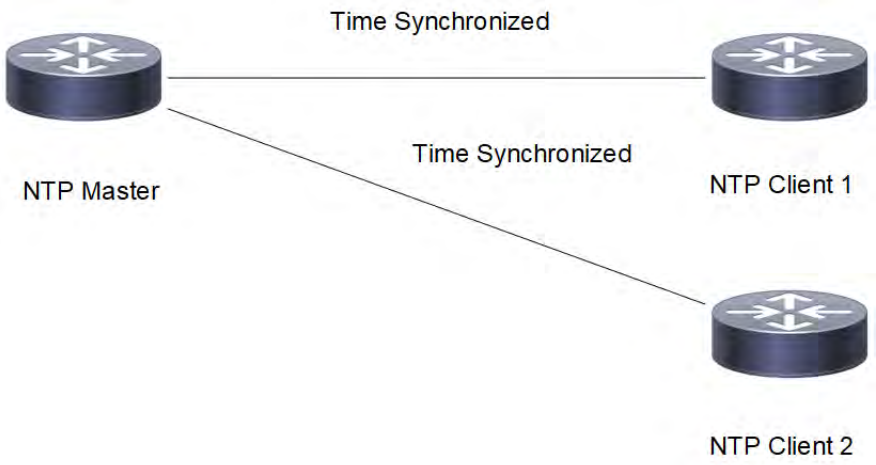


Figure 2-19: Synchronization of NTP Master and NTP Clients with NTP ACL as noserve

Configuration of VRF Management

NTP Master

#configure terminal	Enter configure mode
(config)# feature ntp vrf management	Enable feature ntp
(config)# ntp enable vrf management	Enable ntp
(config)# ntp master vrf management	Configure the node as NTP master
(config)# ntp master stratum 1 vrf management	Configure the ntp stratum level as 1 indicating that it is using local clock
(config)# ntp authenticate vrf management	Configure ntp server for authentication
(config)# ntp authentication-key 65 md5 test123 vrf management	Configure ntp authentication key with password
(config)# ntp trusted-key 65 vrf management	Configure ntp trusted key
(config)# ntp allow 10.12.20.6 mask 255.255.255.0 noserve vrf management	Configure the ntp acl noserve in the ntp allow list
(config)#commit	Commit the configuration
(config)# exit	Exit configure mode

NTP Client1

#configure terminal	Enter configure mode.
(config)#feature ntp vrf management	Enable feature ntp.
(config)#ntp enable vrf management	Enable ntp
(config)#ntp authenticate vrf management	Configure ntp client for authentication
(config)#ntp authentication-key 65 md5 test123 vrf management	Configure ntp authentication key with password
(config)#ntp trusted-key 65 vrf management	Configure ntp trusted key
(config)#ntp server 10.12.20.5 key 65 vrf management	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)#exit	Exit Configure mode

NTP Client2

#configure terminal	Enter configure mode.
(config)#feature ntp vrf management	Enable feature ntp.
(config)#ntp enable vrf management	Enable ntp
(config)#ntp authenticate vrf management	Configure ntp client for authentication
(config)#ntp authentication-key 65 md5 test123 vrf management	Configure ntp authentication key with password
(config)#ntp trusted-key 65 vrf management	Configure ntp trusted key
(config)#ntp server 10.12.20.5 key 65 vrf management	Configure ntp server address for the sync to happen with authentication key

(config)#commit	Commit the configuration
(config)#exit	Exit Configure mode

Validation

Check that with NTP acl configured as noserve, Normal Time synchronization is affected and there is no synchronization.

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   41   64  377    0.000    0.000   0.000
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.12.20.5      .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.12.20.5      .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

Configuration of User Defined VRF

NTP Master

#configure terminal	Enter configure mode
(config)# feature ntp vrf vrf1	Enable feature ntp
(config)# ntp enable vrf vrf1	Enable ntp
(config)# ntp master vrf vrf1	Configure the node as NTP master
(config)# ntp master stratum 1 vrf vrf1	Configure the ntp stratum level as 1 indicating that it is using local clock
(config)# ntp authenticate vrf vrf1	Configure ntp server for authentication

(config)# ntp authentication-key 65 md5 test123 vrf vrf1	Configure ntp authentication key with password
(config)# ntp trusted-key 65 vrf vrf1	Configure ntp trusted key
(config)# ntp allow 10.12.20.6 mask 255.255.255.0 noserve vrf vrf1	Configure the ntp acl noserve in the ntp allow list
(config)#commit	Commit the configuration
(config)# exit	Exit configure mode

NTP Client1

#configure terminal	Enter configure mode
(config)#feature ntp vrf vrf1	Enable feature ntp
(config)#ntp enable vrf vrf1	Enable ntp
(config)#ntp authenticate vrf vrf1	Configure ntp client for authentication
(config)#ntp authentication-key 65 md5 test123 vrf vrf1	Configure ntp authentication key with password
(config)#ntp trusted-key 65 vrf vrf1	Configure ntp trusted key
(config)#ntp server 10.12.20.5 key 65 vrf vrf1	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)#exit	Exit Configure mode

NTP Client2

#configure terminal	Enter configure mode.
(config)#feature ntp vrf vrf1	Enable feature ntp.
(config)#ntp enable vrf vrf1	Enable ntp
(config)#ntp authenticate vrf vrf1	Configure ntp client for authentication
(config)#ntp authentication-key 65 md5 test123 vrf vrf1	Configure ntp authentication key with password
(config)#ntp trusted-key 65 vrf vrf1	Configure ntp trusted key
(config)#ntp server 10.12.20.5 key 65 vrf vrf1	Configure ntp server address for the sync to happen with authentication key
(config)#commit	Commit the configuration
(config)#exit	Exit Configure mode

Validation

Check that with NTP acl configured as noserve, Normal Time synchronization is affected and there is no synchronization.

Check the local clock synchronization in the NTP Master as mentioned below:

```
VTEP1#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
```

```
================================================================================
*127.127.1.0     .LOCL.           1 l   41   64  377    0.000    0.000   0.000
```

Check the ntp client1 synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.12.20.5      .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

Check the ntp client2 synchronization status as mentioned below:

```
VTEP2#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 10.12.20.5      .INIT.          16 u    -   64    0    0.000    0.000   0.000
```

Synchronization of NTP Client with Stratum 2 NTP Master

In the below section, check Synchronization of NTP Client with Stratum 2 NTP Master.

Topology

The procedures in this section use the topology as mentioned below:

Setup consists of three nodes. First node acting as Stratum 1 NTP Master, Second node acting as Stratum 2 NTP master and the third node acting as NTP client.

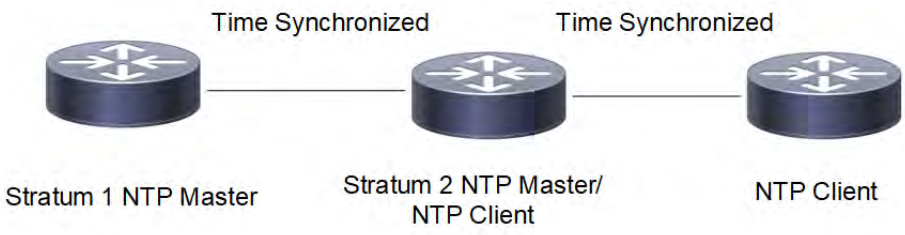


Figure 2-20: Synchronization of Stadium 2 NTP Master with NTP Client

Configuration of Management VRF

Stratum 1 NTP Master

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf management`	Enable feature ntp
`(config)#ntp enable vrf management`	Enable ntp
`(config)#ntp master vrf management`	Configure the node as NTP master
`(config)#ntp master stratum 1 vrf management`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)#ntp allow 10.12.20.5 vrf management`	Configure the ntp client ip address in the ntp allow list
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode

Stratum 2 NTP Server/NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Enable feature ntp.
`(config)#ntp enable vrf management`	Enable ntp
`(config)#ntp master vrf management`	Configure the node as NTP Master
`(config)#ntp master stratum 2 vrf management`	Configure the node as stratum 2 ntp master
`(config)#ntp allow 10.12.20.6  vrf management`	Configure NTP client ip address in the ntp allow list
`(config)#ntp server 10.12.20.7 vrf management`	Configure the stratum 1 NTP master ip address for time synchronization
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit Configure mode

NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf management`	Enable feature ntp.
`(config)#ntp enable vrf management`	Enable ntp
`(config)#ntp server 10.12.20.5 vrf management`	Configure ntp server address for the sync to happen
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit Configure mode

Validation

Check that NTP Client successfully synchronizes the time with stratum 2 NTP Master.

Check the local clock synchronization in the Stratum 1 NTP Master as mentioned below:

```
VTEP2#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   22   64  377    0.000    0.000   0.000
```

Check the Stratum 2 NTP Master/NTP client synchronization status as mentioned below:

```
VTEP1#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.7      LOCAL(0)         2 u   33   64  377    0.145    0.010   0.009
 127.127.1.0     .LOCL.           2 l 110m   64    0    0.000    0.000   0.000
```

Check the NTP Client synchronization status as mentioned below:

```
#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      10.12.20.7       3 u   16   64  377    0.137   -2.596   0.235
```

Configuration of User Defined VRF

Stratum 1 NTP Master

`#configure terminal`	Enter configure mode
`(config)#feature ntp vrf vrf1`	Enable feature ntp
`(config)#ntp enable vrf vrf1`	Enable ntp
`(config)#ntp master vrf vrf1`	Configure the node as NTP master
`(config)#ntp master stratum 1 vrf vrf1`	Configure the ntp stratum level as 1 indicating that it is using local clock
`(config)#ntp allow 192.168.3.0 vrf vrf1`	Configure the ntp client ip address in the ntp allow list
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit configure mode

Stratum 2 NTP Server/NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf vrf1`	Enable feature ntp.
`(config)#ntp enable vrf vrf1`	Enable ntp
`(config)#ntp master vrf vrf1`	Configure the node as NTP Master
`(config)#ntp master stratum 2 vrf vrf1`	Configure the node as stratum 2 ntp master
`(config)#ntp allow 192.168.3.0 vrf vrf1`	Configure NTP client ip address in the ntp allow list
`(config)#ntp server 192.168.2.2 vrf vrf1`	Configure the stratum 1 NTP master ip address for time synchronization
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit Configure mode

NTP Client

`#configure terminal`	Enter configure mode.
`(config)#feature ntp vrf vrf1`	Enable feature ntp.
`(config)#ntp enable vrf vrf1`	Enable ntp
`(config)#ntp server 192.168.3.2 vrf vrf1`	Configure ntp server address for the sync to happen
`(config)#commit`	Commit the configuration
`(config)#exit`	Exit Configure mode

Validation

Check that NTP Client successfully synchronizes the time with stratum 2 NTP Master.

Check the local clock synchronization in the Stratum 1 NTP Master as mentioned below:

```
VTEP2#show ntp peer-status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.           1 l   22   64  377    0.000    0.000   0.000
```

Check the Stratum 2 NTP Master/NTP client synchronization status as mentioned below:

```
VTEP1#show ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.7      LOCAL(0)         2 u   33   64  377    0.145    0.010   0.009
 127.127.1.0     .LOCL.           2 l 110m   64    0    0.000    0.000   0.000
```

Check the NTP Client synchronization status as mentioned below:

```
#show ntp peer-status
```

```
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.12.20.5      10.12.20.7       3 u   16   64  377    0.137   -2.596   0.235
```

NTP Command Reference

CHAPTER 1 Network Time Protocol

This chapter is a reference for Network Time Protocol (NTP) commands.

NTP synchronizes clocks between computer systems over packet-switched networks. NTP can synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

NTP uses a hierarchical, layered system of time sources. Each level of this hierarchy is called a “stratum” and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Note: The default time-to-live value for the unicast packets is 64.

This chapter contains these commands:

- clear ntp statistics
- debug ntp
- feature ntp
- ntp acl
- ntp authenticate
- ntp authentication-key
- ntp enable
- ntp discard
- ntp logging
- ntp master
- ntp master stratum
- ntp peer
- ntp request-key
- ntp server
- ntp sync-retry
- ntp trusted-key
- show ntp authentication-keys
- show ntp authentication-status
- show ntp logging-status
- show ntp peer-status
- show ntp peers
- show ntp statistics
- show ntp trusted-keys
- show running-config ntp

© 2025 IP Infusion Inc. Proprietary

clear ntp statistics

Use this command to reset NTP statistics.

Command Syntax

```
clear ntp statistics (all-peers | io | local | memory)
```

Parameters

`all-peers`	Counters associated with all peers
`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ntp statistics all-peers
```

debug ntp

Use this command to display NTP debugging messages.

Use the `no` form of this command to stop displaying NTP debugging messages.

Command Syntax

```
debug ntp
```

```
no debug ntp
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#debug ntp
```

```
(config)#no debug ntp
```

feature ntp

Use this command to enable to NTP feature.

Use the `no` form of this command to disable NTP feature and delete all the NTP related configurations.

Command Syntax

```
feature ntp (vrf (NAME|management)|)
no feature ntp (vrf (NAME|management)|)
```

Parameters

`NAME`	User defined vrf
`management`	Virtual Routing and Forwarding name

Default

By default, feature ntp is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. The parameter `NAME` is added in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#feature ntp vrf management
(config)#feature ntp vrf NAME
(config)#no feature ntp vrf management
(config)#no feature ntp vrf NAME
```

ntp acl

Use this command to allow paticular client to communicate with NTP server.

Use the `no` form of this command to remove the particular client from NTP server.

Note: ntp discard option and limited rate flag are required for sending the KOD packet.

Command Syntax

```
ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D| <1-128>)|)
({nopeer|noserve|noquery|nomodify|kod|limited|notrap}|) (vrf (NAME|management)|)
no ntp allow (A.B.C.D | X:X::X:X) (mask (A.B.C.D| <1-128>)|(vrf
  (NAME|management)|))
({nopeer|noserve|noquery|nomodify|kod|limited|notrap}|) (vrf (NAME|management)|)
```

Parameters

`A.B.C.D`	IPV4 address of the client
`X:X::X:X`	IPV6 address of the client
`A.B.C.D`	Mask for the IPv4 address
`1-128`	Mask for the IPv6 address
`nopeer`	Prevent the client from establishing a peer association
`noserve`	Prevent the client from performing time queries
`noquery`	Prevent the client from performing NTPq and NTPdc queries, but not time queries
`nomodify`	Restrict the client from making any changes to the NTP configurations
`kod`	Send a kiss-of-death packet if the client limit has exceeded
`limited`	Deny time service if the packet violates the rate limits established by the discard command
`notrap`	Prevent the client from configuring control message traps
`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, only local host is permitted.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 4.1. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp allow 1.1.1.1 mask 255.255.255.0 nopeer kod notrap noserve vrf
management
```

```
(config)#ntp allow 1.1.1.1 mask 255.255.255.0 nopeer kod notrap noserve vrf
NAME
```

ntp authenticate

Use this command to enable NTP authentication.

Use the `no` form of this command to disable authentication.

Command Syntax

```
ntp authenticate (vrf (NAME|management)|)
no ntp authenticate (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, ntp authenticate is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp authenticate vrf management

(config)#ntp authenticate vrf NAME
```

ntp authentication-key

Use this command to set an NTP Message Digest Algorithm 5 (MD5) authentication key.

Use the `no` form of this command to delete an authentication key.

Command Syntax

```
ntp authentication-key <1-65535> md5 WORD (vrf (NAME|management)|)
ntp authentication-key <1-65535> md5 WORD 7 (vrf (NAME|management)|)
no ntp authentication-key <1-65535> (vrf (NAME|management)|)
```

Parameters

`<1-65534>`	Authentication key number
`Word`	MD5 string (maximum 8 characters)
`7`	Encrypt using weak algorithm
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp authentication-key 535 md5 J@u-b;l2 vrf management

config)#ntp authentication-key 552 md5 J@u-b;l4 vrf NAME
```

ntp enable

Use this command to enable NTP feature and start the NTP service.

Use the `no` form of this command to stop the NTP service.

Command Syntax

```
ntp enable (vrf (NAME|management)|)
no ntp enable (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name.

Default

By default, ntp is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME in` OcNOS version 6.5.3

Example

```
#configure terminal
(config)#ntp enable vrf management

(config)#ntp enable vrf NAME
```

ntp discard

Use this command to enable rate limiting access to the NTP service running on a system.

Use the no form of this command to disable rate limiting access to the NTP service running on a system.

This NTP discard option and limited rate flag are required for sending the KOD packet. KOD (Kiss of Death) packets have the leap bits set unsynchronized and stratum set to zero and the reference identifier field set to a four-byte ASCII code. If the noserve or notrust flag of the matching restrict list entry is set, the code is "DENY"; if the limited flag is set and the rate limit is exceeded, the code is "RATE".

Command Syntax

```
ntp discard {  minimum <1-65535> } (vrf (NAME|management)|)
no ntp discard {  minimum <1-65535> } (vrf (NAME|management)|)
```

Parameters

`minimum`	Specify the minimum interpacket spacing <default 2>
`<0-65535>`	Minimum value
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, the minimum value is 2.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 4.2. Added parameter `NAME in` OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp discard minimum 50 vrf management

(config)#ntp discard minimum 60 vrf NAME
```

ntp logging

Use this command to log NTP events.

Use the `no` form of this command to disable NTP logging.

Command Syntax

```
ntp logging (vrf (NAME|management)|)
no ntp logging (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, ntp logging message is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME in` OcNOS version 6.5.3

Example

```
#configure terminal
(config)#ntp logging vrf management

(config)#ntp logging vrf NAME
```

ntp master

Use this command to run a device as an NTP server.

Use the `no` command to disable the NTP server.

Command Syntax

```
ntp master (vrf (NAME|management)|)
no ntp master (vrf (NAME|management)|)
```

Parameters

`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, NTP master is disabled

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 4.1.Added parameter `NAME in` OcNOS version 6.5.3

Example

```
#configure terminal
(config)#ntp master vrf management

(config)#ntp master vrf NAME
```

ntp master stratum

Use this command to set stratum value for NTP server.

Use the `no` command to remove stratum value.

The NTP Stratum model is a representation of the hierarchy of time servers in an NTP network, where the Stratum level (0-15) indicates the device's distance to the reference clock.

Command Syntax

```
ntp master stratum <1-15> (vrf (NAME|management)|)
no ntp master stratum (vrf (NAME|management)|)
```

Parameters

`<1-15>`	Stratum value for NTP server
`vrf`	Virtual Router and Forwarding
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, NTP startum value is 16.

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 4.1. Added parameter `NAME in` OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp master stratum 2 vrf management

(config)#ntp master stratum 2 vrf name
```

ntp peer

Use this command to configure a peer association. In a peer association, this system can synchronize with the other system or the other system can synchronize with this system.

Use the `no` command to remove a peer association.

Command Syntax

```
ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
no ntp peer (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf (NAME|management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
no ntp peer (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf (NAME|management|)
```

Parameters

`A.B.C.D`	IPv4 address of the peer
`HOSTNAME`	Host name of the peer
`X:X::X:X`	IPv6 address of the peer
`prefer`	Prefer this peer; preferred peer responses are discarded only if they vary dramatically from other time sources
`key`	Peer authentication key
`<1-65534>`	Peer authentication key
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, value of `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME in` OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ntp peer 10.10.0.23 vrf management
(config)#ntp peer 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp peer 10.10.0.23 vrf management

#configure terminal
(config)#ntp peer 10.10.0.24 vrf management
(config)#ntp peer 10.10.0.24 prefer key 12355 vrf NAME

(config)#no ntp peer 10.10.0.24 vrf NAME
```

ntp request-key

Use this command to define NTP request-key which is used by the NTPDC utility program. NTP client should be able to modify NTP server configuration by using this request-key. Request key must be a trusted key.

Use `no` form of this command to remove a request key.

Command Syntax

```
ntp request-key <1-65534> (vrf (NAME|management)|)
no ntp request-key <1-65534> (vrf (NAME|management)|)
```

Parameter

`<1-65534>`	Request key number
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

No default value

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 5.1 MR. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp request-key 123 vrf management

(config)#ntp request-key 123 vrf NAME
```

ntp server

Use this command to configure an NTP server so that this system synchronizes with the server, but not vice versa.

Use the `no` option with this command to remove an NTP server.

Command Syntax

```
ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) vrf (NAME|management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) vrf (NAME|management|)
no ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-16>}|) (vrf (NAME|management|)
no ntp server (A.B.C.D | HOSTNAME) ({prefer|key|minpoll|maxpoll}|) vrf (NAME|management|)
```

Parameters

`A.B.C.D`	IPv4 address of the server
`HOSTNAME`	Host name of the server
`X:X::X:X`	IPv6 address of the server
`prefer`	Prefer this server; preferred server responses are discarded only if they vary dramatically from other time sources
`key`	Server authentication key
`<1-65534>`	Server authentication key
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#ntp server 10.10.0.23 vrf management
(config)#ntp server 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp server 10.10.0.23 vrf management

(config)#ntp server 10.10.0.24 vrf NAME
(config)#ntp server 10.10.0.24 prefer key 12345 vrf NAME

(config)#no ntp server 10.10.0.24 vrf NAME
```

ntp sync-retry

Use this command to retry NTP synchronization with configured servers.

Command Syntax

```
ntp sync-retry (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#ntp sync-retry vrf management

#ntp sync-retry vrf NAME
```

ntp trusted-key

Use this command to define a “trusted” authentication key. If a key is trusted, the device will synchronize with a system that specifies this key in its NTP packets.

Use the `no` option with this command to remove a trusted key.

Command Syntax

```
ntp trusted-key <1-65535> (vrf (NAME|management)|)
no ntp trusted-key <1-65535> (vrf (NAME|management)|)
```

Parameter

`<1-65534>`	Authentication key number
`management`	Virtual Routing and Forwarding name
`NAME`	User defined vrf name

Default

By default, ntp trusted key is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Example

```
#configure terminal
(config)#ntp trusted-key 234676 vrf management

(config)#ntp trusted-key 234676 vrf NAME
```

show ntp authentication-keys

Use this command to display authentication keys.

Command Syntax

```
show ntp authentication-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ntp authentication-keys
--------------------------
 Auth Key       MD5 String
--------------------------
123             0xa2cb891442844220
#
```

Table 3 explains the output fields.

Table 3: show ntp authentication-key fields

Entry	Description
Auth key	Authentication key (password). Use the password to verify the authenticity of packets sent from this interface or peer interface.
MD5 String	One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list.

show ntp authentication-status

Use this command to display whether authentication is enabled or disabled.

Command Syntax

```
show ntp authentication-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp authentication-status
Authentication enabled
```

show ntp logging-status

Use this command to display the NTP logging status.

Command Syntax

```
show ntp logging-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp logging-status
NTP logging enabled
```

show ntp peer-status

Use this command to display the peers for which the server is maintaining state along with a summary of that state.

Command Syntax

```
show ntp peer-status
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh ntp peer-status
Total peers : 1
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode,
x - source false ticker
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*216.239.35.4    .GOOG.           1 u   24   64  377   38.485    0.149   0.053
#
```

Table 4 explains the output fields.

Table 4: show ntp peer-status fields

Entry	Description
Total peers	Number of servers and peers configured.
* - selected for sync, + - peer mode (active), - - peer mode (passive), = - polled in client mode x - source false ticker	Fate of this peer in the clock selection process.
Remote	Address of the remote peer.
refid	Reference ID (0.0.0.0 for an unknown reference ID).
st	The stratum of the remote peer (a stratum of 16 indicated remote peer is unsynchronized).
t	Type of peer (local, unicast, multicast and broadcast).
when	Time the last packet was received.

Table 4: show ntp peer-status fields

Entry	Description
poll	The polling interval (seconds).
reach	The reachability register (octal).
delay	Current estimated delay in seconds.
offset	Current estimated offset in seconds.
jitter	Current dispersion of the peer in seconds.

show ntp peers

Use this command to display NTP peers.

Command Syntax

```
show ntp peers
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp peers
-----------------------------------------------------------
Peer IP Address                          Serv/Peer
-----------------------------------------------------------
216.239.35.4                             Server (configured)
```

Table 5 explains the output fields.

Table 5: show ntp peers fields

Entry	Description
Peer IP Address	Address of the neighbor protocol.
Serv/Peer	List of NTP peers and servers configured or dynamically learned.

show ntp statistics

Use this command to display NTP statistics.

Command Syntax

```
show ntp statistics (io | local | memory | peer ( ipaddr (A.B.C.D | X:X::X:X ) |
  name (HOSTNAME)) )
```

Parameters

`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation
`peer`	Counters associated with the specified peer
`A.B.C.D`	Peer IPv4 address
`X:X::X:X`	Peer IPv6 address
`HOSTNAME`	Peer host name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp statistics local
time since restart:     1685
time since reset:       1685
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0
bad length or format:   0
bad authentication:     0
rate exceeded:          0
#show ntp statistics memory
time since reset:     1698
total peer memory:    15
free peer memory:     15
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
```

Table 6 explains the output fields.

Table 6: show ntp statisticsfields

Entry	Description
Time since restart	Time when the ntp protocols were last started and how long they have been running.
Time since reset	Time when the ntp protocols were last reset and how long they have been running.
Packets received	Number of packets received from the peers.
Packets processed	Number of packets processed to the peers.
Current version	Current version of the protocol that is being used.
Previous version	Previous version of the protocol that has been used.
Declined	Access to the protocol declined
Access denied	Number of attempts denied to access protocol
Bad length or format	Number of messages received with length or format errors so severe that further classification could not occur.
Bad authentication	Number of messages received with incorrect authentication.
Rate exceeded	Exceed the configured rate if additional bandwidth is available from other queues
Total peer memory	Actual memory available to the peer system.
Free peer memory	Free memory available to the peer system.
Calls to find peer	Number of calls to find peer.
New peer allocations	Number of allocations from the free peer list.
Peer demobilizations	Number of structures freed to free peer list.
Hash table counts	Peer hash table’s each bucket count.

© 2025 IP Infusion Inc. Proprietary

show ntp trusted-keys

Use this command to display keys that are valid for authentication.

Command Syntax

```
show ntp trusted-keys
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ntp trusted-keys

Trusted Keys:
333
#
```

Table 7 explains the output fields.

Table 7: show ntp trusted-keys fields

Entry	Description
Trusted Keys	Keys that are valid for authentication.

show running-config ntp

Use this command to display the NTP running configuration.

Command Syntax

```
show running-config ntp (|all)
```

Parameters

`all`	Reserved for future use

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh running-config ntp
feature ntp vrf management
ntp enable vrf management
ntp authenticate vrf management
ntp logging vrf management
ntp authentication-key 123 md5 0xa2cb891442844220 7 vrf management
ntp trusted-key 123 vrf management
ntp server 216.239.35.4 vrf management
```

Fault Management System Configuration

CHAPTER 1 Fault Management System Configuration

The Fault Management System (FMS) provides a framework for event detection, correlation, and alarm generation. Each event triggers an alarm based on correlation logic parameters specified by individual Protocol Modules. Events, as OPER_LOGs relayed from the VLOGd module, are processed according to the correlation rules in the configuration file `alarm_def_config.yaml`. The generated alarms persist to indicate faults and are maintained in a database accessible via `show` commands.

Note:

- FMS is disabled by default. Once enabled, it triggers alarms for all valid `OPER_LOG` events received by the FMS node.js process.
- The FMS event-alarm correlation configuration is stored in a YAML file (`alarm_def_config.yaml`), which cannot be modified via CMLSH commands. If changes are required, an operator with the appropriate privileges can edit the file in YAML syntax, but only before starting FMS. Once FMS is active, editing this file is prohibited, as changes take effect only after FMS is disabled, updated, and then re-enabled.
- The device's logging level must be set to at least 4 (NOTIFY) to ensure that FMS receives notification events and can take appropriate action. Setting a lower logging level may prevent FMS from receiving clear events, resulting in unresolved active alarms. FMS does not manage the system logging level.
- FMS relies on the loopback interface (`lo0`) for communication with VLOGd, so the operational status of `lo0` is essential for both FMS and VLOGd.
- If Localhost communication is blocked by the Access Control List (ACL), FMS must be disabled. Conversely, if FMS is enabled, the ACL must not block Localhost.
- If FMS reboots due to a device reboot, upgrade, downgrade, or manual restart, active alarms are closed. Use the show alarm closed CLI command to view closed active alarms.

FMS applies correlation procedures based on the configurations specified

Table 1-1: FMS correlation procedures

Correlation type	Description
Generalization	• Groups two or more events into a single alarm. • A generalized alarm will further use one of the correlation types (none, time-bound, counting and compression) for applying correlation logic to the new alarm.
Time-bound	• Stipulates that when the event is received, a timer is started for that event. • While the timer is running, subsequent events of the same type are suppressed. • On the expiry of the timer, an alarm will be raised for that event stating the count for the number of times that event was received in this duration.
Counting	Considers a specified number of similar events as one. In this correlation type, the respective alarm will be raised after the event has occurred for count times.
Compression	Check multiple occurrences of the same event for duplicate/redundant event information, remove the redundancies, and report them as a single alarm.
Severity	Correlates events based on the severity of the events.

Implementation

FMS was developed with NodeJS with scripts written in JavaScript with a `*.js` extension and configuration files with a `*.yaml` extension. These files are in the below paths in OcNOS.

Table 1-2: FMS script and configuration files

`/usr/local/bin/js`	JavaScript files (`*.js` files)
`/usr/local/etc`	Configuration files (`*.yaml` files)

Enabling and Disabling the Fault Management System

Follow the below steps to enable or disable FMS:

Enabling FMS

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#fault-management enable
(config)#
```

Disabling FMS

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#
(config)#fault-management disable
(config)#
```

Alarm Configuration File

The alarm configuration file contains the configurations/rules for the alarms that will be referred by FMS to generate alarms upon receiving events. This file is in `*.yaml` format (human readable) in `/usr/local/etc`.

This file can be edited before starting FMS to include correlation rules for specific events.

Alarm Configuration File Template

```
#-------Template-------
#- Event_Group:
#  - ALARM_ID:                          # Integer number identifying alarm
#    ALARM_TYPE_ID:                    # Alarm Type-id(AIS, EQPT, LOS, OTS, OPWR, UNKNOWN)
#    EVENT:                            # Event name(oper_log)
#    GENERALIZED_EVENT_NAME:           # Event name for the Generalization Event Group
#    ALARM_DESC:                       # Alarm string which will be generated
#    CORRELATION_TYPE:                 # Correlation logic type(0:No-Correlation,
1:Generalization, 2:Timebound, 3:Counting, 4:Compression, 5:Drop-Event, 6:Severity)
```

```
#    GENERALIZED_CORRELATION_TYPE     # Correlation type, in which generalized event
will be sent
#    CORRELATION_COUNTER:             # Counter value that will be considered during
counting logic to raise alarm
#    CORRELATION_TIMER_DURATION:      # Timer duration to be considered for time bound
logic
#    CORRELATION_SEVERITY:            # Alarm Severity(0:Critical, 1:Major, 2:Warning,
3:Minor, 4:Unknown)
#    QUALIFIER_STRING_POSITION:       # List of positions where qualifier values present
#      QUALIFIER_POSITION_1_EVENT_1:  # First position of the qualifier value in the
first event
#    RESOURCE_STRING_POSITION:        # List of positions where resource values present
#      RESOURCE_POSITION_1_EVENT_1:   # First position of the resource value in the
first event
#    SNMP_TRAP:                       # SNMP TRAP (true(1) or false(0))
#    SNMP_OID:                        # OID for SNMP TRAP
#    NETCONF_NOTIFICATION:            # Netconf Notification (true(1) or false(0))
#    CLEAR_ALARM:                    # Clear Alarm (oper_log enum, Status for Alarm will
be made In-active if this event is received)
#    CLEAR_EVENT_PATTERN_VALUES:     # Pattern values which will be searched in event's
description to identify clear event and to clear active alarm (required if both active
and clear event types are same)
#    SNMP_TRAP_CLEAR:                # true(1) or false(0, if CLEAR_ALARM is null then
SNMP_TRAP_CLEAR will be null)
#    SNMP_CLEAR_OID:                  # OID for SNMP TRAP CLEAR
#    NETCONF_CLEAR_NOTIFICATION:      # Clear Netconf Notification information
```

Auto Generating the Alarm Configuration File

The `auto_yaml_generator.js` file is a NodeJS script that generates the alarm configuration file (`alarm_def_config.yaml`) for the oper logs which are listed in the `oper_logs_list.yaml` file with the default values as shown below.

```
# Integer number identifying alarm
ALARM_ID:  1000
# Event name (oper_log)
EVENT:  oper_log string
# Event name for the Generalization Event Group
GENERALIZED_EVENT_NAME:      null
# Alarm string which will be generated
ALARM_DESC:  oper_log string
# Correlation logic type (0: No-Correlation, 1: Generalization, 2: Time Bound, 3:
Counting, 4: Compression, 5: Drop-Event)
CORRELATION_TYPE:  0
# Correlation type, in which generalized event will be sent
GENERALISED_CORRELATION_TYPE: null
# Counter value that will be considered during counting logic to raise alarm
CORRELATION_COUNTER: 3
# Timer duration to be considered for time bound logic
CORRELATION_TIMER_DURATION:   20000
# Alarm Severity(1:Emergency, 2:Alert, 3:Critical, 4:Error, 5:Warning, 6:Notification,
7:Informational, 8:Debugging, 9:Cli)
CORRELATION_SEVERITY: null
```

```
# QUALIFIER_STRING_POSITION
   QUALIFIER_POSITION_1_EVENT_1: null
# RESOURCE_STRING_POSITION
   RESOURCE_POSITION_1_EVENT_1: null
SNMP_TRAP: 0
# OID for SNMP TRAP
SNMP_OID: null
# Netconf Notification (true (1) or false (0))
NETCONF_NOTIFICATION: 1
# Clear Alarm (oper_log enum, Status for Alarm will be made In-active if this event is
received)
CLEAR_ALARM: null
# Clear Event's pattern values which will be searched in event's description to identify
clear event
CLEAR_EVENT_PATTERN_VALUES: null
# True (1) or False (0, if CLEAR_ALARM is null then SNMP_TRAP_CLEAR will be null)
SNMP_TRAP_CLEAR: 0
# OID for SNMP TRAP CLEAR
SNMP_CLEAR_OID: null
# Clear Netconf Notification information
NETCONF_CLEAR_NOTIFICATION: 0
```

Alarm Configuration File Generation Steps

1. List all the oper_log enums in the `oper_logs_list.yaml` file and keep the file in the same path with `auto_yaml_generator.js`.
2. Copy `auto_yaml_generator.js` and `oper_logs_list.yaml` files into `/usr/local/bin/js`.
3. Run the `auto_yaml_generator.js` script with the following command.

   ```
   #node auto_yaml_generator.js
   ```
4. After executing the above commands, you will see the `alarm-def-config.yaml` file in the same directory.

Sample oper_logs_list.yaml File

```
EVENT_GROUP:
  IFMGR_IF_DOWN,
  IFMGR_IF_UP,
  STP_SET_PORT_STATE,
  STP_IPC_COMMUNICATION_FAIL,
  STP_ROOTGUARD_PORT_BLOCK,
  :
  :
```

Alarm Descriptions

Table 1-3 describes the supported alarms.

Table 1-3: FMS alarms

Alarm	Description
CMM_DDM_MONITOR_CURRENT	Transceiver Bias Current crossed the threshold limit
CMM_DDM_MONITOR_FREQ	Transceiver Frequency crossed the threshold limit
CMM_DDM_MONITOR_RxPOWER	Transceiver Rx Power crossed the threshold limit
CMM_DDM_MONITOR_TEC	Transceiver Thermoelectric Cooler fault
CMM_DDM_MONITOR_TEMP	Transceiver Temperature crossed the threshold limit
CMM_DDM_MONITOR_TxPOWER	Transceiver Tx Power crossed the threshold limit
CMM_DDM_MONITOR_VOLT	Transceiver Voltage crossed the threshold limit
CMM_DDM_MONITOR_WAVE	Transceiver Wavelength crossed the threshold limit
CMM_FAN_CTRL	Fan insertion, removal, speed, or fault condition alarm
CMM_MONITOR_CPU	CPU load average crossed the threshold limit
CMM_MONITOR_CPU_CORE	CPU core usage crossed the threshold limit
CMM_MONITOR_CURRENT	Current crossed the threshold limit
CMM_MONITOR_DISK_READ_ACTIVITY	Disk read activity crossed the threshold limit
CMM_MONITOR_DISK_REMAIN_LIFE	Disk remaining life crossed the threshold limit
CMM_MONITOR_DISK_WRITE_ACTIVITY	Disk write activity crossed the threshold limit
CMM_MONITOR_FAN	FAN RPM crossed the threshold limit
CMM_MONITOR_PSU_IIN	Power supply unit input current crossed the threshold limit
CMM_MONITOR_PSU_IOUT	Power supply unit output current crossed the threshold limit
CMM_MONITOR_PSU_PIN	Power supply unit input power crossed the threshold limit
CMM_MONITOR_PSU_POUT	Power supply unit output power crossed the threshold limit
CMM_MONITOR_PSU_POWER	Power supply unit insertion, removal, or fault condition
CMM_MONITOR_PSU_PRESENCE	Power supply unit is present
CMM_MONITOR_PSU_TEMP1	Power supply unit temperature 1 crossed the threshold limit
CMM_MONITOR_PSU_TEMP2	Power supply unit temperature 2 crossed the threshold limit
CMM_MONITOR_PSU_VIN	Power supply unit input voltage crossed the threshold limit
CMM_MONITOR_PSU_VOUT	Power supply unit output voltage crossed the threshold limit
CMM_MONITOR_RAM	RAM memory usage crossed the threshold limit

© 2025 IP Infusion Inc. Proprietary

Table 1-3: FMS alarms (Continued)

Alarm	Description
CMM_MONITOR_SDCARD	Hard-disk usage crossed the threshold limit or fault condition
CMM_MONITOR_TEMP	Temperature sensor crossed the threshold limit
CMM_MONITOR_VOLTAGE	Voltage crossed the threshold limit
CMM_TRANSCEIVER	Transceiver on fault condition
HW_PROFILE_MONITOR	TCAM Utilization
IFMGR_IF_DOWN	Interface state down
IFMGR_IF_UP	Interface state up
HW_PROFILE_MONITOR	TCAM group utilization

CHAPTER 2 Event Manager

Overview

The event manager feature facilitates the automatic execution of a particular action item based on the event (operator log messages) that occurred in a device. This feature is configured by command line interface (CLI) and NetConf.

The following are the three parameters in the event manager feature:

Event: It is a trigger where event manager functionality starts. Once the syslog message with the details mentioned in the event occurs, an action is triggered. Some sample events are as follows:

- IFMGR_IF_DOWN
- IFMGR_IF_UP
- STP_SET_PORT_STATE
- STP_IPC_COMMUNICATION_FAIL

Action: Once an event has occurred, an action is triggered if there is a match of the event ID in the database. An action is executed by the execution of a Python script consisting of executable OcNOS commands and configurations.

The sample action script is as follows:

```
import sys,os,time
import subprocess

#MACROS#
########
TIME = 1

#VARIABLES#
##############
cmd_db_lock = "cmlsh -e 'configure terminal force "+str(TIME)+"'"
cli_commands ="cmlsh -e 'configure terminal' -e 'interface xe11' -e 'shutdown'
-e 'commit' -e'end'"

if __name__ == '__main__':
#if name == 'main':
  #Force user out of config mode after X seconds
  os.system (cmd_db_lock)
  #Wait X seconds before running clis
  time.sleep(TIME)

  os.system(cli_commands)
```

Policy: It maps the action with an event.

Feature Characteristics

- The feature creates a database of event IDs and the corresponding actions as configured through CLI. When an event occurs, the event is matched in the database with the existing event ID, severity, and log pattern. If the event matches with the existing event in the database, it triggers a corresponding action automatically. If there is no match with the database, then no action is taken.

© 2025 IP Infusion Inc. Proprietary

- Configurable parameters for an event are event ID, severity, and log pattern, which are matched with the incoming log. In order to be unique, the recommendation is to have all these parameters configured for an event. Configuring the event ID is mandatory, while severity and pattern are optional. No manual configuration of severity applies the default severity of `all` (`0-6`).
- Duplicate event configuration with the same value for event ID, severity, and log pattern as an existing event with a new event name is not allowed and displays an error.
- The feature facilitates the configuration of one action for multiple events.
- Place the action script file in the path */usr/local/etc*. A warning message is displayed if the script file is not in the path, but the configuration is accepted.
- The execution count or the trigger count per policy is stored and maintained. When a policy is cleared, the event and the action associated with the policy get cleared. When an action is associated with multiple policies, the action associated with the cleared policy is removed, and the same action associated with other policies remains.
- This feature consumes a certain amount of CPU performance because it matches the logs recorded by the system with every configured event. Hence, a maximum number of 50 events, actions, and policies is configurable.
- The command line shell (cmlsh) uses a locking mechanism. Follow the recommendation when a user or script file gets into the configure mode:
  - Disable the event manager feature while executing manual configuration in the system. This prevents the Python script from interfering with the manual configuration. After executing the manual configuration, enable the event manager feature.
  - There is a possibility of multiple Python scripts executing simultaneously. In order to sequence the configure mode execution, the Python script has the logic to wait for 45 seconds in the configure mode. This prevents the Python script from exiting without executing the commands if another script is still in configure mode.
  - If the script fails to execute, the event manager does not record such failures.

Validation checks:

- When the feature is neither enabled nor disabled, the event, action, or policy configuration displays an error.
- The event manager displays an error if an event is edited when associated with a policy.
- The event manager exercises priority-based selection of policies for any incoming logs. When there are more actions associated with the same event with different event IDs, severity levels, and pattern, the priority sequence is as follows:

  1. Matches the incoming log against a policy that has an event configured with all the parameters, which are event ID, severity, and pattern string.
  2. Matches the incoming log against a policy that has an event configured with only event ID and severity.
  3. Matches the incoming log against a policy that has an event configured only with the event ID.

Example 1:

For the following configuration, when actual log "`2020 Jan 03 08:46:56.455 : MH2 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe3 changed state to up`" is received, event-manager execute `action a2` (file2) than `action a1` as this configuration matches the best.

```
#event-manager event e1 IFMGR_IF_UP severity 2
#event-manager event e2 IFMGR_IF_UP severity 2 pattern "Interface xe3"
#event-manager action a1 script file1
#event-manager action a2 script file2
#event-manager policy p1 event e1 action a1
```

```
#event-manager policy p2 event e2 action a2
```

Example 2:

For the following configuration, when actual log "`2020 Jan 03 08:46:56.455 : MH2 : NSM : CRITI : [IFMGR_IF_UP_2]: Interface xe3 changed state to up`" is received, event-manager executes either `action a1` (file1) or `action a2` based on whichever gets hit first during database search. The recommendation is not to mix the same event configuration with a pattern and without a pattern for the same event ID.

```
#event-manager event e1 IFMGR_IF_UP severity 2 pattern "Interface "
#event-manager event e2 IFMGR_IF_UP severity 2 pattern "Interface xe3"
#event-manager action a1 script file1
#event-manager action a2 script file2
#event-manager policy p1 event e1 action a1
#event-manager policy p2 event e2 action a2
```

- The solution supports the validation of event-id against configurable event-ids. It displays an error if the entered event-id is not supported.

Benefits

The event manager feature allows the execution of an automatic action when a failure or any other priority error occurs.

Configuration

This section shows the configuration of the Event Manager feature.

Configuring Event Manager

Follow the steps to configure the Event Manager feature.

1. Configure the command `event-manager enable` to enable event-manager functionality in the device.

   ```
   (config)#event-manager enable
   ```

2. Follow the steps to configure an event or an action.:

   - To create an event, define the `event` name (`E1`), `type (syslog)`, event ID (`IFMGR_IF_UP`), and optional parameters of `severity (0)` and `pattern ("xe5").`

   ```
   (config)#event-manager event E1 type syslog IFMGR_IF_UP severity 0 pattern
   "xe5"
   ```

   - To create an action, save the python script in the */usr/local/etc* path and define the action name (`A1`), the type (`script`) and the type value (`ifup.py`).

   ```
   (config)#event-manager action A1 type script ifup.py
   ```

3. To map an event to an action, create a policy, specify the policy name (`P1`), and map the event name (`E1`) with the action name (`A1`).

   ```
   (config)#event-manager policy P1 event E1 action A1
   ```

Running configurations

The running configuration is as follows:

```
!
event-manager enable
event-manager action A1 type script ifdown.py
```

```
event-manager event E1 type syslog IFMGR_IF_DOWN pattern "xe5"
event-manager policy P1 event E1 action A1
!
```

Validation

Validate the show output after configuration as shown below.

```
#show event-manager event all

Events configured : 1

Event Name                          Type       Type Value   Trigger Cnt    Status     Policy-Mapped
=================================================================================================
E1                                  syslog     IFMGR_IF_U         0        Active     P1


#show event-manager action all

Actions configured : 1

Action Name                                Type       Type Value   Trigger Cnt    Policy-Count   Status
=================================================================================================
A1                                         script     ifup.py           0             1        Active

#show event-manager policy all

Policies configured : 1

Policy Name                        Trigger Cnt      Event      Action     Last Exec Status   Last Exec Time
=================================================================================================
P1                                       0          E1         A1            Not-Run         -

*****************************************************************************************************************
************
```

Event Manager Commands

The Event Manager feature introduces the following configuration and show commands.

- clear event-manager statistics
- event-manager
- event-manager action
- event-manager event
- event-manager policy
- show event-manager action
- show event-manager event
- show event-manager policy
- show event-manager system-event-ids

clear event-manager statistics

Use this command to clear all the policies or a specific policy.

Note: The clear policy removes the action associated with this policy, but the same action associated with other policies remain.

Command Syntax

```
clear event-manager statistics (policy NAME|all|)
```

Parameters

`policy NAME`	Removes the specific policy.
`statistics all`	Removes all the configured policies.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration shows how to clear all the policies:

```
OcNOS#configure terminal
OcNOS(config)#clear event-manager statistics all
OcNOS(config)#commit
OcNOS(config)#exit
```

event-manager

Use this command to enable or disable the event manager feature. The event manager intercepts the incoming logs for the configured event when the event and action are mapped to a policy.

Use the `no` command to remove all the event manager configurations.

Command Syntax

```
event-manager (enable|disable)
```

```
no event-manager
```

Parameters

`enable`	Enables the event manager feature to configure events, actions, and policies.
`disable`	Disables the event manager feature, but the configuration of new events, actions, and policies is allowed, and the existing configuration remains the same.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration shows how to enable the event manager:

```
OcNOS#configure terminal
OcNOS(config)#event-manager enable
OcNOS(config)#commit
OcNOS(config)#exit
```

The below configuration shows how to disable the event manager:

```
OcNOS#configure terminal
OcNOS(config)#event-manager disable
OcNOS(config)#commit
OcNOS(config)#exit
```

event-manager action

Use this command to create an action, configure an action name, and associate a Python script.

Use `no` command to remove an action.

Note: Configuration of an existing action with new parameters overwrites the old configured parameters.

Command Syntax

```
event-manager action NAME type script SCRIPT
no event-manager action NAME
```

Parameters

`action NAME`	Name of the action that is configured.
`script SCRIPT`	Name of the Python script associated with the action.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration shows how to configure an action:

```
OcNOS#configure terminal
OcNOS(config)#event-manager action A1 type script ifup.py
OcNOS(config)#commit
OcNOS(config)#exit
```

event-manager event

Use this command to configure an event with the event name and event ID, along with the options to configure the severity and the pattern.

Use no form of the command to remove an event or remove the parameters from an event.

Note: Configuration of an event with a different event name but the same event ID, severity, and pattern is not supported, and an error is displayed.

Note: Configuration of an existing event with new parameters overwrites the old configured parameters.

Command Syntax

```
event-manager event NAME type syslog EVENT-ID (severity <0-5>|all|) (pattern
  "PATTERN"|)
no event-manager event NAME (severity|pattern|)
```

Parameters

`event NAME`	Name of the event that is configured.
`syslog EVENT-ID`	A problem keyword that gets matched with the incoming logs to trigger the configured action.
`severity <0-5>`	(Optional) If configured with a severity level, this parameter is matched with the incoming logs to trigger an event with the configured severity level only. The range is from 0 to 5.
`severity all`	(Optional) If not configured, this parameter is matched with the incoming logs to trigger an event with all the severity levels (from 0 to 5).
`pattern "PATTERN"`	(Optional) If configured with a sub-string, this parameter matches the sub-string with the incoming log to trigger an event.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration shows how to configure an event:

```
OcNOS#configure terminal
(config)#event-manager event E1 type syslog IFMGR_IF_UP severity 0 pattern
"xe5"
OcNOS(config)#commit
```

```
OcNOS(config)#exit
```

event-manager policy

Use this command to map an event to an action.

Use no command to remove a policy.

Note: Configuration of an existing policy with a new event and action overwrites the old configured mapping of the event with the action.

Command Syntax

```
event-manager policy NAME event NAME action NAME
no event-manager policy NAME
```

Parameters

`policy NAME`	Name of the policy configured to associate an event with an action.
`event NAME`	Name of the event that is associated with an action.
`action NAME`	Name of the action that runs the Python script for its associated event.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration shows how to configure a policy:

```
OcNOS#configure terminal
OcNOS(config)#event-manager policy P1 event E1 action A1
OcNOS(config)#commit
OcNOS(config)#exit
```

show event-manager action

Use this command to display the action name, the action type, the Python script name, the number of times the script runs, the number of associated policies, and the status.

Command Syntax

```
show event-manager action (NAME|all|)
```

Parameters

`action NAME`	Displays the configuration details of a specific action.
`action all`	Displays the configuration details of all the configured actions.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration displays all the actions configured:

```
#show event-manager action all

Actions configured : 1

Action Name                          Type       Type Value    Trigger Cnt    Policy-Count   Status
=============================================================================================================
A1                                   script     ifup.py           0              1        Active
```

Table P-2-4 explains the show command output fields.

Table 2-4: show event-manager action

Field	Description
Action Name	Displays the name of the configured action or actions.
Type	Displays the type of the action or actions.
Type Value	Displays the name of the Python script.
Trigger Cnt	Displays the number of time the action runs the script.
Policy-Count	Displays the number of policies associated with the action.
Status	Displays if the action is active or not. The action remains inactive if not mapped with a policy.

show event-manager event

Use this command to display the event name, the event type, the event ID, the number of times the event was triggered, the event status, and the associated policy.

Command Syntax

```
show event-manager event (NAME|all|)
```

Parameters

`event NAME`	Displays the configuration details of a specific event.
`event all`	Displays the configuration details of all the configured events.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration displays all the event configured:

```
OcNOS#show event-manager event all

Events configured : 1

Event Name                      Type       Type Value    Trigger Cnt    Status     Policy-Mapped
=============================================================================================
E1                              syslog     IFMGR_IF_U         0        Active     P1
```

Table P-2-5 explains the show command output fields.

Table 2-5: show event-manager event output fields

Field	Description
Event Name	Displays the name of the configure event or events.
Type	Displays the type of the event or events.
Type Value	Displays the event IDs.
Trigger Cnt	Displays the number of time the event is matched with the incoming log and triggered an action.
Status	Displays if the event is active or not. The event remains inactive if not mapped with a policy.
Policy-Mapped	Displays the policy name associated with the event.

show event-manager policy

Use this command to display the policy name, number of times the event triggers the action, the event name, the action name, the status of the last action triggered, and the time of last action triggered.

Command Syntax

```
show event-manager policy (NAME|all|)
```

Parameters

`policy NAME`	Displays the configuration details of a specific policy.
`policy all`	Displays the configuration details of all the configured policies.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The below configuration displays all the event configured:

```
#show event-manager policy all

Policies configured : 1

Policy Name                    Trigger Cnt      Event      Action     Last Exec Status   Last Exec Time
=============================================================================================================
P1                                   0          E1         A1            Not-Run         -
```

Table P-2-6 explains the show command output fields.

Table 2-6: show event-manager policy

Field	Description
Policy Name	Displays the name of the configured policy or policies.
Trigger Cnt	Displays the number of time the action runs the script.
Event	Displays the name of the associated event.
Action	Displays the name of the associated action.
Last Exec Status	Status of the last action triggered.
Last Exec Time	Time of the last action triggered.

show event-manager system-event-ids

Use this command to display all the event IDs.

Command Syntax

```
show event-manager system-event-ids (all| SUBSTRING)
```

Parameters

`system-event-ids all`	Displays all the event IDs.
`system-event-ids SUBSTRING`	Displays the event IDs with this substring.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Examples

The command below displays all the event IDs supported in OcNOS.

```
OcNOS#show event-manager system-event-ids all

IFMGR_IF_DOWN                       IFMGR_IF_UP
STP_SET_PORT_STATE                  STP_IPC_COMMUNICATION_FAIL
STP_ROOTGUARD_PORT_BLOCK            STP_BPDUGUARD_PORT_BLOCK
MCEC_CONF_MISMATCH                  BGP_VPLS_CREATE_ERR
BGP_VPLS_SAME_VE_ID_ERR             BGP_VPLS_MTU_MISMATCH_ERR
LDP_INTERNAL_ERR                    LDP_MSG_DECODE_ERR
:::::
:::::
```

The command below displays all the event IDs configured with substring “OSPF” supported in OcNOS.

```
OcNOS#show event-manager system-event-ids ospf
OSPF_OPR_INIT_FAILED                    OSPF_OPR_GRACEFUL_RESTART_FAILED
OSPF_OPR_MEM_EXHAUST                    OSPF_OPR_DUPLICATE_ROUTER_ID
OSPF_OPR_SELF_ORIGINATED_LSA_RECVD      OSPF_OPR_IFMGR_FAIL
OSPF_OPR_SESSION_DOWN                   OSPF_OPR_TERMINATE
OSPF_OPR_SOCK_FAIL                      OSPF_OPR_SPF_EMPTY_RLSA
OSPF_OPR_INACTIVITY_TIMER_EXPIRED       OSPF_OPR_LOWER_LEVEL_DOWN
OSPF_OPR_BFD_SESSION_DOWN               OSPF_OPR_LSDB_OVERFOW
:::
:::
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
Python script	This is a script file containing a sequence of code that executes an action when an event is triggered. This is a text file with “.py” extension.

Fault Management Sytem Command Reference

CHAPTER 1 FMS Command Reference

This chapter describes the fault management system (FMS) commands:

- fault-management (enable | disable)
- fault-management close
- fault-management flush-db
- fault-management shelve
- show alarm active
- show alarm closed
- show alarm history
- show alarm shelved
- show alarm statistics
- show alarm transitions
- show fms status
- show fms supported-alarm-types
- show running-config fault-management

© 2025 IP Infusion Inc. Proprietary

fault-management (enable | disable)

Use this command to enable or disable the fault management system (FMS).

Note: If the loopback interface is down, FMS will not receive logs, preventing it from generating and clearing alarms, resulting in the loss of these logs.

Command Syntax

```
fault-management (enable | disable)
```

Parameters

`enable`	Enable FMS
`disable`	Disable FMS

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

Enable FMS:

```
(config)# fault-management enable
(config)#commit
%% Warning : FMS requires logging level all to be configured to minimum 4, please
configure accordingly
(config)#
```

Validation:

```
#show fms status
% FMS Status: Enabled
% FMS Node Application Status: Up
```

Disable FMS:

```
(config)# fault-management disable
(config)#commit
```

Validation:

```
#show fms status
% FMS Status: Disabled
```

fault-management close

Use this command to close an active alarm.

Command Syntax

```
fault-management close ACTIVE-ALARM-ID
```

Parameter

`ACTIVE-ALARM-ID`

Identifier of an active alarm

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

After closing an active alarm, it should not be displayed in the active alarms list.

The alarm ID can be found with show alarm history, specifying the `all` parameter.

```
#sh alarm history all
Alarm Count: 1
Severity   Alarm_Type_ID   Alarm_ID          Description
------------------------------------------------------
MAJOR      EQPT            IFMGR_IF_DOWN::ce3/1     2019-02-18T15:07:57.755Z : OcNOS
[IFMGR_IF_DOWN] Interface ce3/1 changed state to down

#sh alarm active
Active Alarms received:-
Active Alarm Count: 1
Severity    Status    Alarm Description
-----------------------------------------
MAJOR       Active    OcNOS [IFMGR_IF_DOWN] Interface ce3/1 changed state to down

#
#fault-management close IFMGR_IF_DOWN::ce3/1
% FMS Response: IFMGR_IF_DOWN::ce3/1 closed
#
#sh alarm active
Active Alarms received:-
There are no active alarms present in the Database
```

fault-management flush-db

Use this command to flush the alarms from the database.

Command Syntax

```
fault-management flush-db
```

Parameter

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#fault-management flush-db
% FMS Response: Database flush completed
```

Validation:

Check that after `fault-management flush-db`, all alarms in the database are flushed:

```
#show alarm active
Active Alarms received:-
There are no active alarms present in the Database
#show alarm history all
There are no alarms present in the Database
#show alarm closed
No alarms are manually closed
#show alarm shelved
No alarm-types are shelved
#show alarm statistics
There are no alarms present in the Database
#show alarm transitions
There are no transition alarms present in the Database
```

fault-management shelve

Use this command to shelve (disable) an alarm type.

Command Syntax

```
fault-management shelve ALARM-TYPE
```

Parameter

ALARM-TYPE	Type of alarm as displayed by show fms supported-alarm-types

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#fault-management shelve CMM_MONITOR_CPU
% FMS Response: Alarm-type CMM_MONTOR_CPU shelved.
#
```

Validation:

Check that after shelving an alarm type, active alarms of that type are not being raised.

```
#fault-management shelve IFMGR_IF_DOWN
% FMS Response: Alarm-type IFMGR_IF_DOWN shelved.
#
#show alarm shelved
Alarm-type Count: 1
Alarm Type
------------------
IFMGR_IF_DOWN
#
(config)#interface ce1/1
(config-if)#shutdown
(config-if)#commit
2019 Feb 18 15:21:31.229 : OcNOS : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface ce1/1
changed state to down
(config-if)#end
#
#show alarm history all
There are no alarms present in the Database
#show alarm active
Active Alarms received:-
There are no active alarms present in the Database
#
```

show alarm active

Use this command to display the current active alarms in the database.

Command Syntax

```
show alarm active
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0 and the output changed in OcNOS version 6.1.0.

Example

```
#show alarm active
Active Alarms received:-
Active-Alarms-Count: 1
Alarm-Date-Time              Severity     Alarm-ID          Alarm-Description
------------------------------------------------------------------------------
2019-02-15T19:57:14.525Z     MAJOR        IFMGR_IF_DOWN::xe8     OcNOS [IFMGR_IF_DOWN]
Interface xe8 changed state to down
#
```

show alarm closed

Use this command to display alarms that are manually closed.

Command Syntax

```
show alarm closed
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show alarm closed
Alarm Count: 1
Severity   Alarm_Type_ID   Alarm_ID          Description
------------------------------------------------------
MAJOR      EQPT            IFMGR_IF_DOWN::xe7     FMS [IFMGR_IF_DOWN] Interface xe7
changed state to down

#
```

show alarm history

Use this command to show the alarm history.

Command Syntax

```
show alarm history (1-day | 1-hr | 1-week | all)
```

Parameters

`1-day`	Display alarms in the last 1 day
`1-hr`	Display alarms in the last 1 hour
`1-week`	Display alarms in the last 1 week
`all`	Display all the alarms

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show alarm history ?
  1-day   Display alarms in the last 1 day
  1-hr    Display alarms in the last 1 hour
  1-week  Display alarms in the last 1 week
  all     Display all the alarms
```

show alarm shelved

Use this command to display shelved (disabled) alarm types.

Command Syntax

```
show alarm shelved
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show alarm shelved
Alarm-type Count: 1
Alarm Type
-------------------
IFMGR_IF_DOWN

#
```

show alarm statistics

Use this command to display the alarm statistics.

Command Syntax

```
show alarm statistics
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show alarm statistics
Alarm Statistics :-
Alarm Count: 1
Current Severity    Count    Alarm ID
---------------------------------------
MAJOR               1        IFMGR_IF_UP::ce3/1

#
#
```

show alarm transitions

Use this command to display severity transitions for every alarm in the device.

Command Syntax

```
show alarm transitions
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show alarm transitions
Alarms received:-
Alarm Count: 3
Downgraded     CRITI    MAJOR    CMM_MONITOR_CPU:1min_load:CPU
Upgraded       MAJOR    CRITI    CMM_MONITOR_CPU:1min_load:CPU
Downgraded     CRITI    MAJOR    CMM_MONITOR_CPU:1min_load:CPU


#
```

show fms status

Use this command to display the FMS status.

Command Syntax

```
show fms status
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#
#show fms status
% FMS Status: Enabled
% FMS Node Application Status: Up
#
```

show fms supported-alarm-types

Use this command to display the supported alarm types.

Command Syntax

```
show fms supported-alarm-types
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

```
#show fms supported-alarm-types
Alarm-types Count: 38

IFMGR_IF_DOWN
IFMGR_IF_UP
CMM_MONITOR_RAM
CMM_MONITOR_CPU
...
#
```

show running-config fault-management

Use this command to display FMS status in the running configuration.

Command Syntax

```
show running-config fault-management
```

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show running-config fault-management
!
fault-management enable
!
#
```

SNMP Configuration

CHAPTER 1 Simple Network Management Protocol

Overview

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried by SNMP managers.

In SNMP, administration groups are known as communities. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption

SNMP is defined in RFCs 3411-3418.

Topology

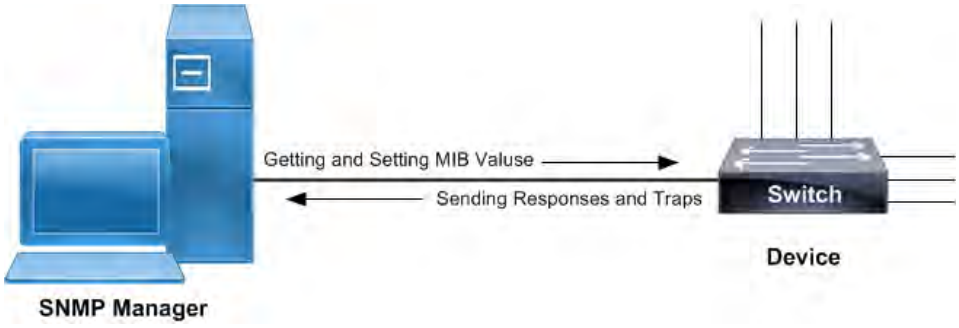


Figure 1-21: SNMP sample topology

Standard SNMP Configurations

`#configure terminal`	Enter configure mode.
`(config)#snmp-server view all .1 included vrf management`	Creates SNMP view labeled as “all” for OID-Tree as “.1” for vrf management.
`(config)#snmp-server community test group network-operator vrf management`	Set community string as “test” for group of users having “network-operator” privilege.
`(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management`	Specify host “10.12.6.63” to receive SNMP version 2 notifications at udp port number 162 with community string as “test”.
`(config)#snmp-server enable snmp vrf management`	Use this command to start the SNMP agent.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode.

sing IPv6 address.

Standard SNMP Configurations over User Defined VRF

OcNOS supports SNMP over the user defined VRFs as well apart from default and management VRFs via in-band interface. Users must be able to enable SNMP service over any user defined vrf however it only runs on one VRF at once.

`#configure terminal`	Enter configure mode.
`(config)#ip vrf snmp-vrf`	Creates a user-defined vrf called snmp-vrf
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)# snmp-server view newview 1.3.6.1.2.1.6.13.1.1.127.0.0.1 excluded vrf snmp-vrf`	Creates SNMP view labeled as “newview” for OID-Tree “1.3.6.1.2.1.6.13.1.1.127.0.0.1” excluded for vrf snmp-vrf.
`(config)# snmp-server community newcom group network-operator vrf snmp-vrf`	Set community string as “newcom” for group of users having “network-operator” privilege.
`(config)# snmp-server user newv3user auth sha AuthNewPass@123 priv aes PrivNewPass@123 vrf snmp-vrf`	Creates SNMP V3 user “newv3user” with authentication encryption “sha” and privacy encryption “aes” passwords for added security on the snmp-vrf
`(config)# snmp-server host 172.18.19.22 traps version 2c newcom udp-port 162 vrf snmp-vrf`	Specify host “172.18.19.22” to receive SNMP version 2 notifications at udp port number 162 with community string as “newcom”.
`(config)#snmp-server host 172.18.19.20 informs version 3 auth newv3user udp-port 65535 vrf snmp-vrf`	Specify host “172.18.19.20” to receive SNMP v3 informs at udp-port number 65535 for user “newv3user” if correct authpriv passwords are used
`(config)#snmp-server enable snmp vrf snmp-vrf`	Use this command to start the SNMP agent on the user defined vrf (snmp-vrf)
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configure mode.

Validation

Use the below commands to verify the SNMP configuration:

```
#show running-config snmp
snmp-server view all .1 included vrf management
snmp-server community test group network-operator vrf management
snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management

#show snmp group
-------------------------------------------------------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
-------------------------------------------------------------------------------
test          network-operator    2c/1       all        none           all

#show snmp host
-------------------------------------------------------------------------------
Host                Port   Version   Level          Type           SecName
-------------------------------------------------------------------------------
10.12.6.63          162    2c        noauth         trap           test
```

SNMP GET Command

```
# snmpget -v2c -c test 10.12.45.238
.1.3.6.1.2.1.6.13.1.2.10.12.45.238.22.10.12.6.63.52214

TCP-MIB::tcpConnLocalAddress.10.12.45.238.22.10.12.6.63.52214 = IpAddress:
10.12.45.238
```

SNMP WALK Command

SNMP WALK for particular OID

```
#snmpwalk -v2c -c test 10.12.45.238 .1.3.6.1.2.1.25.3.8.1.8
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.1 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.4 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.5 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.6 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.10 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.12 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.13 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.14 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.15 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.16 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.17 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.18 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.19 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.20 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.21 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.22 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.23 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.24 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.25 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.26 = STRING: 0-1-1,0:0:0.0
```

Complete SNMP WALK

```
#snmpwalk -v2c -c test 10.12.45.238 .1
```

SNMP Trap Server Configuration with IPv6 Address

Snmpwalk is performed by using IPv6 address. SNMP trap server is configured on the Router with IPv6 address.

Topology

Figure 1-22 shows the sample configuration of SNMP trap server.

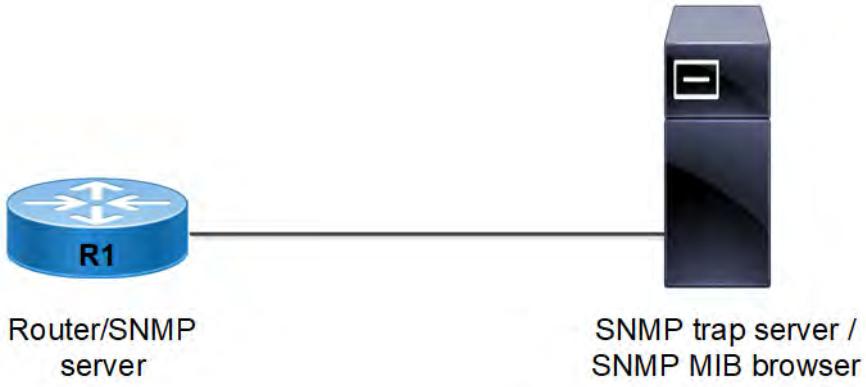


Figure 1-22: SNMP trap server topology

R1

`#configure terminal`	Enter configure mode.
`(config)#snmp-server view all .1 included vrf management`	Configure SNMP server view
`(config)#snmp-server view test1 1.3.6.1 included vrf management`	Configure SNMP server view
`(config)#snmp-server user test1 network-admin  auth md5 test1234 vrf management`	Configure SNMP server user
`(config)#snmp-server user test2 network-admin vrf management`	Configure SNMP server user
`(config)#snmp-server user test3 network-admin auth md5 test1234 priv des test1234 vrf management`	Configure SNMP server user
`(config)#snmp-server community test group network-operator vrf management`	Configure SNMP server community
`(config)#snmp-server community test1 group network-admin vrf management`	Configure SNMP server community
`(config)#snmp-server host 2001:db8:100::2 traps version 2c test udp-port 162 vrf management`	Configure SNMP trap server
`(config)#interface eth0`	Navigate to the interface mode
`(config-if)#ipv6 address 2001:db8:100::5/64`	Configure IPv6 address on the eth0 interface

(config-if)#exit	Exit interface configure mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

Validation

Below is the SNMP configuration in Router node:

```
#show running-config snmp
snmp-server view all .1 included vrf management
snmp-server user test1 network-admin auth MD5 encrypt 0xd1fe6acc88856c90 vrf man
agement
snmp-server user test2 network-admin vrf management
snmp-server user test3 network-admin auth MD5 encrypt 0xd1fe6acc88856c90 priv DE
S 0xd1fe6acc88856c90 vrf management
snmp-server community test group network-operator vrf management
snmp-server community test1 group network-admin vrf management
snmp-server enable snmp vrf management
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp

#show ipv6 interface eth0 brief
Interface            IPv6-Address                                    Admin-Sta
tus
eth0                 2001:db8:100::5
                     fe80::218:23ff:fe30:e6ba                        [up/up]
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv3

```
snmpwalk -v3 -u test3 -a MD5 -A test1234 -x DES -X test1234 -l authPriv 2001:db8:100::5
.1.3.6.1.2.1.25.3.8.1.8
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv2

```
snmpwalk -v2c -c  test 2001:db8:100::5 1.3.6.1.2.1.31
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv1

```
snmpwalk -v1 -c test 2001:db8:100::5  1.3.6.1.2.1.31

#show snmp trap

-------------------------------------------------

Trap type        Description      Enabled
-------------------------------------------------
link             linkUp           yes
link             linkDown         yes
vxlan            notification     no
mpls             notification     no
```

```
mpls              pw               no
mpls              pw delete        no
mpls-l3vpn        notification     no
ospf              notification     no
ospf6             notification     no
isis              notification     no
snmp              authentication   no
mpls              rsvp             no
vrrp              notification     no
bgp               notification     no
```

As mentioned above, perform link down and link up of any interface in Router node. Check that SNMP trap is sent u

SNMP Informs with IPv6 Address over User Defined VRF

Snmpwalk is performed by using IPv6 address. SNMP trap server is configured on the Router with IPv6 address.

Topology

Figure 1-22 shows the sample configuration of SNMP trap server.

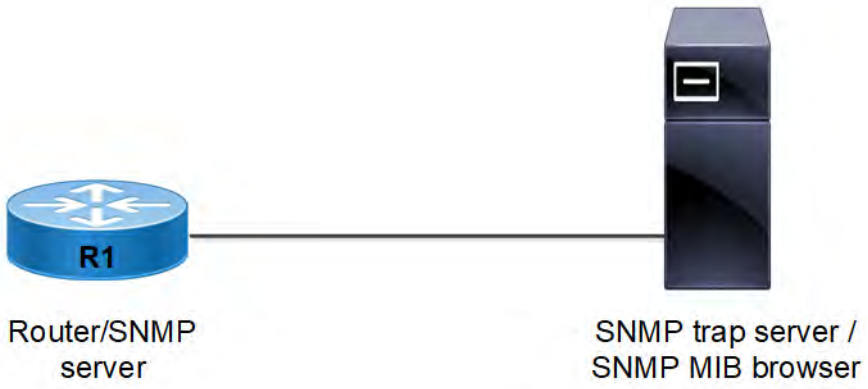


Figure 1-23: SNMP trap server topology

R1

`#configure terminal`	Enter configure mode.
`(config)#ip vrf snmp-vrf`	Creates a user-defined vrf called snmp-vrf
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#snmp-server view all .1 included vrf snmp-vrf`	Configure SNMP server view
`(config)#snmp-server view test1 1.3.6.1 included vrf snmp-vrf`	Configure SNMP server view
`(config)# snmp-server user newv3user auth sha AuthNewPass@123 priv aes PrivNewPass@123 vrf snmp-vrf`	Configure SNMP server user

(config)#snmp-server community test group network-operator vrf snmp-vrf	Configure SNMP server community
(config)#snmp-server community test1 group network-admin vrf snmp-vrf	Configure SNMP server community
(config)# snmp-server host 8901:DB8:0:1::1 informs version 3 auth newv3user udp-port 60000 vrf snmp-vrf	Configure SNMP informs server
(config)#interface xe0.6	Navigate to the interface mode
(config-if)#ipv6 address 8901:db8:0:1::2/64	Configure IPv6 address on the xe0.6 sub vlan interface
(config-if)#exit	Exit interface configure mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit configure mode

Validation

Below is the SNMP configuration in Router node:

```
#show running-config snmp
snmp-server view all .1 included vrf snmp-vrf
snmp-server view newview 1.3.6.1.2.1.6.13.1.1.127.0.0.1 excluded vrf snmp-vrf
snmp-server view test1 1.3.6.1 included vrf snmp-vrf
snmp-server user newv3user auth sha encrypt 0xd01d08043ea89bd3f77ccf8992973502 priv aes 0x7517e1def71063d7f77ccf8992973502 vrf snmp-vrf
snmp-server community newcom group network-operator vrf snmp-vrf
snmp-server community test group network-operator vrf snmp-vrf
snmp-server community test1 group network-admin vrf snmp-vrf
snmp-server host 172.18.19.22 traps version 2c newcom udp-port 162 vrf snmp-vrf
snmp-server host 172.18.19.20 informs version 3 auth newv3user udp-port 65535 vrf snmp-vrf
snmp-server host 8901:db8:0:1::1 informs version 3 auth newv3user udp-port 60000 vrf snmp-vrf
snmp-server enable snmp vrf snmp-vrf
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
snmp-server enable traps link include-interface-name
snmp-server enable traps vxlan
snmp-server enable traps pwdelete
snmp-server enable traps pw
snmp-server enable traps mpls
snmp-server enable traps mplsl3vpn
snmp-server enable traps snmp authentication
snmp-server enable traps ospf
snmp-server enable traps bgp
snmp-server enable traps ospf6
snmp-server enable traps vrrp
snmp-server enable traps rsvp
snmp-server enable traps rib
snmp-server enable traps isis
snmp-server enable traps pim
```

```
#show ipv6 interface xe0.6 brief
Interface            IPv6-Address                                    Admin-Status
xe0.6                8901:db8:0:1::2
                     fe80::5e07:58ff:fe51:caea                       [up/up]
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv3

```
snmpwalk -v3 -u newv3user -a SHA -A AuthNewPass@123 -x AES -X PrivNewPass@123 -l
authPriv 8901:DB8:0:1::2 .1.3.6.1.2.1.25.3.8.1.8 -m all
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv2

```
snmpwalk -v2c -c newcom 8901:DB8:0:1::2 -t 5 -r 20 1.3.6.1.2.1.31 -Cp -Ct -m all
```

Perform snmpwalk as mentioned below with IPv6 address using SNMPv1

```
snmpwalk -v1 -c newcom 8901:DB8:0:1::2 -t 5 -r 20 1.3.6.1.2.1.31 -Cp -Ct -m all
```

```
#show snmp trap

-------------------------------------------------

Trap type        Description      Enabled
-------------------------------------------------
link             linkUp           yes
link             linkDown         yes
link             linkWithIfname   yes
vxlan            notification     yes
mpls             notification     yes
mpls             pw               yes
mpls             pw delete        yes
mpls-l3vpn       notification     yes
ospf             notification     yes
ospf6            notification     yes
isis             notification     yes
snmp             authentication   yes
mpls             rsvp             yes
pim              notification     yes
vrrp             notification     yes
rib              notification     yes
bgp              notification     yes
```

As mentioned above, perform link down and link up of any interface in Router node. Check that SNMP trap is sent u

SNMP Command Reference

CHAPTER 1 Simple Network Management Protocol

This chapter is a reference for Simple Network Management Protocol (SNMP) commands.

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried by SNMP managers.

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption.

SNMP is defined in RFCs 3411-3418.

Note: The commands below are supported on the “management” and default VRF.

This chapter contains these commands:

- debug snmp-server
- show running-config snmp
- show snmp
- show snmp community
- show snmp context
- show snmp engine-id
- show snmp group
- show snmp host
- show snmp user
- show snmp view
- snmp context
- snmp ent-ipi-iftable
- snmp-server community
- snmp-server community-map

- snmp-server contact
- snmp-server context
- snmp-server disable default
- snmp-server enable snmp
- snmp-server enable traps
- snmp-server engineID
- snmp-server group
- snmp-server host
- snmp-server location
- snmp restart
- snmp-server smux-port-disable
- snmp-server tcp-session
- snmp-server trap-cache
- snmp-server user
- snmp-server view

debug snmp-server

Use this command to display SNMP debugging information.

Use the `no` form of this command to stop displaying SNMP debugging information.

Command Syntax

```
debug snmp-server
no debug snmp-server
```

Parameters

None

Default

By default, disabled.

Command Mode

Exec and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug snmp-server
```

show running-config snmp

Use this command to display the SNMP running configuration.

Command Syntax

```
show running-config snmp
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config snmp
snmp-server view all .1 included
snmp-server community abc group network-admin
snmp-server enable snmp
```

show snmp

Use this command to display the SNMP configuration, including session status, system contact, system location, statistics, communities, and users.

Command Syntax

```
show snmp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp
SNMP Protocol:Enabled
sys Contact:
sys Location:

--------------------------------------------------------------------------------
Community Group/Access Context acl_filter
--------------------------------------------------------------------------------
public network-admin
_______________________________________________________________________________

                        SNMP USERS
_______________________________________________________________________________
User Auth Priv(enforce) Groups
_______________________________________________________________________________

SNMP Tcp-session :Disabled
```

show snmp community

Use this command to display SNMP communities.

Command Syntax

```
show snmp community
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp community

------------------------------------------------------------------------------
-------------------------
Community                     Group/Access         view-name
version
------------------------------------------------------------------------------
-------------------------
test                                    network-operator
testing                     network-operator          ipi
2c
```

Table 1-7 explains the output fields.

Table 1-7: show snmp community fields

Entry	Description
Community	SNMP Community string.
Group/Access	Community group name.
View-name	Community view name.
Version	Community version.

show snmp context

Use this command to display SNMP server contexts and associated groups.

Command syntax

```
show snmp context
```

Parameters

None

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS-SP version 5.1 MR

Example

```
OcNOS#show snmp context
-----------------------------------------------------------------------
context                                          groups
-----------------------------------------------------------------------
ctx1                                          grp1,grp2
ctx2                                          grp3
```

show snmp engine-id

Use this command to exhibit the SNMP engine identifier.

The SNMP engine identifier is a distinctive string employed to recognize the device for administrative purposes. The default engine-id is formulated using the MAC address, but an option for user-configured engine-id is also provided. The `show` command should be employed to retrieve information about the presently configured SNMP engine-id on the device.

Command Syntax

```
show snmp engine-id
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced prior to OcNOS version 1.3 and its display in the `show` output was enhanced in OcNOS version 6.3.2.

Examples

Default SNMP engine-id:

```
#show snmp engine-id
SNMP ENGINE-ID Type: MAC address
SNMP ENGINE-ID : 80 00 1f 88 03 e8 c5 7a 1a 02 1c
```

User-Configured engine-id:

```
#show snmp engine-id
SNMP ENGINE-ID Type: User configured Text
SNMP ENGINE-ID Text: ipinfusion
SNMP ENGINE-ID : 80 00 1f 88 04 69 70 69 6e 66 75 73 69 6f 6e
```

Table 1-8 explains the output fields.

Table 1-8: show snmp engine-ip fields

Entry	Description
SNMP ENGINE-ID: 80 00 1f 88 04 69 70 69 6e 66 75 73 69 6f 6e	The SNMP engine identifier is a distinct string utilized to uniquely recognize the device for administrative purposes.

show snmp group

Use this command to display SNMP server groups and associated views.

Command Syntax

```
show snmp group
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp group
-------------------------------------------------------------------------------
------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
-------------------------------------------------------------------------------
------------------------------

test          network-operator    2c/1      all          all          all
kedar         network-operator    3         all          none         all
tamil         network-operator    3         all          none         all
```

Table 1-9 explains the output fields.

Table 1-9: show snmp group output

Entry	Description
Community/User	Displays the access type of the user for which the notification is generated.
Group	The name of the SNMP group, or collection of users that have a common access policy.
Version	SNMP version number.
Read-View	A string identifying the read view of the group. For further information on the SNMP views, use the show snmp view command.
Write-View	A string identifying the write view of the group.
Notify-View	A string identifying the notify view of the group. The notify view indicates the group for SNMP notifications, and corresponds to the setting of the snmp-server group group-name version notify notify-view command.

show snmp host

Use this command to display the SNMP trap hosts.

Command Syntax

```
show snmp host
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp host
-------------------------------------------------------------------------
Host            Port    Version    Level       Type      SecName
-------------------------------------------------------------------------

10.10.26.123    162     2c         noauth      trap      test
```

Table 1-10 explains the output fields.

Table 1-10: Show snmp host output

Entry	Description
Host	The IP address of the SNMP host server.
Port	The port being used for SNMP traffic.
Version	SNMP version number.
Level	The security level being used.
Type	The type of SNMP object being sent.
SecName	Secure Name for this SNMP session.

show snmp user

Use this command to display SNMP users and associated authentication, encryption, and group.

Command Syntax

```
show snmp user
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp user

SNMP USERS
_____________________________________________________________________
User            Auth    Priv(enforce)     Groups
_____________________________________________________________________
ntwadmin        MD5     AES               network-admin

#
```

Table 1-11 explains the output fields.

Table 1-11: Show snmp user output

Entry	Description
User	The person attempting to use the SMNMP agent.
Auth	The secure encryption scheme being used.
Priv(enforce)	What enforcement privilege is being used (in this case, it is the Advance Encryption Standard).
Group	The group to which the user belongs.

show snmp view

Use this command to display SNMP views.

Command Syntax

```
show snmp view
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show snmp view

View : all
  OID : .1
  View-type : included
```

snmp context

Use this command to associate the SNMP context with the VRF.

Use the `no` form of this command to remove the SNMP context association from VRF.

Command Syntax

```
snmp context-name WORD
no snmp context-name
```

Parameters

`WORD`	SNMP context name (Maximum 32 alphanumeric characters)

Default

No default value is specified.

Command Mode

Configure VRF mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Examples

```
OcNOS#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
OcNOS(config)#ip vrf red
OcNOS(config-vrf)#snmp context-name context1
```

snmp ent-ipi-iftable

Use this command to enable the display of separate physical and logical interface tables in SNMP requests.

Use the `no` form of this command to disable it.

Command Syntax

```
snmp ent-ipi-iftable
no snmp ent-ipi-iftable
```

Parameters

`ent-ipi-iftable`	Enables the physical and logical interface tables in SNMP requests.

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.5.3.

Examples

```
OcNOS#configure terminal
OcNOS(config)#snmp ent-ipi-iftable
```

snmp-server community

Use this command to create an SNMP community string and access privileges.

Use the `no` form of this command to remove an SNMP community string.

Command Syntax

```
snmp-server community WORD (| (view VIEW-NAME version (v1 | v2c ) ( ro)) |
(group (network-admin|network-operator)) |( ro) | (use-acl WORD) ) (vrf
  (NAME|management)|)
no snmp-server community COMMUNITY-NAME (vrf (NAME|management)|)
```

Parameters

`WORD`	Name of the community (Maximum 32 alphanumeric characters)
`VIEW-NAME`	Name of the snmp view (Maximum 32 alphanumeric characters)
`version`	Set community string and access privileges
`v1`	SNMP v1
`v2c`	SNMP v2c
`ro`	Read-only access
`group`	Community group
`network-admin`	System configured group for read-only
`network-operator`	System configured group for read-only(default)
`ro`	Read-only access
`use-acl`	Access control list (ACL) to filter SNMP requests
`WORD`	ACL name; maximum length 32 characters
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRFs

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#snmp-server community MyComm view MyView1 version v2c ro vrf
management
```

snmp-server community-map

Use this command to map the community name with context and SNMPv2 user.

Use `no` form of this command to remove the community mapping.

Note: Community can be mapped with one context and user.

Command Syntax

```
snmp-server community-map WORD context WORD user WORD (vrf management|)
no snmp-server community-map WORD context WORD user WORD (vrf management|)
```

Parameters

`WORD`	SNMP community name
`context`	SNMP context name
`WORD`	Context string
`user`	SNMP user name
`WORD`	User string
`management`	Virtual Routing and Forwarding name

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS-SP version 5.1 MR.

Examples

```
OcNOS(config)#snmp-server community-map test context ctx2 user testing vrf
management
```

snmp-server contact

Use this command to set the system contact information for the device (`sysContact` object).

Use the `no` form of this command to remove the system contact information.

Command Syntax

```
snmp-server contact (vrf (NAME|management)|) (TEXT|)
no snmp-server contact (vrf (NAME|management)|) (TEXT|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`TEXT`	System contact information; maximum length 1024 characters without spaces
`NAME`	Custom VRF

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added `NAME` parameter in OcNOS version 6.5.3

Examples

```
#configure terminal
(config)#snmp-server contact vrf management Irving@555-0150
```

snmp-server context

Use this command to create SNMP context.

Use `no` form of this command to remove the context.

Command Syntax

```
snmp-server context WORD (vrf (NAME|management)|)
no snmp-server context WORD (vrf (NAME|management)|)
```

Parameters

`context`	SNMP context name
`WORD`	Context string (Maximum 32 alphanumeric characters)
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRFs

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 5.1MR. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
OcNOS(config)#snmp-server context ctx1 vrf management
```

snmp-server disable default

Use this command to disable default instance which is running on OcNOS device. After configuring this command user should not be able to enable default snmp instance. Use no form of this command to unset this after that only user should be able to configure default instance.

Command Syntax

```
snmp-server disable-default
```

Parameters

None

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Examples

```
#configure terminal
(config)#snmp-server disable-default
```

snmp-server enable snmp

Use this command to start the SNMP agent daemon over UDP.

Use the `no` form of this command to stop the SNMP agent daemon over UDP.

Command Syntax

```
snmp-server enable snmp  (vrf (NAME|management)|)
no snmp-server enable snmp  (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added NAME parameter in OcNOS version 6.5.3

Examples

```
#configure terminal
(config)#snmp-server enable snmp vrf management
```

snmp-server enable traps

Use this command to enable or disable SNMP traps and inform requests.

Note: For CMMD, Critical logs in the console are equivalent to Alert traps & Alert logs on the console is equivalent to critical trap in SNMP.

Command Syntax

```
snmp-server enable traps (link(|linkDown|linkUp|include-interface-
  name)|snmp(|authentication)| mpls|pw|pwdelete|ospf|bgp|isis|vxlan|vrrp|ospf6)
no snmp-server enable traps (link(|linkDown|linkUp|include-interface-
  name)|snmp(|authentication)| mpls|pw|pwdelete|ospf|bgp|isis|vxlan|vrrp|ospf6
```

Parameters

`bgp`	bgp notification trap
`isis`	isis notification trap
`link`	Module notifications enable
`linkDown`	IETF Link state down notification
`linkUp`	IETF Link state up notification
`snmp`	Enable RFC 1157 notifications
`authentication`	Send SNMP authentication failure notifications
`mpls`	mpls notification trap
`mplsl3vpn`	mpls-l3vpn notification trap
`ospf`	ospf notification trap
`ospf6`	ospf6 notification trap
`pw`	pw notification trap
`pwdelete`	pwdelete notification trap
`rib`	rib notification trap
`rsvp`	rsvp notification trap
`vrrp`	vrrp notification trap
`vxlan`	vxlan notification trap
`linkDown`	IETF link state down notification
`linkup`	IETF link state up notification
`include-interface-name`	Enable this option to include interface name in the Linkup/Linkdown trap's varbind

Default

By default, SNMP server traps are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and was updated in OcNOS version 4.0.

Examples

```
(config)#snmp-server enable traps snmp
(config)#snmp-server enable traps mpls
(config)#snmp-server enable traps mplsl3vpn
(config)#snmp-server enable traps rsvp
(config)#snmp-server enable traps ospf
(config)#snmp-server enable traps ospf6
(config)#snmp-server enable traps vrrp
(config)#snmp-server enable traps vxlan
(config)#snmp-server enable traps snmp authentication
```

snmp-server engineID

Use this command to establish the SNMPv3 engine ID.

Use the no form of this command to remove the SNMPv3 engine ID.

Command Syntax

```
snmp-server engineID ENGINE_ID_STR
no snmp-server engineID
```

Parameters

ENGINE_ID_STR	String of characters that uniquely identifies the SNMP engine ID.

Default

By Default the SNMP Server Engine ID value is automatically generated using the MAC address.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.3.2.

Examples

```
#configure terminal
(config)#snmp-server engineID ipinfusion
```

snmp-server group

Use this command to create a SNMP group.

Use the `no` form of this command to remove the groups.

Command syntax

```
snmp-server group WORD version (1|2c) (context (all|WORD)|) (vrf management|)
  snmp-server group WORD version 3 (auth|noauth|priv) (context (all|WORD)|) (vrf
  (NAME|management)|)
 no snmp-server group WORD (context (all|WORD)|) (vrf (NAME|management)|)
```

Parameters

`WORD`		Specify the snmp group name (Maximum 32 alphanumeric characters)
`version`		SNMP Version
`1`		SNMP v1
`2c`		SNMP v2c
`3`		SNMP v3 security level
	`noauth`	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
	`auth`	Authentication and no privacy (authNoPriv) security model: use message digest algorithm (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
	`priv`	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
	`context`	SNMP context name
	`WORD`	SNMP context string (Maximum 32 alphanumeric characters)
	`all`	All context name's allowed for this group.
	`management`	Virtual Routing and Forwarding (VRF) name
`NAME`		Custom VRFs

Default

None

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS-SP version 5.1 MR. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
OcNOS#con t
OcNOS(config)#snmp-server context ctx1 vrf management
```

```
OcNOS(config)#snmp-server group grp1 version 3 auth context ctx1 vrf
management
OcNOS(config)#snmp-server group grp3 version 2c context ctx2 vrf management
```

snmp-server host

Use this command to configure an SNMP trap host. An SNMP trap host is usually a network management station (NMS) or an SNMP manager.

Use the `no` form of this command to remove an SNMP trap host.

Note: The maximum number of SNMP trap hosts is limited to 8.

Command Syntax

```
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) ((traps version(( (1 | 2c) WORD )
  | (3 (noauth | auth | priv) WORD))) |(informs version ((2c WORD ) | (3 (noauth |
  auth | priv) WORD))))(|udp-port <1-65535>) (vrf (NAME|management)|)
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) WORD (|udp-port <1-65535>) (vrf
  (NAME|management)|)
snmp-server host (A.B.C.D | X:X::X:X | HOSTNAME) (version(( (1 | 2c) WORD ) | (3
  (noauth | auth | priv) WORD)))(|udp-port <1-65535>) (vrf (NAME|management)|)
no snmp-server  host (A.B.C.D|X:X::X:X|HOSTNAME) (vrf (NAME|management)|)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`HOSTNAME`	DNS host name
`WORD`	SNMP community string or SNMPv3 user name (Maximum 32 alphanumeric characters)
`informs`	Send notifications as informs
`version`	SNMP Version. Default notification is traps
`<1-65535>`	Host UDP port number; the default is 162
`management`	Virtual Routing and Forwarding name
`traps`	Send notifications as traps
`version`	Version
`1`	SNMP v1
`2c`	SNMP v2c
`WORD`	SNMP community string (Maximum 32 alphanumeric characters)
`3`	SNMP v3 security level
`noauth`	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
`auth`	Authentication and no privacy (authNoPriv) security model: use message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
`priv`	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
`WORD`	SNMPv3 user name
`NAME`	Custom VRFs

Default

The default SNMP version is v2c and the default UDP port is 162.Simple Network Management Protocol.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#snmp-server host 10.10.10.10 traps version 3 auth MyUser udp-port 512
vrf management
```

snmp-server location

Use this command to set the physical location information of the device (`sysLocation` object).

Use the `no` form of this command to remove the system location information.

Command Syntax

```
snmp-server location (vrf (NAME|management)|) (TEXT|)
no snmp-server location (vrf (NAME|management)|) (TEXT|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`TEXT`	Physical location information; maximum length 1024 characters
`NAME`	Custom VRF

Default

No system location string is set.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added `NAME` parameter in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#snmp-server location vrf management Bldg. 5, 3rd floor, northeast
```

snmp restart

Use this command to restart SNMP for a given process.

Command Syntax

```
snmp restart (auth | bfd | bgp | isis | lacp| ldp | lldp | mrib | mstp | nsm | ospf
  | ospf6 | pim | rib| rip | rsvp |vrrp)
```

Parameters

`auth`	Authentication
`bfd`	Bidirectional Forwarding Detection (BFD)
`bgp`	Border Gateway Protocol (BGP)
`isis`	Intermediate System - Intermediate System (IS-IS)
`lacp`	Link Aggregation Control Protocol (LACP)
`ldp`	Label Distribution Protocol (LDP)
`lldp`	Link Layer Discovery Protocol (LLDP)
`mrib`	Multicast Routing Information Base (MRIB)
`mstp`	Multiple Spanning Tree Protocol (MSTP)
`nsm`	Network Service Module (NSM)
`ospf`	Open Shortest Path First (OSPFv2)
`ospf6`	Open Shortest Path First (OSPFv3)
`pim`	Protocol Independent Multicast (PIM)
`rib`	Routing Information Base (RIB)
`rip`	Routing Information Protocol (RIP)
`rsvp`	Resource Reservation Protocol (RSVP)
`vrrp`	Virtual Router Redundancy Protocol (VRRP)

Default

N/A

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
OcNOS(config)#snmp restart nsm
```

snmp-server smux-port-disable

Use this CLI to disable the SMUX open port.

Command Syntax

```
snmp-server smux-port-disable
```

Parameters

None

Default

None

Command Mode

Configure mode

Applicability

This command is introduced in OcNOS version 5.1 release.

Examples

```
#configure terminal
#snmp-server smux-port-disable
```

snmp-server tcp-session

Use this command to start the SNMP agent daemon over TCP.

Use the `no` form of this command to close the SNMP agent daemon over TCP.

Command Syntax

```
snmp-server tcp-session (vrf (NAME|management)|)
no snmp-server tcp-session (vrf (NAME|management)|)
```

Parameters

`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRF

Default

By default, snmp server tcp session is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added `NAME` parameter in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#snmp-server tcp-session vrf management
```

snmp-server trap-cache

Use this command to configure the trap caching settings for SNMP.

Use the `no` form of this command to disable caching for SNMP.

Command Syntax

```
snmp-server trap-cache (timeout <timeout> | max-count <max-count> | disable-ping |)
no snmp-server trap-cache
```

Parameters

`timeout <timeout>`	Specifies the maximum time (in seconds) that traps will be cached before being sent. This sets the trap cache timeout.
`max-count <max-trap-count>`	Specifies the maximum number of traps that can be cached before they are flushed and sent.
`disable-ping`	Disables ping check for host availability. If ping is disabled, traps will be sent after the configured timeout.

Default

Disabled

Command Mode

Trap Cache mode

Applicability

This command was introduced in OcNOS version 6.5.3.

Examples

```
OcNOS#configure terminal
OcNOS(config)#snmp-server trap-cache
OcNOS(config-trap-cache)#timeout 60
```

snmp-server user

Use this command to create an SNMP server user.

Use the `no` form of this command to remove an SNMP server user.

Command Syntax

```
snmp-server user WORD ((network-operator|network-admin| WORD|) ((auth (md5 | sha
)(encrypt|) AUTH-PASSWORD) ((priv (des | aes) PRIV-PASSWORD) |) |) (vrf
  (NAME|management)|)
no snmp-server user USER-NAME (vrf (NAME|management)|)
```

Parameters

`WORD`	Specify the snmp user name (Min 5 to Max 32 alphanumeric characters)
`network-operator|network-admin`	
	Name of the group to which the user belongs.
`WORD`	User defined group-name
`auth`	Packet authentication type
`md5`	Message Digest Algorithm 5 (MD5)
`sha`	Secure Hash Algorithm (SHA)
`AUTH-PASSWORD`	
	Authentication password; length 8-32 characters
`priv`	Packet encryption type (“privacy”)
`des`	Data Encryption Standard (DES)
`aes`	Advanced Encryption Standard (AES)
`PRIV-PASSWORD`	
	Encryption password; length 8-33 characters
`management`	Virtual Routing and Forwarding name
`encrypt`	Specify authentication-password and/or privilege-password in encrypted form. This option is provided for reconfiguring a password using an earlier encrypted password that was available in running configuration display or get-config payload. Users are advised not to use this option for entering passwords generated in any other method.
`NAME`	Custom VRFs

Default

By default, snmp server user word is disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

```
#configure terminal
(config)#snmp-server user Fred auth md5 J@u-b;l2e`n,9p_ priv des
t41VVb99i8He{Jt vrf management
```

snmp-server view

Use this command to create or update a view entry

Use the `no` from of this command to remove a view entry.

Note: OIDs to be excluded or included need to be specifically mentioned while configuring the SNMP view. Only when the OIDs are included will they be displayed in SNMP-Walk. When an OID is excluded, other OIDs must be explicitly included for the system to function.

Command Syntax

```
snmp-server view VIEW-NAME OID-TREE (included | excluded) (vrf (NAME|management)|)
no snmp-server view VIEW-NAME (vrf (NAME|management)|)
```

Parameters

`VIEW-NAME`	Name of the snmp view (Maximum 32 alphanumeric characters)
`OID-TREE`	Object identifier of a subtree to include or exclude from the view; specify a text string consisting of numbers and periods, such as 1.3.6.2.4
`included`	Include `OID-TREE` in the SNMP view
`excluded`	Exclude `OID-TREE` from the SNMP view
`management`	Virtual Routing and Forwarding name
`NAME`	Custom VRFs

Default

By default, snmp-server view VIEW-NAME OID-TREE is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Added parameter `NAME` in OcNOS version 6.5.3.

Examples

The following example creates a view named `myView3` that excludes the `snmpCommunityMIB` object (1.3.6.1.6.3.18).

```
#configure terminal
(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded vrf management
```

Logging Server Command Reference

CHAPTER 1 Syslog Commands

This chapter is a reference for the `syslog` commands.

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, an application such as `mail` and `cron` generates messages with a facility names “mail” and “cron”.
- Eight degrees of severity (numbered 0-7) of the message which are explained in Table 1-12.

This chapter contains these commands:

- clear logging logfile
- feature rsyslog
- log syslog
- logging console
- logging level
- logging logfile
- logging monitor
- logging remote facility
- logging remote server
- logging timestamp
- show logging
- show logging last
- show logging logfile
- show logging logfile last-index
- show logging logfile start-seqn end-seqn
- show logging logfile start-time end-time
- show running-config logging

© 2025 IP Infusion Inc. Proprietary

Syslog Severities

In the example log entries in Table 1-12, the prefixes are removed. For example. this is a complete log entry with the prefix:

```
2020 Apr 12 11:20:27.612 : 17U-18U : PSERV : MERG : !!! hsl Module crashed, System reboot halted as it rebooted continuosly 2 times
```

This is the same log entry without the prefix:

```
hsl Module crashed,System reboot halted as it rebooted continuosly 2 times
```

Table 1-12: Syslog severities (Sheet 1 of 2)

Severity Level	Keyword	Description

0	emergency	The whole system is unusable and needs operator intervention to recover. If only a particular port or component is unusable, but the system as a whole is still usable it is not categorized at an emergency level.
		Examples of this type of message:
		`Output Power of PSU XX (psu_no) XX Watt] has exceeded Maximum Output Power Limit[XX Watt]`
		`OSPF Initialization failed.`

1	alert	The operator needs to act immediately or the system might go into emergency state. The system or one of its component's functionality might be critically affected.
		Examples of this type of message:
		`Temperature of sensor is (curr_temp)C. It is nearing Emergency Condition.`
		`OSPF has exceed lsdb limit`
		`OSPF Detected router with duplicate router ID [ID]`

2	critical	A critical system event happened which requires the operator's attention. The event might not require immediate action, but this event can affect functionality or behavior of a system component.
		Examples of this type of message:
		`OSPF Neighbor session went down.`
		`Interface %s changed state to down`

3	error	An error event happened which does not require immediate attention. This log message provides details about error conditions in the system or its components which you can use to troubleshoot problems.
		These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as `debug ospf all`).
		Examples of this type of message:
		`Device i2c bus open error.!!!`
		`[DECODE] Attr ASPATH: Invalid AS Path value.`
		`OSPF MD5 authentication error`

Table 1-12: Syslog severities (Sheet 2 of 2)

Severity Level	Keyword	Description

4	notification	Notifications about important system and protocol events to assure the operator that the system is running properly. If a critical/alert condition has happened and has been corrected, that is also logged at this level.
		Examples of this type of message:
		`OSPF Received link up for interface: xe1`
		`OSPF neighbour [10.1.1.1] Status change Exstart -> Exchange`
		`Interface %s changed state to UP`

5	informational	Detailed informational events happening across the system and protocol modules. These events are not necessarily important and are useful only to find details about the functionality being executed in the system and its components. Some of these events might be periodic events like hello or keep alive messages along with packet dumps. Also, this level includes logs for control packets that are ignored and do not impact the protocol states.
		IP Infusion Inc. recommends to use proper debug filters to log only relevant events and switch off other events; otherwise the logs can get verbose. For example:
		`debug ospf all`
		`no debug ospf packet hello`
		The above enables all OSPF debugging, but disables the periodic hello messages.
		Examples of this type of message:
		`Successfully added dynamic neighbour`
		`[DECODE] KAlive: Received!`
		`[FSM] Ignoring Unsupported event <EVENT> in state <STATE>`
		`Unknown ICMP packet type"`
		`OSPF RECV[%s]: From %r via %s: Version number mismatch`
		`OSPF RECV[%s]: From %r via %s: Network address mismatch`

6	debug informational	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.
7	debug detailed	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.

Log File Rotation

Log rotation is important to maintain the stability of the device, because the larger log files are difficult to manipulate and file system would run out of space. The solution to this common problem is log file rotation.

Log rotation is scheduled to happen for every 5 minutes, here the log file size is used as the condition to perform rotation.

Log rotate operation creates a backup of the current log file, and clears the current log file content. Also these rotated log files are compressed to save disk space. Excluding the current log file, four backup files are maintained in the system, and the older logs are removed as part of the rotation operation.

Default log file `/var/log/messages` rotated, if the size is greater than 100 MB. The following are the rotated log files generated in the path `/var/log`

```
root@host:/var/log# ls messages*
messages  messages.1  messages.2.gz  messages.3.gz  messages.4.gz
```

Manually configured log file `/log/LOG1` gets rotated, if its size is greater than configured size. Here `LOG1` is the manually configured using the command `logging logfile <filename>` and the log file size in bytes can be configured using the command `logging logfile LOG1 <severity> size <4096-419430400>`

```
(config)#logging logfile LOG1 7 size 4096
```

Here configured logging file `/log/LOG1` is rotated if the size is greater than 4096 bytes. The following are the rotated log files generated in the path `/log`

```
root@host:/log# ls LOG*
LOG1  LOG1.1  LOG1.2.gz  LOG1.3.gz  LOG1.4.gz
```

clear logging logfile

Use this command to clear the existing contents of the configured logging logfile.

Note: If the name of the configured logging log file is “mylogfile”, this command clears only the log file mylogfile. But the other rotated or compressed log files are untouched.

Command Syntax

```
clear logging logfile
```

Parameters

None

Default

No default value is specified

Command Mode

Executive mode

Applicability

This command was introduced before OcNOS version 3.0.

Example

```
#clear logging logfile
```

feature rsyslog

Use this command to enable the rsyslog server.

Use the `no` form of this command to disable the rsyslog server.

Command Syntax

```
feature rsyslog vrf (management|)
no feauture rsyslog vrf (management|)
```

Parameters

`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#feature rsyslog vrf management
```

log syslog

Use this command to begin logging to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

Command Syntax

```
log syslog
no log syslog
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#log syslog
```

logging console

Use this command to set the severity level that a message must reach before the messages is sent to the console. The severity levels are from 0 to 7 as shown in Table 1-12.

Use the command logging console disable to disable logging console messages.

Use the `no` form of this command to remove logging console configuration and return to the default severity level.

Note: Below message will be displayed if console severity is set to 6 or 7:

% Warning : If debug volume is huge it can degrade system performance and makes console to be non-responsive

Note: For CMMD, Critical logs in the console are equivalent to Alert traps & Alert logs on the console is equivalent to critical trap in SNMP.

Command Syntax

```
logging console (<0-7>|)
logging console disable
no logging console
```

Parameters

`<0-7>`	Maximum logging level for console messages as shown in Table 1-12.
Note:	Setting the level above 5 might affect performance and is not recommended in a production network.
`disable`	Disables the logging console

Default

If not specified, the default logging level is 2 (Critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and the command `logging console disable` was introduced in the OcNOS version 5.1.

Example

```
#configure terminal
(config)#logging console 6
(config)#commit
(config)#logging console disable
(config)#commit
```

logging level

Use this command to set the severity level that a message for a specific process must reach before the messages is logged. The severity levels are from 0 to 7 as shown in Table 1-12. Logging happens for the messages less than or equal to the configured severity level.

Use the `no` form of this command to disable logging messages.

Note: Default log level is 2 to report Emergency-0, Alert-1 and Critical-2 level events.

Command Syntax

```
logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|onm|oam|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp) <0-7>
no logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|oam|onm|ospf|ospf6|pim|pon|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  |vrrp)
```

Parameters

`all`	All messages
`auth`	Auth messages
`bgp`	BGP messages
`dvmrp`	DVMRP messages
`hostp`	Hostp messages
`hsl`	HSL messages
`isis`	ISIS messages
`l2mrib`	L2MRIB messages
`lacp`	LACP messages
`lagd`	LAGD messages
`ldp`	LDP messages
`mrib`	MRIB messages
`mstp`	MSTP messages
`ndd`	NDD messages
`nsm`	NSM messages
`oam`	OAM messages
`onm`	ONM messages
`ospf`	OSPF messages
`ospf6`	OSPF6 messages
`pim`	PIM messages
`pon`	PON messages
`pservd`	PSERVD messages
`ptp`	PTP messages
`rib`	RIB messages

`rip`	RIP messages
`ripng`	RIPNG messages
`rmon`	RMON messages
`rsvp`	RSVP messages
`sflow`	Sflow messages
`vrrp`	VRRP messages
`<0-7>`	Severity level as shown in Table 1-12.

Default

By default, the logging level is 2 (critical).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

Note: From OcNOS version 4.2, the behavior of the option `all` for the logging level command has changed for the running-config. Now the command logging level `all` is displayed in the running-config with its respective level defined by the user instead of one command for each process. If the user have some logging level configured for some specific process in the system when the logging level `all` command is executed, the level of process that is already configured stays with the level and all other process are configured with the level defined by the `all` option. This change is necessary to support the option `all` for logging level in the Netconf also.

```
#configure terminal
(config)#logging level all 7
(config)#do show running-config logging
logging level ospf 3
logging level hostp 5
logging level all 7
feature rsyslog
(config)#
```

logging logfile

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing debug output and command history to the disk file in the directory `/log/`.

When logging logfile is enabled, OcNOS log information is stored in user configured logging file which is present in "/log" directory. The log is spread across four files total of these files size is the user configured size.

For example, if the name of the logging log file is “mylogFile” and logging file size configured is 4 MB then each file will be maximum size of 1MB. The logging file names will be "mylogFile", "mylogfile.0", "mylogfile.1" and "mylogfile.2".

"mylogFile" will have the latest log information. As soon as it’s size becomes 1 MB this file is renamed as mylogFile.0 and newlog information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost in order to accommodate new set of logs in mylogFile.

Use option no to cancel writing to a specific log file.

Note: Changing logfile paramenters (name/size/severity) will be taken into effect for the next OcNOS session.

Command Syntax

```
logging logfile LOGFILENAME <0-7> ((size <4096-419430400>)|)
no logging logfile
```

Parameter

`LOGFILENAME`	Specify the snmp user name (Min 5 to Max 32 alphanumeric characters).
`<0-7>`	Severity level as shown in Table 1-12.
`<4096-419430400>`	Log file size in bytes.

Default

By default, log file size is 419430400 bytes.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
#configure terminal
(config)#logging logfile test123 7
```

logging monitor

Use this command to set the severity level that a message must reach before a monitor message is logged. The severity levels are shown in Table 1-12.

Use the command logging monitor disable to disable the logging monitor messages.

Use the `no` form of this command to remove logging monitor config and return to the default severity level.

Command Syntax

```
logging monitor (<0-7>|)
logging monitor disable
no logging monitor
```

Parameters

`<0-7>`	Maximum logging level for monitor messages as shown in Table 1-12.
Note:	Setting the level above 5 might affect performance and is not recommended in a production network.
`disable`	Disables logging monitor

Default

If not specified, the default logging level is 7 (debug-details).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and the command `logging monitor disable` was introduced in the OcNOS version 5.1.

Example

```
#configure terminal
(config)#logging monitor 6
(config)#commit
(config)#logging monitor disable
(config)#commit
```

logging remote facility

Use this command to set a syslog servers facility.

OcNOS supports logging messages to one or more remote syslog servers. but the same facility is used for all the servers.

Use the `no` form of this command to use the default facility value, which is `local7`.

Note: Only one facility is supported for all protocol modules across all the configured logging servers.

Command Syntax

```
logging remote facility
  (local0|local1|local2|local3|local4|local5|local6|local7|user)
no logging remote facility
```

Parameters

`facility`	Entity logging the message (user defined); if not specified, the default is local7
`local0`	Local0 entity
`local1`	Local1 entity
`local2`	Local2 entity
`local3`	Local3 entity
`local4`	Local4 entity
`local5`	Local5 entity
`local6`	Local6 entity
`local7`	Local7 entity (default)
`user`	User entity

Default

If not specified, the default `facility` is `local7`.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.1.

Examples

```
#configure terminal
(config)#logging remote facility local 6
(config)#no logging remote facility
```

logging remote server

Use this command to set a syslog server.

OcNOS supports logging messages to a syslog server in addition to logging to a file or the console (local or SSH/telnet console). OcNOS messages can be logged to a local syslog server (the machine on which OcNOS executes) as well as to one or more remote syslog servers.

Use the `no` form of this command to remove a syslog server.

Note: Maximum 8 remote log servers can be configured.

Command Syntax

```
logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|) (port <1024-
  65535>|)(vrf management|)
no logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|)
  (port|)(vrf management|)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`HOSTNAME`	Host name; specify `localhost` to log locally
`0`	Emergency
`1`	Alert
`2`	Critical
`3`	Error
`4`	Notification
`5`	Informational
`6`	Debug informational
`7`	Debug detailed
`<1024-65535>`	Port number Default port is 514
`vrf management`	Virtual Routing and Forwarding name

Note: Severity at which messages are logged as shown in Table 1-12. If not specified, the default is 7.

Default

If not specified, the default severity at which messages are logged is 7 (debug detailed).

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.

Examples

```
#configure terminal
(config)#logging remote server MyLogHost vrf management
(config)#no feature rsyslog vrf management
(config)# (config)#feature rsyslog
(config)#logging remote server 10.10.10.10 7
```

Note: In the latter configuration, the default VRF does not need not to be specified in the command.

logging timestamp

Use this command to set the logging timestamp granularity.

Use the `no` form of this command to reset the logging timestamp granularity to its default (milliseconds).

Note: Any change in timestamp configurations will result in timestamp configured for event logged by protocol modules except for CLI history for the current and active sessions. The timestamp configuration is reflected in CLI history for new CLI sessions.

Changing logging timestamp will be taken into effect for the next OcNOS session.

Command Syntax

```
logging timestamp (microseconds|milliseconds|seconds|none)
no logging timestamp
```

Parameters

`microseconds`	Microseconds granularity
`milliseconds`	Milliseconds granularity
`seconds`	Seconds granularity
`none`	no timestamp in log message

Default

By default, logging time stamp granularity is milliseconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#logging timestamp milliseconds
```

show logging

Use this command to display the logging configuration.

Command Syntax

```
show logging (info|level|server|console|timestamp|monitor)
```

Parameters

`info`	Show server logging configuration
`level`	Show facility logging configuration
`server`	Syslog server configuration
`console`	Console configuration
`timestamp`	Timestamp configuration
`monitor`	Monitor configuration

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging console
Console logging     : enabled Severity: Operator (critical) Level : 2


#show logging monitor
Logging monitor     : enabled Severity: Operator (debugging) Level: 7


#show logging server
  Remote Servers:
                1.1.1.1
                severity: Operator (informational)
                facility: local7
                VRF : management

#sh logging info
  Remote Servers:
                1.1.1.1
                severity: Operator (informational)
                facility: local7
                VRF : management
Logging console     : enabled Severity: operator (critical) Level : 2
Logging monitor     : enabled Severity: Operator (debugging) Level : 7
Logging timestamp   : seconds
File logging        : enabled  File Name   : /log/abc  Severity   : Operator (de
```

```
bugging)  Level   : 7  Size   : 4194304
Cli logging         : enabled

Facility        Default Severity        Current Session Severity
nsm                     2                       2
ripd                    2                       2
ripngd                  2                       2
ospfd                   2                       2
ospf6d                  2                       2
isisd                   2                       2
hostpd                  2                       2
mribd                   2                       2
pimd                    2                       2
authd                   2                       2
mstpd                   2                       2
onmd                    2                       2
HSL                     2                       2
oamd                    2                       2
vlogd                   2                       2
vrrpd                   2                       2
ndd                     2                       2
ribd                    2                       2
bgpd                    2                       2
l2mribd                 2                       2
hslrasmgr               2                       2
lagd                    2                       2
pservd                  2                       2
cmmd                    2                       2
```

show logging last

Use this command to display lines from the end of the log file.

Command Syntax

```
show logging last (<1-9999>)
```

Parameters

<1-9999>	Number of lines to display from end of the log file

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging last 100
2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
Connection refused
```

show logging logfile

Use this command to display whether logging is enabled, the log file name, and the logging severity.

Command Syntax

```
show logging logfile
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile
File logging        : enabled  File Name   : /log/abc  Severity   : (7)
2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
logging server 1.1.1.1 5 vrf management '

2017 Sep 25 17:18:14 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
ex'

2017 Sep 25 17:18:17 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:19:15 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console '

2017 Sep 25 17:19:20 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging monitor '

2017 Sep 25 17:19:32 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging logfile '

2017 Sep 25 17:19:44 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging server '

2017 Sep 25 17:28:26 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging info '

2017 Sep 25 17:29:02 : OcNOS : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : '
sh logging console
```

show logging logfile last-index

Use this command to display the number of line in the log file.

Command Syntax

```
show logging logfile last-index
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile last-index
logfile last-index : 10
```

Table 1-13 explains the output fields.

Table 1-13: show logging logfile last-index fields

Entry	Description
logfile last-index	Number of line in the logfile.

show logging logfile start-seqn end-seqn

Use this command to display a range of lines in the log file.

Command Syntax

```
show logging logfile start-seqn (<0-2147483647>) (|(end-seqn <0-2147483647>))
```

Parameters

`start-seqn`	Starting line number
`end-seqn`	Ending line number

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show logging logfile start-seqn 2 end-seqn 7
2
3 2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile
4
5 2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
6
7 2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
NE4-router#
```

Table 1-14 explains the output fields.

Table 1-14: show logging logfile start-seqn end-seqn fields

Entry	Description
start-seqn	Starting line number
end-seqn	Ending line number

show logging logfile start-time end-time

Use this command to display lines from the log file within a given date-time range.

Command Syntax

```
show logging logfile start-time (<2000-2030> WORD <1-31> WORD) (|(end-time <2000-
  2030> WORD <1-31> WORD))
```

Parameters

`start-time`	Starting date and time:
`<2000-2030>`	Year in YYYY format
`WORD`	Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)
`<1-31>`	Day of month in DD format
`WORD`	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>
`end-time`	Ending date and time:
`<2000-2030>`	Year in YYYY format
`WORD`	Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)
`<1-31>`	Day of month in DD format
`WORD`	Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh logging logfile start-time 2019 Jan 04 06:20:49 end-time 2019 Jan 04
06:21:16
2019 Jan 04 06:20:49.611 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : sh logging logfile

2019 Jan 04 06:21:08.512 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index

2019 Jan 04 06:21:16.246 : NE4-router : CMLSH : CLI_HIST : User root@/dev/
ttyS0 : CLI : show logging logfile last-index
#
```

show running-config logging

Use this command to display the logging configuration.

Command Syntax

```
show running-config logging
```

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show running-config logging
no Logging console
no Logging monitor
logging timestamp milliseconds
```

Monitor and Reporting Server Configuration

CHAPTER 1 Configure sFlow for Single Collector

This chapter provides the steps for configuring Sampled Flow (sFlow).

sFlow is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

The sFlow agent samples packets as well as polling traffic statistics for the device it is monitoring. The packet sampling is performed by the switching/routing device at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs as well as sampled packets to an sFlow collector for analysis.

Note: sFlow egress sampling for multicast, broadcast, or unknown unicast packets is not supported.

The sFlow agent uses the following forms of sampling:

- Sampling packets: samples one packet out of a defined sampling rate. This sampling is done by hardware at wire speed.
- Sampling counters: polls interface statistics such as generic and Ethernet counters at a defined interval.

You must enable the sFlow feature and collector before enabling sFlow sampling on an interface.

You cannot globally enable sFlow sampling monitoring on all interfaces with a single command. Instead you must enable sFlow sampling on the required interfaces individually.

sFlow feature is supported on physical interface as well as LAG interface. Configuring sampling on a LAG interface will enable the same on all member ports part of that LAG interface.

Note: When sflow sampling is in-progress on high rate, CPU usage spike messages from Chassis monitoring module (cmmd) is expected.

Note: The Qumran 1 platform is equipped to handle a total of 9 unique sampling rates. Ingress and egress sampling rate is counted separately.

Note: The Qumran 2 platform is equipped to handle a total of 15 unique sampling rates.

- For egress, maximum 7 unique sampling rates can be created.
- If egress sampling is not used, a total of 15 unique ingress sampling rates can be configured.
- Total ingress sampling = 15 - number of egress sampling rates.

Topology

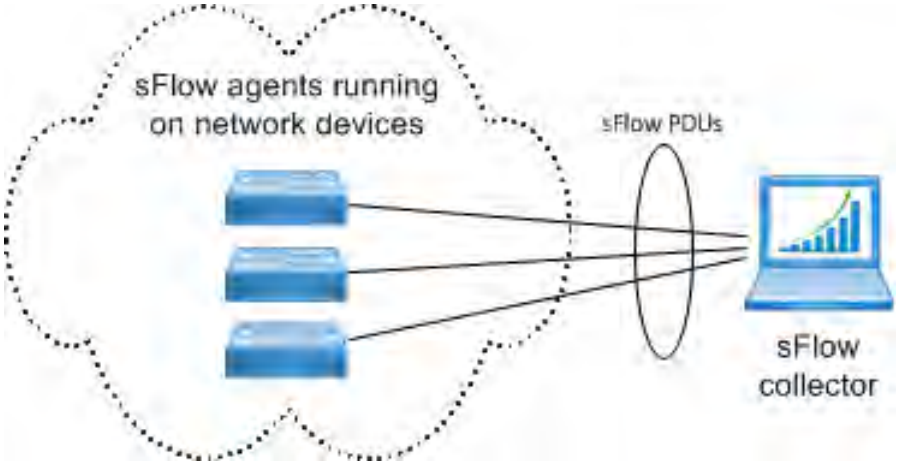


Figure 1-29: Basic sFlow topology

Configuration

sFlow Agent

`#configure terminal`	Enter configure mode.
`(config)#feature sflow`	Enable the sFlow feature.
`(config)#sflow collector 2.2.2.2 port 6343 receiver-time-out 0 max-datagram-size 200`	Configure the sFlow collector.The IP address must be reachable via the management VRF.
`(config)#interface xe1`	Enter interface mode
`(config-if)#sflow poll-interval 5`	Set the counter poll Interval on the interface.
`(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200`	Set the sFlow sampling interval on the interface in ingress directions.
`(config-if)#sflow sampling-rate 1024 direction egress max-header-size 120`	Set the sFlow sampling interval on the interface in egress directions.
`(config-if)#sflow enable`	Start packet sampling on the interface
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#end`	Exit interface and configure mode.

Validation

```
#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.132
Collector IP: 2.2.2.2    Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-
Polling         Maximum Header
                  Rate                    Count               Interval
Count        Size(bytes)
         Ingress     Egress      Ingress     Egress      (sec)
Ingress     Egress
---------  ----------------------   ----------------------  ---------------
-------   --------------------
xe1/1           1024        1024       464564        414532          5
131     120          20
```

CHAPTER 2 Configure sFlow for Multiple Collectors

Overview

The sFlow feature collects sampled traffic data and counters from configured interfaces. The collected data is sent to a collector using the sFlow protocol. For more information, refer to https://datatracker.ietf.org/doc/html/rfc3176.

This functionality is enhanced to support multiple collectors with one connections for each, simultaneously.

Feature Characteristics

- Supports maximum of five concurrent sFlow collectors on the system.
- Uses a specific user defined VRF interface for each collector. If not specified, the management VRF is used.
- Sends the collected sFlow samples on each interface to the corresponding collector configured on the interface.

Benefits

The sFlow with multiple collectors support provides the capability to do multiple analysis simultaneous in a network.

Prerequisites

Make sure to enable the required interface with sflow data collection and a agent IP address. For example,

```
feature sflow
sflow agent-ip 1.2.7.10
```

Configuration

This section provides the configurations required to assign multiple sFlow collectors to OcNOS.

Topology

The following topology illustrates the sFlow multiple collectors connected with one sFlow Packet Data Unit (PDU):

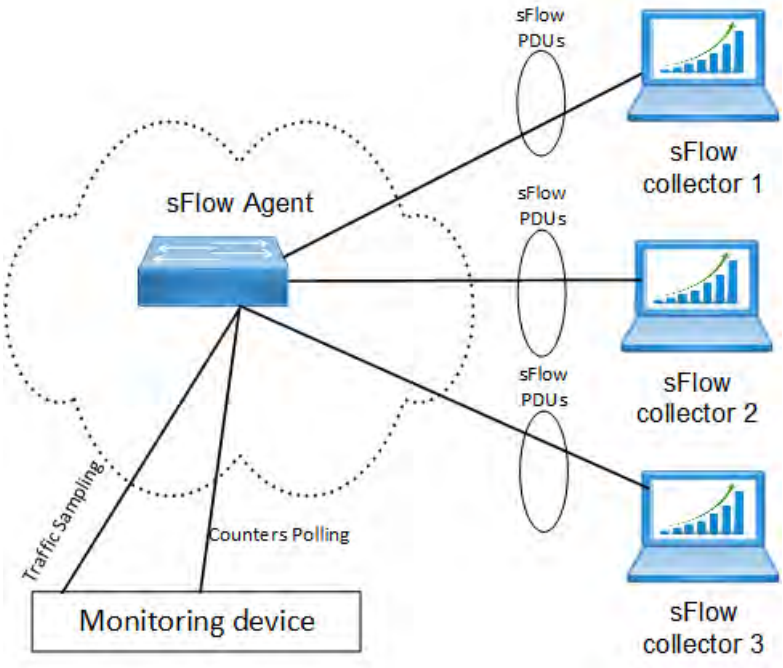


Figure 2-30: sFlow with Multiple Collectors

Perform the following configurations:

1. Configure sFlow using the configuration provided in Configure sFlow for Single Collector section for single collector.

2. In the interface mode, enable sFlow for a particular interface and specify the collector-id for multiple collectors:

```
OcNOS(config)#interface xe12
OcNOS(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 256
OcNOS(config-if)#sflow sampling-rate 2000 direction egress max-header-size 16
OcNOS(config-if)#sflow enable
OcNOS(config-if)#sflow poll-interval 10
OcNOS(config-if)#sflow collector-id 3
```

Show Running Configurations

The following show output display the sample sflow configuration details.

```
OcNOS#show running-config sflow feature sflow
sflow agent-ip 1.2.7.10

sflow collector-id 3 collector 1.2.3.24 port 6345 receiver-time-out 5 max-datagram-
size 1560
sflow collector-id 4 collector 1.2.4.24 port 6346 receiver-time-out 4 max-datagram-
size 1570 vrf default

1570 vrf default
!
interface xe12
 sflow sampling-rate 1024 direction ingress max-header-size 256
 sflow sampling-rate 2000 direction egress max-header-size 16 sflow enable
```

```
 sflow poll-interval 10
 sflow collector-id 3
!
interface xe13
 sflow sampling-rate 2500 direction ingress max-header-size 100
 sflow sampling-rate 2000 direction egress max-header-size 16
 sflow enable
 sflow poll-interval 5
 sflow collector-id 4
!
```

Validation

The following show output displays the sFlow details:

```
OcNOS#show sflow detail
sFlow Feature: Enabled
sFlow Version: 5
Agent IP     : 1.2.7.10
Collector 3:
   IP: 1.2.3.24      Port:  6345
   VRF                          :
   Maximum Datagram Size(bytes): 1560
   Receiver timeout(sec)       : 0
Collector 4:
   IP: 1.2.4.24      Port:  6346
   VRF                          :
   Maximum Datagram Size(bytes): 1570
   Receiver timeout(sec)       : 0

sFlow Port Detailed Information:

Interface  Collector  Packet-Sampling          Packet-Sampling            Counter-Polling        Maximum Header

ID               Rate                    Count              Interval       Count        Size(bytes)

Ingress      Egress       Ingress      Egress       (sec)                    Ingress     Egress

---------  ---------  ----------------------   ----------------------  ----------------------   --------------------

Xe12             3        1024         2000           3           6          10            0     256           16

Xe13             4        2500         2000           4           7           5            3     100           16
```

CLI Commands

The sFlow feature introduces the following configuration command.

sflow collector-id

Use this command to configure the collector id which receives sFlow data collected from the interface.

Command Syntax

```
sflow collector-id <1-5>|
```

Parameter

collector-id <1-5>	Specifies the name of the Collector instance identifier. If the collector-id is not specified, the ID will be 1.

Default

Disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.5.1.

Example

```
OcNOS(config)#interface xe12
OcNOS(config-if)#sflow sampling-rate 1024 direction ingress max-header-size
256
OcNOS(config-if)#sflow enable
OcNOS(config-if)#sflow poll-interval 10
OcNOS(config-if)#sflow collector-id 3
```

Below are the revised commands. For more details, refer to the sFlow Commands section.

- sflow collector

Glossary

Key Terms/Acronym	Description
PDU	A unit of data transmitted as a composite by a protocol.
sFlow	Sampled Flow data sFlow (sFlow) is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

© 2025 IP Infusion Inc. Proprietary

CHAPTER 3 Software Monitoring and Reporting

Overview

OcNOS provides a mechanism (called “watchdogging”) to monitor all OcNOS modules and provides the following functions.

1. Periodic heart beat check.
2. Automatic restarts of a module upon a hung state or crash detection.
3. Upon hanging or crashing of a module, a crash report (including system states) is logged.
4. A proprietary SNMP trap is sent to the trap manager, if configured, after a fault is detected in a protocol module. Similarly a trap is sent when the module recovers.

By default, the software watchdog is enabled and the keep-alive time interval is 60 seconds. All OcNOS processes periodically send keep-alive messages to a monitoring module at the configured keep-alive time interval.

This functionality can be disabled for a particular module or all OcNOS modules by using CLI commands. In order to permanently disable software monitoring functionality, the user has to disable the watchdog feature. If, however, software watchdogging is disabled the monitoring module doesn’t take any action upon a hang or crash of any OcNOS module.

Software Monitoring

`#configure terminal`	Enter Configure mode.
`(config)#feature software-watchdog`	Enable software watchdog for all OcNOS modules — This is the default.
`(config)#no software-watchdog imi`	To disable software watchdog for only imi modules.
`(config)#software-watchdog keep-alive-time 100`	The keep-alive time interval in seconds. Default is 60 seconds and applies to all OcNOS modules.
`(config)#show software-watchdog status`	Display the keep-alive time interval and list of OcNOS process names with watchdog status for each OcNOS modules.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#exit`	Exit configuration

Validation

```
#show software-watchdog status
Software Watchdog timeout in seconds : 100
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ospfd                Enabled
isisd                Enabled
```

```
hostpd                  Enabled
ldpd                    Enabled
rsvpd                   Enabled
mribd                   Enabled
pimd                    Enabled
authd                   Enabled
mstpd                   Enabled
imi                     Disabled
onmd                    Enabled
HSL                     Enabled
oam                     Enabled
vlogd                   Enabled
vrrpd                   Enabled
ndd                     Enabled
ribd                    Enabled
bgpd                    Enabled
l2mribd                 Enabled
lagd                    Enabled
sflow                   Enabled
```

© 2025 IP Infusion Inc. Proprietary

CHAPTER 4 Internet Protocol SLA Configuration

Internet Protocol Service Level Agreement (IP SLA) is an active method of monitoring and reliably reporting on network performance. By "active," I refer to the fact that IP SLA will generate and actively monitor traffic continuously across the network. An IP SLA Router is capable of generating traffic and reporting on it in real time

IP SLA can be configured in two parts. There is the IP SLA router, which generates the traffic, and the IP SLA Responder (which can be any device, not just a router). The IP SLA Responder is not required for IP SLA to function, but it does allow for more detailed information gathering and reporting.

After an IP SLAs operation has been configured, you must schedule the operation to begin capturing statistics and collecting error information. When scheduling an operation, it can start immediately or start at a certain month, day, and hour. There is a pending option to set the operation to start at a later time. The pending option is also an internal state of the operation visible through SNMP. The pending state is also used when an operation is a reaction (threshold) operation waiting to be triggered. You can schedule a single ip slas operation or a group of operations at one time.

Note: IP SLA sessions are scaled to 500 sessions on Edgecore AS7316-26XB switches. This limit may vary on other devices based on the device capacity and performance.

Topology

Figure 4-31: IP SLA Topology

Configuration

Configure IP Address

Configure the IP addresses on the PE-1, P routers.

PE-1

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface (xe1) to be configured.
`(config-if)#ip address 10.1.1.1/24`	Set the IP address of the interface to 10.1.1.1/24.
`(config-if)#exit`	Exit interface mode.
`(config)#commit`	Commit the candidate configuration to the running configuration

P

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Specify the interface (xe1) to be configured.
`(config-if)#ip address 10.1.1.2/24`	Set the IP address of the interface to 10.1.1.2/24.

© 2025 IP Infusion Inc. Proprietary

(config-if)#exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration

Configure IP SLA Configurations on PE 1 router

PE-1

#configure terminal	Enter configure mode.
(config)#ip sla <1-65535>	configure IP SLA with a unique no
(config-ip-sla)# icmp-echo ipv4<destination IP> source-interface <interface name>	configure the icmp-echo using destination Ip Address and source interface name
(config-ip-sla-echo)#threshold <1000-60000>	Configure the threshold value
(config-ip-sla-echo)#timeout <1000-60000>	Configure the Timeout value
(config-ip-sla-echo)#frequency <1-60>	Configure the frequency value
(config-ip-sla-echo)#exit	Exit icmp-echo mode
(config-ip-sla)#exit	Exit from IP SLA mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#time-range <1-60 characters>	configure a time-range
(config-tr)#start-time 11:22 3 july 2021	configure a start-time
(config-tr)#end-time after 200	Configure end-time
(config-tr)#frequency hourly	configure frequency
(config-tr)#exit	exit from time-range
(config)#ip sla schedule <1-65535> time-range echo_schedule	Schedule a IP SLA measurement
(config)#commit	Commit the candidate configuration to the running configuration

Validation

PE-1

```
#sh running-config ip sla
ip sla 1
 icmp-echo ipv4 10.1.1.2 source-interface xe1
  frequency 6
  threshold 50000
  timeout 55000
ip sla schedule 1 time-range tr1
#sh running-config time-range
!
time-range tr1
 start-time 05:00 21 september 2021
 end-time 06:40 21 september 2021
```

```
#ping 10.1.1.2
Press CTRL+C to exit
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=64 time=0.436 ms
1 packets transmitted, 1 received, 0% packet loss, time 0ms
#sh ip sla summary
IP SLA Operation Summary
Codes: * active, ^ inactive

ID       Type        Destination       Stats       Return      Last
                                                    (usec)        Code        Run
-------------------------------------------------------------------
*1      icmp-echo   10.1.1.2         2000         OK        2021 Sep 21 05:01:00

#sh ip sla statistics 1 detail
========================================
            IP SLA Statistics
========================================
  IP SLA ID                : 1
  Start Time               : 2021 Sep 21 05:00:00
  Elapsed time(milli sec)  : 25003
  Packets Sent             : 5
  Packets Received         : 5
  Packet Loss(%)           : 0.0000
  Invalid Tests            : 0
  Round Trip Delay(usec)
      Minimum              : 1000
      Maximum              : 1000
      Average              : 800
```

CHAPTER 5 Control Plane Policing Configuration

Control plane policing (CoPP) manages the traffic flow destined to the host router CPU for control plane processing. CoPP limits the traffic forwarded to the host CPU and avoids impact on system performance.

1. CoPP has organized the handling of control packets by providing per-protocol hardware CPU queues. So, control packets are queued in different CPU queues based on protocol.
2. Per-protocol CPU queue rate limits and buffer allocations are programmed during router initialization, thus, every CPU queue is rate-limited to a default stable and balanced behavior across protocols.
3. When control packets are received at a higher rate than the programmed rate, the excess traffic is dropped at the queue level in the packet processor hardware itself.
4. All CPU queues are pre-programmed with default rate limits and buffer allocations to ensure a default stable and balanced behavior across protocols.
5. Rate limits are in terms of Kbps. Hardware does not support packets per second (PPS).
6. Qumran (MX, AX, and UX) supports per-queue rate shaping configurations within a range of 469 Kbps to 483 Gbps. The granularity is 469 Kbps for the low range and 1.56% for the higher range.

.

Table 5-15: Default CPU queues

Default queues	Default rate In kbps	Maximum configurable rate in kbps	Default queue length in kbytes	Description
CPU0.q0	900	20000	1024	Unclassified protocols and unknown or destination lookup failure packets are redirected to default CPU queues 0-7 based on the packet's `cos/dscp` values. SSH, TELNET, and SNMP traffic destined to host router CPU is remarked to CPU0.q6. SSH: TCP Source/Destination port 22 TELNET: TCP Source/Destination port 23 SNMP: UDP Source/Destination port 161/162
CPU0.q1	900	20000	1024	
CPU0.q2	900	20000	1024	
CPU0.q3	900	20000	1024	
CPU0.q4	900	20000	1024	
CPU0.q5	900	20000	1024	
CPU0.q6	10000	20000	1024	
CPU0.q7	900	20000	1024	

Table 5-16: Per protocol CPU queues

Protocol queues	Default rate In kbps	Maximum configurable Rate in kbps	Default queue length in kbytes	Description
IGMP	1000	1000	2048	Internet Group Management Protocol packets (IP protocol 2)
ISIS/ESIS	8000	8000	1024	ISIS (DMAC 0180:C200:0014/0015) ESIS (DMAC 0900:2B00:0004/0005) Note: ESIS = End System-to-Intermediate System (ISIS point-to-point case)
Reserved Mcast	8000	8000	2048	Reserved IPv4 and IPv6 Multicast packets IPv4: Local Network Control Block (224.0.0.0 - 224.0.0.255 (224.0.0/24)) IPv6: Link-Local Scope Multicast Addresses (FF02::/8)
IPv6 Link Local	1000	1000	1024	IPv6 link local packets DIPv6: FE80::/8
OSPF	8000	8000	1024	OSPF unicast packets (IP protocol 89)
BGP	8000	8000	1024	BGP packets TCP source/destination port number: 179
RSVP/LDP	1500	1500	1024	RSVP and LDP packets RSVP: IP protocol 46 LDP: L4 source/destination port number:646
VRRP/RIP/DHCP	2000	2000	1024	VRRP packets: IP protocol number 112 RIP packets: UDP source and destination port number: 520 RIPNG packets: UDP source and destination port number: 521 DHCP: DHCP v4/v6 server packets, DHCP v4/v6 client packets (L4 source/destination port number: 67 or 68)
PIM	8000	8000	1024	Protocol Independent Multicast packets: IP protocol number 103
ICMP	1000	1000	1024	ICMP packets: IP protocol number 1 Unicast ICMPv6 packets: IP next header number 58
ARP	1000	1000	1024	ARP packets. Ether-type 0x0806
BPDU	8000	8000	1024	xSTP: DMAC 0180:C200:0000 Provider Bridging: 0180:C200:0008 LACP: DMAC 0180:C200:0002, ethertype:0x8809, subtype:1/2 AUTHD: DMAC 0180:C200:0003 LLDP: DMAC 0180:C200:000E EFM: DMAC 0180:C200:0002, ethertype:0x8809, subtype:3 ELMI: DMAC 0180:C200:0007 SYNCE: DMAC 0180:C200:0002, ethertype:0x8809, subtype:0x0A RPVST: DMAC 0100:0CCC:CCCD L2TP: DMAC 0100:C2CD:CDD0/0104:DFCD:CDD0 G8032: DMAC 0119:A700:00XX
OAMP	1000	1000	1024	OAMP packets
sFlow	16384	16384	1024	Ingress and Egress sampled packets.

Table 5-16: Per protocol CPU queues (Continued)

Protocol queues	Default rate In kbps	Maximum configurable Rate in kbps	Default queue length in kbytes	Description
DSP	1500	1500	76800	L2 FDB events
EVPN	468	468	1024	ARP and ND cache queue for packets coming on VXLAN access ports.
nhop	500	500	1024	Inter VRF route leak unresolved data packets for ARP resolution.
ICMP-redirect	400	400	256	Data packets to CPU for ICMP redirect packet generation.
Guest	8000	8000	1024	
CFM	1000	1000	1024	
BFD	4000	4000	1024	BFD Single hop packets: UDP port 3784, TTL 255 BFD Multi hop packets: UDP port 4784 Micro BFD packets: UDP port 6784, TTL 255
PTP	4000	4000	1024	

CHAPTER 6 400G PM Alarm

Overview

The 400G PM alarm monitors and detects performance issues like the bit error rate and signal power in the network. This feature extends OcNOS performance-related monitoring capabilities and provides additional performance monitors and alarms.

400G coherent module is a high-speed optical transceiver capable of transferring data long-distance with high performance. Its compatibility with single-mode optical fiber makes a robust combination in delivering a high-quality network transmission.

Feature Characteristics

Access the additional set of 400G performance monitoring parameters, such as Transmitter FEC Detected Degrade (Tx FDD), Transmitter FEC Excessive Degrade (Tx FED), Receiver FEC Detected Degrade (Rx FDD), and Receiver FEC Excessive Degrade (Rx FED), to receive an automatic alarm notification on the CLI interface, via an SNMP trap, or thorugh the Netconf interface. The automatic alarm is triggered when the monitored parameter crosses the configured value.

For 400G coherent modules, use this feature to configure custom thresholds for Tx FDD, Tx FED, Rx FDD, Rx FED, Tx Power, Rx Total Power, and Rx Signal Power through a new set of CLI configuration commands and Netconf interface.

Note: Configuration of the threshold value is not possible through SNMP.

Benefits

The capability of this feature to configure the alarm threshold allows customization based on the network requirements and expected error rates. If the signal power exceeds the configured threshold value, it sends a notification to take action that prevents the receiving devices from potential damage.

Prerequisites

The availability of specific parameters or flags is vendor-specific, so read the 400G transceiver data-sheet to determine the available parameters or flags.

Configuration

This section shows the configuration of the 400G PM Alarm.

Topology

R1 is connected to the R2 by 400G ZR/ZR+ transceiver. The interface cd 10 and cd20 are 400G interfaces where the 400G ZR/ZR+ transceiver is connected. Cd10 is the host interface and here the configuration of the threshold value for the host-lane occurs. In cd20 interface, we can configure the media-lane threshold value.

Figure 6-1: 400G PM alarm

Media-lane Configuration

The below configuration is to set up the threshold value for the media lane.

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#qsfp-dd 20`	Enter QSFP-DD module configuration.
`R1(config-qsfp-dd)#media-lane 1`	Enter the Media lane configuration
`R1(config-qsfp-dd-media)#threshold rx-fdd`	Enter the BER threshold for FDD under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-fed`	Enter the BER threshold for FED under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-signal-power`	Enter the threshold for Rx Signal Power under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 4`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la -3`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#hw 5`	Configure the High warning threshold
`R1(config-qsfp-dd-media-thresh)#lw -5`	Configure the low warning threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#threshold rx-total-power`	Enter the threshold for Rx Total Power under Threshold configuration
`R1(config-qsfp-dd-media-thresh)#ha 2`	Configure the High alarm threshold
`R1(config-qsfp-dd-media-thresh)#la -2`	Configure the low alarm threshold
`R1(config-qsfp-dd-media-thresh)#hw 3`	Configure the High warning threshold
`R1(config-qsfp-dd-media-thresh)#lw -3`	Configure the low warning threshold
`R1(config-qsfp-dd-media-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#exit`	Exit media Configure mode.
`R1(config-qsfp-dd)#commit`	Commit the candidate configuration to the running configuration

© 2025 IP Infusion Inc. Proprietary

Host-lane Configuration

The below configuration is to set up the threshold value for the host lane.

R1

`R1#configure terminal`	Enter Configure mode
`R1(config)#qsfp-dd 10`	Enter QSFP-DD module configuration
`R1(config-qsfp-dd)#Host-lane 1`	Enter the Media lane configuration
`R1(config-qsfp-dd-host)#threshold tx-fdd`	Enter the BER threshold for FDD under Threshold configuration
`R1(config-qsfp-dd-host-thresh)#ha 0.365`	Configure the High alarm threshold
`R1(config-qsfp-dd-host-thresh)#la 0.165`	Configure the low alarm threshold
`R1(config-qsfp-dd-host-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-host)#threshold tx-fed`	Enter the BER threshold for FED under Threshold configuration
`R1(config-qsfp-dd-host-thresh)#ha 0.765`	Configure the High alarm threshold
`R1(config-qsfp-dd-host-thresh)#la 0.665`	Configure the Low alarm threshold
`R1(config-qsfp-dd-host-thresh)#exit`	Exit threshold Configure mode.
`R1(config-qsfp-dd-media)#exit`	Exit media Configure mode.
`R1(config-qsfp-dd)#commit`	Commit the candidate configuration to the running configuration

Validation

R1

The below is the show output of media lane threshold parameter:

```
qsfp-dd 20
 media-lane 1
  threshold rx-fdd
   ha 0.365500
   la 0.165000
  threshold rx-fed
   ha 0.365000
   la 0.165000
  threshold rx-total-power
   ha 2.000000
   la -2.000000
   hw 3.000000
   lw -3.000000
  threshold rx-signal-power
   ha 4.000000
   la -3.000000
   hw 5.000000
   lw -5.000000
```

```
!
!
end
```

Verify the user-threshold media-lane:

```
#show qsfp-dd 20 user-threshold status media
Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  | Unit |
-------------------------------------------------------------------------------------
 Rx FDD Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FDD Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx Total Power HA   | 1    | 2.00        | 2.00       | 0.00     | 15.00    | dBm  |
 Rx Total Power HW   | 1    | 3.00        | 3.00       | -10.00   | 13.00    | dBm  |
 Rx Total Power LW   | 1    | -3.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Total Power LA   | 1    | -2.00       | -          | -40.00   | -15.00   | dBm  |
 Rx Signal Power HA  | 1    | 4.00        | 4.00       | 0.00     | 15.00    | dBm  |
 Rx Signal Power HW  | 1    | 5.00        | 5.00       | -10.00   | 13.00    | dBm  |
 Rx Signal Power LW  | 1    | -5.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Signal Power LA  | 1    | -3.00       | -          | -40.00   | -15.00   | dBm  |
```

The below is the show output of host lane threshold parameter:

```
qsfp-dd 10
 host-lane 1
  threshold tx-fdd
   ha 0.365000
   la 0.165000
  threshold tx-fed
   ha 0.765000
   la 0.665000
```

Verify the user-threshold host-lane:

```
#show qsfp-dd 10 user-threshold status host
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  | Unit |
-------------------------------------------------------------------------------------
 Tx FDD Active       | 1    | 3.65e-01    | 3.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FDD Clear        | 1    | 1.65e-01    | 1.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Active       | 1    | 7.65e-01    | 7.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Clear        | 1    | 6.65e-01    | 6.65e-01   | 0.00e+00 | 1.00e+00 | NA   |
```

Global Threshold Configuration

The below configuration is to set up the threshold value for the global threshold.

R1

R1#configure terminal	Enter Configure mode
R1(config)#qsfp-dd 20	Enter QSFP-DD module configuration
R1(config-qsfp-dd)#threshold rx-fdd	Enter the media Rx BER threshold for FDD under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.963	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.763	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-fed	Enter the media Rx BER threshold for FED under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.863	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.463	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-signal-power	Enter the media threshold for Rx Signal Power under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 6	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la -6	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#hw 4	conc Configure the High warning threshold
R1(config-qsfp-dd-thresh)#lw -4	conc Configure the Low warning threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode. Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold rx-total-power	Enter the media threshold for Rx Signal Power under Th Enter the media threshold for Rx Total Power under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 7	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la -7	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#hw 9	conc Configure the High warning threshold
R1(config-qsfp-dd-thresh)#lw -9	conc Configure the Low warning threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode. Exit threshold Configure mode.
R1(config)#qsfp-dd 10	Enter QSFP DD module configuration.
R1(config-qsfp-dd)#threshold tx-fdd	Enter the host Rx BER threshold for FDD under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.456	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.321	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.
R1(config-qsfp-dd)#threshold tx-fed	Enter the host Rx BER threshold for FED under Threshold Configuration
R1(config-qsfp-dd-thresh)#ha 0.864	conc Configure the High alarm threshold
R1(config-qsfp-dd-thresh)#la 0.666	conc Configure the Low alarm threshold
R1(config-qsfp-dd-thresh)#exit	Exit threshold Configure mode.

Validation

R1

The below is the show output of global threshold parameter:

```
#sh running-config
qsfp-dd 20
 threshold rx-fdd
  ha 0.963000
  la 0.763000
 threshold rx-fed
  ha 0.863000
  la 0.463000
 threshold rx-total-power
  ha 7.000000
  la -7.000000
  hw 9.000000
  lw -9.000000
 threshold rx-signal-power
  ha 6.000000
  la -6.000000
  hw 4.000000
  lw -4.000000
qspf-dd 10
 threshold tx-fdd
  ha 0.456000
  la 0.321000
 threshold tx-fed
  ha 0.864000
  la 0.666000
```

Verify the global threshold:

```
#sh qsfp-dd 20 user-threshold status media
Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]
Port Number                    : 20
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  | Unit |
-------------------------------------------------------------------------------------
 Rx FDD Active       | 1    | 9.63e-01    | 9.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FDD Clear        | 1    | 7.63e-01    | 7.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Active       | 1    | 8.63e-01    | 8.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx FED Clear        | 1    | 4.63e-01    | 4.63e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Rx Total Power HA   | 1    | 7.00        | 7.00       | 0.00     | 15.00    | dBm  |
 Rx Total Power HW   | 1    | 9.00        | 9.00       | -10.00   | 13.00    | dBm  |
 Rx Total Power LW   | 1    | -9.00       | -          | -33.00   | -10.00   | dBm  |
 Rx Total Power LA   | 1    | -7.00       | -          | -40.00   | -15.00   | dBm  |
 Rx Signal Power HA  | 1    | 6.00        | 6.00       | 0.00     | 15.00    | dBm  |
 Rx Signal Power HW  | 1    | 4.00        | 4.00       | -10.00   | 13.00    | dBm  |
 Rx Signal Power LW  | 1    | -4.00       | -          | -33.00   | -10.00   | dBm  |
```

© 2025 IP Infusion Inc. Proprietary

```
 Rx Signal Power LA  | 1    | -6.00       | -          | -40.00   | -15.00   | dBm  |

#sh qsfp-dd 10 user-threshold status host
Port Number                     : 10
-------------------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  | Unit |
-------------------------------------------------------------------------------------
 Tx FDD Active       | 1    | 4.56e-01    | 4.56e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FDD Clear        | 1    | 3.21e-01    | 3.21e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Active       | 1    | 8.64e-01    | 8.64e-01   | 0.00e+00 | 1.00e+00 | NA   |
 Tx FED Clear        | 1    | 6.66e-01    | 6.66e-01   | 0.00e+00 | 1.00e+00 | NA   |
```

New CLI Commands

ha

Use this command to set the high alarm threshold value for the Tx FDD, Tx FED, Rx FDD, Rx FED, Tx power, Rx Total Power, and Rx Signal Power performance monitoring parameters. High alarm threshold is the highest parameter value for the 400G transceiver to operate safely and reliably. For FEC Detected Degrade (FDD) and FEC Excessive Degrade (FED) monitoring, this command sets the active threshold. FDD suggests that the FEC has detected errors in data transmission. The alarm notification is triggered if the average BER exceeds the configured FDD value.

Command Syntax

```
ha VALUE
no ha
```

Parameters

VALUE	high alarm value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the high warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold tx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no ha
OcNOS(config-qsfp-dd-thresh)#commit
```

hw

Use this command to set the high warning threshold value for Tx power, Rx Total Power, and Rx Signal Power. High warning threshold is the highest parameter value for the 400G transceiver, exceeding which the transceiver performance and operational issues can occur.

Note: This command has no effect for FED and FDD thresholds.

Command Syntax

```
hw VALUE
no hw
```

Parameters

VALUE	high warning value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the high warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#hw 3.0
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no hw
OcNOS(config-qsfp-dd-thresh)#commit
```

la

Use this command to set the low alarm threshold value based on the vendor-specific threshold for all the performance monitoring parameters Tx FDD, Tx FED, Rx FDD, Rx FED, Tx power, Rx Total Power, and Rx Signal Power threshold value. Low alarm threshold is the lowest parameter value for the 400G transceiver to operate with reliability. For FDD and FED monitoring this command sets the clear threshold.

Command Syntax

```
la VALUE
no ha
```

Parameters

VALUE	low alarm value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the low alarm threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-fed
OcNOS(config-qsfp-dd-thresh)#la 0.001234
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no la
OcNOS(config-qsfp-dd-thresh)#commit
```

lw

Use this command to set the low warning threshold value. Low warning threshold is the lowest parameter value for the 400G transceiver, below which the transceiver performance and operational issues can occur.

Note: This command has no effect for FED and FDD thresholds.

Command Syntax

```
lw VALUE
```

```
no lw
```

Parameters

`lw`	low warning value

Command Mode

Global threshold mode, host-lane threshold mode, and media-lane threshold mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the low warning threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#lw -1.0
OcNOS(config-qsfp-dd-thresh)#commit
OcNOS(config-qsfp-dd-thresh)#no lw
OcNOS(config-qsfp-dd-thresh)#commit
```

show qsfp-dd user-threshold status

Use this command to show the current configuration status of user thresholds.

Command Syntax

```
show qsfp-dd <PORT> user-threshold status (host|media)
```

Parameters

PORT	The front panel port number of the device where the transceiver is connected
host	Host side config status
media	Media side config status

Command Mode

Exec mode and privileged Exec mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

This below show command displays the hardware state of the programmed user thresholds.

```
OcNOS#show qsfp-dd 48 user-threshold status host

Port Number                    : 48

-------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  |
-------------------------------------------------------------------------
 Tx FDD Active       | 1    | 9.88e-01    | 9.87e-01   | 0.00e+00 | 1.00e+00 |
 Tx FDD Clear        | 1    | 5.43e-03    | 5.43e-03   | 0.00e+00 | 1.00e+00 |
 Tx FED Active       | 1    | 5.43e-01    | 5.43e-01   | 0.00e+00 | 1.00e+00 |
 Tx FED Clear        | 1    | 9.88e-03    | 9.87e-03   | 0.00e+00 | 1.00e+00 |

OcNOS#show qsfp-dd 48 user-threshold status media

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low
Warning]

Port Number                    : 48

-------------------------------------------------------------------------
      Threshold      | Lane | User Config | H/W Config | Minimum  | Maximum  |
-------------------------------------------------------------------------
 Rx FDD Active       | 1    | 1.23e-01    | 1.23e-01   | 0.00e+00 | 1.00e+00 |
 Rx FDD Clear        | 1    | 6.79e-03    | 6.78e-03   | 0.00e+00 | 1.00e+00 |
 Rx FED Active       | 1    | 6.79e-01    | 6.78e-01   | 0.00e+00 | 1.00e+00 |
 Rx FED Clear        | 1    | 1.23e-03    | 1.23e-03   | 0.00e+00 | 1.00e+00 |
 Rx Total Power HA   | 1    | 4.00        | 4.00       | -26.00   | 9.00     |
 Rx Total Power HW   | 1    | 3.00        | 3.00       | -26.00   | 9.00     |
 Rx Total Power LW   | 1    | -3.00       | -3.00      | -26.00   | 9.00     |
 Rx Total Power LA   | 1    | -4.00       | -4.00      | -26.00   | 9.00     |
 Rx Signal Power HA  | 1    | 2.00        | 2.00       | -26.00   | 9.00     |
 Rx Signal Power HW  | 1    | 1.00        | 1.00       | -26.00   | 9.00     |
 Rx Signal Power LW  | 1    | -1.00       | -1.00      | -26.00   | 9.00     |
 Rx Signal Power LA  | 1    | -2.00       | -2.00      | -26.00   | 9.00     |
```

show qsfp-dd 48 user-threshold status host output details

Field	Description
Threshold	The parameters that are monitored.
Lane	Displays the channel number where the thresholds are applied.
User Config	Displays what the user has configured.
H/W Config	Displays what is programmed in the transceiver hardware.
Minimum	The lowest values that are allowed to be used for this configuration.
Maximum	The highest values that are allowed to be used for this configuration.

threshold (host-lane mode)

Use this command to enter host lane level user threshold configuration mode. Host lane mode is a configuration mode that allows configuring specific values for the host lanes.Host lanes are wires that carry the electrical signal from the host interface to the module and vice-versa.

Command Syntax

```
threshold (tx-fdd|tx-fed)
```

Parameters

`tx-fdd`	Tx FDD
`tx-fed`	Tx FED

Command Mode

host-lane mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the host-lane threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#host-lane 1
OcNOS(config-qsfp-dd-host)#threshold tx-fdd
OcNOS(config-qsfp-dd-host-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-host-thresh)#la 0.005432
OcNOS(config-qsfp-dd-host-thresh)#threshold tx-fed
OcNOS(config-qsfp-dd-host-thresh)#ha 0.5432
OcNOS(config-qsfp-dd-host-thresh)#la 0.009876
OcNOS(config-qsfp-dd-host-thresh)#commit
```

threshold (media-lane mode)

Use this command to enter media lane level user threshold configuration mode. Media lane mode is a configuration mode that allows configuring specific values for each media lane. Media lanes are the electrical wire pairs (copper cables) or optical fibers that carry signals from the module to the other router and vice-versa.

Command Syntax

```
threshold (rx-fdd|rx-fed|rx-total-power|rx-signal-power)
```

Parameters

`rx-fdd`	Rx FDD
`rx-fed`	Rx FED
`rx-total-power`	Rx Total Power
`rx-signal-power`	Rx Signal Power

Command Mode

Media-lane mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the media-lane threshold:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#media-lane 1
OcNOS(config-qsfp-dd-media)#threshold rx-fdd
OcNOS(config-qsfp-dd-media-thresh)#ha 0.1234
OcNOS(config-qsfp-dd-media-thresh)#la 0.006789
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-fed
OcNOS(config-qsfp-dd-media-thresh)#ha 0.6789
OcNOS(config-qsfp-dd-media-thresh)#la 0.001234
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-media-thresh)#ha 4
OcNOS(config-qsfp-dd-media-thresh)#hw 3
OcNOS(config-qsfp-dd-media-thresh)#lw -3
OcNOS(config-qsfp-dd-media-thresh)#la -4
OcNOS(config-qsfp-dd-media-thresh)#threshold rx-signal-power
OcNOS(config-qsfp-dd-media-thresh)#ha 2
OcNOS(config-qsfp-dd-media-thresh)#hw 1
OcNOS(config-qsfp-dd-media-thresh)#lw -1
OcNOS(config-qsfp-dd-media-thresh)#la -2
OcNOS(config-qsfp-dd-media-thresh)#commit
```

threshold (QSFP-DD mode)

Use this command to enter global level user threshold configuration mode.In global mode, configure the same threshold value across all host or media lanes.

Command Syntax

```
threshold (tx-fdd|tx-fed|rx-fdd|rx-fed|rx-total-power|rx-signal-power)
```

Parameters

`tx-fdd`	Tx FDD
`tx-fed`	Tx FED
`rx-fdd`	Rx FDD
`rx-fed`	Rx FED
`rx-total-power`	Rx Total Power
`rx-signal-power`	Rx Signal Power

Command Mode

QSFP-DD mode.

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

The below configuration shows to configure the threshold in global mode:

```
OcNOS#configure terminal
OcNOS(config)#qsfp-dd 48
OcNOS(config-qsfp-dd)#threshold tx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.9876
OcNOS(config-qsfp-dd-thresh)#la 0.005432
OcNOS(config-qsfp-dd-thresh)#threshold tx-fed
OcNOS(config-qsfp-dd-thresh)#ha 0.5432
OcNOS(config-qsfp-dd-thresh)#la 0.009876
OcNOS(config-qsfp-dd-thresh)#threshold rx-fdd
OcNOS(config-qsfp-dd-thresh)#ha 0.1234
OcNOS(config-qsfp-dd-thresh)#la 0.006789
OcNOS(config-qsfp-dd-thresh)#threshold rx-fed
OcNOS(config-qsfp-dd-thresh)#ha 0.6789
OcNOS(config-qsfp-dd-thresh)#la 0.001234
OcNOS(config-qsfp-dd-thresh)#threshold rx-total-power
OcNOS(config-qsfp-dd-thresh)#ha 4
OcNOS(config-qsfp-dd-thresh)#hw 3
OcNOS(config-qsfp-dd-thresh)#lw -3
OcNOS(config-qsfp-dd-thresh)#la -4
OcNOS(config-qsfp-dd-thresh)#threshold rx-signal-power
OcNOS(config-qsfp-dd-thresh)#ha 2
OcNOS(config-qsfp-dd-thresh)#hw 1
OcNOS(config-qsfp-dd-thresh)#lw -1
OcNOS(config-qsfp-dd-thresh)#la -2
OcNOS(config-qsfp-dd-thresh)#commit
```

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
BER	Bit Error Rate
FDD	FEC detected degrade
FEC	Forward error correction
PM	Performance Monitoring
FED	FEC excessive degrade
Rx	Receiver
Tx	Transmitter
SNMP	Simple Network Management Protocol

Glossary

The following provides definitions for key terms used throughout this document.

400G coherent module	400G coherent module is a high-speed optical transceiver capable of transferring data long-distance with high performance. Its compatibility with single-mode optical fiber makes a robust combination in delivering a high-quality network transmission.
Active threshold	This parameter threshold value triggers alarm notification.
Clear threshold	This parameter threshold value does not trigger alarm notification.
FDD	FEC Detected Degrade suggests that the FEC has detected errors in data transmission. The alarm notification is triggered if the average BER exceeds the configured FDD value.
FEC	FEC is a technique that detects and corrects errors during data transmission to maintain the reliability of the communication system.
FED	FEC Excessive Degrade suggests that the FEC has detected very high errors in data transmission. FED is a more severe error condition than FDD and needs more attention. The alarm notification is triggered if the average BER exceeds the configured FED value.
Global mode	In global mode, configure the same threshold value across all host or media lanes.
High alarm threshold	This is the highest parameter value for the 400G transceiver to operate safely. When a given parameter value crosses this threshold, the transceiver operation is unreliable, or the transceiver hardware could get damaged.
High warning threshold	This is the highest parameter value that limits the optimal operation zone. The transceiver can operate after a parameter crosses this threshold, but performance and operational issues can occur.

Host lane	Host lanes are wires that carry the electrical signal from the host interface to the module and vice-versa.
Host-lane mode	Host lane mode is a configuration mode that allows configuring specific values for the host lanes. Contrary to the global mode level that configures the same value across all host lanes.
Low alarm threshold	This is the lowest parameter value for the 400G transceiver to operate safely. When a given parameter value crosses this threshold, the transceiver operation is unreliable.
Low warning threshold	This is the lowest parameter value that limits the optimal operation zone. The transceiver can operate after a parameter crosses this threshold, but performance and operational issues can occur.
Media lane	Media lanes are the electrical wire pairs (copper cables) or optical fibers that carry signals from the module to the other router and vice-versa.
Media-lane mode	Media lane mode is a configuration mode that allows configuring specific values for each media lane (per fiber cable physical channel). Contrary to the global mode level that configures the same value across all media lanes.

CHAPTER 7 IP Flow Information Export

Overview

In OcNOS, the Internet Protocol Flow Information Export (IPFIX) Exporter enables real-time traffic analysis. It achieves this through sampling, which involves selecting a subset of network traffic and exports flow records containing detailed information about the sampled traffic flows. It enables network operators to gain valuable insights into network traffic patterns and behaviors. Note: The IPFIX feature is currently not recommended for use in production networks. **Note:** The IPFIX feature is currently not recommended for use in production networks.

IPFIX Exporter Characteristics

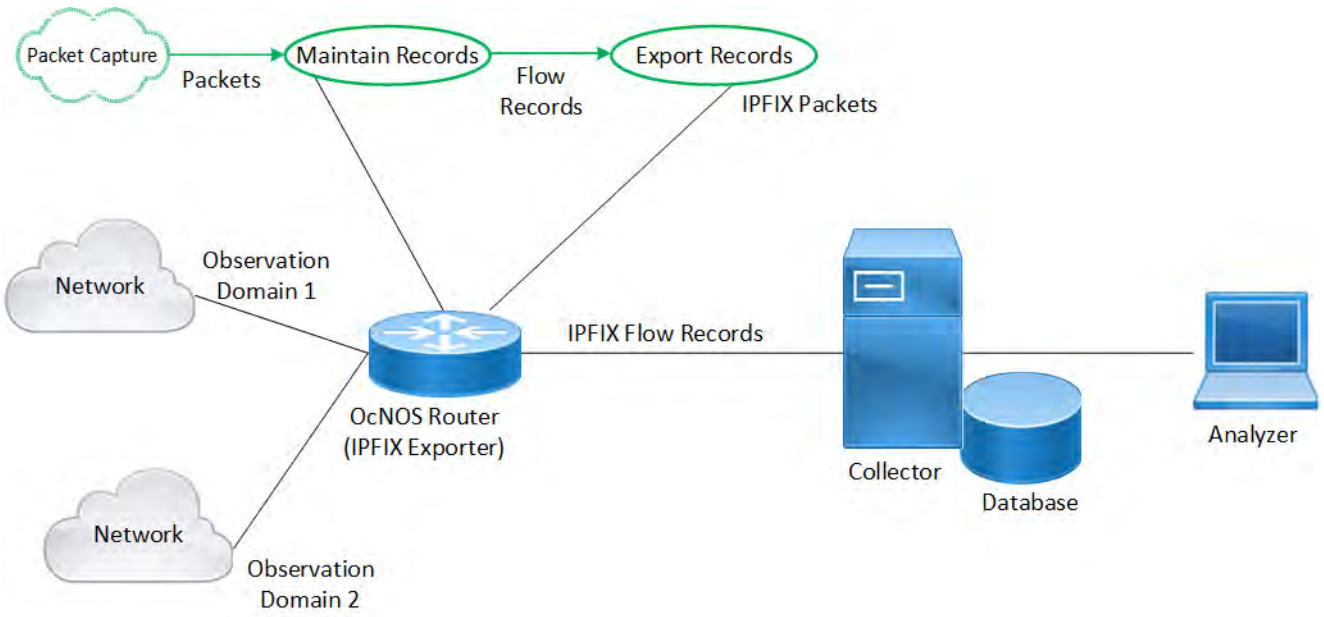
The OcNOS router equipped with IPFIX Exporter functionality within the network infrastructure identifies the customer domain (Observation ID), samples ingress traffic, and generates IPFIX flow records. These flow records are transmitted to a designated collector node for further analysis.

Achieves efficient flow record management and export on the Jericho2 (Broadcom DNX) platform by leveraging hardware acceleration support and utilizing Application Specific Integrated Circuit (ASIC) capabilities, such as the Eventor block. ASIC ensures optimized performance and functionality at the hardware level.

The IPFIX exporter performs three core functions:

1. Selecting flows for sampling
2. Maintaining flow records
3. Exporting flow records

The following diagram illustrates the flow of network (ingress) traffic data in an IPFIX-enabled environment.



IPFIX Exporter

Here's a breakdown of the process steps:

Packet Capture: Capture network traffic data by the IPFIX Exporter (OcNOS Router) from various sources within the network.

Flow Selection for Sampling: IPFIX enables administrators to selectively sample specific network flows, allowing targeted traffic monitoring based on predefined criteria.

Note: IPFIX supports ingress sampling and only one IPv4 template format.

Maintain Records: IPFIX Exporter maintains detailed flow records using hardware-accelerated functions. These records include comprehensive information such as IPv4 traffic details, source and destination addresses, port numbers, protocol specifics, and timestamps.

Export Records: The IPFIX Exporter aggregates and packages the flow records into IPFIX packets. These packets are then exported to configured collector nodes for centralized traffic analysis and management.

The IPFIX Exporter aggregates and packages flow records into IPFIX packets, which it then exports to configured collector nodes for centralized traffic analysis and management.

Transmission: The IPFIX Exporter sends packets to the designated collector device connected through the in-band network using the default UDP port number `4739`. The collector IP address must be configured, and the port number is optional. If the port number is not specified, it defaults to `4739`.

Collector: Collector nodes receive the IPFIX packets and parse the flow records for further analysis and interpretation

Note: OcNOS does not include an IPFIX Collector.

Analyzer: Specialized software or tools analyze the collected flow records to gain insights into network traffic patterns and behaviors.

Limitations:

- IPFIX does not support validating route reachability to collector nodes.
- IPFIX does not support sampling of sub-interfaces, LAG, and SVI interfaces.
- Hardware limitations cause disruptions lasting approximately twelve seconds when changes are made to samples-per-message.
- The `hardware-profile filter` command is not integrated with IPFIX. IPFIX allocates its TCAM resources upon configuration of the first IPFIX monitored interface and releases them when the last IPFIX monitored interface is removed. The key size for IPFIX is 320 bits.

Benefits

The IPFIX Exporter has the following benefits:

Enhanced Network Visibility: IPFIX provides detailed insights into network traffic, enabling network operators to identify and address issues promptly.

Efficient Network Management: By collecting and exporting flow records, IPFIX streamlines network management tasks, allowing for more effective monitoring and troubleshooting.

Optimized Resource Utilization: With targeted flow sampling and detailed flow records, IPFIX helps optimize resource utilization by focusing monitoring efforts on specific network segments or traffic types.

Prerequisites

- Before enabling IPFIX, check if any `hardware-profile filter` entries are enabled. If any entries with a key size less than 320 bits are enabled, it is recommended to first disable them. Then, configure the first IPFIX monitored interface, and finally, re-enable the existing entries. This ensures optimal allocation of TCAM resources. If a CRITICAL error message indicating `No resources for operation` appears when enabling IPFIX or re-

enabling the existing entries, then all these features cannot be enabled simultaneously. Consider disabling other hardware filter entries. For example, on VXLAN Spine nodes, disable the `vxlan filter` to free up TCAM resources.

- Before configuring the IPFIX objects, enable the `hardware-profile statistics cfm-lm enable` filter statistics loss-measurement command in hardware. This action ensures that the necessary hardware functionality is enabled for seamless integration with the IPFIX configuration. It also ensures IPFIX counters are unused by other modules.
- Assign the IP address of a source and ingress interface configured on the exporter device.

  The following show running output illustrates enabling hardware statistics loss-measurement and assigning the IP address to the required interfaces.

```
hardware-profile statistics cfm-lm enable
!
interface xe4
 ip address 198.51.100.4/24
!
interface xe5
 ip address 192.0.2.88/24
!
```

Note:

- The maximum number of unique sampling rates supported by IPFIX Exporter depends on the availability of free mirroring profiles in the ASIC.
- Various features like SFLOW, SNIFF, and Mirror utilize each mirroring profile. Qumran-2A series platform supports a maximum of 32 mirror profiles. For every sampling rate configuration, even if it matches an existing rate on another interface, it requires a new mirror-profile. Therefore, the number of ports that can be enabled with IPFIX is limited by the number of mirror-port profiles available in the system.
- The IPFIX Exporter sends template record format to the collector over the in-band, and the ASIC sends data records over the in-band.

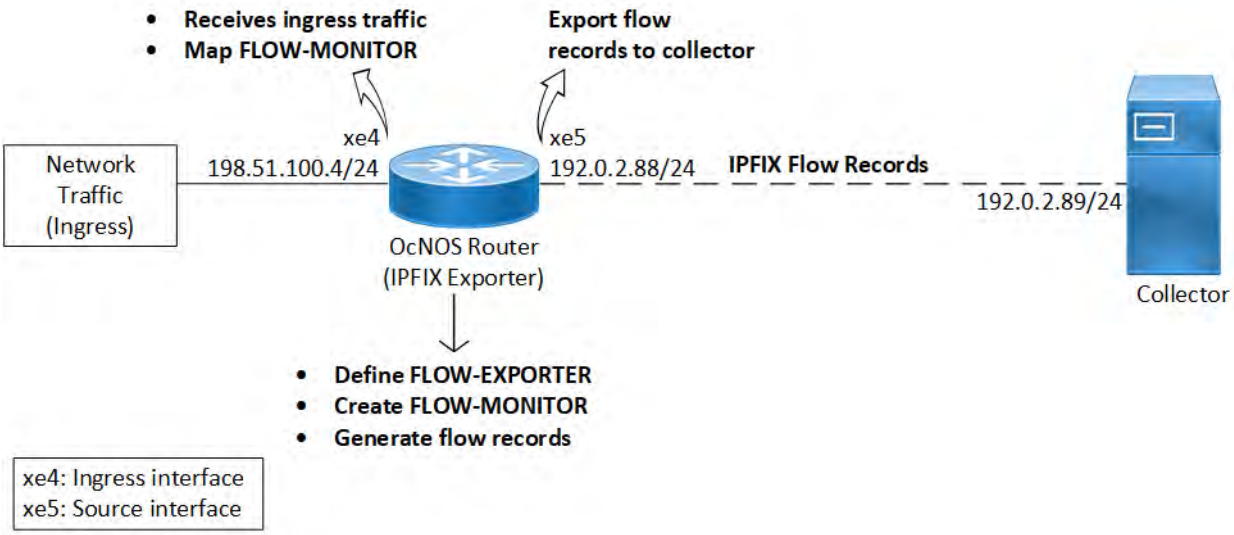
Configuration

The following configuration enables the IPFIX feature on the OcNOS device, facilitating the collection and export of flow-specific information for network traffic analysis and management.

Topology

In this topology, simulated ingress traffic is routed through an OcNOS device equipped with IPFIX Exporter functionality before being transmitted to the collector.

Note: The collector should be operational and actively listening on the configured IP address and port. Additionally, it should be reachable from the OcNOS node.



IPFIX Exporter

The following commands configure the IPFIX Exporter in OcNOS, enabling the collection and export of flow-specific information for ingress traffic analysis and management. For additional information on each command, refer to the IPFIX Commands section.

Note: Ensure all Prerequisites are met before proceeding with the configuration.

1. **Define an IP Flow Exporter for flow records:**

   When configuring the IP flow exporter (`FLOW-EXPORTER`), designate the source interface (`xe5`) for generating flow data and specify the destination collector IP address (`192.0.2.89`) and UDP port (`90`) for receiving the exported data. Assign a unique template ID (`500`) to ensure proper interpretation of the flow records, with templates refreshed at intervals of `600` seconds for accuracy. Also, set the number of flow samples per export message to `7` to determine the granularity of the exported data.

   ```
   OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
   OcNOS(ip-flow-exporter)#source xe5
   OcNOS(ip-flow-exporter)#collector 192.0.2.89 udp-port 90
   OcNOS(ip-flow-exporter)#template-id 500
   OcNOS(ip-flow-exporter)#template-refresh-interval 600
   OcNOS(ip-flow-exporter)#samples-per-message 7
   ```

2. **Create an IP Flow Monitor profile:**

   Establish a flow monitor (`FLOW-MONITOR`) to track network flows. Link it with the exporter (`FLOW-EXPORTER`) to transmit monitored flow data. Define a sampling rate `1024` to sample every 1024th packet for flow monitoring. Set the observation domain identifier (`16`) to identify the flow monitoring domain uniquely.

   ```
   OcNOS(config)#ip-flow-monitor FLOW-MONITOR
   OcNOS(ip-flow-monitor)#flow-exporter FLOW-EXPORTER
   OcNOS(ip-flow-monitor)#sampling-rate 1024
   OcNOS(ip-flow-monitor)#observation-domain-id 16
   ```

3. **Map the flow monitor to the ingress interface:**

   Associate the IP Flow Monitor profile `FLOW-MONITOR` to the ingress interface `xe4` to monitor traffic.

   ```
   OcNOS(config)#interface xe4
   OcNOS(config-if)#ip address 198.51.100.4/24
   OcNOS(config-if)#flow-monitor FLOW-MONITOR
   ```

Validation

1. Verify the IPFIX exporter named `FLOW-EXPORTER` has been configured with the correct parameters using the output of the show ipfix command.

```
OcNOS#show ipfix
Exporters:
  Name:                  FLOW-EXPORTER
    Source:              192.0.2.88
    Destination:         192.0.2.89
    Source UDP:          53859
    Destination UDP:     4739
    Template ID:         500

    Data Template Timeout:600
```

2. Check the exported fields in IPFIX data using the output of the show ipfix all command. Confirm the template ID and examine the list of fields in the template. These fields define the information captured in the flow records, including source and destination IP addresses, port numbers, and protocol details.

```
OcNOS#show ipfix all
Templates:
  Template ID:           500
    DIRECTON (61), Length:1
    IP_VERSION (60), Length:1
    IPV4_TOS (5), Length:1
    IPV4_PKT_LEN (1), Length:2
    IPV4_FRAG_OFFSET (88), Length:2
    PROTOCOL (4), Length:1
    IPV4_SIP (8), Length:4
    IPV4_DIP (12), Length:4
    L4_SRC_PORT (7), Length:2
    L4_DST_PORT (11), Length:2
    TCP_CONTROL (6), Length:2
    ICMP_TYPE (32), Length:2
    INGRESS_VRF (234), Length:4
    INGRESS_IF (10), Length:2
    EGRESS_VRF (235), Length:4
    EGRESS_IF (14), Length:2
    SYS_UPTIME (22), Length:4
Exporters:
   Name:                 FLOW-EXPORTER
    Source:              192.0.2.88
    Destination:         192.0.2.89
    Source UDP:          53859
    Destination UDP:     4739
    Template ID:         500

    Data Template Timeout:600
```

3. Confirm the accuracy of the IPFIX-related configurations by examining the output of the show running-config ipfix command. Ensure the IP flow exporter and monitor profiles are properly configured with the correct parameters.

```
OcNOS#show running-config ipfix
hardware-profile statistics cfm-lm enable
!
ip-flow-exporter FLOW-EXPORTER
 source xe5
 collector destination 192.0.2.89
```

```
 template-id 500
 template-refresh-interval 600
 samples-per-message 7
!
ip-flow-monitor FLOW-MONITOR
 flow-exporter FLOW-EXPORTER
 sampling-rate 1024
 observation-domain-id 16
!
interface xe4
 ip address 198.51.100.4/24
 flow-monitor FLOW-MONITOR
!
interface xe5
 ip address 192.0.2.88/24
!
```

4. Check the association of the IP flow monitor with the ingress interface (`xe4`) of the exporter device by examining the output of the `show running-config interface` command.

```
OcNOS#show running-config interface xe4
!
interface xe4
 ip address 198.51.100.4/24
 flow-monitor FLOW-MONITOR
!
```

Implementation Examples

Billing and Accounting System

Scenario: The Internet Service Provider (ISP) aims to implement a billing and accounting system to accurately track and bill customers based on their network usage.

Use Case: Implementing IPFIX exporters in OcNOS routers at the ISP's network edge enables real-time monitoring of traffic flows, collection of usage data, and generation of detailed reports for billing and accounting purposes. This solution empowers the ISP to implement usage-based billing, enhance transparency, optimize revenue, and ensure compliance with regulatory requirements.

Security Monitoring

Scenario: A large enterprise wants to enhance security and compliance monitoring in its network infrastructure.

Use Case: By leveraging IPFIX exporters in OcNOS routers, the enterprise can monitor network traffic in real-time, detect security threats, and ensure compliance with industry regulations. This implementation allows for collecting detailed flow records, analyzing traffic patterns, and responding rapidly to security incidents. Additionally, it facilitates forensic analysis, audit trail generation, and proactive security measures, thereby strengthening the overall security posture of the enterprise network.

IPFIX Commands

The IPFIX exporter introduces the following configuration commands.

collector destination

Use this command to specify the destination IPv4 address and port number for exporting IPFIX flow records to a collector.

Use `no` parameter of this command to remove the specified collector destination address. This command eliminates the previously configured IPv4 address for data collection, effectively disabling the flow export feature for the specified destination.

Command Syntax

```
collector destination (ipv4-address) port <UINT32>  (|vrf <WORD>)
no collector destination (ipv4-address)
```

Parameters

`destination (ipv4-address)`	Sets the IPv4 address of the collector where IPFIX flow records will be exported.It defines the destination endpoint for sending the flow records.
`port <UINT32>`	Specifies the port number for sending the IPFIX flow records to the collector. The valid port numbers must fall within the range of `1024 to 65535`. The default port number is `4739`.
`vrf <WORD>`	(Optional) Specifies the name of the virtual routing and forwarding (VRF) instance through which the flow records will be sent.

Default

None

Command Mode

IP flow exporter mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following commands configure the ip-flow-exporter (`FLOW-EXPORTER`) profile with the collector destination set to IP address `192.0.2.89` and port `1025`.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#collector destination 192.0.2.89 port 1025
```

flow-exporter

Use this command to associate the flow monitor with an ip-flow-exporter profile, enabling the flow monitor to export flow data to the specified destination defined in the exporter profile.

Command Syntax

```
flow-exporter <WORD>
```

Parameters

`flow-exporter <WORD>`	Specifies the name of the ip-flow-exporter profile, which must be unique within the device and can contain up to 32 alphanumeric characters, hyphens, and underscores.

Default

None

Command Mode

IP flow monitor mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command establishes a connection between an IP flow exporter profile named `FLOW-EXPORTER` and the ip-flow-monitor profile, enabling the flow monitor to export flow data using the settings configured in the exporter profile.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-monitor FLOW-MONITOR
OcNOS(ip-flow-monitor)#flow-exporter FLOW-EXPORTER
```

flow-monitor

Use this command to associate flow monitoring on an ingress interface, enabling the monitoring of traffic based on the settings specified in the ip-flow-monitor profile.

Use `no` parameter of this command to remove the association of flow monitoring from an ingress interface.

Command Syntax

```
flow-monitor <WORD>
no flow-monitor <WORD>
```

Parameters

`flow-monitor <WORD>`	Specifies the name of the ip-flow-monitor profile, which must be unique within the device and can contain up to 32 alphanumeric characters, hyphens, and underscores.

Default

None

Command Mode

Interface mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command associates the flow monitoring profile (`FLOW-MONITOR`) with the ingress interface `xe4`.

```
OcNOS#configure terminal
OcNOS(config)#interface xe4
OcNOS(config-if)#flow-monitor FLOW-MONITOR
OcNOS(config-if)#
```

ip-flow-exporter

Use this command to configure an IP flow exporter profile to collect and export flow data from the network device. This data includes traffic statistics and network behavior information, which is then exported to an external collector or monitoring system for analysis and reporting purposes.

Command Syntax

```
ip-flow-exporter <WORD>
```

Parameters

`ip-flow-exporter <WORD>`	Specifies the name of the flow exporter profile, which must be unique within the device and can contain up to 32 alphanumeric characters, hyphens, and underscores.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command creates an IP flow exporter profile named `FLOW-EXPORTER`.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#
```

ip-flow-monitor

Use this command to create an IP flow monitor profile, defining parameters and settings for monitoring network flows.

Use `no` parameter of this command to remove an existing IP flow monitor profile from the configuration.

Command Syntax

```
ip-flow-monitor <WORD>
no ip-flow-monitor <WORD>
```

Parameters

`ip-flow-monitor <WORD>`	Specifies the name of the flow monitor profile, which must be unique within the device and can contain up to 32 alphanumeric characters, hyphens, and underscores.

Default

None

Command Mode

Configure mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command configures an IP flow monitor profile named `FLOW-MONITOR`.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-monitor FLOW-MONITOR
OcNOS(ip-flow-monitor)#
```

observation-domain-id

Use this command to specify the Observation Domain Identifier (ODID) for flow monitoring. The ODID uniquely identifies the flow monitoring profile. The ODID helps distinguish flow data from different monitoring domains when exported to a collector.

Command Syntax

```
observation-domain-id <0-4294967295>
```

Parameters

`observation-domain-id <0-4294967295>`	Sets the observation domain identifier value within the specified range.

Default

None

Command Mode

IP flow monitor mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command assigns the ODID 16 to the flow monitoring profile.

```
OcNOS#configure terminal
```

```
OcNOS(config)#ip-flow-monitor FLOW-MONITOR
OcNOS(ip-flow-monitor)#observation-domain-id 16
```

samples-per-message

Use this command to set the number of flow records to be included in each export message.

Use `no` parameter of this command to set the number of flow records to be included in each export message.

Command Syntax

```
samples-per-message <1-7>
```

Parameters

`samples-per-message <1-7>`	Specifies the maximum number of data records to be included in a single IPFIX message, which controls the granularity of the exported flow data.

Default

None

Command Mode

IP flow exporter mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command sets the maximum number of data records to be included in each IPFIX message generated by the specified IP flow exporter profile.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#samples-per-message 7
```

sampling-rate

Use this command to configure the rate at which packets are sampled for flow monitoring. Every packet sampled at this rate will be sent to the monitor for IPFIX processing.

Use `no` parameter of this command to remove the sampling rate configuration from the device.

Command Syntax

```
sampling-rate <1024-16777215>
```

```
no sampling-rate <1024-16777215>
```

Parameters

`sampling-rate <1024-16777215>`	Specifies the range of sampling rates that determine how frequently packets are selected for inclusion in the flow monitoring process.

Default

None

Command Mode

IP flow monitor mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The following command configures the sampling rate for the specified IP flow monitor profile to `1024` packets per second.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-monitor FLOW-MONITOR
OcNOS(ip-flow-monitor)#sampling-rate 1024
```

show ipfix

Use this command to display detailed information about the configured IPFIX exporters on the device.

Command Syntax

```
show ipfix
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The show command output provides detailed information about the exporters configured on the device, including exporter name, source and destination addresses, UDP ports, Template ID, and timeout value.

```
OcNOS#show ipfix
Exporters:
  Name:                  FLOW-EXPORTER
    Source:              192.0.2.88
    Destination:         192.0.2.89
    Source UDP:          53859
    Destination UDP:     4739
    Template ID:         500

    Data Template Timeout:600
```

Gain insights into IPFIX exporters with detailed field descriptions provided in the table.

Table 1: show ipfix fields

Field	Description
Exporter Name	Specifies the name of the IPFIX exporter.
Source	Indicates the source IPv4 address of the exporter.
Destination	Specifies the destination IPv4 address of the exporter.
Source UDP	Indicates the source UDP port used by the exporter.
Destination UDP	Specifies the destination UDP port used by the exporter.
Template ID	Specifies the template ID used by the exporter.
Data Template Timeout	Indicates the timeout interval, in seconds, for sending data templates to the collector.

show ipfix all

Use this command to display detailed information and comprehensive insights into the IPFIX configured templates and exporters on the device.

Command Syntax

```
show ipfix all
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The show command output displays detailed information about the IPFIX template records sampled on the device.

```
OcNOS#show ipfix all
Templates:
  Template ID:           500
    DIRECTON (61), Length:1
    IP_VERSION (60), Length:1
    IPV4_TOS (5), Length:1
    IPV4_PKT_LEN (1), Length:2
    IPV4_FRAG_OFFSET (88), Length:2
    PROTOCOL (4), Length:1
```

```
      IPV4_SIP (8), Length:4
      IPV4_DIP (12), Length:4
      L4_SRC_PORT (7), Length:2
      L4_DST_PORT (11), Length:2
      TCP_CONTROL (6), Length:2
      ICMP_TYPE (32), Length:2
      INGRESS_VRF (234), Length:4
      INGRESS_IF (10), Length:2
      EGRESS_VRF (235), Length:4
      EGRESS_IF (14), Length:2
      SYS_UPTIME (22), Length:4
Exporters:
   Name:                FLOW-EXPORTER
    Source:             192.0.2.88
    Destination:        192.0.2.89
    Source UDP:         53859
    Destination UDP:    4739
    Template ID:        500

    Data Template Timeout:600
```

Gain insights into IPFIX configurations and exporters with detailed field descriptions provided in the table.

Table 2: show ipfix all

Field	Description
Template ID	Indicates the unique identifier assigned to each IPFIX template.
DIRECTON	Indicates the direction of the network traffic flow, such as ingress or egress. It has a length of 1 byte.
IP_VERSION	Specifies the version of the Internet Protocol (IPv4) used. It has a length of 1 byte.
IPV4_TOS	Indicates the type of service (TOS) field in an IPv4 header. It has a length of 1 byte.
IPV4_PKT_LEN	Specifies the length of the IPv4 packet. It has a length of 2 bytes.
IPV4_FRAG_OFFSET	Indicates the fragment offset value in an IPv4 header. It has a length of 2 bytes.
PROTOCOL	Specifies the protocol used in the packet, such as TCP, UDP, and ICMP. It has a length of 1 byte.
IPV4_SIP	Indicates the source IPv4 address of the IPv4 packet. It has a length of 4 bytes.
IPV4_DIP	Specifies the destination IPv4 address of the IPv4 packet. It has a length of 4 bytes.
L4_SRC_PORT	Specifies the source port number in the transport layer header. It has a length of 2 bytes.
L4_DST_PORT	Specifies the destination port number in the transport layer header. It has a length of 2 bytes.

Table 2: show ipfix all

Field	Description
TCP_CONTROL	Indicates whether the packet is a TCP control packet (e.g., SYN, ACK, FIN). It has a length of 2 bytes.
ICMP_TYPE	Specifies the type of ICMP message, such as echo request or echo reply. It has a length of 2 bytes.
INGRESS_VRF	Indicates the identifier of the ingress Virtual Routing and Forwarding (VRF) instance. It has a length of 4 bytes.
INGRESS_IF	Specifies the ingress interface (IF) through which the packet enters the device. It has a length of 2 bytes.
EGRESS_VRF	Indicates the identifier of the egress VRF instance. It has a length of 4 bytes.
EGRESS_IF	Specifies the egress interface through which the packet exits the device. It has a length of 2 bytes.
SYS_UPTIME	Indicates the system uptime or the time the device has been operational since its last reboot. It has a length of 4 bytes.
Exporter Name	Specifies the name of the IPFIX exporter.
Source	Indicates the source IPv4 address of the exporter.
Destination	Specifies the destination IPv4 address of the exporter.
Source UDP	Indicates the source UDP port used by the exporter.
Destination UDP	Specifies the destination UDP port used by the exporter.
Template ID	Specifies the template ID used by the exporter.
Data Template Timeout	Indicates the timeout interval, in seconds, for sending data templates to the collector.

show running-config ipfix

Use this command to display a detailed view of the current IPFIX configurations, including flow exporters, flow monitors, and interface settings applied to the device.

Command Syntax

```
show running-config ipfix
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The show command output displays the current IPFIX configurations applied on the device.

```
OcNOS#show running-config ipfix
hardware-profile statistics cfm-lm enable
! ip-flow-exporter FLOW-EXPORTER
source xe5
collector destination 192.0.2.89
template-id 500
template-refresh-interval 600
samples-per-message 1

! ip-flow-monitor FLOW-MONITOR
flow-exporter FLOW-EXPORTER
sampling-rate 100
observation-domain-id 16

! interface xe4
ip address 198.51.100.4/24
flow-monitor FLOW-MONITOR

! interface xe5
ip address 192.0.2.88/24

!
```

source

Use this command to specify the IPv4 source address for the exporter, which is used in the IPFIX message IPv4 header. Enables the export of flow records to the collector.

Use `no` parameter of this command to remove the association of the specified interface as the source address in the IPFIX message IPv4 header.

Command Syntax

```
source IFNAME
```

```
no source IFNAME
```

Parameters

`source IFNAME`	Specifies the interface name from which the IPv4 source address will be derived.

Default

None

Command Mode

IP flow exporter mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The command instructs the system to obtain the IPv4 address associated with `interface xe5` and use it as the source address in the IPFIX message IPv4 header.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#source xe5
```

template-id

Use this command to set the ID for the IPFIX template, specifying the structure and format of the data records sent to the collector, serving as a template for the flow record format within the IPFIX message.

Use `no` parameter of this command to remove the specified template ID from the IPFIX configuration.

Command Syntax

```
template-id <256-65535>
```

```
no template-id <256-65535>
```

Parameters

`template-id <256-65535>`	Specifies the unique identifier for the template used in exporting flow records.

Default

None

Command Mode

IP flow exporter mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The command sets the template ID `500` for the IPFIX exporter profile.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#template-id 500
```

template-refresh-interval

Use this command to set the time interval for refreshing the IPFIX template, determining how often the template updates and sends to the IPFIX collector.

Use `no` parameter of this command to remove the configured time interval.

Command Syntax

```
template-refresh-interval <60-86400>
no template-refresh-interval <60-86400>
```

Parameters

`template-refresh-interval <60-86400>`	Specifies the time interval range, in seconds, for refreshing the IPFIX template. The default value is 600 seconds.

Default

None

Command Mode

IP flow exporter mode

Applicability

Introduced in OcNOS version 6.5.1.

Example

The command sets the template-refresh-interval parameter to `600` seconds for the specified IPFIX exporter profile.

```
OcNOS#configure terminal
OcNOS(config)#ip-flow-exporter FLOW-EXPORTER
OcNOS(ip-flow-exporter)#template-refresh-interval 600
```

Troubleshooting

- If the collector isn't operational or isn't running on the assigned port, follow these steps:
  - Check if the IPFIX collector service is active on the designated device.
  - Ensure the IPFIX collector process is running correctly.
  - Review the collector's configuration, including the specified port.
  - Investigate port conflicts or misconfigurations if the collector is running on the wrong port.
  - Monitor system logs for any error messages related to the IPFIX collector.
- To address TCAM resource availability issues on the exporter impacting IPFIX functionality, follow these steps:
  - Identify which features are currently enabled on the exporter.
  - Consider disabling or optimizing features to free up TCAM resources.
  - Monitor the TCAM resource usage periodically to ensure sufficient availability for IPFIX functionality.

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
IPFIX Exporter (Internet Protocol Flow Information Export)	OcNOS feature that facilitates real-time traffic analysis by sampling network traffic and exporting flow records containing detailed information about sampled traffic flows.
Flow Records	Detailed information about network traffic flows, including source and destination addresses, port numbers, protocol specifics, and timestamps.
Mirroring Profile	Profiles are used by various features, such as SFLOW, SNIFF, and Mirror to enable the mirroring of network traffic.
Jericho2	Broadcom DNX Jericho2, a network routing chipset.
Ingress and Egress Interfaces	The interface through which packets enter and exit the network device.
Security Monitoring	Monitoring network traffic for security threats and compliance with regulations.
ASIC	Application Specific Integrated Circuit
SFLOW	Sampling Flow
SVI	Switched Virtual Interface
LAG	Link Aggregation Group
ICMP	Internet Control Message Protocol
UDP	User Datagram Protocol
VRF	Virtual Routing and Forwarding
ISP	Internet Service Provider
Ternary Content Addressable Memory (TCAM)	TCAM facilitates rapid table lookups based on specific search criteria in networking devices like routers and switches. It performs searches for exact matches, wildcard matches, and ranges swiftly, making it highly efficient for matching patterns against large datasets.

Monitor and Reporting Server Command Reference

CHAPTER 1 Software Monitoring and Reporting

This document describes software watchdog and reporting related commands.

- clear cores
- copy core
- copy techsupport
- feature software-watchdog
- remove file (techsupport)
- show bootup-parameters
- show cores
- show running-config watchdog
- show software-watchdog status
- show system log
- show system login
- show system reboot-history
- show system resources
- show system uptime
- show techsupport
- show techsupport status
- software-watchdog
- software-watchdog keep-alive-time

© 2025 IP Infusion Inc. Proprietary

clear cores

Use this clear command to delete the core files present in /var/log/crash/cores

Syntax

```
clear cores (|WORD)
```

Parameters

WORD	Core file name

Default

NA

Command Mode

Executive Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show cores
Core location :/var/log/crash/cores
Core-File-Name
--------------
core_hostpd.9581_20190324_222313_signal_11.gz
#clear cores core_hostpd.9581_20190324_222313_signal_11.gz
#show cores
Core location :/var/log/crash/cores
Core-File-Name
--------------
#
```

copy core

Use this command to copy the core file to another file.

The core filename is in the form: core_PROCESSNAME.PROCID_YYYMMDD_HHMMSS_signal_SIGNUM.gz

Command Syntax

```
copy core FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf
  (NAME|management)|)
```

Parameters

`core`	Copy Crash core files to remote location. Core file location: `/var/log/crash/cores/`
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

NA

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
# copy core core_hostpd.9581_20190324_222313_signal_11.gz scp scp://10.12.16.17/home/
core core_hostpd.9581_20190324_222313_signal_11.gz vrf management
Enter Username:root
Enter Password:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  681k    0     0    0  681k      0  3588k --:--:-- --:--:-- --:--:-- 3588k
100  681k    0     0    0  681k      0  3588k --:--:-- --:--:-- --:--:-- 3588k
Copy Success
```

copy techsupport

Use this command to copy the contents of a compressed techsupport file (`tar.gz`) to another file.

The default filename is in the form: `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

Command Syntax

```
copy (log|techsupport) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL)
  (vrf (NAME|management)|)
```

Parameters

`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Tech support file storage; on Linux this refers to `/var/log/`
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

NA

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy techsupport tech_support_23_Feb_2019_18_27_00.tar.gz scp scp://10.12.16.17/home/
tech_support_23_Feb_2019_18_27_00.tar.gz vrf management

Enter Username:root
Enter Password:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
Copy Success
#
```

feature software-watchdog

Use this command to enable software watchdog functionality for all OcNOS modules. This feature is enabled by default.

Use the `no` form of this command to disable software watchdog functionality.

Command Syntax

```
feature software-watchdog
no feature software-watchdog
```

Parameter

None

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
    #configure terminal
#(config)feature software-watchdog
```

remove file (techsupport)

Use this command to remove techsupport files from "/var/log" directory.

Command Syntax

```
remove file (techsupport) (all|FILENAME|)
```

Parameter

techsupport	Tech support option for protocol(s).
all	Remove all files.
FILENAME	Name of the file to be deleted.

Default

N/A.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.4.

Examples

```
OcNOS#remove ?
      file  file

OcNOS#remove file ?
      techsupport  Tech Support Option For Protocol(s)

OcNOS#remove file techsupport ?
       FILENAME   Name of the file to be deleted
       all                Remove all files

 OcNOS#remove file techsupport /var/log/
OcNOS_tech_support_all_14_Feb_2019_15_39_34.tar.gz

 OcNOS#remove file techsupport all
```

show bootup-parameters

Use this command to show OcNOS kernel bootup parameters.

Command Syntax

```
show bootup-parameters
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show bootup-parameters
BOOT_IMAGE=/boot/vmlinuz-3.16.7-g490411a-ec-as7712-32x root=UUID=317567fc-
b69e-4

5d9-ab4e-fa1d9e57b

703 console=ttyS1,115200n8 ro
```

show cores

Use this command to list core files in the system or to display information about a given core file.

Note: When cmlsh logged in via non-root user crashes, core files will not get generated. User can further debug the issue based on CLI-history and logs from /var/log/messages.

Command Syntax

```
show cores (|WORD details)
```

Parameter

WORD	Core file name

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#sh cores
Core location :/var/log/crash/cores
Core-File-Name
--------------
core_nsm.683_20191110_103611_signal_5.gz
core_nsm.712_20191107_171803_signal_11.gz
core_nsm.684_20191112_054937_signal_5.gz
core_yangcli.5695_20191107_171715_signal_11.gz
#
```

Table 1-1 explains the output fields.

Table 1-1: show cores fields

Entry	Description
Core-File-Name	Core dump file name.

show running-config watchdog

Use this command to display watchdog configurations.

Command Syntax

```
show running-config watchdog
```

Parameters

None

Command Mode

Privileged EXEC

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#sh running-config watchdog
software-watchdog keep-alive-time 300
```

show software-watchdog status

Use this command to display the software watchdog status for each OcNOS module.

Command Syntax

```
show software-watchdog status
show software-watchdog status detail
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3 and updated in OcNOS version 1.3.4.

Examples

```
#show software-watchdog status
Software Watchdog timeout in seconds : 60
Process name         Watchdog status
============         ===============
nsm                  Enabled
ripd                 Enabled
ripngd               Enabled
ospfd                Enabled
ospf6d               Enabled
isisd                Enabled
hostpd               Enabled
ldpd                 Enabled
rsvpd                Enabled
mribd                Enabled
pimd                 Enabled
authd                Enabled
mstpd                Enabled
imi                  Enabled
onmd                 Enabled
HSL                  Enabled
oamd                 Enabled
vlogd                Enabled
vrrpd                Enabled
ndd                  Enabled
ribd                 Enabled
bgpd                 Enabled
l2mribd              Enabled
lagd                 Enabled
sflow                Enabled
```

```
udld                 Enabled
cmld                 Enabled
cmmd                 Enabled
pcepd                Enabled

#show software-watchdog status detail
Software Watchdog timeout in seconds : 60

Process Watchdog   Process   Disconnect Connect         Last Restart
 Name    Status     Status     Count     Count             Reason
======= ======== =========== ========== ======= ================================
nsm     Enabled  Running     0          1       Fresh bootup
ripd    Enabled  Running     0          1       Fresh bootup
ripngd  Enabled  Running     0          1       Fresh bootup
ospfd   Enabled  Running     0          1       Fresh bootup
ospf6d  Enabled  Running     0          1       Fresh bootup
isisd   Enabled  Running     0          1       Fresh bootup
hostpd  Enabled  Running     3          4       Segmentation fault
ldpd    Enabled  Running     0          1       Fresh bootup
rsvpd   Enabled  Running     0          1       Fresh bootup
mribd   Enabled  Running     0          1       Fresh bootup
pimd    Enabled  Running     0          1       Fresh bootup
authd   Enabled  Running     0          1       Fresh bootup
mstpd   Enabled  Running     0          1       Fresh bootup
imi     Enabled  Running     0          1       Fresh bootup
onmd    Enabled  Running     0          1       Fresh bootup
HSL     Enabled  Running     0          1       Fresh bootup
oamd    Enabled  Running     0          1       Fresh bootup
vlogd   Enabled  Running     0          1       Fresh bootup
vrrpd   Enabled  Running     0          1       Fresh bootup
ndd     Enabled  Running     0          1       Fresh bootup
ribd    Enabled  Running     0          1       Fresh bootup
bgpd    Enabled  Running     0          1       Fresh bootup
l2mribd Enabled  Running     0          1       Fresh bootup
lagd    Enabled  Running     0          1       Fresh bootup
sflow   Enabled  Running     0          1       Fresh bootup
udld    Enabled  Running     0          1       Fresh bootup
cmld    Enabled  Running     0          1       Fresh bootup
cmmd    Enabled  Running     0          1       Fresh bootup
pcepd   Enabled  Running     0          1       Fresh bootup
#
```

Table 1-2 explains the output fields.

Table 1-2: show software-watchdog status output fields

Field	Description
Process Name	The name of a protocol module.
Watchdog Status	Status of a protocol module (Enabled or Disabled).

Table 1-2: show software-watchdog status output fields (Continued)

Field	Description
Process Status	Status of the protocol module Running/Not-running).
Disconnect Count	Number of times the protocol module disconnected from monitoring module.
Connect Count	Number of times the protocol module connected to monitoring module.
Last Restart Reason	Reason why a module disconnected from monitoring module.

show system log

Use this command to display the system's log file.

Command Syntax

```
show system log
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system log
Syslog              : enabled      File Name   : /var/log/messages
Oct 18 18:10:18 localhost rsyslogd: [origin software="rsyslogd"
swVersion="8.4.2
" x-pid="541" x-info="http://www.rsyslog.com"] start
Oct 18 18:10:18 localhost systemd[1]: Started Apply Kernel Variables.
Oct 18 18:10:18 localhost systemd[1]: Started Create Static Device Nodes in /
dev
.
Oct 18 18:10:18 localhost systemd[1]: Starting udev Kernel Device Manager...
Oct 18 18:10:18 localhost systemd[1]: Started udev Kernel Device Manager.
Oct 18 18:10:18 localhost systemd[1]: Starting Copy rules generated while the
ro
ot was ro...
Oct 18 18:10:18 localhost systemd[1]: Starting LSB: Set preliminary keymap...
Oct 18 18:10:18 localhost systemd[1]: Started Copy rules generated while the
roo
t was ro.
Oct 18 18:10:18 localhost nfs-common[163]: Starting NFS common utilities:.
Oct 18 18:10:18 localhost systemd[1]: Found device /dev/ttyS0.
Oct 18 18:10:18 localhost systemd[1]: Found device 16GB_SATA_Flash_Drive
OcNOS-CONFIG.
Oct 18 18:10:18 localhost systemd[1]: Starting File System Check on /dev/disk/
by
-label/OcNOS-CONFIG...
Oct 18 18:10:18 localhost systemd[1]: Starting system-ifup.slice.
Oct 18 18:10:18 localhost systemd-fsck[217]: OcNOS-CONFIG: clean, 85/128016
file
s, 27057/512000 blocks
Oct 18 18:10:18 localhost systemd[1]: Created slice system-ifup.slice.
--More--
```

Table 1-3 explains the output fields.

Table 1-3: show system log fields

Entry	Description
Syslog	Status of the protocol (enabled or disabled).
File Name	Specifies the name of the system log files that you configured.

show system login

Use this command to display the system's login history.

Command Syntax

```
show system login
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system login
eric      ttyS0                        Wed Oct 19 18:31   still logged in
takayuki  ttyS0                        Wed Oct 19 18:14 - 18:25  (00:10)
girish    ttyS0                        Wed Oct 19 16:46 - 17:01  (00:14)

wtmp begins Wed Oct 19 16:46:18 2016
```

show system reboot-history

Use this command to show the device reboot history.

Command Syntax

```
show system reboot-history
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3

Examples

```
#show system reboot-history
DATE-TIME                 REBOOT-REASON
------------------------  -------------------------
Thu Oct 07 12:46:56 2021  Sys-update from NOS shell
Wed Oct 13 09:35:06 2021  Reload from NOS shell
Sat Feb 16 23:19:38 2019  Reload from NOS shell
```

show system resources

Use this command to display the system's current resources.

Command Syntax

```
show system resources (iteration <1-5>|)
```

Parameters

<1-5>	The number of times to check the resources before they are displayed.

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system resources
load average: 0.12, 0.22, 0.20
Tasks: 173 total,   1 running, 172 sleeping,   0 stopped,   0 zombie
%Cpu(s):  3.1 us,  1.6 sy,  0.0 ni, 95.3 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
st
MiB Mem :  15930.2 total,  14277.8 free,   1003.0 used,    649.4 buff/cache


        0 used,        0 free.   252416 cached Mem
```

Table 1-4 explains the output fields.

Table 1-4: show system resource fields

Entry	Description
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.
Tasks	Number of processes in the system and how many processes are actually running when the command is issued.
CPU	Displays the CPU utilization information for processes on the device.

Table 1-4: show system resource fields

Entry	Description
KiB Mem	The memory field (Mem) shows the virtual memory used by processes. The value in the memory field is in KB and MB, and is broken down as follows: Total: The total amount of available virtual memory, in kibibytes (KiBs). Used:The total amount of used virtual memory, in kibibytes (KiBs). Free: The total amount of free virtual memory, in kibibytes (KiBs) Buffers: The size of the memory buffer used to hold data recently called from disk.
KiB Swap	The Swap field shows the total swap space available and how much is unused and is broken down as follows: Total: The total amount of available swap memory, in kibibytes (KiBs). Used: The total amount of used swap memory, in kibibytes (KiBs). Free: The total amount of free swap memory, in kibibytes (KiBs). Cache Memory: Memory that is not associated with any program and does not need to be swapped before being reused.

show system uptime

Use this command to display how lone the system has been up and running.

Command Syntax

```
show system uptime
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
DELL-6K3#show system uptime
 19:10:22 up 1 day,  1:01,  1 user,  load average: 0.08, 0.05, 0.05
```

Table 1-5 explains the output fields.

Table 1-5: show system uptime fields

Entry	Description
Time and up	Current time, in the local time zone, and how long the router or switch has been operational.
Users	Number of users logged in to the router or switch.
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.

show techsupport

Use this command to collect system data for technical support and save the support information in a compressed tar (.gz) file.

- By default, the `show techsupport` uses the file path `/var/log/` and names the file as `OcNOS_tech_support_protocolname_DD_MMM_YYYY_HH_MM_SS.tar.gz`.
- If this filename already exists, a date and timestamp are appended to differentiate it from previous files.
- When a `show techsupport` command is already running, any subsequent `show techsupport` commands issued are ignored until the current command completes.
- If a `show techsupport` command is in progress and a `show running-config` command is issued, the displayed information is derived from the ongoing `show techsupport` command.

Command Syntax

```
show techsupport
  ({all|authd|bgp|cmmd|hostpd|hsl|imi|isis|l2mribd|lag|ldp|mribd|mstp|nd|nsm|oam|o
  nm|ospf|ospf6|pcep|pim|ptp|rib|rip|ripng|rsvp|sflow|synce|vrrp|netconf|gnmi})
```

Parameters

`all`	Specifies the collection of all types of information.
`authd`	Specifies the collection of authentication-related information.
`bgp`	Specifies the collection of BGP-related information.
`cmmd`	Specifies the collection of chassis management related information.
`hostpd`	Specifies the collection of system management related information.
`hsl`	Specifies the collection of HSL-related information.
`imi`	Specifies the collection of IMM-related information.
`isis`	Specifies the collection of ISIS-related information.
`l2mribd`	Specifies the collection of Layer 2 Multicast RIB-related information.
`lag`	Specifies the collection of LAG or LACP-related information.
`ldp`	Specifies the collection of LDP-related information.
`mribd`	Specifies the collection of Multicast RIB-related information.
`mstp`	Specifies the collection of MSTP-related information.
`nd`	Specifies the collection of Neighbor Discovery related information.
`nsm`	Specifies the collection of NSM-related information.
`oam`	Specifies the collection of BFD-related information.
`onm`	Specifies the collection of ONM or LLDP-related information.
`ospf`	Specifies the collection of OSPF-related information.
`ospf6`	Specifies the collection of OSPF6-related information.
`pcep`	Specifies the collection of PCEP-related information.
`pim`	Specifies the collection of PIM-related information.
`ptp`	Specifies the collection of PTP-related information.
`rib`	Specifies the collection of RIB-related information.

`rip`	Specifies the collection of RIP-related information.
`ripng`	Specifies the collection of RIPNG-related information.
`rsvp`	Specifies the collection of RSVP-related information.
`sflow`	Specifies the collection of sFlow-related information.
`synce`	Specifies the collection of SYNCE-related information.
`vrrp`	Specifies the collection of VRRP-related information.
`netconf`	Specifies the collection of NetConf and Callhome related information.
`gnmi`	Specifies the collection of gNMI-related information.

Default

None

Command Mode

Privileged EXEC mode

Applicability

Introduced before OcNOS version 1.3. Introduced the `netconf` and `gnmi` parameters in the OcNOS version 6.5.1.

Example

The following command demonstrates how to use `show techsupport` to collect various types of system information.

```
#show techsupport all
#show techsupport bgp
#show techsupport bgp isis
#show techsupport gnmi
#show techsupport netconf
```

show techsupport status

Use this cli to view the status of `show techsupport` CLI to generate techsupport archive.

Command Syntax

```
show techsupport status
```

Parameters

None

Command Mode

Privileged EXEC

Applicability

This command was introduced before OcNOS version 4.2.

Example

```
#show techsupport status
 Tech Support Command Execution Is Complete
 ##Generated Tech Support File-list
 /var/log/OcNOS_tech_support_18_Jun_2021_10_01_38.tar.gz
 Tar File is generated at /var/log and file name begins with
'OcNOS_tech_support'
```

software-watchdog

Use this command to enable the software watchdog feature for an OcNOS module.

Use the `no` form of this command to disable the software watchdog feature.

Command Syntax

```
software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd|
ldpd|rsvpd|udld|hsl|cmmd|pcepd|ptpd|synced)

no software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd|
ldpd|rsvpd|udld|hsl|cmmd|pcepd|ptpd|synced)
```

Parameters

`authd`	Software watchdog for AUTH module
`bgpd`	Software watchdog for BGP module
`cmld`	Software watchdog for CML module
`cmmd`	Software watchdog for CMM module
`hostpd`	Software watchdog for HOSTP module
`hsl`	Software watchdog for HSL module
`imi`	Software watchdog for IMI module
`isisd`	Software watchdog for ISIS module
`l2mribd`	Software watchdog for L2MRIB module
`lagd`	Software watchdog for LAG module
`ldpd`	Software watchdog for LDP module
`mribd`	Software watchdog for MRIB module
`mstpd`	Software watchdog for MSTP module
`ndd`	Software watchdog for NDD module
`nsm`	Software watchdog for NSM module
`oamd`	Software watchdog for OAM module
`onmd`	Software watchdog for ONM module
`ospf6d`	Software watchdog for OSPF6 module
`ospfd`	Software watchdog for OSPF module
`pcepd`	Software watchdog for PCEP module
`pimd`	Software watchdog for PIM module
`ptpd`	Software watchdog for PTP module

`ribd`	Software watchdog for RIB module
`ripd`	Software watchdog for RIP module
`ripngd`	Software watchdog for RIPNG module
`rsvpd`	Software watchdog for RSVP module
`sflow`	Software watchdog for SFLOW module
`synced`	Software watchdog for SYNCE module
`udld`	Software watchdog for UDLD module
`vlogd`	Software watchdog for VLOG module
`vrrpd`	Software watchdog for VRRP module

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)no software-watchdog imi
#(config)software-watchdog nsm
```

software-watchdog keep-alive-time

Use this command to set the software watchdog keep-alive time interval in seconds. The default keep-alive time interval is 60 seconds.

Use the `no` form of this command to set default keep-alive time interval.

Command Syntax

```
software-watchdog keep-alive-time <30-1800>
no software-watchdog keep-alive-time
```

Parameters

`<30-1800>`	Keep-alive time interval in seconds

Default

By default, software watchdog is enabled and the keep-alive time interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
#(config)software-watchdog keep-alive-time 100
```

CHAPTER 2 sFlow Commands

This chapter describes the Sampled Flow (sFlow) commands.

- clear sflow statistics
- debug sflow
- feature sflow
- sflow agent-ip
- sflow collector
- sflow enable
- sflow poll-interval
- sflow rate-limit
- sflow sampling-rate
- show sflow
- show sflow interface
- show sflow statistics

clear sflow statistics

Use this command to clear sFlow sampling-related counters such as the number of packets sampled and the number of counters sampled.

Command Syntax

```
clear sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear sflow statistics
```

debug sflow

Use this command to display sFlow debugging messages.

Command Syntax

```
debug sflow (all|agent|sampling|polling|)
```

Parameters

`all`	Debug all (agent,sampling,polling)
`agent`	Debug sFlow agent
`sampling`	Debug sFlow sampling
`polling`	Debug sFlow polling

Default

By default, debug command is disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#debug sflow all
#debug sflow agent

#configure terminal
(config)#debug sflow agent
```

feature sflow

Use this command to enable the sFlow feature.

Use the no form to disable the sFlow feature.

Command Syntax

```
feature sflow
no feature sflow
```

Parameters

None

Default

By default, sFlow feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#feature sflow
```

sflow agent-ip

Use this command to set the agent IP address for receivers.

Use the `no` form of this or remove an agent IP address.

Command Syntax

```
sflow agent-ip A.B.C.D
no sflow agent-ip
```

Parameter

`A.B.C.D`	IPv4 address

Default

The default IP address is zero (0).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#sflow agent-ip 10.0.0.12
```

sflow collector

Use this command to configure the collector details such as the collector IPv4 address, port number, receiver time-out and datagram size.

Use the `no` form of this command to disable the sFlow collector.

Command Syntax

```
sflow (collector-id <1-5>|) collector A.B.C.D port <1024-65535> receiver-time-out
  <0-2147483647> max-datagram-size <200-9000> (vrf WORD|)
no sflow collector (A.B.C.D port <1024-65535>|)
```

Parameter

collector-id <1-5>	(Optional) Specifies the name of the Collector instance identifier. If the collector-id is not specified, the ID will be 1.
collector A.B.C.D	Collector IPv4 address. This address must be reachable via the management VRF.<1024-65535>
port <1024-65535>	Collector UDP Port number. The default port number is 6343.
receiver-time-out <0-2147483647>	Receiver time out value in seconds. Zero means no timeout. Upon timeout, value collector information is removed, stopping any ongoing sampling.
max-datagram-size <200-9000>	Maximum datagram size in bytes that can be sent to the collector
vrf WORD	(Optional) Specifies the VRF on which the collector is reachable. In case not specified, the `management` VRF will be used. To use the `default` VRF, the vrf `default` must be specified explicitly.

Default

Disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. Introduced the **`collector-id`** and **`vrf`** parameters in the OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#sflow collector 2.2.2.2 port 1111 receiver time-out 30 max-datagram-
size 500

(config)#no sflow collector

#configure terminal
(config)#sflow collector 4.4.4.5 port 1024 receiver-time-out 10 max-datagram-
size 200 vrf default
(config)#no sflow collector
```

sflow enable

Use this command to enable or disable sampling on an interface after giving the sflow sampling-rate command on the same interface.

Command Syntax

```
sflow enable
no sflow enable
```

Default

By default, sFlow sampling is disabled.

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-datagram-size 200
(config-if)#sflow enable
(config-if)#no sflow enable
```

sflow poll-interval

Use this command to configure the sFlow counter polling interval. Any change in the polling interval restarts ongoing polling of existing data source interfaces, if any.

Use the `no` form of this command to disable the sFlow counter polling interval.

Command Syntax

```
sflow poll-interval <5-60>
no sflow poll-interval
```

Parameters

`<5-60>`	Interface counter. Polling interval in seconds

Default

By default, sFlow counter polling interval is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow poll-interval 25
(config-if)#no sflow poll-interval
```

sflow rate-limit

Use this command to set the CPU rate limit in packets per second.

Use the `no` form of this command to set the CPU rate limit to its default (0).

Command Syntax

```
sflow rate-limit <2000-100000>
no sflow rate-limit
```

Parameters

`<2000-100000>`	Rate limit in packets per second

Default

The default rate limit is zero (0).

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Examples

```
#configure terminal
(config)#sflow rate-limit 5000
```

sflow sampling-rate

Use this command to set the sampling rate on an interface. Any change in the sampling rate restarts the ongoing sampling of existing data-source interfaces, if any.

Use the `no` form of this command to disable the sFlow sampling rate.

Note: Packets to CPU is rate limited. In case of unknown unicast, rate limit is applied to such packets as well as sampled data packets.

Command Syntax

```
sflow sampling-rate <1024-16777215> direction (ingress | egress) max-header-size
  <128-256>
no sflow sampling-rate direction (ingress | egress)
```

Parameters

`<1024-16777215>`	Sampling rate
`direction`	The direction of sampling an interface:
`ingress`	Ingress traffic
`egress`	Egress traffic
`<128-256>`	Maximum header size in bytes

Default

By default, sFlow sampling rate is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200
(config-if)#no sflow sampling-rate direction ingress
```

show sflow

Use this command to display sFlow agent configuration along with statistics for all interfaces.

Command Syntax

```
show sflow (brief | detail)
```

Parameters

`brief`	Display configuration parameters on interfaces along with sampling rate and poll interval.
`detail`	Same as `brief` along with configured and default attributes and values of sFlow agent, sFlow collector, and sampling information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show sflow
sFlow Feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.12.16.38
Collector IP: 2.2.2.2      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-Polling         Maximum Header
                 Rate                      Count               Interval       Count        Size(bytes)
           Ingress      Egress       Ingress      Egress       (sec)                     Ingress     Egress
---------  -----------------------   -----------------------  -----------------------   --------------------
xe1            1024            0           0            0           6            3     128            0

#
#show sflow brief
sFlow Feature: Enabled
Collector IP: 2.2.2.2      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Configuration:
Interface   Status               Sample Rate               Counter-Polling
            Ingress    Egress    Ingress      Egress       Interval(sec)
---------   ------------------   ------------------------  ---------------
xe1       Enabled    Disabled         1024            0      6
```

Table 2-6: Show sflow output

Entry	Description
sFlow feature	Shows whether sFlow is enabled or disabled.
sFlow Version	Displays the sFlow version. Version 5 is the current global standard.
sFlow Global Information	Global Information consists of the Agent IP address, Collector IP, Port number, Maximum Datagram Size, and the Receiver timeout.
Agent IP	IPv4 address of this switch/router.
Collector IP	IPv4 address of the sFlow collector server.
Port	Port number on the sFlow collector server. Standard is port 6343.
Maximum Datagram Size	The maximum size of the datagrams sent by the agent
Receiver timeout	The number of seconds between each sampling – zero means sample continuously.
sFlow Port Interface	The interface of this switch/router on which sFlow is running (e.g. xe1/1).
Packet-Sampling Rate	the number of packets received or transmitted before a sample is taken.
Packet-Sampling Count	The number of sample packets that have been sampled on both the ingress and egress of the interface.
Counter-Polling	Shows the amount of time between polling samples and the count of the total number of polling samples taken.
Maximum Header Size	The maximum header size for both the ingress and egress of the interface.

© 2025 IP Infusion Inc. Proprietary

show sflow interface

Use this command to display the sFlow configuration for the input interface.

Command Syntax

```
show sflow interface IFNAME
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow interface xe1
sFlow feature: Enabled
sFlow Version: 5
sFlow Global Information :
Agent     IP: 10.10.26.104
Collector IP: 2.2.2.2      Port:  6343
Maximum Datagram Size(bytes): 200
Receiver timeout(sec)        : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Counter-Polling           Maximum Header
           Rate         Count        Interval(sec) Count       Size(bytes)
---------  -----------------------   ------------------------  --------------
xe1              1024            0           6           41      128
```

show sflow statistics

Use this command to display sFlow counter information.

Command Syntax

```
show sflow statistics (interface IFNAME|)
```

Parameters

IFNAME	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow statistics

sFlow Port Statistics:
Interface  Packet-Sampling   Counter-Polling
                Count              Count
---------  ---------------   ---------------
xe1                      0                19
```

CHAPTER 3 Control Plane Policing Commands

This chapter is a reference for the Control Plane Policing (CoPP) commands.

- clear interface cpu counters
- cpu-queue
- show interface cpu counters queue-stats
- show cpu-queue details

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax

```
clear interface cpu counters
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OcNOS#clear interface cpu counters
```

cpu-queue

Use this command to set the protocol queue shaper and enable/disable queue monitoring for drop.

Note: Configuring the queue rate for `guest` is not available for Qumran2 devices. Configuring the queue rate for `PTP` is not allowed for Qumran1 and Qumran2 series platforms.

Command Syntax

```
cpu-queue (cpu.q0|cpu.q1|cpu.q2|cpu.q3|cpu.q4|cpu.q5|cpu.q6|cpu.q7|
  arp|bfd|bgp|bpdu|cfm|dsp|evpn|guest|icmp|icmp-redirect|igmp|isis|link-
  local|mgmt-route-leak|nhop|oamp|ospf|pim|reserved-mc|rsvp-ldp|sflow|vrrp-rip-
  dhcp)(monitor|no-monitor|rate <0-100000>)
no cpu-queue (cpu.q0|cpu.q1|cpu.q2|cpu.q3|cpu.q4|cpu.q5|cpu.q6|cpu.q7|
  arp|bfd|bgp|bpdu|cfm|dsp|evpn|guest|icmp|icmp-redirect|igmp|isis|link-
  local|mgmt-route-leak|nhop|oamp|ospf|pim|reserved-mc|rsvp-ldp|sflow|vrrp-rip-
  dhcp)(monitor|no-monitor|rate <0-100000>)
```

Parameters

`cpu.q0`	Represents the parameters for CPU queue 0.
`cpu.q1`	Represents the parameters for CPU queue 1.
`cpu.q2`	Represents the parameters for CPU queue 2
`cpu.q3`	Represents the parameters for CPU queue 3
`cpu.q4`	Represents the parameters for CPU queue 4
`cpu.q5`	Represents the parameters for CPU queue 5
`cpu.q6`	Represents the parameters for CPU queue 6
`cpu.q7`	Represents the parameters for CPU queue 7
`arp`	Defines the parameters for the ARP queue.
`bfd`	Defines the parameters for the BFD queue.
`bgp`	Defines the parameters for the BGP queue.
`bpdu`	Defines the parameters for the BPDU queue.
`cfm`	Defines the parameters for the CFM error queue.

`dsp`	Defines the parameters for the DSP queue.
`evpn`	Defines the parameters for the EVPN queue.
`guest`	Defines the parameters for the Guest queue.
`icmp`	Defines the parameters for the ICMP queue.
`icmp-redirect`	Defines the parameters for the ICMP-redirect queue.
`igmp`	Defines the parameters for the IGMP queue.
`isis`	Defines the parameters for the ISIS queue.
`link-local`	Defines the parameters for the Link-local queue.
`mgmt-route-leak`	Defines the parameters for the Management route leak queue.
`nhop`	Defines the parameters for the Next hop queue.
`oamp`	Defines the parameters for the OAMP queue.
`ospf`	Defines the parameters for the OSPF queue.
`pim`	Defines the parameters for the PIM queue.
`reserved-mc`	Defines the parameters for the Reserved-mc queue.
`rsvp-ldp`	Defines the parameters for the RSVP/ LDP queue.
`sflow`	Defines the parameters for the Sflow queue.
`vrrp-rip-dhcp`	Defines the parameters for the VRRP/ RIP/DHCP queue.
`monitor`	Monitor CPU queue usage. If the rate is exceeded, packets start dropping in the CPU queue. These drops are reported to the user through notifications.
`no-monitor`	Disables monitoring of CPU queue usage.
`rate`	Sets the CPU queue rate within the range of 0 to 100,000.

Default

CPU queues are set with the default values as shown in Table 5-15 and Table 5-16.

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 2.4.

Example

Use the following command to configure rate/monitor/no-monitor for protocol queues:

```
OcNOS#configure terminal
OcNOS(config)#cpu-queue cpu-q0 rate 400
```

Use the following command to verify the rate received on each protocol queue:

```
OcNOS#show int cpu counters rate kbps

+-------------------+--------------+-------------+--------------+-------------+
|    CPU Queue(%)   |    Rx kbps   |    Rx pps   |    Tx kbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 CPU0.q0  (100%)            -              -          470.63         58
 bpdu     (  0%)            -              -          0.54           1
```

Use the following command to verify the maximum, configured, and default configuration values:

```
OcNOS#show cpu-queue details

* - Can not configure the parameter
Cpu queue                    Rate In Kbps                          Monitor Status

Name           Configured     Default    Max Rate Allowed   Configured    Default
=======       ============   =========  ==================  ===========   ==========
cpu.q0               400      900         20000               -             * no-monitor
cpu.q1               -        900         20000               -             * no-monitor
cpu.q2               -        900         20000               -             * no-monitor
cpu.q3               -        900         20000               -             * no-monitor
cpu.q4               -        900         20000               -             * no-monitor
cpu.q5               -        900         20000               -             * no-monitor
cpu.q6               -        10000       20000               -             * no-monitor
cpu.q7               -        900         20000               -             * no-monitor
igmp                 -        1000        1000                -             * no-monitor
is-is                -        8000        8000                -               no-monitor
reservedmc           -        8000        8000                -               no-monitor
link-local           -        1000        1000                -               no-monitor

ospf                 -        8000        8000                -               no-monitor
bgp                  -        8000        8000                -               no-monitor
rsvp/ldp             -        1500        1500                -               no-monitor
```

```
vrrp/rip/dhcp        -       2000       2000               -               no-monitor
pim                  -       8000       8000               -             * no-monitor
icmp                 -       1000       1000               -               no-monitor
arp                  -       1000       1000               -               no-monitor
bpdu                 -       8000       8000               -               no-monitor
oamp                 -       1000       1000               -               no-monitor
sflow                -       16384      16384              -               no-monitor
dsp                  -       1500       1500               -               no-monitor
evpn                 -       468        468                -               no-monitor
nhop                 -       500        500                -               no-monitor
mgmt-route-leak      -       8000       10000              -               no-monitor
icmp-redirect        -       400        400                -               no-monitor
guest                -       8000       8000               -             * no-monitor
cfm                  -       1000       1000               -               no-monitor
bfd                  -       4000       4000               -               no-monitor
ptp                  -       4000       4000               -               no-monitor
```

Use the following command to remove the configuration:

```
OcNOS(config)#no cpu-queue cpu.q0
OcNOS(config)#exit

OcNOS#show cpu-queue details

* - Can not configure the parameter
Cpu queue                    Rate In Kbps                          Monitor Status

Name            Configured     Default    Max Rate Allowed   Configured    Default
=======        ============   =========  ==================  ============   ==========
cpu.q0               -       900        20000               -             * no-monitor
cpu.q1               -       900        20000               -             * no-monitor
cpu.q2               -       900        20000               -             * no-monitor
cpu.q3               -       900        20000               -             * no-monitor
cpu.q4               -       900        20000               -             * no-monitor
cpu.q5               -       900        20000               -             * no-monitor
cpu.q6               -       10000      20000               -             * no-monitor
cpu.q7               -       900        20000               -             * no-monitor
igmp                 -       1000       1000                -             * no-monitor
is-is                -       8000       8000                -               no-monitor
reservedmc           -       8000       8000                -               no-monitor
link-local           -       1000       1000                -               no-monitor

ospf                 -       8000       8000                -               no-monitor
bgp                  -       8000       8000                -               no-monitor
rsvp/ldp             -       1500       1500                -               no-monitor
vrrp/rip/dhcp        -       2000       2000                -               no-monitor
pim                  -       8000       8000                -             * no-monitor
icmp                 -       1000       1000                -               no-monitor
arp                  -       1000       1000                -               no-monitor
bpdu                 -       8000       8000                -               no-monitor
```

oamp	-	1000	1000	-	no-monitor
sflow	-	16384	16384	-	no-monitor
dsp	-	1500	1500	-	no-monitor
evpn	-	468	468	-	no-monitor
nhop	-	500	500	-	no-monitor
mgmt-route-leak	-	8000	10000	-	no-monitor
icmp-redirect	-	400	400	-	no-monitor
guest	-	8000	8000	-	* no-monitor
cfm	-	1000	1000	-	no-monitor
bfd	-	4000	4000	-	no-monitor
ptp	-	4000	4000	-	no-monitor

show interface cpu counters queue-stats

Use this command to display the counters of packets destined to the CPU.

For details about this command, see show interface counters queue-stats.

Example

```
OcNOS#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+----------------+------------------+-----------------+--------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts    |     Tx bytes     |  Dropped pkts   |   Dropped bytes    |
+--------------------+--------+----------------+------------------+-----------------+--------------------+
igmp            (E)    2097152       151              16258              0                 0
reserved mc     (E)    2097152      62826            6324464             0                 0
ospf            (E)    1048576      3184              308548             0                 0
bgp             (E)    1048576      27587            3938124             0                 0
rsvp/ldp        (E)    1048576      29138            3090385             0                 0
icmp            (E)    1048576       176              20924              0                 0
arp             (E)    1048576       751              48064              0                 0
bpdu            (E)    1048576      26833            3129794             0                 0
bfd             (E)    1048576       38               4028               0                 0
dsp             (E)    78643200      507              34476              0                 0
```

show cpu-queue details

Use this command to display CPU queue details.

Command Syntax

```
show cpu-queue details
```

Parameters

None

Default

Monitoring is not enabled by default for any queues, but users have the option to enable monitoring for each queue. The default rate for each queue can be found in the show output. Some queues cannot be monitored, as indicated by an asterisk (*) in the show output.

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS-SP version 2.4.

Example

Use the following command to configure rate for protocol queues:

```
OcNOS#configure terminal
OcNOS(config)#cpu-queue cpu-q0 rate 400
```

Use the following command to verify the maximum, configured, and default configuration values:

```
OcNOS#show cpu-queue details

* - Can not configure the parameter
Cpu queue                    Rate In Kbps                          Monitor Status

Name            Configured     Default    Max Rate Allowed   Configured    Default
=======       ============   =========  =================  ===========   ==========
cpu.q0                400     900        20000              -             * no-monitor
cpu.q1                -       900        20000              -             * no-monitor
cpu.q2                -       900        20000              -             * no-monitor
cpu.q3                -       900        20000              -             * no-monitor
cpu.q4                -       900        20000              -             * no-monitor
cpu.q5                -       900        20000              -             * no-monitor
cpu.q6                -       10000      20000              -             * no-monitor
cpu.q7                -       900        20000              -             * no-monitor
igmp                  -       1000       1000               -             * no-monitor
is-is                 -       8000       8000               -               no-monitor
reservedmc            -       8000       8000               -               no-monitor
link-local            -       1000       1000               -               no-monitor
```

```
ospf                -       8000       8000               -               no-monitor
bgp                 -       8000       8000               -               no-monitor
rsvp/ldp            -       1500       1500               -               no-monitor
vrrp/rip/dhcp       -       2000       2000               -               no-monitor
pim                 -       8000       8000               -             * no-monitor
icmp                -       1000       1000               -               no-monitor
arp                 -       1000       1000               -               no-monitor
bpdu                -       8000       8000               -               no-monitor
oamp                -       1000       1000               -               no-monitor
sflow               -       16384      16384              -               no-monitor
dsp                 -       1500       1500               -               no-monitor
evpn                -       468        468                -               no-monitor
nhop                -       500        500                -               no-monitor
mgmt-route-leak     -       8000       10000              -               no-monitor
icmp-redirect       -       400        400                -               no-monitor
guest               -       8000       8000               -             * no-monitor
cfm                 -       1000       1000               -               no-monitor
bfd                 -       4000       4000               -               no-monitor
ptp                 -       4000       4000               -               no-monitor
```

Use the following command to configure monitor for protocol queues:

```
OcNOS#configure terminal
OcNOS(config)#cpu-queue bpdu monitor rate 4000
```

Use the following command to verify the maximum, configured, and default configuration values:

```
OcNOS#show cpu-queue details

* - Can not configure the parameter
Cpu queue                    Rate In Kbps                          Monitor Status

Name           Configured     Default    Max Rate Allowed   Configured    Default
=======       ============   =========  =================  ===========   ==========
cpu.q0               -       900        20000              -             * no-monitor
cpu.q1               -       900        20000              -             * no-monitor
cpu.q2               -       900        20000              -             * no-monitor
cpu.q3               -       900        20000              -             * no-monitor
cpu.q4               -       900        20000              -             * no-monitor
cpu.q5               -       900        20000              -             * no-monitor
cpu.q6               -       10000      20000              -             * no-monitor
cpu.q7               -       900        20000              -             * no-monitor
igmp                 -       1000       1000               -             * no-monitor
is-is                -       8000       8000               -               no-monitor
reservedmc           -       8000       8000               -               no-monitor
link-local           -       1000       1000               -               no-monitor

ospf                 -       8000       8000               -               no-monitor
bgp                  -       8000       8000               -               no-monitor
rsvp/ldp             -       1500       1500               -               no-monitor
vrrp/rip/dhcp        -       2000       2000               -               no-monitor
```

pim	-	8000	8000	-	* no-monitor
icmp	-	1000	1000	-	no-monitor
arp	-	1000	1000	-	no-monitor
bpdu	4000	8000	8000	monitor	no-monitor
oamp	-	1000	1000	-	no-monitor
sflow	-	16384	16384	-	no-monitor
dsp	-	1500	1500	-	no-monitor
evpn	-	468	468	-	no-monitor
nhop	-	500	500	-	no-monitor
mgmt-route-leak	-	8000	10000	-	no-monitor
icmp-redirect	-	400	400	-	no-monitor
guest	-	8000	8000	-	* no-monitor
cfm	-	1000	1000	-	no-monitor
bfd	-	4000	4000	-	no-monitor
ptp	-	4000	4000	-	no-monitor

CHAPTER 4 IP Service Level Agreements Commands

IP Service Level Agreements (SLAs) is a diagnostic method which generates and analyses the traffic between an OcNOS device and your network. IP SLA monitors and reports network performance data which helps you to identify the actual root cause of a problem when the performance level drops.

This chapter describes the commands used to manage the IP SLA for ICMP echo.

- clear ip sla statistics
- frequency
- icmp-echo
- ip sla
- ip sla schedule
- show ip sla statistics
- show ip sla summary
- show running-config ip sla
- threshold
- timeout

clear ip sla statistics

Use this command to clear the IP SLA statistics.

Command Syntax

```
clear ip sla statistics <1-65535>
```

Parameters

1-65535	IP SLA identifier

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#clear ip sla statistics 1
```

frequency

Use this command to configure the frequency/interval to send ICMP echo packets one by one.

Use the `no` form of this command to remove the configured ICMP echo frequency.

Command Syntax

```
frequency <1-60>
no frequency
```

Parameters

`1-60`	Frequency in seconds

Default

5 seconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#frequency 3
```

icmp-echo

Use this command to select and configure the ICMP echo SLA operation. ICMP echo packets are constructed in the device and sent to the destination address that you specify. These packets are transferred on a specific interface by setting the `source-interface` parameter.

Use the `no` form of this command to un-configure or remove the configured ICMP echo measurement sessions.

Command Syntax

```
icmp-echo (ipv4 A.B.C.D|ipv6 X:X::X:X|HOSTNAME) (source-interface IFNAME|)
no icmp-echo (ipv4 A.B.C.D | ipv6 X:X::X:X | HOSTNAME)
```

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`HOSTNAME`	Host name
`IFNAME`	Source interface name

Default

N/A

Command Mode

IP SLA mode (config-ip-sla)

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#
```

ip sla

Use this command to create an IP SLA instance. One instance maps to a single SLA operation. You can create multiple SLA operations to perform multiple similar or different SLA operations.

Use the `no` form of this command to remove a configured IP SLA configurations.

Command Syntax

```
ip sla <1-65535>
no ip sla <1-65535>
```

Parameters

`1-65535`	IP SLA identifier

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#
```

ip sla schedule

Use this command to schedule an IP SLA operation by associating a time-range object with the IP SLA operation.

Use the `no` form of this command to stop the configured IP SLA measurement.

Command Syntax

```
ip sla schedule <1-65535> time-range WORD (vrf (NAME)|)
```

Parameters

`<1-65535>`	IP SLA identifier.
`time-range`	Time Range
`TR_NAME`	Time range name that you set with the time-range command.
`vrf`	VPN Routing/Forwarding instance
`NAME`	VPN Routing/Forwarding instance name. Maximum limit 32 characters

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip sla schedule 1 time-range t1 vrf v1
```

show ip sla statistics

Use this command to display the statistics of IP SLA measurement.

Command Syntax

```
show ip sla statistics (1-65535) detail
```

Parameters

1-65535	IP SLA identifier.

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show ip sla statistics 1 detail
========================================
            IP SLA Statistics
========================================
  IP SLA ID                : 1
  Start Time               : 2021 Aug 30 17:40:04
  Elapsed time(milli sec)  : 46015
  Packets Sent             : 23
  Packets Received         : 23
  Packet Loss(%)           : 0.0000
  Invalid Tests            : 0
  Round Trip Delay(usec)
      Minimum              : 1000
      Maximum              : 1000
      Average              : 1000
```

Table 4-7 explains the output fields.

Table 4-7: show ip sla statistics fields

Field	Description
IP SLA ID	IP SLA Identifier (1-65535)
Start Time	Measurement start time
Elapsed time(milli sec)	Time taken to complete the measurement in milliseconds
Packets Sent	Number of packet sent

Table 4-7: show ip sla statistics fields (Continued)

Field	Description
Packets Received	Number of packet received
Packet Loss(%)	Packet lost in percentage
Invalid Tests	Received ICMP echo reply packets after configured threshold limit will be marked as invalid tests
Round Trip Delay(usec)	Round trip delay between ICMP echo request and ICMP echo reply: minimum, maximum and average round trip delay in microseconds

show ip sla summary

Use this command to display the summary of all IP SLA measurements.

Command Syntax

```
show ip sla summary
```

Parameters

None

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive

ID       Type        Destination       Stats       Return      Last
                                       (usec)        Code        Run
---------------------------------------------------------------------
^1      icmp-echo    20.2.2.3           0           OK        2021 Aug 23 13:53:37
```

Table 4-8 explains the output fields.

Table 4-8: show ip sla summary fields

Field	Description
ID	IP SLA Identifier (1-65535)
Type	Measurement type
Destination	Destination address
Stats (usec)	Round trip time in microseconds for the measurement
Return Code	Measurement status
Last Run	Measurement last run date and time

show running-config ip sla

Use this command to display the IP SLA running configuration alone.

Command Syntax

```
show running-config ip sla
```

Parameters

None

Default

N/A

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show running-config ip sla
ip sla 1
 icmp-echo ipv4 20.2.2.3
  frequency 2
  threshold 2000
  timeout 5000
ip sla schedule 1 time-range t1 vrf v1
```

threshold

Use this command to configure the threshold for every ICMP echo packet.

Use the `no` form of this command to remove the configured ICMP echo threshold.

Command Syntax

```
threshold <1000-60000>
no threshold
```

Parameters

`1000-60000`	Threshold in milliseconds.

Default

10000 milliseconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#threshold 5000
```

timeout

Use this command to configure the timeout for every ICMP echo packet. Any packet arriving beyond this interval is considered to be lost.

Use the `no` form of this command to remove the configured ICMP echo timeout.

Command Syntax

```
timeout <1000-60000>
no timeout
```

Parameters

`1000-60000`	Timeout in milliseconds.

Default

10000 milliseconds

Command Mode

IP SLA ICMP Echo mode (config-ip-sla-echo)

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip sla 1
(config-ip-sla)#icmp-echo ipv4 10.12.28.1 source-interface xe1
(config-ip-sla-echo)#timeout 5000
```

CHAPTER 5 Object Tracking Commands

This chapter describes the Object Tracking commands:

- track ip sla reachability
- delay up down
- object-tracking
- show track
- show track <1-500>
- show track summary
- show running-config track

track ip sla reachability

Use this command to configure an Object for tracking using IP SLA.

Use the `no` form of this command to delete to object tracking

Command Syntax

```
track <1-500> ip sla <1-65535> reachability)
no track <1-500> ip sla <1-65535> reachability
```

Parameters

`object-number (1-500)` Identifier for the tracked object

`ip-sla-number (1-65535)` Ientifier for IP SLA association with tracking object

Command Mode

Configuration mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
#configure terminal
OcNOS(config)#track 1 ip sla 1 reachability
OcNOS(config-object-track)#commit

OcNOS(config)#no track 1
OcNOS(config)#commit
```

delay up down

Use This command is used to delay the state change notification of Object tracking.

Use the `no` form of this command to remove delay the state change notification of Object

Command Syntax

```
delay (up <1-9999>|)(down <1-9999>|)
no delay (|up|down)
```

Parameters

`<1-999>`	Delay in Notification in seconds.

Default

NA

Command Mode

Object tracking Mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
OcNOS(config-object-track)#delay up 10 down 20
OcNOS(config-object-track)#no delay
OcNOS(config-object-track)#commit
OcNOS(config-object-track)#
OcNOS(config-object-track)#delay down 10
OcNOS(config-object-track)#commit
OcNOS(config-object-track)#no delay down
OcNOS(config-object-track)#commit
OcNOS(config-object-track)#
OcNOS(config-object-track)#delay up 10
OcNOS(config-object-track)#commit
OcNOS(config-object-track)#no delay up
OcNOS(config-object-track)#commit
OcNOS(config-object-track)#
```

show track

Use this command to display Sham link information.

Command Syntax

```
show track
```

Parameters

None

Default

NA

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
OcNOS#sh track
TRACK Id: 1
  IP SLA 1 reachability
  Reachability is DOWN
    0 changes, last change : 2021 Dec 11 05:20:23
OcNOS#
```

show track <1-500>

Use this command to display Sham link information.

Command Syntax

```
show track <1-500>
```

Parameters

<1-500>	object identifier

Default

NA

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
OcNOS#sh track 2
TRACK Id: 2
  IP SLA 2 reachability
  Reachability is DOWN
    0 changes, last change : 2021 Dec 11 05:29:49
OcNOS#
```

show track summary

Use this command to display the summary of all object tracking.

Command Syntax

```
show track summary
```

Parameters

NA

Default

NA

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
OcNOS#sh track summary
Object Tracking Summary
ID       Type        Type-Identifier       State
-----------------------------------------------------
1      ip-sla             1                DOWN
2      ip-sla             2                DOWN
OcNOS#
```

show running-config track

Use this command to display object tracking running configuration alone.

Command Syntax

```
show running-config track
```

Parameters

NA

Default

NA

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command is introduced in OcNOS version 5.1.

Example

```
OcNOS#sh running-config track
track 1 ip sla 1 reachability
 delay up 20
!
track 2 ip sla 2 reachability
!
OcNOS#
```

Hardware System Diagnose Configuration

CHAPTER 1 Show Tech Support Configurations

Overview

OcNOS maintains a collection of consolidated information about system configurations and statistics. This information is for debugging and diagnosing system issues.

Note: Output is displayed on the terminal.

Tech Support Samples

`#show techsupport all`	Collects system configurations and statistics for all modules.

CHAPTER 2 Ethernet Interface Loopback Support

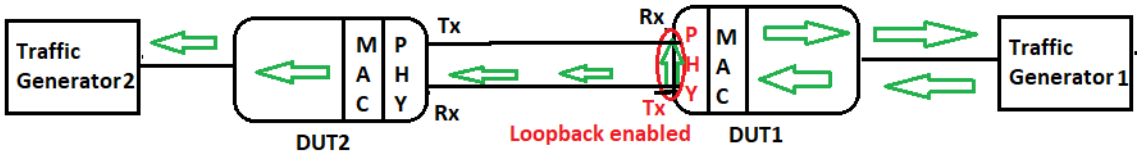
Overview

This feature support is to provide additional hardware diagnostic functionality for physical ports on boards. This feature will enable the user to determine if there are any issues in the physical port at the MAC and the PHY layer.

To achieve this functionality, the Ethernet interfaces can be configured as the loopback interfaces. Looping back the packets are possible either at MAC layer or at PHY layer. Also packets can be looped either from Egress to Ingress or Ingress to Egress. On enabling this feature, if all the TX packets are looped back to RX, it indicates there is no issue with the hardware at the particular layer configured, either MAC or PHY.

Local Loopback

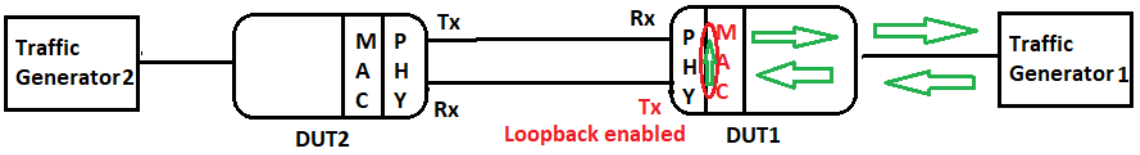
Tx PHY Loopback



When the loopback Tx PHY is enabled on an Ethernet interface, packets that the traffic generator receives on such an interface are loop-backed to the originator and forwarded to the destination.

Because loopback is enabled as the Tx PHY in the diagram above, packets will loop at the physical layer, and the same number of packets will be returned to the traffic generator from the DUT's Egress to Ingress side. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped and also forwarded to their next destination.

Tx MAC Loopback



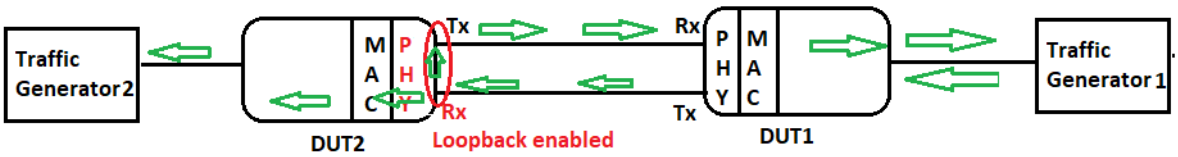
Loopback Tx MAC is enabled on the Ethernet interface, and when packets from the traffic generator arrive on such an interface, they are loop-backed to the originator rather than being forwarded.

In the above diagram, as loopback is enabled as a Tx MAC, the packets will loop at the MAC layer (data link layer), and the same number of packets are returned from the egress side to the ingress side of the DUT to the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped but not forwarded further.

© 2025 IP Infusion Inc. Proprietary

Remote Loopback

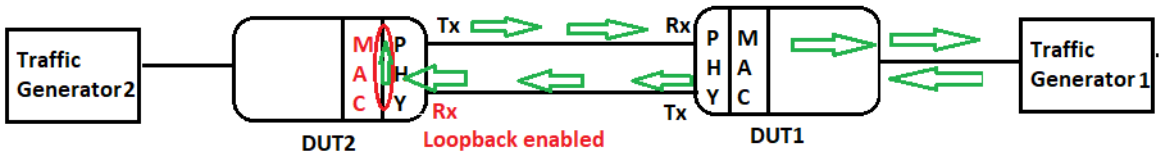
Rx PHY Loopback



Loopback Rx PHY is enabled on the ethernet interface, and when packets from the traffic generator arrive at a remote node via such an interface, they are loop-backed to the originator and forwarded to the next route.

In the above diagram, as loopback is enabled as Rx PHY on DUT2, the packets will loop at the physical layer of the DUT2, and the same number of packets are returned from the ingress to the egress side of the DUT2 to DUT1 and the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped back to Traffic Generator1 as well as forwarded to Traffic Generator2.

Rx MAC Loopback



Loopback Rx MAC is enabled on the ethernet interface, and when packets from the traffic generator arrive at a remote node via such an interface, they are loop-backed to the originator but not forwarded to the next route.

In the above diagram, as loopback is enabled as Rx MAC on DUT2, the packets will loop at the MAC layer (data link layer) of the DUT2, and the same number of packets are returned from the ingress to the egress side of the DUT2 to DUT1 and the traffic generator. Thus, the Tx and Rx counts of receiving and transmitting interfaces are the same. The packets are looped back to Traffic Generator1, but not forwarded to Traffic Generator2.

Topology

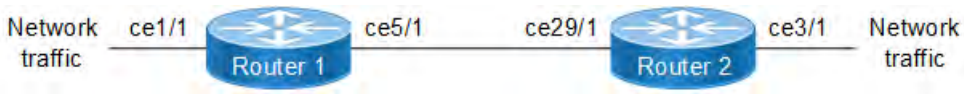


Figure 2-2: Loopback configuration nodes

Configurations

R1

`#configure terminal`	Enter into the configure terminal mode.
`R1(config)#hostname R1`	Configure the hostname
`R1(config)#commit`	Commit the configuration
`R1(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge
`R1(config)#vlan database`	Enter into vlan database
`R1(config-vlan)#vlan 2 bridge 1`	Configure vlans
`R1(config-vlan)#exit`	Exit the vlan database mode
`R1(config)#interface ce1/1`	Enter into interface ce1/1
`R1(config-if)#switchport`	Configure switchport
`R1(config-if)#bridge-group 1`	Configure bridge-group
`R1(config-if)#switchport mode trunk`	Configure switchport mode as trunk
`R1(config-if)#switchport trunk allowed vlan add 2`	Add all the vlans to the interface
`R1(config-if)#exit`	Exit the interface mode
`R1(config)#interface ce5/1`	Enter into interface ce1/1
`R1(config-if)#switchport`	Configure switchport
`R1(config-if)#bridge-group 1`	Configure bridge-group
`R1(config-if)#switchport mode trunk`	Configure switchport mode as trunk
`R1(config-if)#switchport trunk allowed vlan add 2`	Add all the vlans to the interface
`R1(config-if)#loopback tx phy`	Configure loopback tx phy
`R1(config-if)#exit`	Exit the interface level
`R1(config)#no mac-address-table learning bridge 1 interface ce1/1`	Disable the mac-learning on the device
`R1(config)#no mac-address-table learning bridge 1 interface ce5/1`	Disable the mac-learning on the device
`R1(config)#commit`	Commit the configuration
`R1(config)#exit`	Exit from configuration mode

R2

`#configure terminal`	Enter into the configure terminal mode.
`R2(config)#hostname R2`	Configure the hostname
`R2(config)#commit`	Commit the configuration
`R2(config)#exit`	Come out of configuration mode

R2#conf terminal	Enter into the configure terminal mode
R2(config)#bridge 1 protocol rstp vlan-bridge	Configure bridge
R2(config)#vlan database	Enter into vlan database
R2(config-vlan)#vlan 2 bridge 1	Configure vlans
R2(config-vlan)#exit	Exit the vlan database mode
R2(config)#interface ce3/1	Enter into interface ce3/1
R2(config-if)#switchport	Configure switchport
R2(config-if)#bridge-group 1	Configure bridge-group
R2(config-if)#switchport mode trunk	Configure switchport mode as trunk
R2(config-if)#switchport trunk allowed vlan add 2	Add the vlan to the interface
R2(config-if)#exit	Exit the interface mode
R2(config-if)#interface ce29/1	Enter into interface ce29/1
R2(config-if)#switchport	Configure switchport
R2(config-if)#bridge-group 1	Configure bridge-group
R2(config-if)#switchport mode trunk	Configure switchport mode as trunk
R2(config-if)#switchport trunk allowed vlan add 2	Add the vlan to the interface
R2(config-if)#exit	Exit from interface level
R2(config)#no mac-address-table learning bridge 1 interface ce3/1	Disable the mac-learning on the device
R2(config)#no mac-address-table learning bridge 1 interface ce29/1	Disable the mac-learning on the device
R2(config)#commit	Commit the configuration
R2(config)#exit	Exit from configuration mode

Validation

R1

```
R1#show running-config interface ce1/1
!
interface ce1/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
R1#show running-config interface ce5/1
!
interface ce5/1
switchport
 bridge-group 1
```

```
 switchport mode trunk
 switchport trunk allowed vlan add 2
 loopback tx phy
!
R1#  show interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out disabled
  Hardware is ETH  Current HW addr: 34ef.b689.e04a
  Physical:34ef.b689.e04a  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5045
  Metric 1 mtu 1500 duplex-full link-speed 40g
  Debounce timer: disable
  Loopback Type: PHY
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
  Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
  5 minute input rate 255 bits/sec, 0 packets/sec
  5 minute output rate 255 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 2272 broadcast packets 0
    input packets 2272 bytes 153730
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 4333 broadcast packets 0
    output packets 4333 bytes 293304
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

R1# show interface brief
--------------------------------------------------------------------------------
Ethernet   Type         PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                              Ch #
--------------------------------------------------------------------------------
ce5/1        ETH          1     trunk            up      none    10g   --       Br  Yes
PHY
```

R2

```
R2#show running-config interface ce3/1
!
```

```
interface ce3/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!

R2#show running-config interface ce29/1
!
interface ce29/1
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
R2#

Interface counters before configuring loopback on both the devices:
=========================================================
R1#show interface counters rate gbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 ce1/1                8.65           8446138       0.00           0
 ce5/1                0.00           0             8.65           8446125
R1#


R2#show interface counters rate gbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 ce3/1                0.00           0             8.65           8446188
 ce29/1               8.65           8446254       0.00           0
```

Interface counters after configuring loopback tx phy

R1

```
R1#show interface counters rate gbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+--------------------+--------------+-------------+--------------+-------------+
 ce1/1                8.65           8446147       8.65           8446319
 ce5/1                8.65           8446194       8.65           8446194
R1#

R2#show interface counters rate gbps
+--------------------+--------------+-------------+--------------+-------------+
|     Interface      |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
```

```
+-------------------+--------------+-------------+--------------+-------------+
 ce3/1               0.00           0             0.00           0
R2#
```

Removing the Loopback Configuration

R1

`R1#configure terminal`	Enter into configure terminal mode
`R1(config)#in ce5/1`	Enter into interface level
`R1(config-if)#no loopback`	Un-configure the loopback
`R1(config-if)#commit`	Commit the configuration
`R1(config-if)#end`	Exit from the configuration mode

Loopback tx mac

`R1#configure terminal`	Enter into configure terminal mode
`R1(config)#in ce5/1`	Enter into interface level
`R1(config-if)#loopback tx mac`	Configure loopback tx mac
`R1(config-if)#commit`	Commit the configuration
`R1(config-if)#end`	Exit from the configuration mode

Validation

R1

```
R1#show running-config interface ce1/1
!
interface ce1/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
R1#show running-config interface ce5/1
!
interface ce5/1
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 loopback tx mac
!
R1#  sh interface ce5/1
Interface ce5/1
  Flexport: Breakout Control Port (Active): Break Out disabled
```

```
  Hardware is ETH  Current HW addr: 34ef.b689.e04a
  Physical:34ef.b689.e04a  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5045
  Metric 1 mtu 1500 duplex-full link-speed 40g
  Debounce timer: disable
  Loopback Type: MAC
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2021 Oct 23 15:57:01 (00:08:51 ago)
  Statistics last cleared: 2021 Oct 23 15:54:44 (00:11:08 ago)
  5 minute input rate 255 bits/sec, 0 packets/sec
  5 minute output rate 255 bits/sec, 0 packets/sec
  RX
    unicast packets 0 multicast packets 2272 broadcast packets 0
    input packets 2272 bytes 153730
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 7
    Rx pause 0
  TX
    unicast packets 0 multicast packets 4333 broadcast packets 0
    output packets 4333 bytes 293304
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

R1# show interface brief
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                              Ch #
--------------------------------------------------------------------------------
ce5/1        ETH          1     trunk            up      none    10g   --       Br  Yes
MAC
```

R2

```
R2#show running-config interface ce3/1
!
interface ce3/1
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
```

```
!

R2#show running-config interface ce29/1
!
interface ce29/1
switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan add 2
!
R2#
```

Interface counters before configuring loopback on both the devices

```
R1#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce1/1               8.65           8432138       0.00           0
 ce5/1               0.00           0             8.65           8430125
R1#

R2#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce3/1               0.00           0             8.65           8429188
 ce29/1              8.65           8430254       0.00           0
```

Interface counters after configuring loopback tx phy

```
R1#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce1/1               8.65           8446147       8.65           8446319
 ce5/1               8.65           8446194       8.65           8446194
R1#

R2#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce3/1               0.00           0             0.00           0
ce29/1              0.00           0             0.00           0

R2#
```

Removing the Loopback Configuration

R1

R1#configure terminal	Enter into configure terminal mode
R1(config)#in ce5/1	Enter into interface level
R1(config-if)#no loopback	Un-configure the loopback
R1(config-if)#commit	Commit the configuration
R1(config-if)#end	Exit from the configuration mode

Loopback rx phy

R2#configure terminal	Enter into configure terminal mode
R2(config)#in ce29/1	Enter into interface level
R2(config-if)#loopback rx phy	Configure loopback rx phy
R2(config-if)#commit	Commit the configuration
R2(config-if)#end	Exit from the configuration mode

Validation

R2

```
R2#show interface ce29/1
Interface ce29/1
  Flexport: Breakout Control Port (Active): Break Out disable
  Hardware is ETH  Current HW addr: 80a2.357f.4ebd
  Physical:80a2.357f.4ebd  Logical:(not set)
  Forward Error Correction (FEC) configured is Auto (default)
  FEC status is N/A
  Port Mode is trunk
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full link-speed 40g
  Debounce timer: disable
  Loopback Type: R-PHY
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  DHCP client is disabled.
  Last Flapped: 2019 Apr 30 10:03:23 (00:00:58 ago)
  Statistics last cleared: 2019 Apr 30 09:43:30 (00:20:51 ago)
  30 second input rate 8648972937 bits/sec, 8446291 packets/sec
  30 second output rate 20723 bits/sec, 38 packets/sec
  RX
    unicast packets 3390485528 multicast packets 6205 broadcast packets 0
    input packets 3390494721 bytes 433982963744
    jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 1 jabbers 0
    input error 1
```

```
    input with dribble 0 input discard 39330
    Rx pause 0
  TX
    unicast packets 0 multicast packets 6009 broadcast packets 0
    output packets 6009 bytes 408564
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0

R2#show interface brief
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                                 Ch #
--------------------------------------------------------------------------------
ce29/1        ETH           1     trunk             up      none    10g   --       Br
Yes              R-PHY
```

Interface counters before configuring on both the devices

```
R1#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce1/1               8.65           8446138       0.00           0
 ce5/1               0.00           0             8.65           8446125
R1#

R2#show int counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce3/1               0.00           0             8.65           8446188
 ce29/1              8.65           8446254       0.00           0
R2#
```

Interface counters after configuring rx phy on R2 device

```
R1#show interface counters rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
 ce1/1               8.65           8446140       8.65           8446141
 ce5/1               8.65           8446058       8.65           8446058
R1#

R2#show interface cou rate gbps
+-------------------+--------------+-------------+--------------+-------------+
|     Interface     |    Rx gbps   |    Rx pps   |    Tx gbps   |    Tx pps   |
+-------------------+--------------+-------------+--------------+-------------+
```

```
 ce3/1                0.00           0              8.65           8446218
 ce29/1               8.65           8446222        0.00           0
R2#
```

Hardware System Diagnose Command Reference

CHAPTER 1 Chassis Management Module Commands

This chapter provides a description, syntax, and examples of CMM feature commands:

- alrt-max
- alrt-min
- cpu-core-usage
- crit-max
- crit-min
- debug cmm
- disk-activity-monitoring interval
- disk-activity-monitoring threshold
- emer-max
- emer-min
- locator led
- temperature policy (sys-reboot | sys-halt | none)
- temperature threshold
- show system fru
- show system-information
- system-load-average

You can retrieve the same set of information through SNMP that these commands display. This MIB is defined in `CMM-CHASSIS-MIB.txt`:

IP Infusion Inc. enterprise identifier	36673
Chassis MIB identifier	100

The MIB definition is available at:

- https://github.com/IPInfusion/OcNOS/branches

Navigate to the directory for the version of OcNOS that you are using.

Note: Critical logs in the console are equivalent to alert traps and alert logs on the console is equivalent to critical trap in SNMP.

cpu-core-usage

Use this command to set threshold percentage values for monitoring CPU core use.

Use the `no` form of this command to set the default thresholds.

Command Syntax

```
cpu-core-usage warning <51-100> alarm <91-100>
no cpu-core-usage
```

Parameters

`<51-100>`	Warning threshold percentage
`<91-100>`	Alarm threshold percentage

Default

Check the default thresholds using the `show system-information` command with the `cpu-load` parameter.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
(config)#cpu-core-usage warning 56 alarm 97
(config)#end

#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 20 Minutes 12 Seconds

Load Average(1 min)       : 4.24% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.87% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.37% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 2.02%
CPU core 1 Usage          : 0.89% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 3 Usage          : 5.41% (Crit Thresh : 56%, Alert Thresh : 97%)
CPU core 4 Usage          : 2.68% (Crit Thresh : 56%, Alert Thresh : 97%)

#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no cpu-core-usage
(config)#end

#show system-information cpu-load
```

```
System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 21 Minutes 46 Seconds

Load Average(1 min)       : 2.44% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 2.49% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.27% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 1.82%
CPU core 1 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 4.59% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 1.82% (Crit Thresh : 50%, Alert Thresh : 90%)
#
```

debug cmm

Use this command to enable or disable debugging for CMM.

Command Syntax

```
debug cmm
no debug cmm
```

Parameters

None

Default

By default, CMM debugging is disabled.

Command Mode

Configuration mode and exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug cmm
(config)#no debug cmm
```

disk-activity-monitoring interval

Use this command to set the disk activity monitoring interval in seconds.

Use the `no` form of this command to set the disk activity monitoring interval to its default value of 600 seconds.

Command Syntax

```
disk-activity-monitoring interval <30-1200>
no disk-activity-monitoring interval
```

Parameters

`<30-1200>`	Monitoring interval in seconds.

Default

The default monitoring interval is 600 seconds.

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 5.2.

Example

```
(config)#disk-activity-monitoring interval 60
(config)#commit
#
```

disk-activity-monitoring threshold

Use this command to set the threshold activity value for disk reads or writes. When the device reaches the threshold level, operator logs, SNMP traps, and NetConf notifications are displayed/sent. A threshold value of zero means that the monitoring is disabled.

Use the `no` form of this command to set the threshold activity for reads or writes in the default value of zero.

Command Syntax

```
disk-activity-monitoring threshold (read <1-20000> | write <1-20000>)
no disk-activity-monitoring threshold (read | write)
```

Parameters

`read`	Threshold level for reads.
`<1-20000>`	Threshold level in KBps.
`write`	Threshold level for writes.
`<1-20000>`	Threshold level in KBps.

Default

The default threshold activity value for reads and writes is zero (disabled).

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 5.2.

Example

```
(config)#disk-activity-monitoring threshold read 3000
(config)#commit
#

(config)#disk-activity-monitoring threshold write 4500
(config)#commit
```

locator led

Use this command to turn on the locator LED.

Use the `no` form of this command to turn off the locator LED.

Command Syntax

```
locator-led on
no locator-led
```

Parameters

None

Default

By default, the locator LED is turned off.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#locator-led on
(config)#no locator-led
```

show hardware-information

Use this command to display hardware information.

Command Syntax

```
show hardware-information (memory|fan|temperature|led|power (|monitoring-
  thresholds)|transceiver|system-status|all)
```

Parameter

`all`	Hardware details of all modules.
`fan`	Fan status of the boards.
`led`	LED status of the boards.
`memory`	Memory information of the boards.
`power`	PSU information.
`monitoring-thresholds`	Monitoring thresholds (if provided by hardware).
`temperature`	Temperature sensor information of the boards.
`transceiver`	Transceiver presence status and supported list of transceivers.
`system-status`	System fault status.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3. The `monitoring-thresholds` and `system-status` parameters were added in OcNOS version 5.2.

Example

```
#show hardware-information all
-------------------------------------------------------
                RAM INFORMATION
-------------------------------------------------------

Total                                     : 15930 MB
Used                                      : 1073 MB (7 %)
Free                                      : 14857 MB (93 %)
Shared                                    : 25 MB
Buffers                                   : 153 MB
Total Swap                                : 0 MB
Free Swap                                 : 0 MB
Current Processes                         : 253
Total High Memory                         : 0 MB
```

```
Available High Memory                    : 0 MB
Unit Size                                : 1 Bytes
Alert Threshold                          : 90 %
Critical Threshold                       : 80 %
-----------------------------------------------------
               HARD DISK INFORMATION
-----------------------------------------------------

Serial Number                            : 99009190902000000103
Model Number                             : ATP I-Temp M.2 2242
Firmware Revision                        : R0822A  ATP I-Temp M.2 2242
Cylinders                                : 16383
Heads                                    : 16
Sectors                                  : 250000000
Unformatted Bytes/Track                  : 0
Unformatted Bytes/Sector                 : 0
Revision No                              : 1008.0
Usage Alert Threshold                    : 90 %
Usage Critical Threshold                 : 80 %
-----------------------------------------------------------
Filesystem   Total        Used         Free         Use%
-----------------------------------------------------------
/            114365       10889        103476       10%
/cfg         476          79           397          17%
/installers  4911         282          4629         6%
-----------------------------------------------------------

-------------------------------------------------System Sensors-------------------------
--------------------------------
Codes: LNR - Lower Non-Recoverable
       LCR - Lower Critical
       LNC - Lower Non-Critical
       UNC - Upper Non-Critical
       UCR - Upper Critical
       UNR - Upper Non-Recoverable
Note: For discrete sensor, thresholds and value columns are not applicable.

SENSOR          | VALUE      | UNITS      | LNR       | LCR       | LNC       | UNC
| UCR       | UNR       | STATE
-------------------------------------------------------------------------------------------
-----------------------------------
Temp_MAC        | 41.000     | degrees C  | na        | na        | na        | 96.000
| 101.000   | 106.000   | ok
Temp_CPU        | 39.000     | degrees C  | na        | na        | na        | 92.000
| 97.000    | 102.000   | ok
Temp_BMC        | 33.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_10GPHY     | 35.000     | degrees C  | na        | na        | na        | 92.000
| 95.000    | 98.000    | ok
Temp_DDR4       | 31.000     | degrees C  | na        | na        | na        | 85.000
| 90.000    | 92.000    | ok
```

```
Temp_FANCARD1    | 29.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_FANCARD2    | 28.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
PSU0_Temp        | 38.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
PSU1_Temp        | 27.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
VSENSE_BMC_P12V  | 12.200     | Volts      | 11.200    | 11.400    | na        | na
| 12.600    | 12.750    | ok
VSENSE_HEATER    | 0.000      | Volts      | na        | na        | na        | 9.900
| 10.000    | 10.100    | ok
VSENSE_BMC_P2V5  | 2.520      | Volts      | 2.320     | 2.360     | na        | na
| 2.640     | 2.680     | ok
VSENSE_1VDDR     | 1.010      | Volts      | 0.900     | 0.940     | na        | na
| 1.060     | 1.080     | ok
VSENSE_BMC_P5VT  | 5.040      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_P5V_SB    | 5.010      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_BMC_1.26V | 1.260      | Volts      | 1.150     | 1.200     | na        | na
| 1.320     | 1.360     | ok
VSENSE_BMC_1.53V | 1.550      | Volts      | 1.380     | 1.460     | na        | na
| 1.610     | 1.690     | ok
VSENSE_BMC_P3V3  | 3.280      | Volts      | 3.020     | 3.140     | na        | na
| 3.480     | 3.640     | ok
FAN_0            | 12400.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_1            | 12500.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_2            | 11600.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_3            | 11900.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_4            | 12200.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
PSU0_FAN         | 8190.000   | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | ok
PSU1_FAN         | 0.000      | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | Lower Non-Recov
erable
HWM_VCORE_IN     | 1.000      | Volts      | 0.910     | 0.940     | na        | na
| 1.060     | 1.090     | ok
HWM_P1V0_VIN     | 1.000      | Volts      | 0.900     | 0.950     | na        | na
| 1.050     | 1.070     | ok
HWM_P1V2_VIN     | 1.180      | Volts      | 1.110     | 1.140     | na        | na
| 1.260     | 1.290     | ok
HWM_P1V25_VIN    | 1.240      | Volts      | 1.150     | 1.190     | na        | na
| 1.310     | 1.340     | ok
HWM_P1V8_VIN     | 1.770      | Volts      | 1.660     | 1.710     | na        | na
| 1.900     | 1.950     | ok
HWM_P3V3_VIN     | 3.280      | Volts      | 3.040     | 3.120     | na        | na
| 3.480     | 3.580     | ok
HWM_Temp_MAC     | 34.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_Heater  | 39.000     | degrees C  | -45.000   | -42.000   | -40.000   | 73.000
| 75.000    | 78.000    | ok
```

```
HWM_Temp_BMC     | 34.000     | degrees C  | -45.000   | -42.000   | -40.000   | 80.000
| 85.000    | 89.000    | ok
HWM_Temp_CPU     | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_AMB     | 28.000     | degrees C  | -45.000   | -42.000   | -40.000   | 76.000
| 80.000    | 84.000    | ok
HWM_Temp_PHY3    | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
CPU_PROC_HOT     | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
CPU_CAT_ERROR    | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
CPU_THERMAL_TRIP | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
CPU_TO_BMC_INT   | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
Thermal_NMI      | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
Thermal_BMC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
Thermal_PHY_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
Thermal_MAC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
Thermal_DDR_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Limit Not Excee
ded
CPLD_NMI         | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
VCORE_Fault      | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
FAN_CARD_INT     | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
BMC_LOADDEFAULT  | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | State Deasserte
d
CPU_BOOT_Done    | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Device Enabled
CPU_Presence     | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Device Present
Fan0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Device Present
Fan1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na        | Device Present
```

```
Fan2_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Present
Fan3_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Present
Fan4_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Present
CPU_POWEROK      | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Enabled
MB_POWEROK       | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Enabled
PSU0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Present
PSU1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Present
PSU0_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Enabled
PSU1_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | Device Disabled
PSU0_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | State Deasserte
d
PSU1_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na        | na         | State Deasserte
d
PSU0_VIN         | 118.000    | Volts      | na        | na        | na        | na
| na        | na         | ok
PSU0_VOUT        | 11.900     | Volts      | na        | na        | na        | na
| na        | na         | ok
PSU0_IIN         | 0.850      | Amps       | na        | na        | na        | na
| na        | na         | ok
PSU0_IOUT        | 2.480      | Amps       | na        | na        | na        | na
| na        | na         | ok
PSU1_VIN         | 0.000      | Volts      | na        | na        | na        | na
| na        | na         | ok
PSU1_VOUT        | 0.000      | Volts      | na        | na        | na        | na
| na        | na         | ok
PSU1_IIN         | 0.000      | Amps       | na        | na        | na        | na
| na        | na         | ok
PSU1_IOUT        | 0.000      | Amps       | na        | na        | na        | na
| na        | na         | ok

------------------------------------------------
LED             COLOR              DESCRIPTION
------------------------------------------------
POWER           GREEN              PSU operates Normally
SYSTEM          GREEN              Normal
GNSS            GREEN              GNSS in Normal State
SYNCE           GREEN              Synchronized to external timing source

------------------------------------------------------
           Transceiver DDM support list
------------------------------------------------------
Type                        :SFP
Vendor Name                 :FINISAR CORP.
Vendor Part Number          :FTLF8519P2BNL
```

```
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :EVERTZ
Vendor Part Number        :SFP10G-TR13S
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FS
Vendor Part Number        :SFP-10GSR-85
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FS
Vendor Part Number        :SFP-10G-BX40
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FS
Vendor Part Number        :SFP-10G-BX
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FS
Vendor Part Number        :SFP-10GZRC-55
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FS
Vendor Part Number        :SFP-10G-BX80
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :JDSU
Vendor Part Number        :PLRXPLSCS4322N
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :DELL
Vendor Part Number        :CN04HG0091IAA1B
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :DELL
Vendor Part Number        :WTRD1
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FINISAR CORP.
Vendor Part Number        :FTLF1318P3BTL-FC
```

```
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :DELL
Vendor Part Number        :RN84N
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP10G-LRi
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP10G-SRi
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-SX
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-LX
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-EX
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-ZX
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP10G-SR
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP10G-LR
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP10G-ER
```

```
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFPP-ER
DDM Supported             :Yes

Type                      :SFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP28-SR
DDM Supported             :Yes

Type                      :SFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP28-LR
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-SXi
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-SFP1G-LXi
DDM Supported             :Yes

Type                      :SFP+
Vendor Name               :OCLARO,INC.
Vendor Part Number        :TRS7081AHCPA00A
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FINISAR CORP.
Vendor Part Number        :FTLX8574D3BCL
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :FINISAR CORP.
Vendor Part Number        :FCLF8522P2BTL
DDM Supported             :NO

Type                      :SFP
Vendor Name               :Edgecore
Vendor Part Number        :ET5402-AOC-10M
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :Hisense
Vendor Part Number        :LTE3680P-BH+
```

```
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :Hisense
Vendor Part Number        :LTF5308B-BHA+
DDM Supported             :Yes

Type                      :SFP
Vendor Name               :Hisense
Vendor Part Number        :LTF7226B-BHA+
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :AVAGO
Vendor Part Number        :AFBR-79E4Z
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :FINISAR CORP
Vendor Part Number        :FCCN410QD3C
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :FINISAR CORP
Vendor Part Number        :FTL410QE4C
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :DELL
Vendor Part Number        :119N6
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFP85P1040PD000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFPQL010400D000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFPQL010400B000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFPQL002400D000
```

```
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFP85P3040PD000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFP85P1040PB000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQC504000000
DDM Supported             :NO

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM014000000
DDM Supported             :NO

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM034000000
DDM Supported             :NO

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM054000000
DDM Supported             :NO

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFP1301040PD000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :Skylane Optics
Vendor Part Number        :QFPQL040400D000
DDM Supported             :Yes

Type                      :QSFP
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :IPIENQSFP40GSR4
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :DELL
Vendor Part Number        :4WJ41
```

```
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FINISAR CORP
Vendor Part Number        :FCBN425QE1C
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FINISAR CORP.
Vendor Part Number        :FTLC1151RDPL
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FINISAR CORP
Vendor Part Number        :FTLC9551REPM
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :INPHI CORP
Vendor Part Number        :IN-Q2AY2
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FS
Vendor Part Number        :QSFP28-SR4-100G
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :FS
Vendor Part Number        :QSFP-PC03
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-QSFP28-SR4
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :E.C.I.NETWORKS
Vendor Part Number        :EN-QSFP28-LR4
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C07D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q2885P30C0PF000
```

```
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD020C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM01C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM02C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM03C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM05C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM07C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM10C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM20C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQM30C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAOQQP10C00D000
```

```
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q2885P10C0PF000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C00F000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C00D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD010C04D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C05F000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :Q28QD040C05D000
DDM Supported             :Yes

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM03C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM01C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM02C000000
DDM Supported             :NO

Type                      :QSFP28
Vendor Name               :Skylane Optics
Vendor Part Number        :DAPQQM05C000000
```

```
DDM Supported              :NO

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :DAPQQC50C000000
DDM Supported              :NO

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q28QL002C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2C31002C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2C31P50C00F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q2B85M70C00D000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :Skylane Optics
Vendor Part Number         :Q28QD080C05F000
DDM Supported              :Yes

Type                       :QSFP28
Vendor Name                :E.C.I.NETWORKS
Vendor Part Number         :IPIENQSFP28SR4
DDM Supported              :Yes


TX     : Transmit status
RX-Los : Receive status
RESET  : Normal (Out of reset), Reset (In reset)
POWER  : Power level Low/High
 -     : NotApplicable

SFP:[0-27]
---------------------------------------------
PORT   PRESENCE        Tx         Rx-Los
---------------------------------------------
0      Not Present     Off        -
1      Not Present     Off        -
```

```
2      Not Present     Off        -
3      Present         On         -
4      Present         On         -
5      Not Present     Off        -
6      Present         On         -
7      Present         On         Off
8      Not Present     Off        -
9      Not Present     Off        -
10     Present         On         -
11     Present         On         -
12     Present         On         On
13     Not Present     Off        -
14     Not Present     Off        -
15     Present         On         Off
16     Present         On         Off
17     Not Present     Off        -
18     Present         On         -
19     Present         On         Off
20     Present         On         Off
21     Not Present     Off        -
22     Present         On         -
23     Present         On         -
24     Not Present     Off        -
25     Not Present     Off        -
26     Not Present     Off        -
27     Not Present     Off        -

QSFP:[0-1]
-------------------------------------------------------------------------------------
-----
PORT   PRESENCE        RESET      POWER                                LANE
-------------------------------------------------------------------------------------
-----
                                                      1          2          3          4
-------------------------------------------------------------------------------------
-----
0      Not Present     Reset      Low        Tx        off        off        off        off
                                            Rx-Los     Off        Off        Off        Off
                                            Tx-Los     Off        Off        Off        Off
1      Present         Normal     High       Tx         on         on         on         on
                                            Rx-Los     Off        Off        Off        Off
                                            Tx-Los     Off        Off        Off        Off

System Over all status   : Normal

---------------------------
Components status
---------- ----------------
CPU        : Normal
RAM        : Normal
DISK       : Normal
```

```
SOFTWARE    : Normal

Codes: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major

Component  Fault  Timestamp            Thresh   Violation-Status
---------  -----  ---------            ------   ----------------
```

Table 1-9 explains the show command output fields.

Table 1-9: show hardware-information all output

Field	Description
Ram Information	Used memory, free memory, shared, buffers, total swap, and free swap memory.
Hard Disk Information	Hard drive serial number, model, firmware revision, cylinders, heads, and sectors, as well as revision number and total size.
Fans	Fan tray numbers, numbers of fans per tray, and their speed in RPM.
Board Temp Sensors Temperature	Sensor type, current temperature, and operating range.
BCM Chip Internal Temperature	Broadcom chip current internal temperature, Operating range and average temperature.
System Power Information	System power Information. Shows Voltage on all rails, and whether the power is up or has failed.
PSU	Main power supply statistics: Volts in, volts out, current in and out amperes, power in and out in watts, temperature of each power supply, and fan speed in RPM.
LED	What the LEDs represent, what state the LEDs mean, and a description of what the LEDs current color means.
Transceiver DDM support list	Transceivers: type, vendor name, part number, and whether Digital Diagnostic Monitoring (DDM) is supported.
Port Number	Port numbers, port type (SFP, QSFP, etc) and whether a transceiver is in the port.

```
#show hardware-information power
-----------------------------------------------------
                Hardware Thresholds
-----------------------------------------------------
PSU1 [Input Voltage]
-----------------------------
Shutdown(O)    : 62.00 Volts
Resume(O)      : 60.00 Volts
Shutdown(U)    : 38.00 Volts
Resume(U)      : 36.00 Volts
PSU1 [Temperature 1]
-----------------------------
Shutdown(O)    : 85.00 Celsius
Resume(O)      : 80.00 Celsius
PSU2 [Input Voltage]
```

```
-----------------------------
Shutdown(O)    : 62.00 Volts
Resume(O)      : 60.00 Volts
Shutdown(U)    : 38.00 Volts
Resume(U)      : 36.00 Volts

-----------------------------------------------------
                System Power Information
-----------------------------------------------------
CMM_PS1_12V_PG                          : FAIL
CMM_PS2_12V_PG                          : GOOD
CMM_PS1_AC_ALERT                        : FAIL
CMM_PS2_AC_ALERT                        : GOOD

Codes:     * Not Supported by device    NA Not Applicable     O Over    U Under

PSU        VOLT-IN    VOLT-OUT   CURR-IN    CURR-OUT   PWR-IN     PWR-OUT    TEMP-1
TEMP-2     FAN-1      FAN-2      PWR_
OUT_MAX
           (Volt)     (Volt)     (Ampere)   (Ampere)   (Watt)     (Watt)     (Celsius)
(Celsius)  (Rpm)      (Rpm)
-------------------------------------------------------------------------------------------
-------------------------------------
------
2          225.00     12.00      1.47       25.50      330.00     306.00     27.00
31.00      4512       NA*        NA*

#
```

Table 1-10 explains the `show hardware-information power` command output fields.

Table 1-10: show hardware-information power output fields

Field	Description
PSU Input Voltage	Shutdown and resume over and under voltages
PSU Temperature	Shutdown and resume over temperatures
System Power Information	Overall status of each PSU
PSU	Power supply unit identifier
VOLT-IN	Input voltage
VOLT-OUT	Output voltage
CURR-IN	Input current (ampere)
CURR-OUT	Output current (ampere)
PWR-IN	Input power (watts)
PWR-OUT	Output power (watts)

Table 1-10: show hardware-information power output fields (Continued)

Field	Description
TEMP-1	Temperature (Celsius)
TEMP-2	Temperature (Celsius)
FAN-1	FAN 1 RPM
FAN-2	FAN 2 RPM
PWR_OUT_MAX	Power out maximum

```
#show hardware-information power monitoring-thresholds
-----------------------------------------------------
         Input Voltage [PSU1]
-----------------------------------------------------
High Alarm        : 60.00 Volts
Low Alarm         : 40.00 Volts
High Warning      : 58.00 Volts
Low Warning       : 42.00 Volts
-----------------------------------------------------
         Temperature 1 [PSU1]
-----------------------------------------------------
High Alarm        : 75.00 Celsius
Low Alarm         : -10.00 Celsius
High Warning      : 73.00 Celsius
Low Warning       : -8.00 Celsius
-----------------------------------------------------
         Input Voltage [PSU2]

-----------------------------------------------------
High Alarm        : 60.00 Volts
Low Alarm         : 40.00 Volts
High Warning      : 58.00 Volts
Low Warning       : 42.00 Volts
```

Table 1-11 explains the `show hardware-information power monitoring-thresholds` command output fields.

Table 1-11: show hardware-information power monitoring-thresholds output fields

Field	Description
Input Voltage	Voltages for high alarm, low alarm, high warning, and low warning thresholds
Temperature	Temperatures for high alarm, low alarm, high warning, and low warning thresholds

```
#show hardware-information system-status

System Over all status   : Normal
```

```
---------------------------

Components status

---------- ----------------

CPU        : Normal

RAM        : Normal

DISK       : Normal

FAN        : Normal

POWER      : Normal

SOFTWARE   : Normal

Codes: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major

Component  Fault  Timestamp            Thresh   Violation-Status

---------  -----  ---------            ------   ----------------

DISK       H-Mi   12-02-2021 18:39:32  > 80.00  84.00%

POWER      L-Mi   12-02-2021 18:43:46  < 42.00  Psu [1] of VOLT-IN is 42.00

                  12-02-2021 18:42:35           Psu [2] of VOLT-IN is 42.00

           L-Ma   12-02-2021 18:41:44  < 40.00  Psu [1] of VOLT-IN is 24.00

           H-Ma   12-02-2021 18:44:27  > 75.00  Psu [1] of TEMP1 is 80.00

#
```

Table 1-12 explains the `show hardware-information system-status` command output fields.

Table 1-12: show hardware-information system-status output fields

Field	Description
System Over all status	Self explantory
Components status	Status of CPU, RAM, disk, fan, power, and software
Component	Component name

Table 1-12: show hardware-information system-status output fields (Continued)

Field	Description
Fault	Type of fault: H-Mi- High Minor H-Ma- High Major L-Mi- Low Minor L-Ma- Low Major
Timestamp	Date and time of the faullt
Thresh	Threshold limit
Violation-Status	Explanation of violation

show system fru

Use this command to display Field Replaceable Unit (FRU) information controlled by the baseboard management controller (BMC).

Command Syntax

```
show system fru
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 3.0.

Example

```
#show system fru
--------------System FRUs------------------
FRU Device Description : MAINBOARD_FRU
Board Mfg Date        : 2018-09-17 13:34:00
Board Mfg             : UFISPACE
Board Product         : S9500-30XS-Board
Board Serial          : WB2N9470004
Product Manufacturer  : UFISPACE
Product Name          : S9500-30XS
Product Version       : PVT
Product Serial        : WE61A47S00016
Product Asset Tag     : 00

FRU Device Description : PSU0_FRU
Product Manufacturer  : FSPGROUP
Product Name          : VICTO451AM
Product Part Number   : YNEB0450
Product Version       : BM-2R01P10
Product Serial        : T0A060Y322009000053
Product extra 1       : P3H800A03
Product extra 2       : A

FRU Device Description : PSU1_FRU
Product Manufacturer  : FSPGROUP
Product Name          : VICTO451AM
Product Part Number   : YNEB0450
Product Version       : BM-2R01P10
Product Serial        : T0A060Y322009000052
Product extra 1       : P3H800A03
Product extra 2       : A
```

show system-information

Use this command to display system information.

Command Syntax

```
show system-information (all|fan|psu|os|cpu|bios|cpu-load|board-info)
```

Parameter

`all`	System information of all modules.
`bios`	BIOS information.
`board-info`	Board EEPROM details.
`cpu`	Processor information.
`cpu-load`	CPU load information.
`fan`	Fan Field Replaceable Units (FRU) EEPROM information.
`os`	OS and Kernel version information.
`psu`	Power Supply Field Replaceable Units (FRU) EEPROM information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show system-information psu
System PSU FRU Information
=========================
PSU 2 Country of Origin          : CN
PSU 2 PPID Part Number           : 0T9FNW
PSU 2 PPID Part Number Rev       : A00
PSU 2 Manufacturer ID            : 28298
PSU 2 Date Code                  : 52R
PSU 2 Serial Number              : 0298
PSU 2 Part Number                : 0T9FNW
PSU 2 Part Number Revision       : A00
PSU 2 Number of Fans in the tray : 1
PSU 2 Type                       : AC Normal
PSU 2 Service Tag                : AEIOU
```

The following tables explain the show command output fields.

Table 1-13: show system-information topics

Topic	Description
all	Show all topics of system information..
bios	Display BIOS information.
board-info	Display information related to the board.
cpu	Displays Central Processing Unit information
cpu-load	Displays the load on the system’s CPU.
fan	Displays fan information contain in the EEPROM.
os	Displays information regarding the host operating system
psu	Displays information regarding Field Replaceable Units (FRU).

Table 1-14: Show fan topic displays

System Fan FRU Information	Description
Fan Tray “#” PPID Part Number	The vendor’s part number for the fan.
Fan Tray Serial Number	As stated
Service Tag	The Service Tag can help identify your device for on-line support and upgrading drivers
Vendor Name	As stated

Table 1-15: Show system BIOS information

BIOS Information	Description
# dmidecode	The dmidecode is a tool for dumping a computer's DMI table contents in a human-readable format. This table contains a description of the system's hardware components, as well as other useful pieces of information such as serial numbers and BIOS revisions.
SMBIOS	The System Management BIOS (SMBIOS) defines data structures (and access methods) that can be used to read management information produced by the BIOS of a computer. Also, it is involved with the DMI Address –
Handle 0x0000, DMI type 0, 24 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 0 indicates the following information is specific to BIOS properties, and is 24 bytes long.
BIOS Physical Information	• Vendor – The manufacture of the BIOS. • Version – The Version number. • Release Date – as stated. • Address – starting address (in memory) of the BIOS.

Table 1-15: Show system BIOS information (Continued)

BIOS Information	Description
Characteristics	• Is PCI supported. • Is BIOS upgradeable. • Is boot from a CD supported. • Is selectable boot devices supported. • Is BIOS ROM socketed. • Is Enhanced Disk Drive (EDD) vectoring supported. • Is 5.25"/1.2 MB floppy services supported (int 13h) • Is 3.5"/720 kB floppy services supported (int 13h) • Is 3.5"/2.88 MB floppy services supported (int 13h) • Is Print screen service supported (int 5h) • Is 8042 keyboard services supported (int 9h) • Is Serial services supported (int 14h) • Is Printer services supported (int 17h) • Is Advanced Configuration and Power Interface (ACPI) supported • Is USB legacy supported • Is BIOS boot specification supported • Is Targeted content distribution supported • Is Unified Extensible Firmware Interface (UEFI) supported
BIOS Revision	The BIOS revision number.
Handle 0x0043, DMI type 13, 22 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 13 indicates the following information is specific to BIOS language information, and is 22 bytes long.
BIOS Language Informantion	• Language Description Format – A term that describes the number of bits used to represent the BIOS Language information parameters. • Installable Languages – The number of languages that can be used by the BIOS at any time. • Currently Installed Language – United States English (or Latin-1) as described by the ISO standard, en|US|iso8859-1.

Table 1-16: Show CPU information

System CPU Information	Description
processor	The processor number of each CPU
model name	Details about each CPU. For example, Intel(R) Atom(TM) CPU C2538 @ 2.40GHz.

Table 1-17: Show system CPU load information

Load Information	Description
Uptime	As stated in days, hours, minutes, and seconds.
Load Average for past 1min	As stated in percent.
Load Average for past 5 min	As stated in percent.

Table 1-17: Show system CPU load information (Continued)

Load Information	Description
Load Average for past 15 min	As stated in percent.
CPU Usage at this instant	As stated in percent.
Max threshold for CPU-usage	As stated in percent.

Table 1-18: Show system board information

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated
Manufacture Date	As state
Platform Name	The platform on which the product is based.
ONIE Version	The version of the Open Network Install Environment (ONIE).
MAC addresses	Number of MAC addresses related to the device.
Manufacture	As stated
Country Code	The code that represents the country of manufacture. For example, US = United States, TW = Taiwan, and so on.
Diag Version	As stated
CRC-32	Cyclic Redundancy Check value.
Switch Chip Revision	As stated
MAIN BOARD REVISION	As stated
CPU CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the CPU.
SW CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the switch.
MAIN BOARD TYPE	An identifying string for the main board.
CPU BOARD ID	An identifying string for the CPU board.
CPU BOARD VERSION	As stated
SW BOARD ID	NA
SW BOARD VERSION	As stated
VCC 5V	The state of the VCC 5V power rail (Enabled \ Disabled)
MAC 1V	The state of the MAC 1V power rail Enabled \ Disabled

Table 1-18: Show system board information (Continued)

System Information	Description
VCC 1.8V	The state of the VCC 1.8V power rail (Enabled \ Disabled)
MAC AVS 1V	The state of the MAC AVS 1V power rail (Enabled \ Disabled)
HOT SWAP1	Enabled \ Disabled
HOT SWAP2	Enabled \ Disabled

Table 1-19: Show host system details

Host Information	Description
OS Distribution	The operating system on which the device is to run.
Kernel Version	A string that identifies the operating kernel.

show system sensor

Use this command to display the system sensors controlled by the baseboard management controller (BMC).

Command Syntax

```
show system sensor
```

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before OcNOS version 3.0.

Example

```
#show system sensor
-------------------------------------------------System Sensors-------------------------
--------------------------------
Codes: LNR - Lower Non-Recoverable
LCR - Lower Critical
LNC - Lower Non-Critical
UNC - Upper Non-Critical
UCR - Upper Critical
UNR - Upper Non-Recoverable
Note: For discrete sensor, thresholds and value columns are not applicable.

SENSOR          | VALUE      | UNITS      | LNR       | LCR       | LNC       | UNC
| UCR       | UNR       | STATE
-------------------------------------------------------------------------------------
----------------------------------
Temp_MAC        | 43.000     | degrees C  | na        | na        | na        | 96.000
| 101.000   | 106.000   | ok
Temp_CPU        | 40.000     | degrees C  | na        | na        | na        | 92.000
| 97.000    | 102.000   | ok
Temp_BMC        | 32.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_10GPHY     | 35.000     | degrees C  | na        | na        | na        | 92.000
| 95.000    | 98.000    | ok
Temp_DDR4       | 33.000     | degrees C  | na        | na        | na        | 85.000
| 90.000    | 92.000    | ok
Temp_FANCARD1   | 29.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
Temp_FANCARD2   | 27.000     | degrees C  | na        | na        | na        | 80.000
| 85.000    | 89.000    | ok
PSU0_Temp       | 37.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
PSU1_Temp       | 28.000     | degrees C  | na        | na        | na        | 86.000
| 90.000    | 95.000    | ok
```

```
VSENSE_BMC_P12V  | 12.050     | Volts      | 11.200    | 11.400    | na        | na
| 12.600    | 12.750    | ok
VSENSE_HEATER    | 0.000      | Volts      | na        | na        | na        | 9.900
| 10.000    | 10.100    | ok
VSENSE_BMC_P2V5  | 2.500      | Volts      | 2.320     | 2.360     | na        | na
| 2.640     | 2.680     | ok
VSENSE_1VDDR     | 1.020      | Volts      | 0.900     | 0.940     | na        | na
| 1.060     | 1.080     | ok
VSENSE_BMC_P5VT  | 5.040      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_P5V_SB    | 4.980      | Volts      | 4.680     | 4.740     | na        | na
| 5.250     | 5.310     | ok
VSENSE_BMC_1.26V | 1.250      | Volts      | 1.150     | 1.200     | na        | na
| 1.320     | 1.360     | ok
VSENSE_BMC_1.53V | 1.540      | Volts      | 1.380     | 1.460     | na        | na
| 1.610     | 1.690     | ok
VSENSE_BMC_P3V3  | 3.280      | Volts      | 3.020     | 3.140     | na        | na
| 3.480     | 3.640     | ok
FAN_0            | 12900.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_1            | 13000.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_2            | 12400.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_3            | 12300.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
FAN_4            | 11800.000  | RPM        | 2400.000  | 3200.000  | 6000.000  | na
| na        | na        | ok
PSU0_FAN         | 8280.000   | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | ok
PSU1_FAN         | 0.000      | RPM        | 3330.000  | 3600.000  | 3960.000  | na
| na        | na        | Lower Non-Recoverable
HWM_VCORE_IN     | 1.000      | Volts      | 0.910     | 0.940     | na        | na
| 1.060     | 1.090     | ok
HWM_P1V0_VIN     | 1.000      | Volts      | 0.900     | 0.950     | na        | na
| 1.050     | 1.070     | ok
HWM_P1V2_VIN     | 1.210      | Volts      | 1.110     | 1.140     | na        | na
| 1.260     | 1.290     | ok
HWM_P1V25_VIN    | 1.250      | Volts      | 1.150     | 1.190     | na        | na
| 1.310     | 1.340     | ok
HWM_P1V8_VIN     | 1.780      | Volts      | 1.660     | 1.710     | na        | na
| 1.900     | 1.950     | ok
HWM_P3V3_VIN     | 3.300      | Volts      | 3.040     | 3.120     | na        | na
| 3.480     | 3.580     | ok
HWM_Temp_MAC     | 35.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_Heater  | 39.000     | degrees C  | -45.000   | -42.000   | -40.000   | 73.000
| 75.000    | 78.000    | ok
HWM_Temp_BMC     | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 80.000
| 85.000    | 89.000    | ok
HWM_Temp_CPU     | 33.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
HWM_Temp_AMB     | 28.000     | degrees C  | -45.000   | -42.000   | -40.000   | 76.000
| 80.000    | 84.000    | ok
HWM_Temp_PHY3    | 35.000     | degrees C  | -45.000   | -42.000   | -40.000   | 86.000
| 90.000    | 95.000    | ok
```

```
CPU_PROC_HOT     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPU_CAT_ERROR    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
CPU_THERMAL_TRIP | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPU_TO_BMC_INT   | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
Thermal_NMI      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_BMC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_PHY_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_MAC_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
Thermal_DDR_ALRT | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Limit Not Exceeded
CPLD_NMI         | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
VCORE_Fault      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
FAN_CARD_INT     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
BMC_LOADDEFAULT  | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
CPU_BOOT_Done    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
CPU_Presence     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan2_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan3_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
Fan4_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
CPU_POWEROK      | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
MB_POWEROK       | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
PSU0_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
PSU1_Presence    | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Present
PSU0_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Enabled
PSU1_POWEROK     | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | Device Disabled
PSU0_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
PSU1_INT1        | 0x0        | discrete   | na        | na        | na        | na
| na         | na         | State Deasserted
```

```
PSU0_VIN         | 99.000     | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU0_VOUT        | 11.900     | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU0_IIN         | 0.420      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU0_IOUT        | 0.850      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU1_VIN         | 0.000      | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU1_VOUT        | 0.000      | Volts      | na        | na        | na        |  na
| na         | na         | ok
PSU1_IIN         | 0.000      | Amps       | na        | na        | na        |  na
| na         | na         | ok
PSU1_IOUT        | 1.950      | Amps       | na        | na        | na        |  na
| na         | na         | ok
#
```

system-load-average

Use this command to set threshold percentage values for monitoring the system load average for the last 1 minute, 5 minutes, and 15 minutes.

Use the `no` form of this command to set the default thresholds.

Command Syntax

```
system-load-average (1min warning <41-100> alarm <51-100> 5min alarm <51-100> 15min
  alarm <51-100>)
no system-load-average
```

Parameters

`1min warning`	Load average for last 1 minute
`<41-100>`	Warning threshold in percent
`alarm`	Alarm
`<51-100>`	Alarm threshold in percent
`5min alarm`	Load average for last 5 minutes
`<51-100>`	Alarm threshold in percent
`15min alarm`	Load average for last 15 minutes
`<51-100>`	Alarm threshold in percent

Default

Check the default thresholds using the `show system-information` command with the `cpu-load` parameter.

Command Mode

Config Mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
(config)#system-load-average 1min warning 45 alarm 55 5min alarm 65 15min
alarm 75
(config)#end

#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                     : 64 Days 17 Hours 56 Minutes 22 Seconds

Load Average(1 min)        : 5.74% (Crit Thresh : 45%, Alert Thresh : 55%)
Load Average(5 min)        : 3.71% (Crit Thresh : N/A, Alert Thresh : 65%)
Load Average(15 min)       : 3.21% (Crit Thresh : N/A, Alert Thresh : 75%)

Avg CPU Usage              : 4.67%
```

```
CPU core 1 Usage          : 4.42% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 2.68% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 6.19% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 5.36% (Crit Thresh : 50%, Alert Thresh : 90%)

#con t
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no system-load-average
(config)#end

#show system-information cpu-load

System CPU-Load Information
===========================

Uptime                    : 64 Days 18 Hours 16 Minutes 34 Seconds

Load Average(1 min)       : 0.63% (Crit Thresh : 40%, Alert Thresh : 50%)
Load Average(5 min)       : 1.90% (Crit Thresh : N/A, Alert Thresh : 50%)
Load Average(15 min)      : 3.11% (Crit Thresh : N/A, Alert Thresh : 50%)

Avg CPU Usage             : 2.07%
CPU core 1 Usage          : 1.83% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 2 Usage          : 0.00% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 3 Usage          : 6.36% (Crit Thresh : 50%, Alert Thresh : 90%)
CPU core 4 Usage          : 0.93% (Crit Thresh : 50%, Alert Thresh : 90%)
```

CHAPTER 2 Modifying Temperature Sensor Threshold Value

Overview

Typically, the temperature policies of hardware equipments are predefined and enforced through hardware or software by hardware vendors. However, for hardwares without baseboard management controller (BMC) built-in, the temperature policies are managed through software from Network Operating System (NOS) vendors.

OcNOS is enhanced to manage the hardware temperature through new commands line interfaces from 6.5.3 release. These newly defined software policy based temperature control CLIs are compliance to the hardware vendor standards. However, to satisfy some users who wants to modify the present threshold values at their convenience can do so. They are willing to take risks by stretching the predefined threshold values by the hardware vendor.

However, IPI strongly recommends not to modify the default policy as it may lead to hardware component failure.

Feature Characteristics

Using this feature users can control both or any one of them based on the requirement.

- the threshold values for each severity level and temperature sensor,

and

- the system action upon a violation to either HALT, REBOOT or NONE.

The hardware's default policy is applied if no user configuration exists or is removed.

A warning message alerts users if they set thresholds beyond the “Emergency Max/Min” values or configure the policy to “none,” emphasizing the potential risks involved.

These commands are applicable only to EdgeCore and UfiSpace hardwares without BMC built-in.

Benefits

This feature enables an exceptional control for users. With the current default hardware temperature policy, when OcNOS detects the temperature threshold value violation, it shuts down the system to prevent hardware damage. Some customers have deployed the units in far remote areas, and whenever this happens it becomes troublesome for them to switch the units back ON. In such exceptional cases, enables the user to modify the predefined thresholds value and change the behaviors of the system to either REBOOT or NONE instead of HALT.

Prerequisites

The hardware should be up and active.

CLI Commands

The Chassis Management Module Commands section introduces the following new configuration commands.

temperature threshold

Use this command to set temperature threshold for each severity level of the sensor.

Use the `no` form of this command to set the default thresholds.

Command Syntax

```
temperature threshold <1-15>
no temperature threshold <1-15>
```

Parameters

`<1-15>`	Specifies the sensor number to be configured. Refer to temperature threshold temperature CLI command section to view the available sensor types.

Default

Check the default temperature thresholds using the `show hardware-information` temperature command.

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 1
OcNOS(config-temperature-threshold)#
```

The mode changes to temperature threshold mode.

```
#(config-temperature-threshold)#emer-min 5
#(config-temperature-threshold)#commit
```

To remove the configuration, execute:

```
OcNOS(config)#no temperature threshold 1
```

To view the current hardware temperature, execute

```
#show running-config |include temperature | emer-min
temperature threshold 1
emer-min 5
```

```
OcNOS#show hardware-information temperature
```

```
Board Temp Sensors Temperature in Degree C
```

```
-------------------------------------------------------------------------------------------------------
SENSOR TYPE                      CURR  EMER  ALRT CRIT CRIT ALRT EMER   MIN-TEMP  MAX-TEMP  AVG-TEMP
                                 TEMP  MIN   MIN  MIN  MAX  MAX  MAX  (Monitored since 72 hour,00 min)

-------------------------------------------------------------------------------------------------------
[ 1] CPU                         42.00  5    10   14   60   65   70      37.50     44.00     40.40
[ 2] Mainboard Front middle      37.50  0    10   14   60   65   70      33.50     39.50     36.41
[ 3] Mainboard Rear Left         35.00  0    10   14   60   65   70      32.00     36.50     33.92
[ 4] Mainboard Right             33.00  0    10   14   60   65   70      28.50     34.50     31.59
[ 5] BCM Chip                    54.20  0    10   14   75   80   95      48.90     56.90     52.25
[ 6] Intel CPU Core ID 2         54.00  0    3    6    66   71   91      47.00     57.00     52.06
[ 7] Intel CPU Core ID 6         52.00  0    3    6    66   71   91      46.00     56.00     50.38
[ 8] Intel CPU Core ID 8         53.00  0    3    6    66   71   91      46.00     55.00     50.17
[ 9] Intel CPU Core ID 12        54.00  0    3    6    66   71   91      46.00     57.00     51.23

BCM Chip Internal Temperature
-----------------------------------------
TEMP MONITOR    CURRENT TEMP    PEAK TEMP
                (Degree C)      (Degree C)
-----------------------------------------
1               49.40           52.10
2               49.90           52.10
3               52.60           55.30
4               49.90           52.10
5               54.20           55.30
6               53.10           55.30
7               52.60           54.70
8               52.10           54.70
9               49.90           53.10
10              49.90           52.60
#
```

emer-max

Use this command to configure hardware emergency temperature threshold maximum value.

Use `no` parameter to remove the replace the configured emergency temperature maximum value to default threshold value.

Command Syntax

```
emer-max <-50-150>
no emer-max
```

Parameters

`<-50-150>`	Specifies the emergency Temperature-threshold maximum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the emergency temperature sensor's maximum threshold value, execute:

```
OcNOS(config-temperature-threshold)#emer-max 78
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no emer-max
```

emer-min

Use this command to configure hardware emergency temperature threshold minimum value.

Use `no` parameter to remove the replace the configured emergency temperature minimum value to default threshold value.

Command Syntax

```
emer-min <-50-150>
no emer-min
```

Parameters

`<-50-150>`	Specifies the emergency Temperature-threshold minimum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the emergency temperature sensor's minimum threshold value, execute:

```
OcNOS(config-temperature-threshold)#emer-min 1
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no emer-min
```

alrt-max

Use this command to configure hardware alert temperature threshold maximum value.

Use `no` parameter to remove the replace the configured alert temperature maximum value to default threshold value.

Command Syntax

```
alrt-max <-50-150>
no alrt-max
```

Parameters

`<-50-150>`	Specifies the alert Temperature-threshold maximum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the alert temperature sensor's maximum threshold value, execute:

```
OcNOS(config-temperature-threshold)#alrt-max 73
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no alrt-max
```

alrt-min

Use this command to configure hardware alert temperature threshold minimum value.

Use `no` parameter to remove the replace the configured alert temperature minimum value to default threshold value.

Command Syntax

```
alrt-min <-50-150>
no alrt-min
```

Parameters

`<-50-150>`	Specifies the alert Temperature-threshold minimum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the alert temperature sensor's minimum threshold value, execute:

```
OcNOS(config-temperature-threshold)#alrt-min 11
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no alrt-min
```

crit-max

Use this command to configure hardware critical temperature threshold maximum value.

Use `no` parameter to remove the replace the configured critical temperature maximum value to default threshold value.

Command Syntax

```
crit-max <-50-150>
no crit-max
```

Parameters

`<-50-150>`	Specifies the critical Temperature-threshold maximum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the critical temperature sensor's maximum threshold value, execute:

```
OcNOS(config-temperature-threshold)#crit-max 69
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no crit-max
```

crit-min

Use this command to configure hardware critical temperature threshold minimum value.

Use `no` parameter to remove the replace the configured critical temperature minimum value to default threshold value.

Command Syntax

```
crit-min <-50-150>
no crit-min
```

Parameters

`<-50-150>`	Specifies the critical Temperature-threshold minimum range value.

Default

None

Command Mode

Temperature-threshold

Applicability

Introduced in OcNOS version 6.5.3.

Example

To configure the hardware device temperature threshold value, execute:

```
OcNOS(config)#temperature threshold 2
OcNOS(config-temperature-threshold)#
```

The mode changes, to configure the critical temperature sensor's minimum threshold value, execute:

```
OcNOS(config-temperature-threshold)#crit-min 15
```

The hardware threshold is over-written with user configured threshold. To unconfigure the user defined threshold values, execute:

```
OcNOS(config-temperature-threshold)#no crit-min
```

temperature policy (sys-reboot | sys-halt | none)

Use this command to configure the temperature policy.

Use `no` parameter to remove the configured temperature policy.

Command Syntax

```
temperature policy (sys-reboot | sys-halt | none)
no temperature policy
```

Parameters

`none`	None
`sys-halt`	System halt
`sys-reboot`	System reboot

Default

None

Command Mode

Configuration Mode

Applicability

Introduced in OcNOS version 6.5.3.

Example

Execute the following command to apply the temperature policy and reboot the system.

```
(config)#temperature policy sys-reboot
(config)#commit
(config)#no temperature policy
(config)#commit
```

Glossary

Key Terms/Acronym	Description
BMC	Baseboard Management Controller
NOS	Network Operating System

CHAPTER 3 Digital Diagnostic Monitoring Commands

This chapter is a reference for Digital Diagnostic Monitoring (DDM) commands:

- clear ddm transceiver alarm
- clear ddm transceiver alarm all
- ddm monitor
- ddm monitor all
- ddm monitor interval
- debug ddm
- service unsupported-transceiver
- show controller details
- show interface frequency grid
- show interface transceiver details
- show supported-transceiver
- tx-disable
- wavelength

clear ddm transceiver alarm

Use this command to clear the transceiver alarm in the DDM monitor interface.

Command Syntax

```
clear ddm transceiver alarm
```

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#clear ddm transceiver alarm
(config-if)#exit
```

clear ddm transceiver alarm all

Use this command to clear the transceiver DDM alarm for all interface.

Command Syntax

clear ddm transceiver alarm all

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
# clear ddm transceiver alarm all
```

ddm monitor

Use this command to enable or disable DDM monitoring for interfaces which have a supported transceiver.

Use the `no` form of this command to remove DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor (disable|enable)
no ddm monitor
```

Parameters

`enable`	Enable DDM monitoring.
`disable`	Disable DDM monitoring.

Default

By default, DDM monitoring is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ddm monitor enable
(config-if)#ddm monitor disable
(config-if)#exit

(config)#interface xe1
(config-if)#no ddm monitor
(config-if)#exit
```

ddm monitor all

Use this command to enable DDM monitoring for all transceiver.s

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax

```
ddm monitor all
```

```
no ddm monitor all
```

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor all

(config)#no ddm monitor all
```

ddm monitor interval

Use this command to set the monitoring interval for the transceiver.

Use no form with this command to set the monitoring interval to its default.

Command Syntax

```
ddm monitor interval <60-3600>
no ddm monitor interval
```

Parameters

<60-3600>	Interval period in seconds.

Default

The default monitoring interval is 60 seconds.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ddm monitor interval 60
```

debug ddm

Use this command to enable or disable debugging for DDM.

Command Syntax

```
debug ddm
no debug ddm
```

Parameters

None

Default

By default, debug command is not configured.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#debug ddm
(config)#no debug ddm
```

service unsupported-transceiver

Use this command to allow an unsupported transceiver to be enabled for DDM monitoring.

Use the `no` form of this command to disable DDM on an unsupported transceiver.

Command Syntax

```
service unsupported-transceiver
no service unsupported-transceiver
```

Parameters

None

Default

By default, DDM on an unsupported transceiver is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service unsupported-transceiver

(config)#no service unsupported-transceiver
```

show controller details

Use this command to display the EEPROM details of transceivers.

Command Syntax

```
show interface (IFNAME|) controllers
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe52/1 controllers
Port Number              : 52
Vendor oui               : 0x0 0x17 0x6a
Vendor name              : AVAGO
Vendor part_no           : AFBR-79E4Z
serial_number            : QB380161
transceiver_type         : QSFP OR LATER
connector_type           : MPO 1x12
qsfp_transceiver_code    : 1X-LX
vendor_rev               : 01
date_code                : 110920    (yymmddvv, v=vendor specific)
encoding                 : SONET
br_nominal               : 103       (100 MHz)
length_km                : 0
length_mtr               : 50
length_50mt              : 0
length_62_5mt            : 0
length_cu                : 0
cc_base                  : 0x7d
cc_ext                   : 0x28
DDM Support              : yes
```

show interface frequency grid

Use this command to display channel-number and wavelength mapping.

Command Syntax

```
show interface (IFNAME) frequency-grid
```

Parameters

IFNAME	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 4.1.

Example

```
#show interface xe7 frequency-grid
-----------------------------------------------------
Channel Number  Frequency (THz) Wavelength (nm)
-----------------------------------------------------
1         191.40          1566.314
2         191.50          1565.496
3         191.60          1564.679
4         191.70          1563.862
5         191.80          1563.047
6         191.90          1562.233
7         192.00          1561.419
8         192.10          1560.606
9         192.20          1559.794
10        192.30          1558.983
11        192.40          1558.172
12        192.50          1557.363
13        192.60          1556.554
14        192.70          1555.746
15        192.80          1554.939
16        192.90          1554.133
17        193.00          1553.328
18        193.10          1552.524
19        193.20          1551.720
20        193.30          1550.917
21        193.40          1550.115
22        193.50          1549.314
23        193.60          1548.514
24        193.70          1547.714
25        193.80          1546.916*
26        193.90          1546.118
27        194.00          1545.321
```

```
28        194.10          1544.525
29        194.20          1543.729
30        194.30          1542.934
31        194.40          1542.141
32        194.50          1541.348
33        194.60          1540.556
34        194.70          1539.765
35        194.80          1538.974
36        194.90          1538.184
37        195.00          1537.396
38        195.10          1536.607
39        195.20          1535.820
40        195.30          1535.034
41        195.40          1534.248
42        195.50          1533.463
43        195.60          1532.679
44        195.70          1531.896
45        195.80          1531.114
46        195.90          1530.332
47        196.00          1529.551
48        196.10          1528.771
#
```

show interface transceiver details

Use this command to display details of transceivers and threshold violations.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|)
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
detail	Transceiver information such as voltage, temperature, power, and current.
threshold violation	Transceiver threshold violations.
Codes	* Not Qualified By IP Infusion, ** Not Supported By Module.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
OcNOS#sh int transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable


Intf       DDM        Temp       AlertMax   CritMax    CritMin    AlertMin
                      (Celsius)  (Celsius)  (Celsius)  (Celsius)  (Celsius)
-------------------------------------------------------------------------


ce0        Active*    +22.52     +85.00     +80.00     -5.00      -10.00
ce2        Active     +20.32     +75.00     +70.00     +0.00      -5.00
xe4        Active*    +23.62     +95.00     +85.00     -40.00     -50.00
xe5        Active*    +19.79     +100.00    +95.00     -35.00     -40.00
xe16       Active*    +25.84     +95.00     +85.00     -10.00     -50.00
xe26       Active     +19.01     +95.00     +90.00     -20.00     -25.00


Intf       DDM        Volt       AlertMax   CritMax    CritMin    AlertMin
                      (Volts)    (Volts)    (Volts)    (Volts)    (Volts)
-------------------------------------------------------------------------
ce0        Active*    +3.314     +3.600     +3.500     +3.100     +2.900
```

```
ce2         Active     +3.260     +3.630     +3.465     +3.135     +2.970
xe4         Active*    +3.260     +3.600     +3.500     +3.100     +3.000
xe5         Active*    +3.253     +3.600     +3.500     +2.900     +2.800
xe16        Active*    +3.284     +3.630     +3.500     +3.030     +2.930
xe26        Active     +3.289     +3.900     +3.700     +2.900     +2.700



Intf        DDM        Lane       Curr       AlertMax   CritMax    CritMin
AlertMin
                                  (mA)       (mA)       (mA)       (mA)
(mA)
-------------------------------------------------------------------------------
-------
ce0         Active*    1          +6.114     +15.000    +12.000    +2.000
+0.000
                       2          +6.120     +15.000    +12.000    +2.000
+0.000
                       3          +6.110     +15.000    +12.000    +2.000
+0.000
                       4          +6.116     +15.000    +12.000    +2.000
+0.000
ce2         Active     1          +7.464     +13.000    +11.000    +5.000
+3.000
                       2          +7.540     +13.000    +11.000    +5.000
+3.000
                       3          +7.444     +13.000    +11.000    +5.000
+3.000
                       4          +7.474     +13.000    +11.000    +5.000
+3.000
xe4         Active*    -          +6.100     +110.000   +100.000   +1.000
+1.000
xe5         Active*    -          +7.552     +15.000    +13.000    +2.000
+1.000
xe16        Active*    -          +5.800     +15.000    +12.000    +3.000
+2.000
xe26        Active     -          +7.050     +17.000    +14.000    +2.000
+1.000



Intf        DDM        Lane       RxPwr      AlertMax   CritMax    CritMin
AlertMin
                                  (dBm)      (dBm)      (dBm)      (dBm)
(dBm)
-------------------------------------------------------------------------------
-------
ce0         Active*    1          -0.185     +4.400     +3.400     -13.298    -
14.306
                       2          +0.342     +4.400     +3.400     -13.298    -
14.306
                       3          +0.396     +4.400     +3.400     -13.298    -
14.306
                       4          -2.927     +4.400     +3.400     -13.298    -
14.306
ce2         Active     1          +1.302     +3.400     +2.400     -11.002    -
14.001
                       2          +1.486     +3.400     +2.400     -11.002    -
14.001
```

```
                        3          +1.581     +3.400     +2.400     -11.002    -
14.001
                        4          +1.594     +3.400     +2.400     -11.002    -
14.001
xe4         Active*     -          -1.890     +2.500     +0.500     -14.401    -
16.402
xe5         Active*     -          -40.000    +3.000     +0.000     -13.002    -
16.003
xe16        Active*     -            --       +2.000     +1.000     -14.401    -
16.402
xe26        Active      -          -5.933     +1.000     -1.002     -18.013    -
20.000


Intf        DDM         Lane       TxPwr      AlertMax   CritMax    CritMin
AlertMin
                                   (dBm)      (dBm)      (dBm)      (dBm)
(dBm)
-------------------------------------------------------------------------------
-------
ce0         Active*     1          -0.085     +4.400     +3.400     -9.201     -
10.205
                        2          -0.161     +4.400     +3.400     -9.201     -
10.205
                        3          +0.217     +4.400     +3.400     -9.201     -
10.205
                        4          +0.204     +4.400     +3.400     -9.201     -
10.205
ce2         Active      1          +0.297     +5.000     +3.000     -8.000     -
10.000
                        2          -0.078     +5.000     +3.000     -8.000     -
10.000
                        3          +0.131     +5.000     +3.000     -8.000     -
10.000
                        4          +0.323     +5.000     +3.000     -8.000     -
10.000
xe4         Active*     -          -1.316     +2.500     +0.500     -8.199     -
10.200
xe5         Active*     -          -2.299     +1.000     +0.000     -7.001     -
8.000
xe16        Active*     -          -1.000     +2.500     +2.000     -8.199     -
10.200
xe26        Active      -          -4.441     -2.000     -2.000     -11.024    -
11.739

Intf        DDM         Lane       Freq-Err   AlertMax   CritMax    CritMin
AlertMin
                                   (GHz)      (GHz)      (GHz)      (GHz)
(GHz)
-------------------------------------------------------------------------------
-------

Intf        DDM         Lane       Wave-Err   AlertMax   CritMax    CritMin
AlertMin
                                   (nm)       (nm)       (nm)       (nm)
(nm)
-------------------------------------------------------------------------------
-------

Intf        DDM         Lane       Tx         Rx-LOS     Tx-LOS
-------------------------------------------------------------------------------
```

```
ce0         Active*     1           On          Off         Off
                        2           On          Off         Off
                        3           On          Off         Off
                        4           On          Off         Off
ce2         Active      1           On          Off         Off
                        2           On          Off         Off
                        3           On          Off         Off
                        4           On          Off         Off
xe4         Active*     -           On          Off         -
xe5         Active*     -           On          On          -
xe9         Inactive*   -           On          On          -
xe11        Inactive*   -           On          On          -
xe13        Inactive*   -           On          On          -
xe14        Inactive*   -           On          On          -
xe16        Active*     -           On          On          -
xe26        Active      -           On          Off
```

Table 3-20 explains the output fields.

Table 3-20: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliamperes used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.
Codes *	Not Qualified By IP Infusion, ** Not Supported By Module

show supported-transceiver

Use this command to display supported transceivers.

Command Syntax

```
show supported-transceiver
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show supported-transceiver
-----------------------------------------------------
          Transceiver DDM support list
-----------------------------------------------------
Type                        :SFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTLF8519P2BNL
DDM Supported               :Yes

Type                        :SFP
Vendor Name                 :EVERTZ
Vendor Part Number          :SFP10G-TR13S
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes
```

tx-disable

Use this command to disable the transceiver tx-power (disable laser).

Use the `no` form of this command to enable tx-power (enable laser).

Command Syntax

```
tx-disable
no tx-disable
```

Default

By default, `tx-disable` is false.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.2.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#tx-disable
(config-if)#exit

(config)#interface xe1
(config-if)#no tx-disable
(config-if)#exit
```

wavelength

Use this command to set the transceiver wavelength using the channel-number or the wavelength for interfaces having a supported transceiver.

Use the no form of this command to remove the wavelength configuration.

Command Syntax

```
wavelength ((channel-number <1-96>) | (update <1528773-1566723>))
```

Parameters

`channel-number`	Sets wavelength corresponding to the channel number
`update`	Sets wavelength value

Default

By default, the interface comes up with a random wavelength chosen by autotuning.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 4.1.

Example

```
(config)#int xe7
(config-if)#wavelength channel-number 10
(config-if)#no wavelength
(config-if)#

(config-if)#wavelength update 1528773
(config-if)#no wavelength
(config-if)#
```

Link Configuration Guide

CHAPTER 1 Trigger Failover Configuration

This chapter contains Trigger Failover (TFO) configuration examples.

This example shows the complete configuration to enable TFO in a simple network topology. TFO complements NIC teaming functionality supported on blade servers. TFO allows a switch module to monitor specific uplink ports to detect link failures. When the switch module detects a link failure, it disables the corresponding downlink ports automatically.

TFO uses these components:

- A Fail Over Group (FOG) contains a Monitor Port Group (MPG) and a Control Port Group (CPG).
- An MPG contains only uplink ports.
- A CPG contains only downlink ports.

Note:

- TFO is supported in STP, RSTP, and MSTP bridge modes but not in RPVST+ bridge mode.
- For MSTP, failure notifications rely on the PHY down state.
- For STP and RSTP, the failure notifications rely on the STP port state and are triggered on encountering blocked state.
- Can configure TFO on a LAG interface.

Basic Configuration

Figure 1-3: Basic topology

Switch

`#configure terminal`	Enter configure mode.
`(config)#tfo enable`	Enable TFO globally.
`(config)#fog 1 enable`	Create a Fail over group (FOG) and enable it.
`(config)#interface xe35`	Enter interface mode
`(config-if)#link-type uplink`	Specify the link-type as Uplink.
`(config-if)#fog 1 type mpg`	Specify the MPG member for FOG 1.
`(config-if)#fog 1 type cpg`	Specify the CPG member for FOG 1.
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface xe34`	Enter interface mode
`(config-if)#link-type downlink`	Specify the link-type as Downlink.

© 2025 IP Infusion Inc. Proprietary

(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#end	Exit interface and configure mode

Validation

```
OcNOS#show tfo

TFO : Enable

Failover Group 1 : Enable
No. of links to trigger failover : 0
MPG Port : po1
CPG Port : po1
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
OcNOS#

interface po1
port-channel load-balance src-dst-ip
link-type uplink
fog 1 type mpg
fog 1 type cpg
!
```

Port-Channel Configuration

Topology

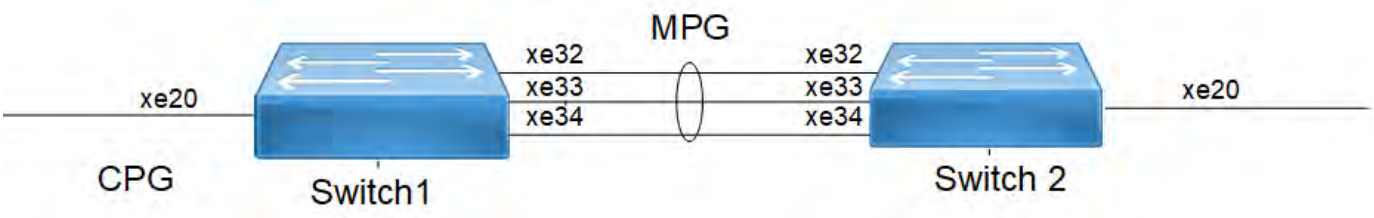


Figure 1-4: TFO with port-channel

Switch 1

#configure terminal	Enter configure mode.
(config)#tfo enable	Enable TFO globally.
(config)#fog 1 enable	Create a Fail over group (FOG) and enable it.
(config)#interface po1	Enter interface mode

(config-if)#switchport	Make the interface Layer2.
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe20	Enter interface mode
(config-if)#link-type downlink	Specify the link-type as Downlink.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface po1	Enter port-channel mode
(config-if)#link-type uplink	Specify the link-type as Uplink.
(config-if)#fog 1 type mpg	Specify the MPG member for FOG 1.
(config-if)#fog 1 type cpg	Specify the CPG member for FOG 1.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#end	Exit interface and configure mode

Switch 2

#configure terminal	Enter configure mode.
(config)#interface po1	Enter interface mode

(config-if)#switchport	Make the interface as Layer2.
(config-if)#exit	Exit interface mode
(config-if)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe32	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config-if)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe33	Enter interface mode
(config-if)#switchport	Make the interface as Layer2.
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe34	Enter interface mode
(config-if)#switchport	Make the interface as Layer2
(config-if)#channel-group 1 mode active	Specify the channel group in interface
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration

Validation

```
#show interface brief | include up
xe20        ETH   --    --                up      none    10g   --
xe32        ETH   --    --                up      none    10g   --
xe33        ETH   --    --                up      none    10g   --
xe34        ETH   --    --                up      none    10g   --
eth0          METH             up      --      100m
lo                                                 up          --
lo.management                                      up          --


#show tfo

TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
po1   Status : DOWN
CPG Port :
xe20   Status : DOWN
No. of times MPG link failure : 0
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 0
No. of times CPG got auto enable : 0
```

CHAPTER 2 Link Detection Debounce Timer

The link debounce timer avoids frequent updates (churn) to higher layer protocols during flapping of an interface. The initial link state is UP. The link goes DOWN. If the Link comes UP and goes DOWN, The link DOWN AND link UP timer is started and being restarted on each flap (link comes up and goes down again). For each link DOWN, link down timer will start and it restarts on flap within the link debounce interval. For each link UP, link up timer will start and it restarts on flap within the link debounce interval

Note: Keep the following in mind when using the Link detection debounce timer:

- Link debounce timer is supported only for physical L2 and L3 interfaces.
- When debounce timer is configured we won't be able to configure the link-debounce-timer config and viceversa.
- The link debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the link debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to minimum of 1.5 times the value of the link-debounce time. Otherwise it could affect the protocol states if the link debounce timer is still running.
- Protocols such as PO, OSPF, BFD, ISIS, BGP which depends on the link status, in this case we should ensure on both the connected interfaces we need to configure the link-debounce timer.
- The debounce timer must be configured on both ends of the network link.
- Enabling the debounce timer delays the detection of link up and down status, resulting in traffic loss during that period and impacting the convergence of some protocols.

Topology

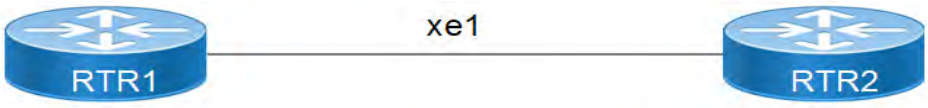


Figure 2-5: Link detection debounce timer topology

Configuration

RTR1

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode
`(config-if)#link-debounce-time 4000 5000`	Configure link-debounce-time where link-up timer is 4000 ms and link-down timer is 5000 ms
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode

RTR2

`#configure terminal`	Enter configure mode.
`(config)#interface xe1`	Enter interface mode
`(config-if)#link-debounce-time 4000 5000`	Configure link-debounce-time where link-up timer is 4000 ms and link-down timer is 5000 ms
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#exit`	Exit interface mode

Validation

```
#show interface xe1 | i Debounce Link Debounce timer: enable
    Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
    Linkup Debounce status : idle
    Linkdown Debounce status : idle
```

RTR1 and RTR2 outputs after interface flap:

```
#show interface xe1 | i debounce Link Debounce timer: enable
Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
Flap Count: 1
Last Debounce Flap :
Linkup Debounce status : idle
Linkdown Debounce status : idle

#show interface xe1 | i debounce
  Link Debounce timer: enable
    Linkup Debounce time 4000 ms Linkdown Debounce time 5000 ms
    Flap Count: 1
    Last Debounce Flap :    Linkup Debounce status : idle
 Linkdown Debounce status : idle
```

Log Messages

The following is a configuration example to log link debounce timer activity

:

`#configure terminal`	Enter Configure mode
`(config)#logging level nsm 7`	Enable operational log to display debounce start and end.

Example Log Messages

```
2019 Feb 28 02:50:40.761 : OcNOS : NSM : INFO : Start UP->DOWN Link Debounce Timer on interface xe1
2019 Feb 28 02:50:40.761 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1 changed state from up to down
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Start DOWN->UP Link Debounce Timer on interface xe1
2019 Feb 28 02:50:43.543 : OcNOS : NSM : INFO : Interface xe1 Flapped, prev_state DOWN new_state UP,flap count 1
```

```
2019 Feb 28 02:50:43.543 : OcNOS : NSM : NOTIF : [DEBOUNCE_EVENT_4]: Interface xe1
changed state from down to up
2019 Feb 28 02:50:45.761 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition up->down), prev_state UP, new_state UP

2019 Feb 28 02:50:47.544 : OcNOS : NSM : INFO : Link Debounce Timer Expired on interface
xe1 (initiated transition down->up), prev_state UP, new_state UP
```

Link Command Reference

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 Trigger Failover Commands

This chapter describes the trigger failover (TFO) commands.

- clear tfo counter
- fog
- fog tfc
- fog type
- link-type
- show tfo
- tfo

clear tfo counter

Use this command to clear the TFO counters. If you do not specify a parameter, this command clears counters for all FOG indexes.

Command Syntax

```
clear tfo counter
clear tfo counter fog <1-64>
```

Parameters

<1-64>	Clear counters for this Failover Group Index

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear tfo counter
```

fog

Use this command to:

- Create or delete a failover group (FOG)
- Enable or disable an exisitng FOG

Even if FOG index do not exit, FOG can be created as enabled with “enable” option in CLI.

If the FOG index already exists:

- When the FOG status is disabled and Control Port Group (CPG) links are previously disabled (because of TFO), then the links are enabled. If a particular CPG member belongs to multiple CPGs, then this CPG member is enabled only if all corresponding Monitor Port Groups (MPG) are enabled.
- When the FOG status is enabled and MPG is down, then the corresponding CPG links are disabled.

Use the `no` form of this command to delete a FOG.

Command Syntax

```
fog <1-64> (enable|disable)
no fog <1-64>
```

Parameters

`<1-64>`	Failover Group Index
`enable`	Enable Failover Group
`disable`	Disable Failover Group

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#fog 5 enable
```

fog tfc

Use this command to set the number of links to trigger failover for a Monitor Port Groups (MPG).

Use the no form of this command to remove the configuration and use default value of 0.

Command Syntax

```
fog <1-64> tfc <0-63>
no fog <1-64> tfc
```

Parameters

<1-64>	Failover Group index
<0-63>	Trigger failover count

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3. The no version of the command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#fog 5 tfc 7
(config)# no fog 5 tfc
```

fog type

Use this command to map upstream/downstream links in a FOG as a Monitor Port Group (MPG) or Control Port Group (CPG).

Use the `no` form of this command to unmap upstream/downstream links.

Command Syntax

```
fog <1-64> type (mpg|cpg)
no fog <1-64> type (mpg|cpg)
```

Parameters

`<1-64>`	Failover Group Index
`mpg`	Map the interface to an MPG
`cpg`	Map the interface to a CPG

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#fog 5 type mpg
```

link-type

Use this command to make a port an uplink or downlink.

Use the `no` form of this command to remove the configuration.

Command Syntax

```
link-type (uplink|downlink)
no link-type
```

Parameters

`uplink`	Make the port an uplink
`downlink`	Make the port a downlink

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#interface eth1
(config-if)#link-type downlink
```

show tfo

Use this command to display FOG configuration and statistics.

Command Syntax

```
show tfo
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tfo

TFO : Enable

Failover Group 1 : Enable
Failover Status : MPG Link Failure
No. of links to trigger failover : 0
MPG Port(s) :
xe9   Status : DOWN
xe12   Status : DOWN
CPG Port :
xe4   Status : DOWN
No. of times MPG link failure : 1
No. of times MPG link recovered : 0
No. of times CPG got auto disabled : 1
No. of times CPG got auto enable : 0
```

Table 1-21 Explains the show command output fields.

Table 1-21: show tfo output fields

Field	Description
Failover Group	Enable the failover group.
Failover Status	Display the failover status.
No. of links to trigger failover	Number of links to trigger the failover group.

Field	Description
MPG Port	Details of the monitor port group.
CPG Port	Details of the control port group.

tfo

Use this command to enable or disable trigger failover (TFO).

Command Syntax

```
tfo (enable|disable)
```

Parameters

`enable`	Enables Trigger failover
`disable`	Disables Trigger failover

Default

By default, TFO is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#tfo enable
```

QSFP-DD Configuration Guide

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 QSFP-DD Configuration

Overview

QSFP-DD is a new module developed but with the same form factor as the current QSFP, to support high-speed solutions. It provides eight lanes electrical interface. Each lane can operate up to 25Gbps NRZ modulation or 50Gbps PAM4 modulation. QSFP modules are designed to be backward compatible with the existing QSFP modules.

System Description

Basically, the system will be developed to support 400Gbps data transmission. This will enable us to support the high-speed solution. The management interface will be used to get the status and control of the module.

CMIS modules have two physical interfaces for signal transmission:

Host Interface (Device to device interconnection)

The host interface is the high-speed electrical interface between the module and the host system. The host interface carries signals traveling from host to module (transmitter input signals) and signals traveling from module to host (receiver output signals). All electrical signals carried over the host interface are transmitted over the wire pairs, each of which is called host lanes.

Media Interface (Device to media interconnection)

The media interface is the high-speed electrical/optical interface between the module and the interconnecting media. The media interface carries signals that travel from module to media (transmitter output signals) and signals that travel from media to module (receiver input signals). Media interface signals are carried either over electrical wire pairs (Copper cables) or over optical wavelengths on physical fibers, which are called media lanes.

Objectives

The objective of this document is to provide a high-speed solution using QSFP-DD. The management characteristics, status, and control of QSFP-DD.

Topology

Figure 1-6: QSFP-DD Sample Topology

Loopback

Use this command to configure the loopback type (input, output, both) on the QSFP-DD module host/media side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

Media Input Loopback

Use this command to configure the input loopback type on the QSFP-DD module media side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)# qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback in media`	Configure input media Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Media Input Loopback

```
OcNOS#show qsfp-dd 0 diagnostics media loopback

Port Number                    : 0

------------------------------
  User Config  |  H/W Config  |
------------------------------
 Input         | Input        |
```

Media Output Loopback

Use this command to configure the output loopback type on the QSFP-DD module media side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback out media`	Configure output media Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Media Output Loopback

```
OcNOS#show qsfp-dd 0 diagnostics media loopback

Port Number                    : 0

------------------------------
```

```
  User Config   |  H/W Config   |
-------------------------------
 Output          | Output        |
```

Media Both Loopback

Use this command to configure the both loopback type on the QSFP-DD module media side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback both media`	Configure both input & output media Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Media Both Loopback

```
OcNOS#show qsfp-dd 0 diagnostics media loopback

Port Number                    : 0

-------------------------------
  User Config   |  H/W Config   |
-------------------------------
 Input/Output          | Input/Output      |
```

Host Input Loopback

Use this command to configure the input loopback type on the QSFP-DD module host side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback in host`	Configure input host Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Host Input Loopback

```
OcNOS#show qsfp-dd 0 diagnostics Host loopback

Port Number                    : 0

-------------------------------
  User Config   |  H/W Config   |
-------------------------------
```

```
 Input          | Input         |
```

Host Output Loopback

Use this command to configure the output loopback type on the QSFP-DD module host side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback out host`	Configure output host Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Host Output Loopback

```
OcNOS#show qsfp-dd 0 diagnostics host loopback

Port Number                    : 0

-------------------------------
  User Config  |  H/W Config  |
-------------------------------
 Output          | Output       |
```

Host Both Loopback

Use this command to configure the both loopback type on the QSFP-DD module Host side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 0`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#loopback both host`	Configure both input & output host Loopback.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation of Host Both Loopback

```
OcNOS#show qsfp-dd 0 diagnostics Host loopback

Port Number                    : 0

-------------------------------
  User Config  |  H/W Config  |
-------------------------------
Input/Output        | Input/Output       |
```

PRBS

Use these commands to configure the PRBS pattern generator/checker type to be used for diagnostics of the QSFP-DD module host/media side and to configure the PRBS pattern generator/checker location (pre-fec/post-fec) on the QSFP-DD module host/media side. If the generator/checker pattern type and location are supported by the QSFP-DD module this will enable the selected function.

Use the no parameter to remove this configuration and disable the generator/checker function.

PRBS Host Checker & Generator

ROUTER1 (checker)

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#prbs checker type 15 host`	Configure PRBS checker type.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

ROUTER2 (generator)

`ROUTER2#configure terminal`	Enter configure mode.
`ROUTER2(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER2(config-qsfp-dd)#prbs generator type 15 host`	Configure PRBS generator type.
`ROUTER2(config-qsfp-dd)#commit`	Commit the configuration.

Validation

ROUTER1

```
OcNOS#show qsfp-dd 3 diagnostics host prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
```

```
 PRBS-15     | PRBS-15    |

-------------------------------------
               Generator
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |

-------------------------------------
                Checker
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Active   |
```

ROUTER2

```
OcNOS#show qsfp-dd 3 diagnostics host prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 PRBS-15     | PRBS-15    |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

-------------------------------------
               Generator
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Active   |

-------------------------------------
                Checker
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |
```

Unconfigure PRBS Host Checker & Generator

ROUTER1 (checker)

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 3	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#no prbs checker type host	Unconfigure PRBS checker type.
ROUTER1(config-qsfp-dd)#commit	Commit the configuration.
ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 3	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#no prbs generator type host	Unconfigure PRBS generator type.
ROUTER1(config-qsfp-dd)#commit	Commit the configuration.

Validation

ROUTER1

```
OcNOS#show qsfp-dd 3 diagnostics host prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

--------------------------------------
               Generator
--------------------------------------
 User Config | H/W Config |  Status  |
--------------------------------------
 None        | Pre-FEC    | Inactive |

--------------------------------------
                Checker
--------------------------------------
 User Config | H/W Config |  Status  |
```

```
-------------------------------------
 None        | Pre-FEC    | Inactive |
```

ROUTER2

```
OcNOS#show qsfp-dd 3 diagnostics host prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

-------------------------------------
               Generator
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |

-------------------------------------
                Checker
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |
```

PRBS Media Checker & Generator

ROUTER1 (checker)

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#prbs checker type 15 media`	Configure PRBS checker type.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

ROUTER2 (generator)

`ROUTER2#configure terminal`	Enter configure mode.
`ROUTER2(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER2(config-qsfp-dd)#prbs generator type 15 media`	Configure PRBS generator type.
`ROUTER2(config-qsfp-dd)#commit`	Commit the configuration.

Validation

ROUTER1

```
OcNOS#show qsfp-dd 3 diagnostics media prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 PRBS-15     | PRBS-15    |

-------------------------------------
               Generator
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |

-------------------------------------
                Checker
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Active   |
```

ROUTER2

```
OcNOS#show qsfp-dd 3 diagnostics media prbs

Port Number                    : 3
```

```
---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 PRBS-15     | PRBS-15    |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

--------------------------------------
               Generator
--------------------------------------
 User Config | H/W Config |  Status  |
--------------------------------------
 None        | Pre-FEC    | Active   |

--------------------------------------
                Checker
--------------------------------------
 User Config | H/W Config |  Status  |
--------------------------------------
 None        | Pre-FEC    | Inactive |
```

Unconfigure PRBS Media Checker & Generator

ROUTER1 (checker)

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#no prbs checker type media`	Unconfigure PRBS checker type.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.
`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 3`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#no prbs generator type media`	Unconfigure PRBS generator type.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation

ROUTER1

```
OcNOS#show qsfp-dd 3 diagnostics media prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

---------------------------
        Checker Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |

--------------------------------------
               Generator
--------------------------------------
 User Config | H/W Config |  Status  |
--------------------------------------
 None        | Pre-FEC    | Inactive |

--------------------------------------
                Checker
--------------------------------------
 User Config | H/W Config |  Status  |
--------------------------------------
 None        | Pre-FEC    | Inactive |
```

ROUTER2

```
OcNOS#show qsfp-dd 3 diagnostics media prbs

Port Number                    : 3

---------------------------
       Generator Type
---------------------------
 User Config | H/W Config |
---------------------------
 None        | PRBS-31Q   |
```

```
--------------------------
        Checker Type
--------------------------
 User Config | H/W Config |
--------------------------
 None        | PRBS-31Q   |

-------------------------------------
               Generator
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |

-------------------------------------
                Checker
-------------------------------------
 User Config | H/W Config |  Status  |
-------------------------------------
 None        | Pre-FEC    | Inactive |
```

EEPROM Details for a ZR+ Optics

Note: The below show command has output for "**SO-TQSFPDD4CCZRP**" optics.

```
#show qsfp-dd 3 eeprom

Port Number                   : 3
Identifier                    : QSFP-DD Double Density 8X Pluggable Transceiver
Name                          : SmartOptics
OUI                           : 0x0 0x53 0x4f
Part No                       : SO-TQSFPDD4CCZRP
Revision Level                : A
Serial_Number                 : 223950575
Manufacturing Date            : 220926   (yymmddvv, v=vendor specific)
Module Power Class            : 8
Module Max Power              : 23.75 Watt
Cooling Implemented           : Yes
Module Temperature Max        : 80 Celsius
Module Temperature Min        : 0 Celsius
Operating Voltage Min         : 3.12 Volt
Optical Detector              : PIN
Rx Power Measurement          : Average Power
Tx Disable Module Wide        : No
Cable Assembly Link Length    : Separable Media
Connector Type                : LC (Lucent Connector)
Media Interface Technology    : 1550 nm DFB
CMIS Revision                 : 4.1
Memory Model                  : Paged
MCI Max Speed                 : 1000 kHz
Active Firmware Revision      : 61.20
```

```
Inactive Firmware Revision    : 61.20
Hardware Revision             : 1.2
Media Type                    : Optical SMF
Max SMF Link Length           : 630.0 Kilometer
Wavelength Nominal            : 1547.70 nm
Wavelength Tolerance          : 166.55 nm
```

Application

Use this command to select the application ID to be configured for this QSFP-DD module.

Note: Only 400G application modes are supported.

Note: For checking the supported applications modes `show qsfp-dd <port no.> advertisement applications` command.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)# qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#application 2`	Select the application ID to be configured for this QSFP-DD module
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation

```
OcNOS#sh qsfp-dd 49 application

Port Number                     : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 2  |   Application 2

OcNOS#sh qsfp-dd 49 advertisement applications

Port Number                   : 49
> Application 1:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2.000000
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, DWDM, Amplified
         Application BR       : 478.75
```

```
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 2:
  | Host |
        Interface            : 400GAUI-8 C2M
        Application BR       : 425.00
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
  | Media |
        Interface            : 400ZR, Single Wavelen., Unamp.
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 3:
  | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
        Interface            : 400ZR, DWDM, Amplified
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 4:
  | Host |
        Interface            : 400GAUI-8 C2M
        Application BR       : 425.00
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
  | Media |
        Interface            : ZR400-OFEC-16QAM
```

```
        Application BR       : 481.108374
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 5:
  | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
        Interface            : ZR400-OFEC-16QAM
        Application BR       : 481.108374
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 6:
  | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
        Interface            : ZR300-OFEC-8QAM
        Application BR       : 360.831281
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-8QAM
        Bits Per Unit Intvl  : 6.000000
        Lane Assigned        : Lane-1
Application 7:
  | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
```

```
        Interface            : ZR200-OFEC-QPSK
        Application BR       : 240.554187
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
  Application 8:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR100-OFEC-QPSK
        Application BR       : 120.277094
        Lane Count           : 1
        Lane Sig BR          : 30.069273
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
```

Custom Application

Custom Application feature provides support to extend the current limitation of 15 applications imposed by the Common Management Interface Specification (CMIS) standard. The transceiver vendor provides support for the additional applications as a customized CMIS extension and in order to provide access to this custom extension the following new CLIs are introduced:

`custom-app-host-id <1-32>`

`custom-app-media-id <1-32>`

Note: Use `show qsfp-dd <port no> advertisement applications custom` CLI to view the supported custom applications mode.

Configurations

Perform the following configurations to configure QSFP DD custom application on the router.

1. Enter the config mode and configure the QSFP DD.

```
#configure terminal
(config)# qsfp-dd 0
```

2. Select the Custom application ID to be configured for this QSFP-DD module.

```
(config-qsfp-dd)#application 15
(config-qsfp-dd)# custom-app-host-id 1
(config-qsfp-dd)# custom-app-media-id 2
(config-qsfp-dd)#commit
```

Validation

```
Port Number                          : 0
----------------------------------------
              | User Config | H/W Config
----------------------------------------
 Application  | 15 (custom) | 15 (custom)
 Host ID      | 1           | 1
 Media ID     | 2           | 2
```

Implementation Examples

1. Media interface ID bandwidth should be compatible with the host interface ID bandwidth requirements.

   a. Example of valid combinations:

   ```
   400GAUI-8 <--> ZR400-OFEC-16QAM ==> (1x400G breakout)
   200GAUI-4 <--> PKT-MAX-200G-SFEC-60 ==> (1x200G breakout)
   100GAUI-2 <--> OTN-STD-100G-OFEC-31 ==> (1x100G breakout)
   100GAUI-4 <--> ZR400-OFEC-16QAM ==> (4x100G breakout)
   ```

   b. Example of invalid combinations:

   ```
   400GAUI-8 <--> PKT-MAX-200G-SFEC-60
   200GAUI-4 <--> OTN-STD-100G-OFEC-31
   ```

2. When host interface ID bandwidth is lower than media interface ID bandwidth, for some cases only one breakout interface is possible

   a. Example of valid combinations:

   ```
   100GAUI-2 <--> ZR400-OFEC-16QAM ==> (4x100G breakout is possible)
   100GAUI-2 <--> PKT-MAX-200G-SFEC-60 ==> (2x100G breakout is possible)
   100CAUI-4 <--> ZR400-OFEC-16QAM ==> (2x100G breakout is possible. Only 2
   interfaces because CAUI-4 uses 4 lanes and only 8 lanes are physically
   available).
   ```

   b. Example of invalid combinations:

   ```
   200GAUI-4 <--> ZR400-OFEC-16QAM ==> (2x200G breakout is not possible)
   ```

Custom Application Advertisement Details

```
OcNOS#show qsfp-dd 0 advertisement applications custom

Port Number             : 0
Application Selector    : 12

-------------------------------------------------
Host IDs
-------------------------------------------------
Host ID 1:
    Interface           : CAUI-4 C2M without FEC
    Application BR      : 103.13
    Lane Count          : 4
    Lane Sig BR         : 25.78125
    Modulation Format   : NRZ
```

```
    Bits Per Unit Intvl : 1.000000

Host ID 2:
    Interface           : CAUI-4 C2M with RS FEC
    Application BR      : 103.13
    Lane Count          : 4
    Lane Sig BR         : 25.78125
    Modulation Format   : NRZ
    Bits Per Unit Intvl : 1.000000

Host ID 3:
    Interface           : 100GAUI-2 C2M
    Application BR      : 106.25
    Lane Count          : 2
    Lane Sig BR         : 26.5625
    Modulation Format   : PAM4
    Bits Per Unit Intvl : 2.000000

Host ID 4:
    Interface           : 200GAUI-4 C2M
    Application BR      : 212.50
    Lane Count          : 4
    Lane Sig BR         : 26.5625
    Modulation Format   : PAM4
    Bits Per Unit Intvl : 2.000000

-------------------------------------------------
Media IDs
-------------------------------------------------
Media ID 1:
    Interface           : 100G-OFEC-31.5
    Application BR      : 100
    Lane Count          : 1
    Lane Sig BR         : 31.5
    Modulation Format   : DP-QPSK
    Bits Per Unit Intvl : 4.000000

Media ID 2:
    Interface           : 200G-OFEC-31.5
    Application BR      : 200
    Lane Count          : 1
    Lane Sig BR         : 31.5
    Modulation Format   : DP-16QAM
    Bits Per Unit Intvl : 8.000000
```

New CLI Commands

The QSFP-DD introduces the following commands to configure custom applications for both host and media interface ID.

custom-app-host-id

Use this command to set the custom application host interface ID while using the port breakout for 400G transceivers.

Command Syntax

```
custom-app-host-id <1-32>
```

Note: Use `show qsfp-dd PORT advertisement applications custom` to check the list of valid IDs. The number of available host IDs varies from transceiver to transceiver.

Parameters

`<1-32>`

Host ID range

Default

None

Command Mode

QSFP DD mode

Applicability

Introduced in OcNOS 6.5.3.

Example

```
#configure terminal
(config)# qsfp-dd 0
(config-qsfp-dd)#custom-app-host-id 4
(config-qsfp-dd)#commit
```

custom-app-media-id

Use this command to set the custom application media interface ID while using the port breakout for 400G transceivers.

Command Syntax

```
custom-app-media-id <1-32>
```

Note: Use `show qsfp-dd PORT advertisement applications custom` to check the list of valid IDs. The number of available media IDs varies from transceiver to transceiver..

Parameters

`<1-32>`

Media ID range

Default

None

Command Mode

QSFP DD mode

Applicability

Introduced in OcNOS 6.5.3.

Example

```
#configure terminal
(config)# qsfp-dd 0
(config-qsfp-dd)#custom-app-media-id 7
(config-qsfp-dd)#commit
```

Laser Tuning

Laser Tuning only supports for tunable Transceivers.

Laser Grid Configuration

Use this command to configure the Laser Grids in the QSFP-DD port. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#laser grid 100`	Configure Laser Grid at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation

```
ROUTER-1#sh qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 193.100000  | THz  |
 Channel Number       |  1   | 0           | --   |
 Wavelength           |  1   | 1552.52     | nm   |

-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress  |  1   | No     |
 Wavelength locked   |  1   | Yes    |
```

```
-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | No         |
 Channel number valid     |  1   | No         |
```

Laser Grid Unconfiguration

ROUTER1

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 49	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#no laser grid	Unconfigure Laser Grid at QSFP-DD level.
ROUTER1(config-qsfp-dd)#commit	Commit the configuration.

Laser Channel Configuration

Use this command to configure the Laser Channel in the QSFP-DD port. Using Channel Number we can set different Frequency and Wavelength for that port .Every Laser Grid have their own Channel Numbers. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 49	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#laser channel 20	Configure Laser Channel at QSFP-DD level.
ROUTER1(config-qsfp-dd)#commit	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 195.100000  | THz  |
 Channel Number       |  1   | 20          | --   |
 Wavelength           |  1   | 1536.61     | nm   |

-------------------------------------
        Flag         | Lane | Status |
```

```
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

---------------------------------------------
          Flag           | Lane | Status (L) |
---------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | No         |
```

Laser Channel Unconfiguration

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#no laser channel`	Unconfigure Laser Channel at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Laser Fine-tune-freq Configuration

Use this command to configure the Laser fine-tune-freq in the QSFP-DD port. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#laser fine-tune-freq 5`	Configure laser fine-tune-freq at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 195.104000  | THz  |
 Channel Number       |  1   | 20          | --   |
 Wavelength           |  1   | 1536.58     | nm   |
```

```
-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | Yes        |
```

Laser Fine-tune-freq Unconfiguration

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#no laser fine-tune-freq`	Unconfigure laser fine-tune-freq at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Laser Output-power Configuration

Use this command to configure the Laser output-power in the QSFP-DD port. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#laser output-power 2`	Configure laser output-power at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
```

```
 Laser Frequency      |  1   | 195.104000 | THz  |
 Channel Number       |  1   | 20         | --   |
 Wavelength           |  1   | 1536.58    | nm   |

-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | No         |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | Yes        |
```

Laser Output-power Unconfiguration

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#no laser output-power`	Unconfigure laser output-power at QSFP-DD level.
`ROUTER1(config-qsfp-dd)#commit`	Commit the configuration.

Laser Grid at Media-lane Configuration

Use this command to configure the Laser Grids in the media-lane. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#media-lane 1`	Entering to Media lane.
`ROUTER1(config-qsfp-dd-media)#laser grid 100`	Configure laser grid at Media level.
`ROUTER1(config-qsfp-dd-media)#commit`	Commit the configuration.

Validation

```
ROUTER-1#sh qsfp-dd 49 laser status

Port Number          : 49

-----------------------------------------------
```

```
       Attribute      | Lane |    Value    | Unit |
-----------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 193.100000  | THz  |
 Channel Number       |  1   | 0           | --   |
 Wavelength           |  1   | 1552.52     | nm   |

-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | No         |
 Channel number valid     |  1   | No         |
```

Laser Grid at Media-lane Unconfiguration

ROUTER1 (checker)

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#media-lane 1`	Entering to Media lane.
`ROUTER1(config-qsfp-dd-media)#no laser grid`	Unconfigure laser grid at Media level.
`ROUTER1(config-qsfp-dd-media)#commit`	Commit the configuration.

Laser Channel at Media-lane Configuration

Use this command to configure the Laser Channel in the media-lane. Using Channel Number we can set different Frequency and Wavelength for that port .Every Laser Grid have their own Channel Numbers. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#media-lane 1`	Entering to Media lane.
`ROUTER1(config-qsfp-dd-media)#laser channel 20`	Configure laser channel at Media level.
`ROUTER1(config-qsfp-dd-media)#commit`	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 195.100000  | THz  |
 Channel Number       |  1   | 20          | --   |
 Wavelength           |  1   | 1536.61     | nm   |

-------------------------------------
        Flag        | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | No         |
```

Laser Channel at Media-lane Unconfiguration

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.
`ROUTER1(config-qsfp-dd)#media-lane 1`	Entering to Media lane.
`ROUTER1(config-qsfp-dd-media)#no laser channel`	Unconfigure laser channel at Media level.
`ROUTER1(config-qsfp-dd-media)#commit`	Commit the configuration.

Laser Fine-tune-freq at Media-lane Configuration

Use this command to configure the Laser fine-tune-freq in the media-lane. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

`ROUTER1#configure terminal`	Enter configure mode.
`ROUTER1(config)#qsfp-dd 49`	Entering to QSFP-DD mode.

ROUTER1(config-qsfp-dd)#media-lane 1	Entering to Media lane.
ROUTER1(config-qsfp-dd-media)#laser fine-tune-freq 5	Configure laser fine-tune-freq at Media level.
ROUTER1(config-qsfp-dd-media)#commit	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 195.104000  | THz  |
 Channel Number       |  1   | 20          | --   |
 Wavelength           |  1   | 1536.58     | nm   |

-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | Yes        |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | Yes        |
```

Laser Fine-tune-freq at Media-lane Unconfiguration

ROUTER1

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 49	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#media-lane 1	Entering to Media lane.
ROUTER1(config-qsfp-dd-media)#no laser fine-tune-freq	Unconfigure laser fine-tune-freq at Media level.
ROUTER1(config-qsfp-dd-media)#commit	Commit the configuration.

Laser Output-power at Media-lane Configuration

Use this command to configure the Laser output-power in the media-lane. These commands only supports for modules which supports for laser Tuning Transceivers.

ROUTER1

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 49	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#media-lane 1	Entering to Media lane.
ROUTER1(config-qsfp-dd-media)#laser output-power 2	Configure laser output-power at Media level.
ROUTER1(config-qsfp-dd-media)#commit	Commit the configuration.

Validation

```
ROUTER-1#show qsfp-dd 49 laser status

Port Number          : 49

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 195.104000  | THz  |
 Channel Number       |  1   | 20          | --   |
 Wavelength           |  1   | 1536.58     | nm   |

-------------------------------------
        Flag         | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
           Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | No         |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | Yes        |
```

Laser Output-power at Media-lane Unconfiguration

ROUTER1

ROUTER1#configure terminal	Enter configure mode.
ROUTER1(config)#qsfp-dd 49	Entering to QSFP-DD mode.
ROUTER1(config-qsfp-dd)#media-lane 1	Entering to Media lane.
ROUTER1(config-qsfp-dd-media)#no laser output-power	Unconfigure laser output-power at Media level.
ROUTER1(config-qsfp-dd-media)#commit	Commit the configuration.

QSFP-DD Monitored Alarms

Table 1-22:

Alarms	
Module	
S.No.	Name
1	Temperature
2	Voltage
3	TEC Current Magnitude
4	Laser temperature
Host	
S.No.	Name
1	Tx LOS
2	Tx Cdr Loss of Lock
3	Tx Adapttive Eq Failure
4	Rx Output Status
5	FEC Excessive Degrade(FED)
6	FEC Detected Degrade(FDD)
7	Remote Degrade
8	Local Degrade
9	Flexe Loss of pad block
10	Flexe loss of Multiframe
11	Flexe loss of frame
12	Flexe instance ID mismatch
13	Flexe calender mismatch
14	Flexe instance map mismatch
15	Flexe GID mismatch
16	Tx local fault
17	Tx remote fault
18	Tx loss of alignment

Table 1-22:

Alarms	
19	Rx local fault
20	Rx remote fault
21	Rx loss of alignment
Media	
S.No.	Name
1	Rx Optical Power
2	Tx Optical Power
3	Tx Bias
4	Rx LOS
5	Rx Cdr Loss of Lock
6	Tx Failure
7	Tx Output Status
8	Tx FIFO error alarm
9	Tx Deskew Loss of Lock alarm
10	Tx Reference Clock Loss of Lock alarm
11	Tx CMU Loss of Lock alarm
12	Tx Out of Alignment alarm
13	Tx Loss of Alignment alarm
14	Rx FIFO Loss of Lock alarm
15	Rx Deskew Loss of Lock alarm
16	Rx Out of Alignment alarm
17	Rx Loss of Alignment alarm
18	Rx Chromatic Dispersion Compensation Loss of Lock alarm
19	Rx Demodulator Loss of Lock alarm
20	Rx Loss of Multi Frame alarm
21	Rx Loss of Frame alarm
22	Remote PHY Fault alarm
23	Local Degrade alarm

Table 1-22:

Alarms	
24	Remote Degrade alarm
25	FEC Detected Degrade over PM Interval alarm
26	FEC Excessive Degrade over PM Interval alarm
27	Laser Age
28	Laser Frequency Error

Table 1-23:

Performance Monitoring	
Host	
S.No.	Name
1	eSNR Input
2	PAM4 Level Trans
3	Pre-FEC BER
4	FERC
5	Tx Bits & Corrected Bits
6	Tx Frames & Uncorrected Frames
Media	
S.No.	Name
1	eSNR Input
2	PAM4 Level Trans
3	Pre-FEC BER
4	FERC
5	Mod Bias X/I
6	Mod Bias X/Q
7	Mod Bias Y/I
8	Mod Bias Y/Q
9	Mod Bias X_Phase
10	Mod Bias Y_Phase

Table 1-23:

Performance Monitoring	
11	CD - HG Short link
12	CD - LG Long link
13	DGD
14	SOPMD - HG
15	PDL
16	OSNR
17	eSNR
18	CFO
19	EVM_modem
20	Tx Power
21	Rx Total Power
22	Rx Sig Power
23	SOP ROC
24	MER
25	Clk recovery loop
26	SOPMD - LG
27	Rx Bits & Corrected Bits
28	Rx Frames & Uncorrected Frames

Example

Given a few examples of Alarms.

For Rx Optical Power & Rx Los:

```
2023 May 25 18:23:20.545 : OcNOS : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface cd52
changed state to down
2023 May 25 18:23:24.116 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Rx Optical
Power[Low Alarm] detected on Lane[1] Port[52] module. Reading[100.000 dBm], Threshold[-
28.239 dBm]. Vendor[SmartOptics     ] Serial[214156190       ]
```

```
2023 May 25 18:23:24.164 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Rx LOS
detected on Lane[1] Port[52] module. Vendor[SmartOptics     ] Serial[214156190       ]
OcNOS#sh qsfp-dd 52 monitors media

Alarm Codes: TFIFO - Tx FIFO Error, TLOLDS - Tx Deskew Loss of Lock
             TLOLRC - Tx Reference Clock Loss of Lock, TLOLCMU - Tx CMU Loss of Lock
             TOOA - Tx Out of Alignment, TLOA - Tx Loss of Alignment
             RFIFO - Rx FIFO Error, RLOLDS - Tx Deskew Loss of Lock
```

```
            ROOA - Rx Out of Alignment, RLOA - Rx Loss of Alignment
            RLOLCD - Rx Chromatic Dispersion Compensation Loss of Lock
            RLOLD - Tx Demodulator Loss of Lock, RLOM - Rx Loss of Multi Frame
            RLOF - Rx Loss of Frame, FDD - FEC Detected Degrade
            FED - FEC Excessive Degrade, RPF - Remote Phy Fault
            LD - Local Degrade, RD - Remote Degrade

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]

Port Number                    : 52
-------------------------------------------------------------------------------------------------------------
       Monitors       | Lane |  Value       |  High Alarm  | High Warning | Low Warning  |  Low Alarm   |  Unit  |
-------------------------------------------------------------------------------------------------------------
Rx Optical Power      |  1   |  --     [LA] |  2.0         |  0.0         |  -23.0       |  -28.2       | dBm    |
Tx Optical Power      |  1   |  -7.4        |  0.0         |  -2.0        |  -16.0       |  -18.0       | dBm    |
Tx Bias                     |  1   |  293.6       |  0.0         |  0.0         |  0.0         |  0.0         | mA     |
-------------------------------------------------------------------------------------------------------------
          VDM          | Lane |  Value       |  High Alarm  | High Warning | Low Warning  |  Low Alarm   |  Unit  |
-------------------------------------------------------------------------------------------------------------
Laser Age         [DP]|  1   |  0.0         |  65534.0     |  58983.0     |  0.0         |  0.0         | %      |
Pre-FEC BER Min In[DP]|  1   |  5.00e-01    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Max In[DP]|  1   |  5.00e-01    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Avg In[DP]|  1   |  5.00e-01    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Cur In[DP]|  1   |  5.00e-01    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Min Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Max Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Avg Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Curr Input   [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Mod Bias X/I      [DP]|  1   |  38.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
Mod Bias X/Q      [DP]|  1   |  39.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
Mod Bias Y/I      [DP]|  1   |  43.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
Mod Bias Y/Q      [DP]|  1   |  41.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
Mod Bias X_Phase  [DP]|  1   |  34.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
Mod Bias Y_Phase  [DP]|  1   |  42.0        |  89.0        |  84.0        |  14.0        |  4.0         | %      |
CD - HG Short link[DP]|  1   |  0.0         |  -1.0        |  -1.0        |  0.0         |  0.0         | Ps/nm  |
CD - LG Long link [DP]|  1   |  0.0         |  -20.0       |  -20.0       |  0.0         |  0.0         | Ps/nm  |
DGD               [DP]|  1   |  0.0         |  655.3       |  655.3       |  0.0         |  0.0         | Ps     |
SOPMD - HG        [DP]|  1   |  0.0         |  655.3       |  655.3       |  0.0         |  0.0         | Ps^2   |
PDL               [DP]|  1   |  0.0         |  6553.5      |  6553.5      |  0.0         |  0.0         | dB     |
OSNR              [DP]|  1   |  0.0         |  6553.5      |  6553.5      |  0.0         |  0.0         | dB     |
eSNR              [DP]|  1   |  0.0         |  6553.5      |  6553.5      |  0.0         |  0.0         | dB     |
CFO               [DP]|  1   |  0.0         |  -1.0        |  -1.0        |  0.0         |  0.0         | MHz    |
Tx Power          [DP]|  1   |  -7.4        |  0.0         |  -2.0        |  -16.0       |  -18.0       | dBm    |
Rx Total Power    [DP]|  1   |  -46.5       |  13.0        |  10.0        |  -18.0       |  -21.0       | dBm    |
Rx Sig Power      [DP]|  1   |  -40.0       |  13.0        |  10.0        |  -18.0       |  -21.0       | dBm    |
SOP ROC           [DP]|  1   |  0.0         |  65535.0     |  65535.0     |  0.0         |  0.0         | krad/s |
SOPMD - LG        [DP]|  1   |  0.0         |  0.0         |  0.0         |  0.0         |  0.0         | Ps^2   |

-------------------------------------------------
         Flag          | Lane |    Status (L)    |
-------------------------------------------------
Rx LOS                 |  1   |  True            |
Tx Failure             |  1   |  False           |
Rx CDR LOL             |  1   |  True            |

-------------------------------------------------------------------------------
       Link Performance       | Lane | Average  | Minimum  | Maximum  |  Unit   |
-------------------------------------------------------------------------------
Rx DSP CCD                    |  1   | 0        | 0        | 0        | ps/nm   |
Rx DSP DGD                    |  1   | 0.00     | 0.00     | 0.00     | ps      |
Rx Low Granularity SOPMD      |  1   | 0.0      | 0.0      | 0.0      | ps^2    |
Rx PDL                        |  1   | 0.0      | 0.0      | 0.0      | dB      |
Rx OSNR                       |  1   | 0.0      | 0.0      | 0.0      | dB      |
Rx ESNR                       |  1   | 0.0      | 0.0      | 0.0      | dB      |
Rx CFO                        |  1   | 0        | 0        | 0        | MHz     |
Tx Power                      |  1   | -7.44    | -7.44    | -7.43    | dBm     |
Rx Input Optical Power        |  1   | -48.18   | -50.30   | -44.67   | dBm     |
Rx Input Optical Signal Power |  1   | -40.00   | -40.00   | -40.00   | dBm     |
Rx SOPCR                      |  1   | 0        | 0        | 0        | krads/s |
Rx MER                        |  1   | 0.0      | 0.0      | 0.0      | dB      |

-------------------------------------------------------
       FEC Performance        | Lane |      Value     |
```

```
-------------------------------------------------------
Rx Bits                     |  1   | 0            |
Rx Corrected Bits           |  1   | 0            |
Rx Frames                   |  1   | 0            |
Rx Uncorrected Frames       |  1   | 0            |
```

For TX LOS & TX Cdr Loss:

```
2023 May 25 18:45:39.031 : OcNOS : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface cd0
changed state to down
OcNOS(config-if)#2023 May 25 18:45:40.340 : OcNOS : CMM : CRITI :
[CMM_CMIS_MODULE_MONITOR_2]: Tx LOS detected on Lane[1] Port[0] module.
Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.349 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[1] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.373 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[2] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.381 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[2] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.406 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[3] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.414 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[3] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.438 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[4] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.446 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[4] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.471 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[5] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.478 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[5] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.503 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[6] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]


2023 May 25 18:45:40.511 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[6] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


2023 May 25 18:45:40.535 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[7] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]
```

```
2023 May 25 18:45:40.543 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[7] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]

2023 May 25 18:45:40.568 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx LOS
detected on Lane[8] Port[0] module. Vendor[SmartOptics     ] Serial[214156344       ]

2023 May 25 18:45:40.575 : OcNOS : CMM : CRITI : [CMM_CMIS_MODULE_MONITOR_2]: Tx Cdr
Loss of Lock detected on Lane[8] Port[0] module. Vendor[SmartOptics     ]
Serial[214156344       ]


OcNOS(config-if)#end
OcNOS#show qsfp-dd 0 monitors host

Alarm Codes: FDD - FEC Detected Degrade, FED - FEC Excessive Degrade
             LD - Local Degrade, RD - Remote Degrade
             FLOPB - Flexe Loss of Pad Block, FLOMF - Flexe Loss of Multi-Frame
             FLOF - Flexe Loss of Frame, FIIDM - Flexe Instance Id Mismatch
             FCM - Flexe Calendar Mismatch, FIMM - Flexe Instance Map Mismatch
             FGIDM - Flexe GID Mismatch, TLF - Transmit Local Fault
             TRF - Transmit Remote Fault, TLOA - Transmit Loss of Alignment
             RLF - Receive Local Fault, RRF - Receive Remote Fault
             RLOA - Receive Loss of Alignment

Port Number                    : 0
-------------------------------------------------
         Flag          | Lane |    Status (L)    |
-------------------------------------------------
Tx LOS                 |  1   |  True            |
                       |  2   |  True            |
                       |  3   |  True            |
                       |  4   |  True            |
                       |  5   |  True            |
                       |  6   |  True            |
                       |  7   |  True            |
                       |  8   |  True            |
Tx CDR LOL             |  1   |  True            |
                       |  2   |  True            |
                       |  3   |  True            |
                       |  4   |  True            |
                       |  5   |  True            |
                       |  6   |  True            |
                       |  7   |  True            |
                       |  8   |  True            |
Tx Adaptive Input Eq   |  1   |  Good            |
                       |  2   |  Good            |
                       |  3   |  Good            |
                       |  4   |  Good            |
                       |  5   |  Good            |
                       |  6   |  Good            |
                       |  7   |  Good            |
                       |  8   |  Good            |

-------------------------------------------------------------------------------------------------------------------
          VDM          | Lane |  Value       |  High Alarm  | High Warning | Low Warning  |  Low Alarm   |  Unit  |
-------------------------------------------------------------------------------------------------------------------
Pre-FEC BER Min In[DP]|  1   |  1.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Max In[DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Avg In[DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
Pre-FEC BER Cur In[DP]|  1   |  5.00e-01    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Min Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Max Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Avg Input    [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |
FERC Curr Input   [DP]|  1   |  0.00e+00    |  2.05e+10    |  2.05e+10    |  0.00e+00    |  0.00e+00    | NA     |


-------------------------------------------------
       FEC Performance        | Lane |      Value     |
```

```
-------------------------------------------------------
Tx Bits                       |  1   | 0             |
Tx Corrected Bits             |  1   | 0             |
Tx Frames                     |  1   | 0             |
Tx Uncorrected Frames         |  1   | 0             |
```

Remote Fault and Local Fault Alarms

Local Fault: A local fault occurs when there is an issue with the line port, indicating a problem detected at the local end, such as bad data or signal.

Remote Fault: A remote fault is triggered when a port receives a remote fault frame from the far end (the port experiencing the local fault).

To address these faults, perform the "Shut/No Shut" operation at the interface level after enabling logging levels on the DUT (Device Under Test). Configure the "create-subscription" in the Netconf terminal, and to generate SNMP traps, connect the DUT to an MIB browser or a Linux server. Once configured, the "Shut" operation can be executed to generate alarms, and the "No Shut" operation can be used to recover from those alarms. Below, we have highlighted some alarms and their corresponding recovery processes in CLMSH mode, Netconf mode, and via SNMP traps.

Validation

Perform the Shut operation on the interface level to generate the alarms. To validate the remote fault and local fault alarms, use the following commands.

```
Ocnos#con t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Ocnos(config)#int cd1
Ocnos(config-if)#shutdown
Ocnos (config-if)#commit


2024 Sep 01 22:30:33.527 : OCNOS : NSM : CRITI : [IFMGR_IF_DOWN_2]: Interface cd1
changed state to down    --> Interface went to down state
2024 Sep 01 22:30:33.580 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx LOS detected on Lane[6] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]


OCNOS(config-if)#2024 Sep 01 22:30:34.816 : OCNOS : CMM : CRITI :
[CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]: Tx LOS detected on Lane[7] Port[1] module.
Vendor[CIENA           ] Serial[Q00JF7FD        ]


2024 Sep 01 22:30:43.250 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx LOS detected on Lane[1] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]


2024 Sep 01 22:30:44.363 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx Loss of Alignment detected on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ]
2024 Sep 01 22:30:44.363 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx Local Fault detected on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ] --> Here we can see the Local fault alarm.


2024 Sep 01 22:30:44.363 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Rx Remote Fault detected on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ] --> Here we can see the Remote fault alarm.
```

```
2024 Sep 01 22:30:44.364 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Pre-FEC BER Current Sample Input[High Alarm] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[239.000 1e-6]. Vendor[CIENA        ] Serial[Q00JF7FD
]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Pre-FEC BER Current Sample Input[High Warning] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[43.800 1e-6]. Vendor[CIENA        ] Serial[Q00JF7FD
]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
FERC Maximum Sample Value Input[High Alarm] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Maximum Sample Value Input[High Warning] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
FERC Sample Average Value Input[High Alarm] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Sample Average Value Input[High Warning] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.364 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
FERC Current Sample Value Input[High Alarm] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.365 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Current Sample Value Input[High Warning] detected on Lane[1] Port[1] module.
Reading[0.000 1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:30:44.497 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx LOS detected on Lane[2] Port[1] module. Vendor[CIENA         ] Serial[Q00JF7FD
]

2024 Sep 01 22:30:44.797 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[7] Port[1] module. Vendor[CIENA         ] Serial[Q00JF7FD
]

2024 Sep 01 22:30:44.849 : OCNOS : CMM : CRITI : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]:
Tx LOS detected on Lane[8] Port[1] module. Vendor[CIENA         ] Serial[Q00JF7FD
]

OCNOS(config-if)#2024 Sep 01 22:30:54.371 : OCNOS : CMM : NOTIF :
[CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]: FERC Maximum Sample Value Input[High Alarm]
recovered on Port[1] module. Reading[0.000 1e-6], Threshold[500000.000 1e-6].
Vendor[CIENA           ] Serial[Q00JF7FD        ]
```

```
2024 Sep 01 22:30:54.371 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Maximum Sample Value Input[High Warning] recovered on Port[1] module. Reading[0.000
1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

2024 Sep 01 22:30:54.371 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Sample Average Value Input[High Alarm] recovered on Port[1] module. Reading[0.000
1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

2024 Sep 01 22:30:54.371 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Sample Average Value Input[High Warning] recovered on Port[1] module. Reading[0.000
1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

Ocnos (config-if)#2024 Sep 01 22:30:54.596 : OCNOS : CMM : CRITI :
[CMM_CMIS_MODULE_HOST_LANE_MONITOR_2]: Tx LOS detected on Lane[4] Port[1] module.
Vendor[CIENA           ] Serial[Q00JF7FD        ]

2024 Sep 01 22:30:54.845 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[8] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]

Here we are going to perform the NO Shut operation on the interface level to recover the
alarms.

Ocnos (config-if)#no shutdown
Ocnos (config-if)#commit

2024 Sep 01 22:31:04.538 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[2] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]

2024 Sep 01 22:31:04.683 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[4] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]

2024 Sep 01 22:31:04.788 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[6] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]

2024 Sep 01 22:31:14.372 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx LOS recovered on Lane[1] Port[1] module. Vendor[CIENA          ] Serial[Q00JF7FD
]

2024 Sep 01 22:31:14.511 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx Local Fault recovered on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ] --> Here we can see that alarm is getting recovered.

2024 Sep 01 22:31:14.511 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx Remote Fault recovered on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ] --> Here we can see that alarm is getting recovered.

2024 Sep 01 22:31:18.535 : OCNOS : NSM : CRITI : [IFMGR_IF_UP_2]: Interface cd1 changed
state to up --> Here we can see that interface came UP.

2024 Sep 01 22:31:33.387 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Tx Loss of Alignment recovered on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ]
```

```
2024 Sep 01 22:31:33.387 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Rx Remote Fault recovered on Lane[1] Port[1] module. Vendor[CIENA           ]
Serial[Q00JF7FD        ]

2024 Sep 01 22:31:33.387 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Pre-FEC BER Current Sample Input[High Alarm] recovered on Port[1] module. Reading[0.001
1e-6], Threshold[239.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

2024 Sep 01 22:31:33.387 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
Pre-FEC BER Current Sample Input[High Warning] recovered on Port[1] module.
Reading[0.001 1e-6], Threshold[43.800 1e-6]. Vendor[CIENA        ] Serial[Q00JF7FD
]

2024 Sep 01 22:31:33.387 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Current Sample Value Input[High Alarm] recovered on Port[1] module. Reading[0.000
1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

2024 Sep 01 22:31:33.388 : OCNOS : CMM : NOTIF : [CMM_CMIS_MODULE_HOST_LANE_MONITOR_4]:
FERC Current Sample Value Input[High Warning] recovered on Port[1] module. Reading[0.000
1e-6], Threshold[500000.000 1e-6]. Vendor[CIENA           ] Serial[Q00JF7FD        ]

Netconf:-
====================================

yangcli ocnos@127.1>
Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:37Z</eventTime>
  <netconf-config-change xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-
notifications">
    <changed-by>
      <username>root</username>
      <session-id>0</session-id>
    </changed-by>
    <datastore>running</datastore>
    <edit>
      <target
        xmlns:ipi-interface="http://www.ipinfusion.com/yang/ocnos/ipi-interface">/ipi-
interface:interfaces/ipi-interface:interface[ipi-interface:name='cd1']/ipi-
interface:config</target>
      <operation>merge</operation>
    </edit>
  </netconf-config-change>
</notification>

Incoming notification:   Interface went to down state
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:37Z</eventTime>
  <interface-link-state-change-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-interface">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <name>cd1</name>
```

```
    <oper-status>down</oper-status>
  </interface-link-state-change-notification>
</notification>

Incoming notification:  Here we can see the TX-LOS alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FEC-Detected-Degrade</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-Loss-of-Alignment</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification: Here we can see the Remote Fault alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
```

```
    <name>CMIS-MODULE-1</name>
    <alarm-id>Rx-Remote-Fault</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Pre-FEC-BER-Current-Sample-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>239.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Pre-FEC-BER-Current-Sample-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>43.80</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>1000000.00</current-value>
```

```
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>1000000.00</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>1000000.00</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>1000000.00</current-value>
```

```
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

yangcli ocnos@127.1>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Current-Sample-Value-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:43Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Current-Sample-Value-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:44Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
```

```
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:44Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>4</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:44Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>6</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:53Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:53Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>6</number>
    <name>CMIS-MODULE-1</name>
```

```
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:20:53Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>7</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
```

```
  <eventTime>2024-09-01T23:21:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:03Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:04Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>3</number>
```

```
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:04Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>7</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:04Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>8</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

yangcli ocnos@127.1>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:13Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:14Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
```

```
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>4</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:14Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>5</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:14Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>6</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:14Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>8</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:24Z</eventTime>
```

```
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:24Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>3</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:24Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>4</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:24Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>5</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
```

```
  <eventTime>2024-09-01T23:21:34Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>4</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:34Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>5</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:34Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>7</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:43Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>6</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
```

```
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:43Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>7</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:43Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>8</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

yangcli ocnos@127.1>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:50Z</eventTime>
  <netconf-config-change xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-
notifications">
    <changed-by>
      <username>root</username>
      <session-id>0</session-id>
    </changed-by>
    <datastore>running</datastore>
    <edit>
      <target
        xmlns:ipi-interface="http://www.ipinfusion.com/yang/ocnos/ipi-interface">/ipi-
interface:interfaces/ipi-interface:interface[ipi-interface:name='cd1']/ipi-
interface:config</target>
      <operation>merge</operation>
    </edit>
  </netconf-config-change>
</notification>

Incoming notification:  Here we can see the Local Fault alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
```

```
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-Local-Fault</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-flag-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-Remote-Fault</alarm-id>
  </cmis-module-host-flag-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
```

```
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <alarm-type>High-alarm</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-monitor-alarm-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>critical</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <alarm-type>High-warning</alarm-type>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-alarm-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>2</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>
```

```
Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:54Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>5</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:21:55Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>8</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:  Here we can see the recovery of TX-LOS alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-LOS</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:  Here we can see the recovery of Local fault alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-Local-Fault</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>
```

```
Incoming notification:  Here we can see the recovery of Remote fault alarm.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-flag-recovery-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>Tx-Remote-Fault</alarm-id>
  </cmis-module-host-flag-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Maximum-Sample-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
```

```
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z</eventTime>
  <cmis-module-host-monitor-recovery-notification xmlns="http://www.ipinfusion.com/
yang/ocnos/ipi-platform">
    <severity>info</severity>
    <eventClass>state</eventClass>
    <number>1</number>
    <name>CMIS-MODULE-1</name>
    <alarm-id>FERC-Sample-Average-Value-Input</alarm-id>
    <current-value>0.0</current-value>
    <threshold-minimum>0.0</threshold-minimum>
    <threshold-maximum>500000.00</threshold-maximum>
  </cmis-module-host-monitor-recovery-notification>
</notification>

Incoming notification:  Here we can see that interface came UP.
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0">
  <eventTime>2024-09-01T23:22:03Z </eventTime>
  <interface-link-state-change-notification xmlns="http://www.ipinfusion.com/yang/
ocnos/ipi-interface">
    <severity> minor </severity>
    <eventClass>state</eventClass>
    <name>cd1</name>
    <oper-status>up</oper-status>
  </interface-link-state-change-notification>
</notification>
yangcli ocnos@127.1>
SNMP:-
1.3.6.1.2.1.1.3.0
SNMP TRAP FOR LINK DOWN:-
Source: 10.12.95.32Timestamp: 98 hours 9 minutes 26 secondsSNMP Version: 2
Trap OID: .1.3.6.1.6.3.1.1.5.3Community: test
Variable Bindings:

_____________________________________
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 98 hours 9 minutes 26 seconds

_____________________________________
Name: ifIndex
Value: [Integer] 10002
```

```
_____________________________________________
Name: ifAdminStatus
Value: [Integer] down(2)

_____________________________________________
Name: ifOperStatus
Value: [Integer] down(2)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
Value: [OctetString] OCNOS

_____________________________________________
Description:
SNMP TRAP FOR LINK UP:-
SNMP TRAP FOR Local fault alarm:-
Source: 10.12.95.32 Timestamp: 100 hours 39 minutes 3 seconds SNMP Version: 2
Trap OID: cmmCmisModuleHostFlagsNotifyAlarm Community: test
Variable Bindings:

_____________________________________________
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 100 hours 39 minutes 3 seconds (36234300)

_____________________________________________
Name: snmpTrapOID
Value: [OID] cmmCmisModuleHostFlagsNotifyAlarm

_____________________________________________
Name: cmmStackUnitIndex
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleType
Value: [Integer] qsfp-dd (1)

_____________________________________________
Name: cmmCmisModulePortNumber
Value: [Integer] 3

_____________________________________________
Name: cmmCmisModuleLaneNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleDescreteAlarmType
Value: [Integer] true (1)

_____________________________________________
Name: cmmCmisModuleHostLaneAttrFlagType
Value: [Integer] rxlocalfault (19)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
Value: [OctetString] OCNOS

_____________________________________________
Description: When cmis module host lane descrete attributes flags are set
SNMP TRAP FOR Remote fault Alarm:-
Source: 10.12.95.32 Timestamp: 100 hours 16 minutes 14 seconds SNMP Version: 2
Trap OID: cmmCmisModuleHostFlagsNotifyAlarm Community: test
Variable Bindings:

_____________________________________________
```

```
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 100 hours 16 minutes 14 seconds (36097400)

_____________________________________________
Name: snmpTrapOID
Value: [OID] cmmCmisModuleHostFlagsNotifyAlarm

_____________________________________________
Name: cmmStackUnitIndex
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleType
Value: [Integer] qsfp-dd (1)

_____________________________________________
Name: cmmCmisModulePortNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleLaneNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleDescreteAlarmType
Value: [Integer] true (1)

_____________________________________________
Name: cmmCmisModuleHostLaneAttrFlagType
Value: [Integer] rxremotefault (20)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
Value: [OctetString] OCNOS

_____________________________________________
Description: When cmis module host lane descrete attributes flags are set
SNMP TRAP FOR Local fault Recovery:-
Source: 10.12.95.32 Timestamp: 100 hours 27 minutes 34 seconds SNMP Version: 2
Trap OID: cmmCmisModuleHostFlagsNotifyAlarmRecovery Community: test
Variable Bindings:

_____________________________________________
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 100 hours 27 minutes 34 seconds (36165400)

_____________________________________________
Name: snmpTrapOID
Value: [OID] cmmCmisModuleHostFlagsNotifyAlarmRecovery

_____________________________________________
Name: cmmStackUnitIndex
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleType
Value: [Integer] qsfp-dd (1)

_____________________________________________
Name: cmmCmisModulePortNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleLaneNumber
Value: [Integer] 1
```

```
_____________________________________________
Name: cmmCmisModuleDescreteAlarmType
Value: [Integer] 0

_____________________________________________
Name: cmmCmisModuleHostLaneAttrFlagType
Value: [Integer] txlocalfault (16)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
Value: [OctetString] OCNOS

_____________________________________________
Description: When cmis module host lane descrete attributes flags are recovered
SNMP TRAP FOR TX Remote fault Recovery:-
Source: 10.12.95.32 Timestamp: 100 hours 27 minutes 34 seconds SNMP Version: 2
Trap OID: cmmCmisModuleHostFlagsNotifyAlarmRecovery Community: test
Variable Bindings:

_____________________________________________
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 100 hours 27 minutes 34 seconds (36165400)

_____________________________________________
Name: snmpTrapOID
Value: [OID] cmmCmisModuleHostFlagsNotifyAlarmRecovery

_____________________________________________
Name: cmmStackUnitIndex
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleType
Value: [Integer] qsfp-dd (1)

_____________________________________________
Name: cmmCmisModulePortNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleLaneNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleDescreteAlarmType
Value: [Integer] 0

_____________________________________________
Name: cmmCmisModuleHostLaneAttrFlagType
Value: [Integer] txremotefault (17)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
SNMP TRAP FOR  Loss RX of alignment:-:-
Source: 10.12.95.32 Timestamp: 100 hours 16 minutes 14 seconds SNMP Version: 2
Trap OID: cmmCmisModuleHostFlagsNotifyAlarm Community: test
Variable Bindings:

_____________________________________________
Name: .1.3.6.1.2.1.1.3.0
Value: [TimeTicks] 100 hours 16 minutes 14 seconds (36097400)

_____________________________________________
Name: snmpTrapOID
```

```
Value: [OID] cmmCmisModuleHostFlagsNotifyAlarm

_____________________________________________
Name: cmmStackUnitIndex
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleType
Value: [Integer] qsfp-dd (1)

_____________________________________________
Name: cmmCmisModulePortNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleLaneNumber
Value: [Integer] 1

_____________________________________________
Name: cmmCmisModuleDescreteAlarmType
Value: [Integer] true (1)

_____________________________________________
Name: cmmCmisModuleHostLaneAttrFlagType
Value: [Integer] rxlossofalignment (18)

_____________________________________________
Name: .1.3.6.1.2.1.1.5.0
Value: [OctetString] OCNOS

_____________________________________________
Description: When cmis module host lane descrete attributes flags are set
```

Signal Integrity

The Signal integrity in the context of Quad Small Form Factor Pluggable Double Density (QSFP-DD) refers to the maintenance of the quality of electrical signals transmitted and received by the QSFP-DD module. QSFP-DD is a high-speed, high-density interface used primarily in data center applications to interconnect switches, servers, and other networking equipment.

Maintaining signal integrity is crucial in high-speed data transmission because any degradation or distortion of the signals can lead to errors, reduced performance, or even complete failure of communication between devices. In the case of QSFP-DD, which supports data rates of up to 400 Gbps per port, ensuring signal integrity is particularly challenging due to the high data rates and the compact form factor of the module.

Feature Characteristics

The signal integrity involves addressing various factors such as impedance matching, jitter, noise, reflections, and equalization to ensure the accurate and reliable transmission of electrical signals in electronic systems.

Benefits

Optimizing signal integrity in QSFP-DD modules offers numerous benefits:

- Enhanced reliability
- High-speed data transmission
- Reduced latency

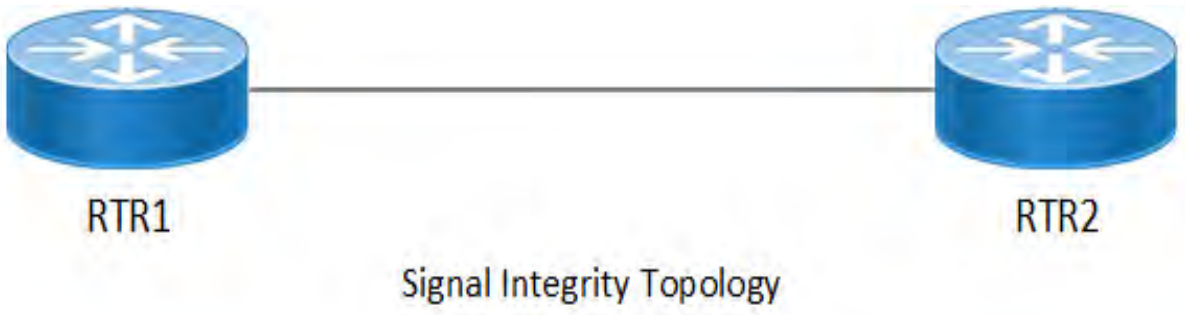
- Compatibility
- Longer reach
- Scalability
- Cost-efficiency
- Compliance assurance.

Configuration

To configure Signal Integrity (SI) parameters like Rx Pre-Cursor Equalization, Rx Post-Cursor Equalization, Tx Equalization, and Rx Amplitude on a QSFP-DD module, you usually interact with the management interface or CLI provided by the networking equipment hosting the module. This involves accessing the configuration settings specific to the QSFP-DD module within the device's interface.

Topology

In this topology, the Signal Integrity RTR1 to RTR2 interface configuration in QSFP-DD.



Signal Integrity Topology

R1 Tx Equalization

For the Tx equalization configuration in R1 route, follow these steps:

1. To configure Tx equalization, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 11
   R1(config-qsfp-dd)# tx-input eq-target 5
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Tx equalization configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status
Port Number                    : 11
-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | 5           | 5          |
```

```
                    | 2    | 5           | 5           |
                    | 3    | 5           | 5           |
                    | 4    | 5           | 5           |
                    | 5    | 5           | 5           |
                    | 6    | 5           | 5           |
                    | 7    | 5           | 5           |
                    | 8    | 5           | 5           |
-------------------------------------------------------
 Rx Pre-Cursor Eq   | 1    | None        | 0           |
                    | 2    | None        | 0           |
                    | 3    | None        | 0           |
                    | 4    | None        | 0           |
                    | 5    | None        | 0           |
                    | 6    | None        | 0           |
                    | 7    | None        | 0           |
                    | 8    | None        | 0           |
-------------------------------------------------------
 Rx Amplitude       | 1    | None        | 2           |
                    | 2    | None        | 2           |
                    | 3    | None        | 2           |
                    | 4    | None        | 2           |
                    | 5    | None        | 2           |
                    | 6    | None        | 2           |
                    | 7    | None        | 2           |
                    | 8    | None        | 2           |
-------------------------------------------------------
 Tx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
```

R2 Tx Equalization

For the Tx equalization configuration in R2 route, follow these steps:

1. To configure Tx equalization, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# tx-input eq-target 5
   ```

2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Tx equalization configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------
 Tx Equalization     | 1    | 5           | 5          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-----------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------
 Rx Amplitude        | 1    | None        | 2          |
                     | 2    | None        | 2          |
                     | 3    | None        | 2          |
                     | 4    | None        | 2          |
                     | 5    | None        | 2          |
                     | 6    | None        | 2          |
                     | 7    | None        | 2          |
                     | 8    | None        | 2          |
-----------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
                     | 8    | None        | Disabled   |
-----------------------------------------------------
 Rx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
```

```
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-------------------------------------------------------
```

Tx Equalization Unconfiguration

For the Tx equalization unconfiguration in R2 route, follow these steps:

1. To unconfigure Tx equalization, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# no tx-input eq-target 5
   ```
2. To uncongifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Tx Equalization Unconfiguration Validation

To validate the Tx equalization unconfiguration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-------------------------------------------------------
 Rx Amplitude        | 1    | None        | 2          |
                     | 2    | None        | 2          |
                     | 3    | None        | 2          |
                     | 4    | None        | 2          |
                     | 5    | None        | 2          |
```

```
                     | 6    | None         | 2           |
                     | 7    | None         | 2           |
                     | 8    | None         | 2           |
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
```

To configure the Tx Equalization on any specific host lanes, do the following configuration.

R1 Tx Equalization

For the Tx equalization configuration on any specific host lanes, follow these steps:

1. To configure Tx equalization on any specific host lanes, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 11
   R1(config-qsfp-dd)# host-lane 1
   R1(config-qsfp-dd)# tx-input eq-target 7
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Tx equalization configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
```

```
                    | 7    | 5           | 5           |
                    | 8    | 5           | 5           |
-------------------------------------------------------
 Rx Pre-Cursor Eq   | 1    | None        | 0           |
                    | 2    | None        | 0           |
                    | 3    | None        | 0           |
                    | 4    | None        | 0           |
                    | 5    | None        | 0           |
                    | 6    | None        | 0           |
                    | 7    | None        | 0           |
                    | 8    | None        | 0           |
-------------------------------------------------------
 Rx Amplitude       | 1    | None        | 2           |
                    | 2    | None        | 2           |
                    | 3    | None        | 2           |
                    | 4    | None        | 2           |
                    | 5    | None        | 2           |
                    | 6    | None        | 2           |
                    | 7    | None        | 2           |
                    | 8    | None        | 2           |
-------------------------------------------------------
 Tx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
-------------------------------------------------------
```

R2 Tx Equalization

For the Tx equalization configuration in R2 route, follow these steps:

1. To configure Tx equalization, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# host-lane 1
   R2(config-qsfp-dd)# tx-input eq-target 7
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Tx equalization configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude        | 1    | None        | 2          |
                     | 2    | None        | 2          |
                     | 3    | None        | 2          |
                     | 4    | None        | 2          |
                     | 5    | None        | 2          |
                     | 6    | None        | 2          |
                     | 7    | None        | 2          |
                     | 8    | None        | 2          |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
                     | 8    | None        | Disabled   |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
```

```
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-----------------------------------------------------------
```

Tx Equalization Unconfiguration

For the Tx equalization unconfiguration on any specific host lanes, follow these steps:

1. To unconfigure Tx equalization on any specific host lanes, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 11
   R1(config-qsfp-dd)# host-lane 1
   R1(config-qsfp-dd)# no tx-input eq-target 7
   ```
2. To uncongifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Tx Equalization Unconfiguration Validation

To validate the Tx equalization unconfiguration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Tx Equalization     | 1    | 5           | 5          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude        | 1    | None        | 2          |
                     | 2    | None        | 2          |
                     | 3    | None        | 2          |
                     | 4    | None        | 2          |
                     | 5    | None        | 2          |
                     | 6    | None        | 2          |
                     | 7    | None        | 2          |
```

```
                      | 8    | None         | 2           |
-------------------------------------------------------------
 Tx CDR Bypass        | 1    | None         | Disabled    |
                      | 2    | None         | Disabled    |
                      | 3    | None         | Disabled    |
                      | 4    | None         | Disabled    |
                      | 5    | None         | Disabled    |
                      | 6    | None         | Disabled    |
                      | 7    | None         | Disabled    |
                      | 8    | None         | Disabled    |
-------------------------------------------------------------
 Rx CDR Bypass        | 1    | None         | Disabled    |
                      | 2    | None         | Disabled    |
                      | 3    | None         | Disabled    |
                      | 4    | None         | Disabled    |
                      | 5    | None         | Disabled    |
                      | 6    | None         | Disabled    |
                      | 7    | None         | Disabled    |
                      | 8    | None         | Disabled    |
-------------------------------------------------------------
```

R1 Rx Amplitude

Use this command to configure the Rx Amplitude on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx amplitude, execute the following command in the config mode:
   ```
   R1(config)#qsfp-dd 11
   R1(config-qsfp-dd)# rx-output amp-target 2
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx amplitude configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-------------------------------------------------------------
      Parameter       | Lane | User Config | H/W Config |
-------------------------------------------------------------
 Tx Equalization      | 1    | 7           | 7           |
                      | 2    | 5           | 5           |
                      | 3    | 5           | 5           |
                      | 4    | 5           | 5           |
                      | 5    | 5           | 5           |
                      | 6    | 5           | 5           |
                      | 7    | 5           | 5           |
                      | 8    | 5           | 5           |
-------------------------------------------------------------
 Rx Pre-Cursor Eq     | 1    | None         | 0           |
```

```
                     | 2    | None         | 0           |
                     | 3    | None         | 0           |
                     | 4    | None         | 0           |
                     | 5    | None         | 0           |
                     | 6    | None         | 0           |
                     | 7    | None         | 0           |
                     | 8    | None         | 0           |
-----------------------------------------------------------
 Rx Amplitude        | 1    | 2            | 2           |
                     | 2    | 2            | 2           |
                     | 3    | 2            | 2           |
                     | 4    | 2            | 2           |
                     | 5    | 2            | 2           |
                     | 6    | 2            | 2           |
                     | 7    | 2            | 2           |
                     | 8    | 2            | 2           |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-----------------------------------------------------------
```

OcNOS#

R2 Rx Amplitude

Use this command to configure the Rx Amplitude on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx amplitude, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# rx-output amp-target 2
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx amplitude configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude        | 1    | 2           | 2          |
                     | 2    | 2           | 2          |
                     | 3    | 2           | 2          |
                     | 4    | 2           | 2          |
                     | 5    | 2           | 2          |
                     | 6    | 2           | 2          |
                     | 7    | 2           | 2          |
                     | 8    | 2           | 2          |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
                     | 8    | None        | Disabled   |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
```

```
                      | 8    | None         | Disabled   |
-------------------------------------------------------

OcNOS#
```

Rx Amplitude Unconfiguration

For the Rx amplitude unconfiguration, follow these steps.

1. To unconfigure Rx amplitude, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# no rx-output amp-target 2
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Rx Amplitude Unconfiguration Validation

To validate the Rx amplitude unconfiguration, use the following command.

```
OcNOS#sh qsfp-dd 11 advertisement si

Port Number                    : 11

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 6          |
                     | 2    | None        | 6          |
                     | 3    | None        | 6          |
                     | 4    | None        | 6          |
                     | 5    | None        | 6          |
                     | 6    | None        | 6          |
                     | 7    | None        | 6          |
                     | 8    | None        | 6          |
-------------------------------------------------------
 Rx Amplitude        | 1    | None        | 3          |
                     | 2    | None        | 3          |
                     | 3    | None        | 3          |
                     | 4    | None        | 3          |
                     | 5    | None        | 3          |
                     | 6    | None        | 3          |
                     | 7    | None        | 3          |
                     | 8    | None        | 3          |
```

```
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None         | Disabled   |
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled   |
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-------------------------------------------------------
```

To configure the Rx Amplitude on any specific host lanes, do the following configuration.

R1 Rx Amplitude

Use this command to configure the Rx Amplitude on the QSFP-DD module on any specific host lanes, follow these steps.

1. To configure Rx amplitude, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 11
   R1(config-qsfp-dd)# host-lane 1
   R1(config-qsfp-dd-host)# rx-output amp-target 3
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx amplitude configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
```

```
-------------------------------------------------------
 Rx Pre-Cursor Eq     | 1    | None         | 0          |
                      | 2    | None         | 0          |
                      | 3    | None         | 0          |
                      | 4    | None         | 0          |
                      | 5    | None         | 0          |
                      | 6    | None         | 0          |
                      | 7    | None         | 0          |
                      | 8    | None         | 0          |
-------------------------------------------------------
 Rx Amplitude         | 1    | 3            | 3          |
                      | 2    | 2            | 2          |
                      | 3    | 2            | 2          |
                      | 4    | 2            | 2          |
                      | 5    | 2            | 2          |
                      | 6    | 2            | 2          |
                      | 7    | 2            | 2          |
                      | 8    | 2            | 2          |
-------------------------------------------------------
 Tx CDR Bypass        | 1    | None         | Disabled   |
                      | 2    | None         | Disabled   |
                      | 3    | None         | Disabled   |
                      | 4    | None         | Disabled   |
                      | 5    | None         | Disabled   |
                      | 6    | None         | Disabled   |
                      | 7    | None         | Disabled   |
                      | 8    | None         | Disabled   |
-------------------------------------------------------
 Rx CDR Bypass        | 1    | None         | Disabled   |
                      | 2    | None         | Disabled   |
                      | 3    | None         | Disabled   |
                      | 4    | None         | Disabled   |
                      | 5    | None         | Disabled   |
                      | 6    | None         | Disabled   |
                      | 7    | None         | Disabled   |
                      | 8    | None         | Disabled   |
-------------------------------------------------------
```

R2 Rx Amplitude

Use this command to configure the Rx Amplitude on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx amplitude, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# host-lane 1
   R2(config-qsfp-dd-host)# rx-output amp-target 3
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx amplitude configuration, use the following command.

```
OcNOS#show qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude        | 1    | 3           | 3          |
                     | 2    | 2           | 2          |
                     | 3    | 2           | 2          |
                     | 4    | 2           | 2          |
                     | 5    | 2           | 2          |
                     | 6    | 2           | 2          |
                     | 7    | 2           | 2          |
                     | 8    | 2           | 2          |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
                     | 8    | None        | Disabled   |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
```

```
                     | 8    | None         | Disabled   |
-------------------------------------------------------
```

Rx Amplitude Unconfiguration

For the Rx amplitude unconfiguration, follow these steps.

1. To unconfigure Rx amplitude, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 11
   R2(config-qsfp-dd)# host-lane 1
   R2(config-qsfp-dd)# no rx-output amp-target 3
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Rx Amplitude Unconfiguration Validation

To validate the Rx amplitude unconfiguration, use the following command.

```
OcNOS#sh qsfp-dd 11 advertisement si

Port Number                    : 11

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Tx Equalization     | 1    | 7           | 7          |
                     | 2    | 5           | 5          |
                     | 3    | 5           | 5          |
                     | 4    | 5           | 5          |
                     | 5    | 5           | 5          |
                     | 6    | 5           | 5          |
                     | 7    | 5           | 5          |
                     | 8    | 5           | 5          |
-------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-------------------------------------------------------
 Rx Amplitude        | 1    | 2           | 2          |
                     | 2    | 2           | 2          |
                     | 3    | 2           | 2          |
                     | 4    | 2           | 2          |
                     | 5    | 2           | 2          |
                     | 6    | 2           | 2          |
                     | 7    | 2           | 2          |
                     | 8    | 2           | 2          |
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
```

```
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled   |
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-------------------------------------------------------
```

R1 Rx Pre-Cursor Eq

Use this command to configure the Rx Pre-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx Pre-Cursor Eq, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 0
   R1(config-qsfp-dd)# rx-output eq-pre-cursor-target 4
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Pre-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 4           | 4          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
```

```
                     | 5    | None         | 0           |
                     | 6    | None         | 0           |
                     | 7    | None         | 0           |
                     | 8    | None         | 0           |
-------------------------------------------------------
 Rx Amplitude        | 1    | None         | 0           |
                     | 2    | None         | 0           |
                     | 3    | None         | 0           |
                     | 4    | None         | 0           |
                     | 5    | None         | 0           |
                     | 6    | None         | 0           |
                     | 7    | None         | 0           |
                     | 8    | None         | 0           |
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
```

R2 Rx Pre-Cursor Eq

Use this command to configure the Rx Pre-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx Pre-Cursor Eq, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 0
   R2(config-qsfp-dd)# rx-output eq-pre-cursor-target 4
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Pre-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-------------------------------------------------------
```

Parameter	Lane	User Config	H/W Config
Rx Pre-Cursor Eq	1	4	4
	2	4	4
	3	4	4
	4	4	4
	5	4	4
	6	4	4
	7	4	4
	8	4	4
Rx Post-Cursor Eq	1	None	0
	2	None	0
	3	None	0
	4	None	0
	5	None	0
	6	None	0
	7	None	0
	8	None	0
Rx Amplitude	1	None	0
	2	None	0
	3	None	0
	4	None	0
	5	None	0
	6	None	0
	7	None	0
	8	None	0
Tx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled
Rx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled

```
OcNOS#
```

Rx Pre-Cursor Eq Unconfiguration

Use this command to unconfigure the Rx Pre-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To unconfigure Rx Pre-Cursor Eq, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 0
   R1(config-qsfp-dd)# no rx-output eq-pre-cursor-target 4
   ```
2. To uncongifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Rx Pre-Cursor Eq Unconfiguration Validation

To validate the Rx Pre-Cursor Eq Unconfiguration, use the following command.

```
OcNOS#sh qsfp-dd 11 si status

Port Number                    : 11

-----------------------------------------------------------
      Parameter       | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Rx Pre-Cursor Eq     | 1    | None        | 0          |
                      | 2    | None        | 0          |
                      | 3    | None        | 0          |
                      | 4    | None        | 0          |
                      | 5    | None        | 0          |
                      | 6    | None        | 0          |
                      | 7    | None        | 0          |
                      | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Post-Cursor Eq    | 1    | None        | 0          |
                      | 2    | None        | 0          |
                      | 3    | None        | 0          |
                      | 4    | None        | 0          |
                      | 5    | None        | 0          |
                      | 6    | None        | 0          |
                      | 7    | None        | 0          |
                      | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude         | 1    | None        | 0          |
                      | 2    | None        | 0          |
                      | 3    | None        | 0          |
                      | 4    | None        | 0          |
                      | 5    | None        | 0          |
                      | 6    | None        | 0          |
                      | 7    | None        | 0          |
                      | 8    | None        | 0          |
-----------------------------------------------------------
 Tx CDR Bypass        | 1    | None        | Disabled   |
                      | 2    | None        | Disabled   |
                      | 3    | None        | Disabled   |
```

```
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled   |
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-----------------------------------------------------------
```

To configure the Rx Pre-Cursor Eq on any specific host lanes, do the following configuration.

R1 Rx Pre-Cursor Eq

Use this command to configure the Rx Pre-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To configure Rx Pre-Cursor Eq, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 0
   R1(config-qsfp-dd)# host-lane 1
   R1(config-qsfp-dd-host)# rx-output eq-pre-cursor-target 3
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Pre-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 3           | 3          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-----------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
```

```
                     | 4    | None         | 0           |
                     | 5    | None         | 0           |
                     | 6    | None         | 0           |
                     | 7    | None         | 0           |
                     | 8    | None         | 0           |
-------------------------------------------------------
 Rx Amplitude        | 1    | None         | 0           |
                     | 2    | None         | 0           |
                     | 3    | None         | 0           |
                     | 4    | None         | 0           |
                     | 5    | None         | 0           |
                     | 6    | None         | 0           |
                     | 7    | None         | 0           |
                     | 8    | None         | 0           |
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled    |
                     | 2    | None         | Disabled    |
                     | 3    | None         | Disabled    |
                     | 4    | None         | Disabled    |
                     | 5    | None         | Disabled    |
                     | 6    | None         | Disabled    |
                     | 7    | None         | Disabled    |
                     | 8    | None         | Disabled    |
-------------------------------------------------------
```

R2 Rx Pre-Cursor Eq

Use this command to configure the Rx Pre-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To configure Rx Pre-Cursor Eq, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 0
   R2(config-qsfp-dd)# host-lane 1
   R2(config-qsfp-dd-host)# rx-output eq-pre-cursor-target 3
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Pre-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0
```

Parameter	Lane	User Config	H/W Config
Rx Pre-Cursor Eq	1	3	3
	2	4	4
	3	4	4
	4	4	4
	5	4	4
	6	4	4
	7	4	4
	8	4	4
Rx Post-Cursor Eq	1	None	0
	2	None	0
	3	None	0
	4	None	0
	5	None	0
	6	None	0
	7	None	0
	8	None	0
Rx Amplitude	1	None	0
	2	None	0
	3	None	0
	4	None	0
	5	None	0
	6	None	0
	7	None	0
	8	None	0
Tx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled
Rx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled

Rx Pre-Cursor Eq Unconfiguration

Use this command to unconfigure the Rx Pre-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To unconfigure Rx Pre-Cursor Eq, execute the following command in the config mode.
```
R1(config)#qsfp-dd 0
R1(config-qsfp-dd)# host-lane 1
R1(config-qsfp-dd-host)# no rx-output eq-pre-cursor-target 3
```
2. To unconfigure, execute the following command.
```
R1(config-qsfp-dd)#commit
```

Rx Pre-Cursor Eq Validation

To validate the Rx Pre-Cursor Eq unconfigure, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-----------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 4           | 4          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-----------------------------------------------------
 Rx Post-Cursor Eq   | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------
 Rx Amplitude        | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
```

```
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-----------------------------------------------------------
 Rx CDR Bypass       | 1    | None         | Disabled   |
                     | 2    | None         | Disabled   |
                     | 3    | None         | Disabled   |
                     | 4    | None         | Disabled   |
                     | 5    | None         | Disabled   |
                     | 6    | None         | Disabled   |
                     | 7    | None         | Disabled   |
                     | 8    | None         | Disabled   |
-----------------------------------------------------------
```

R1 Rx Post-Cursor Eq

Use this command to configure the Rx Post-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx Post-Cursor Eq, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 0
   R1(config-qsfp-dd)# rx-output eq-pre-cursor-target 4
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Post-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 3           | 3          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-----------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | 4           | 4          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
```

```
                     | 6    | 4           | 4           |
                     | 7    | 4           | 4           |
                     | 8    | 4           | 4           |
-------------------------------------------------------
 Rx Amplitude        | 1    | None        | 0           |
                     | 2    | None        | 0           |
                     | 3    | None        | 0           |
                     | 4    | None        | 0           |
                     | 5    | None        | 0           |
                     | 6    | None        | 0           |
                     | 7    | None        | 0           |
                     | 8    | None        | 0           |
-------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled    |
                     | 2    | None        | Disabled    |
                     | 3    | None        | Disabled    |
                     | 4    | None        | Disabled    |
                     | 5    | None        | Disabled    |
                     | 6    | None        | Disabled    |
                     | 7    | None        | Disabled    |
                     | 8    | None        | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass       | 1    | None        | Disabled    |
                     | 2    | None        | Disabled    |
                     | 3    | None        | Disabled    |
                     | 4    | None        | Disabled    |
                     | 5    | None        | Disabled    |
                     | 6    | None        | Disabled    |
                     | 7    | None        | Disabled    |
                     | 8    | None        | Disabled    |
-------------------------------------------------------
```

R2 Rx Post-Cursor Eq

Use this command to configure the Rx Post-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To configure Rx Post-Cursor Eq, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 0
   R2(config-qsfp-dd)# rx-output eq-pre-cursor-target 4
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Post-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
```

```
-------------------------------------------------------
 Rx Pre-Cursor Eq     | 1    | 3           | 3          |
                      | 2    | 4           | 4          |
                      | 3    | 4           | 4          |
                      | 4    | 4           | 4          |
                      | 5    | 4           | 4          |
                      | 6    | 4           | 4          |
                      | 7    | 4           | 4          |
                      | 8    | 4           | 4          |
-------------------------------------------------------
 Rx Post-Cursor Eq    | 1    | 4           | 4          |
                      | 2    | 4           | 4          |
                      | 3    | 4           | 4          |
                      | 4    | 4           | 4          |
                      | 5    | 4           | 4          |
                      | 6    | 4           | 4          |
                      | 7    | 4           | 4          |
                      | 8    | 4           | 4          |
-------------------------------------------------------
 Rx Amplitude         | 1    | None        | 0          |
                      | 2    | None        | 0          |
                      | 3    | None        | 0          |
                      | 4    | None        | 0          |
                      | 5    | None        | 0          |
                      | 6    | None        | 0          |
                      | 7    | None        | 0          |
                      | 8    | None        | 0          |
-------------------------------------------------------
 Tx CDR Bypass        | 1    | None        | Disabled   |
                      | 2    | None        | Disabled   |
                      | 3    | None        | Disabled   |
                      | 4    | None        | Disabled   |
                      | 5    | None        | Disabled   |
                      | 6    | None        | Disabled   |
                      | 7    | None        | Disabled   |
                      | 8    | None        | Disabled   |
-------------------------------------------------------
 Rx CDR Bypass        | 1    | None        | Disabled   |
                      | 2    | None        | Disabled   |
                      | 3    | None        | Disabled   |
                      | 4    | None        | Disabled   |
                      | 5    | None        | Disabled   |
                      | 6    | None        | Disabled   |
                      | 7    | None        | Disabled   |
                      | 8    | None        | Disabled   |
-------------------------------------------------------
```

R1 Rx Post-Cursor Eq Unconfiguration

Use this command to unconfigure the Rx Post-Cursor Eq on the QSFP-DD module on all eight host lanes, follow these steps.

1. To unconfigure Rx Post-Cursor Eq, execute the following command in the config mode.
```
R1(config)#qsfp-dd 0
R1(config-qsfp-dd)# rx-output eq-pre-cursor-target 4
```
2. To unconfigure, execute the following command.
```
R1(config-qsfp-dd)#commit
```

R1 Rx Post-Cursor Eq Unconfiguration Validation

To validate the Rx Post-Cursor Eq unconfigure, use the following command.

```
OcNOS#show qsfp-dd 0 advertisement si

Port Number                    : 0

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Rx Amplitude        | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
```

```
                      | 8    | None         | Disabled   |
-------------------------------------------------------------
 Rx CDR Bypass        | 1    | None         | Disabled   |
                      | 2    | None         | Disabled   |
                      | 3    | None         | Disabled   |
                      | 4    | None         | Disabled   |
                      | 5    | None         | Disabled   |
                      | 6    | None         | Disabled   |
                      | 7    | None         | Disabled   |
                      | 8    | None         | Disabled   |
-------------------------------------------------------------

OcNOS#
```

To configure the Rx Post-Cursor Eq on any specific host lanes, do the following configuration.

R1 Rx Post-Cursor Eq

Use this command to configure the Rx Post-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To configure Rx Post-Cursor Eq, execute the following command in the config mode.
   ```
   R1(config)#qsfp-dd 0
   R1(config-qsfp-dd)# host-lane 1
   R1(config-qsfp-dd-host)# rx-output eq-pre-cursor-target 3
   ```
2. To congifure, execute the following command.
   ```
   R1(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Post-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0

-------------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-------------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 3           | 3          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-------------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | 3           | 3          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
```

```
                    | 5    | 4           | 4           |
                    | 6    | 4           | 4           |
                    | 7    | 4           | 4           |
                    | 8    | 4           | 4           |
-------------------------------------------------------
 Rx Amplitude       | 1    | None        | 0           |
                    | 2    | None        | 0           |
                    | 3    | None        | 0           |
                    | 4    | None        | 0           |
                    | 5    | None        | 0           |
                    | 6    | None        | 0           |
                    | 7    | None        | 0           |
                    | 8    | None        | 0           |
-------------------------------------------------------
 Tx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
-------------------------------------------------------
 Rx CDR Bypass      | 1    | None        | Disabled    |
                    | 2    | None        | Disabled    |
                    | 3    | None        | Disabled    |
                    | 4    | None        | Disabled    |
                    | 5    | None        | Disabled    |
                    | 6    | None        | Disabled    |
                    | 7    | None        | Disabled    |
                    | 8    | None        | Disabled    |
-------------------------------------------------------
```

R2 Rx Post-Cursor Eq

Use this command to configure the Rx Post-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To configure Rx Post-Cursor Eq, execute the following command in the config mode.
   ```
   R2(config)#qsfp-dd 0
   R2(config-qsfp-dd)# host-lane 1
   R2(config-qsfp-dd-host)# rx-output eq-post-cursor-target 3
   ```
2. To congifure, execute the following command.
   ```
   R2(config-qsfp-dd)#commit
   ```

Validation

To validate the Rx Post-Cursor Eq configuration, use the following command.

```
OcNOS#show qsfp-dd 0 si status

Port Number                    : 0
```

Parameter	Lane	User Config	H/W Config
Rx Pre-Cursor Eq	1	3	3
	2	4	4
	3	4	4
	4	4	4
	5	4	4
	6	4	4
	7	4	4
	8	4	4
Rx Post-Cursor Eq	1	3	3
	2	4	4
	3	4	4
	4	4	4
	5	4	4
	6	4	4
	7	4	4
	8	4	4
Rx Amplitude	1	None	0
	2	None	0
	3	None	0
	4	None	0
	5	None	0
	6	None	0
	7	None	0
	8	None	0
Tx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled
Rx CDR Bypass	1	None	Disabled
	2	None	Disabled
	3	None	Disabled
	4	None	Disabled
	5	None	Disabled
	6	None	Disabled
	7	None	Disabled
	8	None	Disabled

R1 Rx Post-Cursor Eq Unconfiguration

Use this command to unconfigure the Rx Post-Cursor Eq on the QSFP-DD module on any specific host lanes, follow these steps.

1. To unconfigure Rx Post-Cursor Eq, execute the following command in the config mode.
```
R1(config)#qsfp-dd 0
R1(config-qsfp-dd)# host-lane 1
R1(config-qsfp-dd-host)# rx-output eq-pre-cursor-target 3
```
2. To unconfigure, execute the following command.
```
R1(config-qsfp-dd)#commit
```

R1 Rx Post-Cursor Eq Unconfiguration Validation

To validate the Rx Post-Cursor Eq unconfiguration, use the following command.

```
OcNOS#show qsfp-dd 0 advertisement si

Port Number                    : 0

-----------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | 3           | 3          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-----------------------------------------------------
 Rx Post-Cursor Eq   | 1    | 4           | 4          |
                     | 2    | 4           | 4          |
                     | 3    | 4           | 4          |
                     | 4    | 4           | 4          |
                     | 5    | 4           | 4          |
                     | 6    | 4           | 4          |
                     | 7    | 4           | 4          |
                     | 8    | 4           | 4          |
-----------------------------------------------------
 Rx Amplitude        | 1    | None        | 0          |
                     | 2    | None        | 0          |
                     | 3    | None        | 0          |
                     | 4    | None        | 0          |
                     | 5    | None        | 0          |
                     | 6    | None        | 0          |
                     | 7    | None        | 0          |
                     | 8    | None        | 0          |
-----------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
```

```
                    | 3    | None         | Disabled   |
                    | 4    | None         | Disabled   |
                    | 5    | None         | Disabled   |
                    | 6    | None         | Disabled   |
                    | 7    | None         | Disabled   |
                    | 8    | None         | Disabled   |
-------------------------------------------------------
 Rx CDR Bypass      | 1    | None         | Disabled   |
                    | 2    | None         | Disabled   |
                    | 3    | None         | Disabled   |
                    | 4    | None         | Disabled   |
                    | 5    | None         | Disabled   |
                    | 6    | None         | Disabled   |
                    | 7    | None         | Disabled   |
                    | 8    | None         | Disabled   |
-------------------------------------------------------
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
QSFP-DD	QSFP-DD stands for Quad Small Form Factor Pluggable Double Density. QSFP-DD modules provide a scalable, high-bandwidth solution for data center networking, enabling efficient data transmission and network performance in modern computing environments.
SI	Signal integrity in networking refers to the reliability and fidelity of electrical signals as they propagate through various components of a network infrastructure.

QSFP-DD Command Reference

CHAPTER 1 QSFP-DD Commands

This chapter is a reference for the QSFP-DD configuration and status commands:

- application
- ha
- hw
- la
- laser channel
- laser grid
- laser fine-tune-freq
- laser output-power
- loopback
- lw
- prbs
- qsfp-dd
- rx-output eq-pre-cursor-target
- rx-output eq-post-cursor-target
- rx-output amp-target
- rx cdr-bypass
- show qsfp-dd advertisement applications
- show qsfp-dd advertisement controls
- show qsfp-dd advertisement diagnostics host
- show qsfp-dd advertisement diagnostics media
- show qsfp-dd advertisement diagnostics module
- show qsfp-dd advertisement durations
- show qsfp-dd advertisement laser
- show qsfp-dd advertisement monitors host
- show qsfp-dd advertisement monitors media
- show qsfp-dd advertisement monitors module
- show qsfp-dd advertisement pages
- show qsfp-dd application
- show qsfp-dd diagnostics host
- show qsfp-dd diagnostics media
- show qsfp-dd eeprom
- show qsfp-dd laser grid
- show qsfp-dd laser status
- show qsfp-dd monitors host
- show qsfp-dd monitors media

© 2025 IP Infusion Inc. Proprietary

- show qsfp-dd monitors module
- show qsfp-dd state
- show qsfp-dd user-threshold status
- tx-input eq-target
- tx cdr-bypass
- threshold (host-lane mode)
- threshold (media-lane mode)
- threshold (QSFP-DD mode)

application

Use this command to select the application ID to be configured for this QSFP-DD module.

Use the `no` parameter with this command to remove this configuration. If no application is configured then application ID 1 will be selected as per module default.

Note: Only 400G application modes are supported.

Note: For checking the supported applications modes `show qsfp-dd <port no.> advertisement applications` command, see the example.

Example:

```
OcNOS#show qsfp-dd 49 application

Port Number                     : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 2  |   Application 2

OcNOS#sh qsfp-dd 49 advertisement applications

Port Number                   : 49
> Application 1:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2.000000
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, DWDM, Amplified
         Application BR       : 478.75
         Lane Count           : 1
         Lane Sig BR          : 59.84375
         Modulation Format    : DP-16QAM
         Bits Per Unit Intvl  : 8.000000
         Lane Assigned        : Lane-1
  Application 2:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2.000000
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, Single Wavelen., Unamp.
         Application BR       : 478.75
         Lane Count           : 1
         Lane Sig BR          : 59.84375
         Modulation Format    : DP-16QAM
```

```
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 3:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : 400ZR, DWDM, Amplified
       Application BR       : 478.75
       Lane Count           : 1
       Lane Sig BR          : 59.84375
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 4:
  | Host |
       Interface            : 400GAUI-8 C2M
       Application BR       : 425.00
       Lane Count           : 8
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-1
  | Media |
       Interface            : ZR400-OFEC-16QAM
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 5:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR400-OFEC-16QAM
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 6:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
```

```
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR300-OFEC-8QAM
        Application BR       : 360.831281
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-8QAM
        Bits Per Unit Intvl  : 6.000000
        Lane Assigned        : Lane-1
  Application 7:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR200-OFEC-QPSK
        Application BR       : 240.554187
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
  Application 8:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR100-OFEC-QPSK
        Application BR       : 120.277094
        Lane Count           : 1
        Lane Sig BR          : 30.069273
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
```

Command Syntax

```
application <2-15>
```

Parameters

`<2-15>`	Configurable application IDs

Command Mode

QSFP-DD mode

Default

By default, application ID 1 is selected.

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#application 8
(config-qsfp-dd)#commit
(config-qsfp-dd)#no application
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

laser channel

Use this command to configure the laser channel number for the QSFP-DD module.

Command Syntax

```
laser channel NUMBER
no laser channel
```

Parameters

NUMBER	channel number

Default

None.

Command Mode

QSFP-DD mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#laser channel 10
(config-qsfp-dd)#commit
(config-qsfp-dd)#no laser channel
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

laser grid

Use this command to configure the laser grid spacing frequency for the QSFP-DD module.

Command Syntax

```
laser grid (3p125|6p25|12p5|25|33|50|75|100)
no laser grid
```

Parameters

3p125	3.125 GHz
6p25	6.25 GHz
12p5	12.5 GHz
25	25 GHz
33	33 GHz
50	50 GHz
75	75 GHz
100	100 GHz

Default

None.

Command Mode

QSFP-DD mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#laser grid 50
(config-qsfp-dd)#commit
(config-qsfp-dd)#no laser grid
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

laser fine-tune-freq

Use this command to configure the laser fine tune frequency offset for the QSFP-DD module.

Command Syntax

```
laser fine-tune-freq VALUE
no laser fine-tune-freq
```

Parameters

VALUE	Fine tune frequency offset in GHz

Default

None.

Command Mode

QSFP-DD mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#laser fine-tune-freq 1.5
(config-qsfp-dd)#commit
(config-qsfp-dd)#no laser fine-tune-freq
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

laser output-power

Use this command to configure the laser target output power for the QSFP-DD module.

Command Syntax

```
laser output-power VALUE
no laser output-power
```

Parameters

VALUE	Laser target output power

Default

None.

Command Mode

QSFP-DD mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#laser output-power -9.2
(config-qsfp-dd)#commit
(config-qsfp-dd)#no laser output-power
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

loopback

Use this command to configure the loopback type (input, output, both) on the QSFP-DD module host/media side. If the loopback type is supported by the QSFP-DD module this will enable the loopback function.

Use the `no` parameter to remove this configuration and disable the loopback function.

Command Syntax

```
loopback (in|out|both) (host|media)
no loopback (host|media)
```

Parameters

`in`	Configure input loopback
`out`	Configure output looback
`both`	Configure input and output loopback
`host`	Configure host side
`media`	Configure media side

Command Mode

QSFP-DD mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
(config)#qsfp-dd 0
(config-qsfp-dd)#loopback in host
(config-qsfp-dd)#loopback out media
(config-qsfp-dd)#commit
(config-qsfp-dd)#loopback both media
(config-qsfp-dd)#no loopback host
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

prbs

Use these commands to configure the PRBS pattern generator/checker type to be used for diagnostics of the QSFP-DD module host/media side and to configure the PRBS pattern generator/checker location (pre-fec/post-fec) on the QSFP-DD module host/media side. If the generator/checker pattern type and location are supported by the QSFP-DD module this will enable the selected function.

Use the `no` parameter to remove this configuration and disable the generator/checker function.

Command Syntax

```
prbs (generator|checker) type (31q|31|23q|23|15q|15|13q|13|9q|9|7q|7|ssprq)
  (host|media)
prbs (generator|checker) (pre-fec|post-fec) (host|media)
no prbs (generator|checker) type (host|media)
no prbs (generator|checker) (host|media)
```

Parameters

`generator`	Configure the pattern generator
`checker`	Configure the pattern checker
`31q`	Configure PRBS-31Q type
`31`	Configure PRBS-31 type
`23q`	Configure PRBS-23Q type
`23`	Configure PRBS-23 type
`15q`	Configure PRBS-15Q type
`15`	Configure PRBS-15 type
`13q`	Configure PRBS-13Q type
`13`	Configure PRBS-13 type
`9q`	Configure PRBS-9Q type
`9`	Configure PRBS-9 type
`7q`	Configure PRBS-7q type
`7`	Configure PRBS-7 type
`ssprq`	Configure SSPRQ type
`pre-fec`	Configure to generate before the FEC encoder / check before the FEC decoder
`post-fec`	Configure to generate after the FEC encoder / check after the FEC decoder
`host`	Configure host side
`media`	Configure media side

Command Mode

QSFP-DD mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#prbs generator type 15 host
(config-qsfp-dd)#prbs checker type 23q host
(config-qsfp-dd)#prbs generator type 7q media
(config-qsfp-dd)#prbs checker type ssprq media
(config-qsfp-dd)#commit
(config-qsfp-dd)#no prbs generator type host
(config-qsfp-dd)#no prbs checker type media
(config-qsfp-dd)#commit
(config-qsfp-dd)#
```

qsfp-dd

Use this command to select a QSFP-DD port to configure and enter the `qsfp-dd` command mode. Use the `exit` command to quit from this mode.

Command Syntax

```
qsfp-dd PORTNUM
```

Parameters

`PORTNUM`	QSFP-DD front panel port number

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#
```

rx-output eq-pre-cursor-target

Use this command to configure the Rx output equalizer pre-cursor target override value.

Use the no form of this command to remove the Rx output equalizer pre-cursor target override value.

Command Syntax

```
rx-output eq-pre-cursor-target <1-15>
no rx-output eq-pre-cursor-target
```

Parameters

<1-15>	Output equalizer pre-cursor target value

Default

None.

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#rx-output eq-pre-cursor-target 4
(config-qsfp-dd)#commit
(config-qsfp-dd)#no rx-output eq-pre-cursor-target
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 2
(config-qsfp-dd-host)#rx-output eq-pre-cursor-target 1
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no rx-output eq-pre-cursor-target
(config-qsfp-dd-host)#commit
```

© 2025 IP Infusion Inc. Proprietary

rx-output eq-post-cursor-target

Use this command to configure the Rx output equalizer post-cursor target override value.

Use the no form of this command to remove the Rx output equalizer post-cursor target override value..

Command Syntax

```
rx-output eq-post-cursor-target <1-15>
no rx-output eq-post-cursor-target
```

Parameters

<1-15>	Output equalizer post-cursor target value

Default

None.

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#rx-output eq-post-cursor-target 2
(config-qsfp-dd)#commit
(config-qsfp-dd)#no rx-output eq-post-cursor-target
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 7
(config-qsfp-dd-host)#rx-output eq-post-cursor-target 6
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no rx-output eq-post-cursor-target
(config-qsfp-dd-host)#commit
```

rx-output amp-target

Use this command to configure the Rx output amplitude target override value.

Use the no form of this command to remove the Rx output amplitude target override value.

Command Syntax

```
rx-output amp-target <0-15>
no rx-output amp-target
```

Parameters

<1-15>	Output amplitude target value

Default

None.

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#rx-output amp-target 0
(config-qsfp-dd)#commit
(config-qsfp-dd)#no rx-output amp-target
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 3
(config-qsfp-dd-host)#rx-output amp-target 1
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no rx-output amp-target
(config-qsfp-dd-host)#commit
```

rx cdr-bypass

Use this command to enable the Rx CDR bypass.

Use the no form of this command to disable the Rx CDR bypass.

Command Syntax

```
rx cdr-bypass
no rx cdr-bypass
```

Parameters

None

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#rx cdr-bypass
(config-qsfp-dd)#commit
(config-qsfp-dd)#no rx cdr-bypass
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 2
(config-qsfp-dd-host)#rx cdr-bypass
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no rx cdr-bypass
```

© 2025 IP Infusion Inc. Proprietary

show qsfp-dd advertisement applications

Use this command to show QSFP-DD module advertised applications.

Command Syntax

```
show qsfp-dd PORTNUM advertisement applications
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement applications

Port Number                   : 0
> Application 1:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, DWDM, Amplified
         Application BR       : 478.75
         Lane Count           : 1
         Lane Sig BR          : 59.84375
         Modulation Format    : DP-16QAM
         Bits Per Unit Intvl  : 8
         Lane Assigned        : Lane-1
  Application 2:
    | Host |
         Interface            : 400GAUI-8 C2M
         Application BR       : 425.00
         Lane Count           : 8
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2
         Lane Assigned        : Lane-1
    | Media |
         Interface            : 400ZR, Single Wavelen., Unamp.
         Application BR       : 478.75
         Lane Count           : 1
         Lane Sig BR          : 59.84375
         Modulation Format    : DP-16QAM
```

```
       Bits Per Unit Intvl  : 8
       Lane Assigned        : Lane-1
Application 3:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : 400ZR, DWDM, Amplified
       Application BR       : 478.75
       Lane Count           : 1
       Lane Sig BR          : 59.84375
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8
       Lane Assigned        : Lane-1
Application 4:
  | Host |
       Interface            : 400GAUI-8 C2M
       Application BR       : 425.00
       Lane Count           : 8
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2
       Lane Assigned        : Lane-1
  | Media |
       Interface            : 400ZRP, DWDM, amplified 120Km
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8
       Lane Assigned        : Lane-1
Application 5:
  | Host |
       Interface            : 400GAUI-8 C2M
       Application BR       : 425.00
       Lane Count           : 8
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2
       Lane Assigned        : Lane-1
  | Media |
       Interface            : 400ZRP, DWDM, Amplified 450Km
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8
       Lane Assigned        : Lane-1
Application 6:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
```

```
          Lane Count           : 2
          Lane Sig BR          : 26.5625
          Modulation Format    : PAM4
          Bits Per Unit Intvl  : 2
          Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
      | Media |
          Interface            : 400ZRP, DWDM, Amplified 450Km
          Application BR       : 481.108374
          Lane Count           : 1
          Lane Sig BR          : 60.1385468
          Modulation Format    : DP-16QAM
          Bits Per Unit Intvl  : 8
          Lane Assigned        : Lane-1
    Application 7:
      | Host |
          Interface            : 100GAUI-2 C2M
          Application BR       : 106.25
          Lane Count           : 2
          Lane Sig BR          : 26.5625
          Modulation Format    : PAM4
          Bits Per Unit Intvl  : 2
          Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
      | Media |
          Interface            : 100ZRP, DWDM, Amplified 600Km
          Application BR       : 360.831281
          Lane Count           : 1
          Lane Sig BR          : 60.1385468
          Modulation Format    : DP-8QAM
          Bits Per Unit Intvl  : 6
          Lane Assigned        : Lane-1
    Application 8:
      | Host |
          Interface            : 400GAUI-8 C2M
          Application BR       : 425.00
          Lane Count           : 8
          Lane Sig BR          : 26.5625
          Modulation Format    : PAM4
          Bits Per Unit Intvl  : 2
          Lane Assigned        : Lane-1
      | Media |
          Interface            : 400ZRP, DWDM, amplified 450Km (Enhanced
  Constellation)
          Application BR       : 481.108374
          Lane Count           : 1
          Lane Sig BR          : 60.1385468
          Modulation Format    : DP-16QAM
          Bits Per Unit Intvl  : 8
          Lane Assigned        : Lane-1
    Application 9:
      | Host |
          Interface            : 100GAUI-2 C2M
          Application BR       : 106.25
          Lane Count           : 2
          Lane Sig BR          : 26.5625
          Modulation Format    : PAM4
          Bits Per Unit Intvl  : 2
          Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
```

```
    | Media |
         Interface            : 400ZRP, DWDM, amplified 450Km (Enhanced
Constellation)
         Application BR       : 481.108374
         Lane Count           : 1
         Lane Sig BR          : 60.1385468
         Modulation Format    : DP-16QAM
         Bits Per Unit Intvl  : 8
         Lane Assigned        : Lane-1
  Application 10:
    | Host |
         Interface            : 100GAUI-2 C2M
         Application BR       : 106.25
         Lane Count           : 2
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2
         Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
         Interface            : 100ZRP, DWDM, amplified 600Km (Enhanced
Constellation)
         Application BR       : 360.831281
         Lane Count           : 1
         Lane Sig BR          : 60.1385468
         Modulation Format    : DP-8QAM
         Bits Per Unit Intvl  : 6
         Lane Assigned        : Lane-1
  Application 11:
    | Host |
         Interface            : 100GAUI-2 C2M
         Application BR       : 106.25
         Lane Count           : 2
         Lane Sig BR          : 26.5625
         Modulation Format    : PAM4
         Bits Per Unit Intvl  : 2
         Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
         Interface            : 100ZRP, DWDM, Amplified 1000Km
         Application BR       : 240.554187
         Lane Count           : 1
         Lane Sig BR          : 60.1385468
         Modulation Format    : DP-QPSK
         Bits Per Unit Intvl  : 4
         Lane Assigned        : Lane-1
  Application 12:
    | Host |
         Interface            : CAUI-4 C2M without FEC
         Application BR       : 103.13
         Lane Count           : 4
         Lane Sig BR          : 25.78125
         Modulation Format    : NRZ
         Bits Per Unit Intvl  : 1
         Lane Assigned        : Lane-5/Lane-1
    | Media |
         Interface            : 100ZRP, DWDM, Amplified 1000Km
         Application BR       : 240.554187
         Lane Count           : 1
```

```
        Lane Sig BR           : 60.1385468
        Modulation Format     : DP-QPSK
        Bits Per Unit Intvl   : 4
        Lane Assigned         : Lane-1
Application 13:
  | Host |
        Interface             : 100GAUI-2 C2M
        Application BR        : 106.25
        Lane Count            : 2
        Lane Sig BR           : 26.5625
        Modulation Format     : PAM4
        Bits Per Unit Intvl   : 2
        Lane Assigned         : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
        Interface             : 100ZRP, DWDM, amplified 2000Km
        Application BR        : 120.277094
        Lane Count            : 1
        Lane Sig BR           : 30.069273
        Modulation Format     : DP-QPSK
        Bits Per Unit Intvl   : 4
        Lane Assigned         : Lane-1
Application 14:
  | Host |
        Interface             : CAUI-4 C2M without FEC
        Application BR        : 103.13
        Lane Count            : 4
        Lane Sig BR           : 25.78125
        Modulation Format     : NRZ
        Bits Per Unit Intvl   : 1
        Lane Assigned         : Lane-5/Lane-1
  | Media |
        Interface             : 100ZRP, DWDM, amplified 2000Km
        Application BR        : 120.277094
        Lane Count            : 1
        Lane Sig BR           : 30.069273
        Modulation Format     : DP-QPSK
        Bits Per Unit Intvl   : 4
        Lane Assigned         : Lane-1
```

show qsfp-dd advertisement controls

Use this command to show QSFP-DD module advertised controls.

Command Syntax

```
show qsfp-dd PORTNUM advertisement controls
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement controls

Port Number                    : 0
Wavelength Control             : Yes
Tunable Transmitter            : Yes
Tx Output Squelching           : Not Supported
Forced Tx Output Squelching    : No
Tx Output Squelching Disable   : No
Tx Output Disable              : Yes
Input Polarity Flip Tx         : Yes
Rx Output Squelching Disable   : Yes
Rx Output Disable              : Yes
Output Polarity Flip Rx        : Yes
```

show qsfp-dd advertisement diagnostics host

Use this command to show QSFP-DD module advertised host side diagnostics.

Command Syntax

```
show qsfp-dd PORTNUM advertisement diagnostics host
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement diagnostics host

Port Number                    : 0
| Supported Loopback Modes |
     Output                    : Yes
     Input                     : Yes
     Per Lane                  : Yes
| Reporting Capabilities |
     Input SNR                 : No
     FEC                       : Yes
| PRBS Checker |
     Post FEC                  : Yes
     Pre FEC                   : Yes
     Types                     : PRBS-31Q, PRBS-31, PRBS-23Q, PRBS-23, PRBS-
15Q, PRBS-15, PRBS-13Q, PRBS-13, PRBS-9Q, PRBS-9, PRBS-7Q, PRBS-7
| PRBS Generator |
     Post FEC                  : Yes
     Pre FEC                   : Yes
     Types                     : PRBS-31Q, PRBS-31, PRBS-23Q, PRBS-23, PRBS-
15Q, PRBS-15, PRBS-13Q, PRBS-13, PRBS-9Q, PRBS-9, PRBS-7Q, PRBS-7
```

show qsfp-dd advertisement diagnostics media

Use this command to show QSFP-DD module advertised media side diagnostics.

Command Syntax

```
show qsfp-dd PORTNUM advertisement diagnostics media
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement diagnostics media

Port Number                    : 0
| Supported Loopback Modes |
     Output                    : Yes
     Input                     : No
     Per Lane                  : Yes
| Reporting Capabilities |
     Input SNR                 : Yes
     FEC                       : Yes
| PRBS Checker |
     Post FEC                  : Yes
     Pre FEC                   : No
     Types                     : PRBS-31, PRBS-23, PRBS-15, PRBS-7
| PRBS Generator |
     Post FEC                  : Yes
     Pre FEC                   : Yes
     Types                     : PRBS-31, PRBS-23, PRBS-15, PRBS-7
```

show qsfp-dd advertisement diagnostics module

Use this command to show QSFP-DD module advertised diagnostics.

Command Syntax

```
show qsfp-dd PORTNUM advertisement diagnostics module
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement diagnostics module

Port Number                    : 0
| Supported Loopback Modes |
     Simul. Host & Media Side  : Yes
| Reporting Capabilities |
     Bit Error Ratio           : Yes
     Bits & Errors Counting    : Yes
```

show qsfp-dd advertisement durations

Use this command to show module advertised durations

Command Syntax

```
show qsfp-dd PORTNUM advertisement durations
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement durations

Port Number                    : 0
ModSel Wait                    : 4 us
DP Init Max                    : 10 s <= t < 1 min
DP Deinit Max                  : 1 s <= t < 5 s
DP Tx Turn On Max              : 50 ms <= t < 100 ms
DP Tx Turn Off Max             : 1 ms <= t < 5 ms
Module Power Up Max            : 10 s <= t < 1 min
Module Power Down Max          : 1 s <= t < 5 s
```

© 2025 IP Infusion Inc. Proprietary

show qsfp-dd advertisement laser

Use this command to show QSFP-DD module advertised laser controls.

Command Syntax

```
show qsfp-dd PORTNUM advertisement laser
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement laser

Port Number                          : 0
Supported Grids                      : 6.25 GHz, 12.5 GHz, 25 GHz, 50 GHz, 100
GHz, 75 GHz
   6.25 GHz Channels                 : Low=191.275 THz, High=196.125 THz,
Total=776
   12.5 GHz Channels                 : Low=191.275 THz, High=196.125 THz,
Total=388
   25 GHz Channels                   : Low=191.275 THz, High=196.125 THz,
Total=194
   50 GHz Channels                   : Low=191.300 THz, High=196.100 THz,
Total=96
   100 GHz Channels                  : Low=191.300 THz, High=196.100 THz,
Total=48
   75 GHz Channels                   : Low=191.300 THz, High=196.100 THz,
Total=64
Fine Tuning Support                  : Yes
   Fine Tuning Resolution            : 0.001 GHz
   Fine Tuning Low Offset            : -6.000 GHz
   Fine Tuning High Offset           : 6.000 GHz
Output Power Programmable Per Lane : Yes
   Min Output Power Programmable     : -22.90 dBm
   Max Output Power Programmable     : 4.00 dBm
```

show qsfp-dd advertisement monitors host

Use this command to show QSFP-DD module advertised host side monitors.

Command Syntax

```
show qsfp-dd PORTNUM advertisement monitors host
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement monitors host

Port Number                         : 0
Pre-FEC BER Minimum Input           : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
Pre-FEC BER Maximum Input           : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
Pre-FEC BER Average Input           : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
Pre-FEC BER Current Value Input     : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
FERC Minimum Input                  : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
FERC Maximum Input                  : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
FERC Average Input                  : Yes [Lane 1, Lane 3, Lane 5, Lane 7]
FERC Current Value Input            : Yes [Lane 1, Lane 3, Lane 5, Lane 7]

| Link Performance |
     Tx FDD                         : Yes
     Tx FED                         : Yes
```

show qsfp-dd advertisement monitors media

Use this command to show QSFP-DD module advertised media side monitors.

Command Syntax

```
show qsfp-dd PORTNUM advertisement monitors media
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement monitors media

Port Number                          : 0
Rx Optical Power                     : Yes
Tx Optical Power                     : Yes
Tx Bias                              : Yes
Rx Los                               : Yes
Tx Failure                           : Yes
Rx CDR LOL                           : Yes
Laser Age                            : Yes [Lane 1]
Pre-FEC BER Minimum Input            : Yes [Lane 1]
Pre-FEC BER Maximum Input            : Yes [Lane 1]
Pre-FEC BER Average Input            : Yes [Lane 1]
Pre-FEC BER Current Value Input      : Yes [Lane 1]
FERC Minimum Input                   : Yes [Lane 1]
FERC Maximum Input                   : Yes [Lane 1]
FERC Average Input                   : Yes [Lane 1]
FERC Current Value Input             : Yes [Lane 1]
Modular Bias X/I                     : Yes [Lane 1]
Modular Bias X/Q                     : Yes [Lane 1]
Modular Bias Y/I                     : Yes [Lane 1]
Modular Bias Y/Q                     : Yes [Lane 1]
Modular Bias X_Phase                 : Yes [Lane 1]
Modular Bias Y_Phase                 : Yes [Lane 1]
CD - high granularity, short link    : Yes [Lane 1]
CD - low granularity, long link      : Yes [Lane 1]
DGD                                  : Yes [Lane 1]
SOPMD - high granularity             : Yes [Lane 1]
PDL                                  : Yes [Lane 1]
OSRN                                 : Yes [Lane 1]
eSRN                                 : Yes [Lane 1]
CFO                                  : Yes [Lane 1]
Tx Power                             : Yes [Lane 1]
Rx Total Power                       : Yes [Lane 1]
Rx Signal Power                      : Yes [Lane 1]
```

```
SOP ROC                              : Yes [Lane 1]
SOPMD - low granularity              : Yes [Lane 1]

| FEC Performance |
     Rx Bits                         : Yes
     Rx Correct Bits                 : Yes
     Rx Frames                       : Yes
     Rx Uncorrect Frames             : Yes

| Link Performance |
     Rx DSP CCD                      : Yes
     Rx DSP DGD                      : Yes
     Rx SOPM                         : Yes
     Rx PDL                          : Yes
     Rx oSNR                         : Yes
     Rx eSNR                         : Yes
     Rx CFO                          : Yes
     Rx EvmModem                     : No
     Tx Power                        : Yes
     Rx Input Optical Power          : Yes
     Rx input Optical Signal Power   : Yes
     Rx SOPCR                        : Yes
     Rx SOPMD Low Granularity        : No
     Rx Clock Recovery Monitor       : No
     Rx FDD                          : Yes
     Rx FEC                          : Yes
```

show qsfp-dd advertisement monitors module

Use this command to show QSFP-DD module advertised monitors

Command Syntax

```
show qsfp-dd PORTNUM advertisement monitors module
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 advertisement monitors module

Port Number                    : 0
Voltage                        : Yes
Temperature                    : Yes
TEC Current                    : Yes
Laser Temperature              : Yes
Laser Temperature [2]          : No

Rx Power                       : Yes
Rx Signal Power                : Yes
```

show qsfp-dd advertisement pages

Use this command to show QSFP-DD module advertised supported pages.

Command Syntax

```
show qsfp-dd PORTNUM advertisement pages
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 application

Port Number                     : 0
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   None           |   Application 1
OcNOS>show qsfp-dd 0 advertisement pages

Port Number                     : 0
Network Path                    : No
VDM                             : Yes
VDM Support                     : Groups 1-2 (Page 20h-21h, 24h-25h, 28h-29h,
first 1/2 of 2Ch, 2Dh)
Diagnostics                     : Yes
User(Page 03h)                  : Yes
Banks(Page 10h-1Fh)             : Bank 0 (8 Lanes)
```

show qsfp-dd advertisement si

Use this command to display which signal integrity configuration capabilities the transceiver supports.

Command Syntax

```
show qsfp-dd <port> advertisement si
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#show qsfp-dd 0 advertisement si

-------------------------------------------------
                    Codes
-------------------------------------------------
Tx Equalization     >  1 - 12  : 1dB - 12db
                       13 - 15 : Vendor Specific
-------------------------------------------------
Rx Pre-Cursor Eq    >  1 - 7   : 0.5 - 3.5dB
                       8 - 10  : Reserved
                       11 - 15 : Vendor Specific
-------------------------------------------------
Rx Post-Cursor Eq   >  1 - 7   : 1 - 7dB
                       8 - 10  : Reserved
                       11 - 15 : Vendor Specific
-------------------------------------------------
Rx Amplitude        >  0       : 100-400mV (P-P)
                       1       : 300-600mV (P-P)
                       2       : 400-800mV (P-P)
                       3       : 600-1200mV (P-P)
                       4 - 15  : Reserved
-------------------------------------------------
Port Number                    : 0

Manual Tx Input Eq.            : No

Rx Output Eq. Type             : P-P with constant amplitude/NA/Unknown

Rx Output Amplitude            : No

Rx Output Eq.                  : Pre and post-cursor
Rx Output Eq. Pre-Cursor Max   : Code 7(3.5dB)
Rx Output Eq. Post-Cursor Max  : Code 7(7dB)

Tx CDR Supported               : Yes
```

```
Tx CDR Bypass Supported        : No

Rx CDR Supported               : Yes
Rx CDR Bypass Supported        : No
```

show qsfp-dd si status

Use this command to display what is the current signal integrity configuration status. It displays what is the current user configuration and what are the values programmed in the transceiver hardware.

Command Syntax

```
show qsfp-dd <port> si status
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#show qsfp-dd 0 si status

Port Number                    : 0

-----------------------------------------------------------
      Parameter      | Lane | User Config | H/W Config |
-----------------------------------------------------------
 Rx Pre-Cursor Eq    | 1    | None        | 11         |
                     | 2    | None        | 11         |
                     | 3    | None        | 11         |
                     | 4    | None        | 11         |
                     | 5    | None        | 11         |
                     | 6    | None        | 11         |
                     | 7    | None        | 11         |
                     | 8    | None        | 11         |
-----------------------------------------------------------
 Rx Post-Cursor Eq   | 1    | None        | 11         |
                     | 2    | None        | 11         |
                     | 3    | None        | 11         |
                     | 4    | None        | 11         |
                     | 5    | None        | 11         |
                     | 6    | None        | 11         |
                     | 7    | None        | 11         |
                     | 8    | None        | 11         |
-----------------------------------------------------------
 Tx CDR Bypass       | 1    | None        | Disabled   |
                     | 2    | None        | Disabled   |
                     | 3    | None        | Disabled   |
                     | 4    | None        | Disabled   |
                     | 5    | None        | Disabled   |
                     | 6    | None        | Disabled   |
                     | 7    | None        | Disabled   |
                     | 8    | None        | Disabled   |
-----------------------------------------------------------
```

```
 Rx CDR Bypass        | 1    | None         | Disabled   |
                      | 2    | None         | Disabled   |
                      | 3    | None         | Disabled   |
                      | 4    | None         | Disabled   |
                      | 5    | None         | Disabled   |
                      | 6    | None         | Disabled   |
                      | 7    | None         | Disabled   |
                      | 8    | None         | Disabled   |
-------------------------------------------------------------
```

show qsfp-dd application

Use this command to show QSFP-DD module current selected application.

Command Syntax

```
show qsfp-dd PORTNUM application
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 application

Port Number                     : 0
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   None           |   Application 1
```

show qsfp-dd diagnostics host

Use this command to show QSFP-DD module host side diagnostics information.

Command Syntax

```
show qsfp-dd PORTNUM diagnostics host
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 diagnostics host

Port Number                     : 0
-----------------------------------------------------
       Attribute      | Lane |        Value         |
-----------------------------------------------------
Bit Error Ratio       |  1   | 0.00e+00             |
                      |  2   | 0.00e+00             |
                      |  3   | 0.00e+00             |
                      |  4   | 0.00e+00             |
                      |  5   | 0.00e+00             |
                      |  6   | 0.00e+00             |
                      |  7   | 0.00e+00             |
                      |  8   | 0.00e+00             |
Bit Error Ratio(G)    |  1   | 0.00e+00             |
                      |  2   | 0.00e+00             |
                      |  3   | 0.00e+00             |
                      |  4   | 0.00e+00             |
                      |  5   | 0.00e+00             |
                      |  6   | 0.00e+00             |
                      |  7   | 0.00e+00             |
                      |  8   | 0.00e+00             |
Error Count           |  1   | 0                    |
                      |  2   | 0                    |
                      |  3   | 0                    |
                      |  4   | 0                    |
                      |  5   | 0                    |
                      |  6   | 0                    |
                      |  7   | 0                    |
                      |  8   | 0                    |
Bit Count             |  1   | 0                    |
                      |  2   | 0                    |
                      |  3   | 0                    |
                      |  4   | 0                    |
                      |  5   | 0                    |
```

```
                        |  6   | 0                    |
                        |  7   | 0                    |
                        |  8   | 0                    |
Error Count(G)          |  1   | 0                    |
                        |  2   | 0                    |
                        |  3   | 0                    |
                        |  4   | 0                    |
                        |  5   | 0                    |
                        |  6   | 0                    |
                        |  7   | 0                    |
                        |  8   | 0                    |
Bit Count(G)            |  1   | 0                    |
                        |  2   | 0                    |
                        |  3   | 0                    |
                        |  4   | 0                    |
                        |  5   | 0                    |
                        |  6   | 0                    |
                        |  7   | 0                    |
                        |  8   | 0                    |
```

show qsfp-dd diagnostics media

Use this command to show QSFP-DD module media side diagnostics information.

Command Syntax

```
show qsfp-dd PORTNUM diagnostics media
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 diagnostics media

Port Number                     : 0
-----------------------------------------------------
       Attribute      | Lane |        Value         |
-----------------------------------------------------
Signal To Noise Ratio |  1   | 0.00                 |
Bit Error Ratio       |  1   | 0.00e+00             |
Bit Error Ratio(G)    |  1   | 0.00e+00             |
Error Count           |  1   | 0                    |
Bit Count             |  1   | 0                    |
Error Count(G)        |  1   | 0                    |
Bit Count(G)          |  1   | 0                    |
```

show qsfp-dd eeprom

Use this command to show QSFP-DD module EEPROM information.

Command Syntax

```
show qsfp-dd PORTNUM eeprom
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 eeprom

Port Number                    : 0
Identifier                     : QSFP-DD Double Density 8X Pluggable
Transceiver
Name                           : SmartOptics
OUI                            : 0x0 0x53 0x4f
Part No                        : SO-TQSFPDD4CCZRP
Revision Level                 : A
Serial_Number                  : 214156190
Manufacturing Date             : 220318   (yymmddvv, v=vendor specific)
Module Power Class             : 8
Module Max Power               : 23.75 Watt
Cooling Implemented            : Yes
Module Temperature Max         : 80 Celsius
Module Temperature Min         : 0 Celsius
Operating Voltage Min          : 3.12 Volt
Optical Detector               : PIN
Rx Power Measurement           : Average Power
Tx Disable Module Wide         : No
Cable Assembly Link Length     : Separable Media
Connector Type                 : LC (Lucent Connector)
Media Interface Technology     : 1550 nm DFB
CMIS Revision                  : 4.1
Memory Model                   : Paged
MCI Max Speed                  : 1000 kHz
Active Firmware Revision       : 61.20
Inactive Firmware Revision     : 61.20
Hardware Revision              : 49.48
Media Type                     : Optical SMF
Max SMF Link Length            : 630.0 Kilometer
Wavelength Nominal             : 1547.70 nm
Wavelength Tolerance           : 166.55 nm
```

show qsfp-dd laser grid

Use this command to show QSFP-DD module laser grid spacing information for frequencies of 3.125, 6.25 12.5 25, 33, 50, 75 and 100 GHz.

Command Syntax

```
show qsfp-dd PORTNUM laser grid (3p125|6p25|12p5|25|33|50|75|100)
```

Parameters

PORTNUM	QSFP-DD front panel port number
3p125	3.125 GHz
6p25	6.25 GHz
12p5	12.5 GHz
25	25 GHz
33	33 GHz
50	50 GHz
75	75 GHz
100	100 GHz

Default

None.

Command Mode

Exec mode and Privileged Exec mode.

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
show qsfp-dd 0 laser grid 100

Port Number          : 0

-----------------------------------------------------
Channel Number  Frequency (THz) Wavelength (nm)
-----------------------------------------------------
        -18      191.300000              1567.133
        -17      191.400000              1566.314
        -16      191.500000              1565.496
        -15      191.600000              1564.679
        -14      191.700000              1563.863
        -13      191.800000              1563.047
        -12      191.900000              1562.233
        -11      192.000000              1561.419
        -10      192.100000              1560.606
        -9       192.200000              1559.794
        -8       192.300000              1558.983
```

-7	192.400000	1558.173
-6	192.500000	1557.363
-5	192.600000	1556.555
-4	192.700000	1555.747
-3	192.800000	1554.940
-2	192.900000	1554.134
-1	193.000000	1553.329
0	193.100000	1552.524
1	193.200000	1551.721
2	193.300000	1550.918
3	193.400000	1550.116
4	193.500000	1549.315
5	193.600000	1548.515
6	193.700000	1547.715
7	193.800000	1546.917
8	193.900000	1546.119
9	194.000000	1545.322
10	194.100000	1544.526
11	194.200000	1543.730
12	194.300000	1542.936
13	194.400000	1542.142
14	194.500000	1541.349
15	194.600000	1540.557
16	194.700000	1539.766
17	194.800000	1538.976
18	194.900000	1538.186
19	195.000000	1537.397
20	195.100000	1536.609
21	195.200000	1535.822
22	195.300000	1535.036
23	195.400000	1534.250
24	195.500000	1533.465
25	195.600000	1532.681
26	195.700000	1531.898
27	195.800000	1531.116
28	195.900000	1530.334
29	196.000000	1529.553
30	196.100000	1528.773

© 2025 IP Infusion Inc. Proprietary

show qsfp-dd laser status

Use this command to show QSFP-DD module current laser configuration status and alarm flags.

Command Syntax

```
show qsfp-dd PORTNUM laser status
```

Parameters

PORTNUM	QSFP-DD front panel port number

Default

None.

Command Mode

Exec mode and Privileged Exec mode.

Applicability

This command was introduced in OcNOS version 6.2.0.

Examples

```
show qsfp-dd 0 laser status

Port Number          : 0

-------------------------------------------------
       Attribute      | Lane |    Value    | Unit |
-------------------------------------------------
 Grid Spacing         |  1   | 100.000     | GHz  |
 Laser Frequency      |  1   | 191.900000  | THz  |
 Channel Number       |  1   | -12         | --   |
 Wavelength           |  1   | 1562.23     | nm   |

-------------------------------------
        Flag        | Lane | Status |
-------------------------------------
 Tuning in progress |  1   | No     |
 Wavelength locked  |  1   | Yes    |

-----------------------------------------------
          Flag           | Lane | Status (L) |
-----------------------------------------------
 Target output power OOR  |  1   | No         |
 Fine tuning out of range |  1   | No         |
 Tuning accepted          |  1   | Yes        |
 Channel number valid     |  1   | Yes        |
```

show qsfp-dd monitors host

Use this command to show QSFP-DD module host side monitors information.

Command Syntax

```
show qsfp-dd PORTNUM monitors host
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 monitors host

Alarm Codes: FDD - FEC Detected Degrade, FED - FEC Excessive Degrade
             LD - Local Degrade, RD - Remote Degrade
             FLOPB - Flexe Loss of Pad Block, FLOMF - Flexe Loss of Multi-
Frame
             FLOF - Flexe Loss of Frame, FIIDM - Flexe Instance Id Mismatch
             FCM - Flexe Calendar Mismatch, FIMM - Flexe Instance Map Mismatch
             FGIDM - Flexe GID Mismatch, TLF - Transmit Local Fault
             TRF - Transmit Remote Fault, TLOA - Transmit Loss of Alignment
             RLF - Receive Local Fault, RRF - Receive Remote Fault
             RLOA - Receive Loss of Alignment

Port Number                    : 0
-------------------------------------------------
         Flag          | Lane |    Status (L)    |
-------------------------------------------------
Tx LOS                 |  1   |  False           |
                       |  2   |  False           |
                       |  3   |  False           |
                       |  4   |  False           |
                       |  5   |  False           |
                       |  6   |  False           |
                       |  7   |  False           |
                       |  8   |  False           |
Tx CDR LOL             |  1   |  False           |
                       |  2   |  False           |
                       |  3   |  False           |
                       |  4   |  False           |
                       |  5   |  False           |
                       |  6   |  False           |
                       |  7   |  False           |
                       |  8   |  False           |
Tx Adaptive Input Eq   |  1   |  Good            |
                       |  2   |  Good            |
```

```
                        |  3   |  Good           |
                        |  4   |  Good           |
                        |  5   |  Good           |
                        |  6   |  Good           |
                        |  7   |  Good           |
                        |  8   |  Good           |


-------------------------------------------------------------------------------
---
                                  Host Performance
-------------------------------------------------------------------------------
---
           Attribute          | Lane |                Value
|
-------------------------------------------------------------------------------
---
Alarm Status                  |  1   | LD
|
-------------------------------------------------------------------------------
---

-----------------------------------------------
                FEC Performance
-----------------------------------------------
       Attribute      | Lane |      Value     |
-----------------------------------------------
Tx Bits               |  1   | 2125037470720  |
Tx Corrected Bits     |  1   | 0              |
Tx Frames             |  1   | 390631888      |
Tx Uncorrected Frames |  1   | 0              |
```

show qsfp-dd monitors media

Use this command to show QSFP-DD module media side monitors information.

Command Syntax

```
show qsfp-dd PORTNUM monitors media
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 monitors media

Alarm Codes: TFIFO - Tx FIFO Error, TLOLDS - Tx Deskew Loss of Lock
             TLOLRC - Tx Reference Clock Loss of Lock, TLOLCMU - Tx CMU Loss of Lock
             TOOA - Tx Out of Alignment, TLOA - Tx Loss of Alignment
             RFIFO - Rx FIFO Error, RLOLDS - Tx Deskew Loss of Lock
             ROOA - Rx Out of Alignment, RLOA - Rx Loss of Alignment
             RLOLCD - Rx Chromatic Dispersion Compensation Loss of Lock
             RLOLD - Tx Demodulator Loss of Lock, RLOM - Rx Loss of Multi Frame
             RLOF - Rx Loss of Frame, FDD - FEC Detected Degrade
             FED - FEC Excessive Degrade, RPF - Remote Phy Fault
             LD - Local Degrade, RD - Remote Degrade

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]

Port Number                    : 0
-------------------------------------------------------------------------------------------
------------------------
       Monitors       | Lane |  Value       |  High Alarm  | High Warning | Low Warning
|  Low Alarm   | Unit |
-------------------------------------------------------------------------------------------
------------------------
Rx Optical Power      |  1   |  -18.9       |  2.0         |  0.0         |  -23.0       |
-28.2       | dBm  |
Tx Optical Power      |  1   |  -7.8        |  0.0         |  -2.0        |  -16.0       |
-18.0       | dBm  |
Tx Bias               |  1   |  287.3       |  0.0         |  0.0         |  0.0         |
0.0         | mA   |

-----------------------------------------------
         Flag          | Lane |    Status (L)    |
```

```
-------------------------------------------------
Rx LOS                 |  1   |  False           |
Tx Failure             |  1   |  False           |
Rx CDR LOL             |  1   |  False           |

-------------------------------------------------------------------------------
                               Link Performance
-------------------------------------------------------------------------------
           Attribute           | Lane | Average  | Minimum  | Maximum  |  Unit   |
-------------------------------------------------------------------------------
Rx DSP CCD                     |  1   | -1       | -1       | -1       | ps/nm   |
Rx DSP DGD                     |  1   | 1.00     | 1.00     | 1.00     | ps      |
Rx SOPMD                       |  1   | 40.00    | 40.00    | 40.00    | ps^2    |
Rx PDL                         |  1   | 0.5      | 0.5      | 0.5      | dB      |
Rx OSNR                        |  1   | 36.4     | 36.4     | 36.4     | dB      |
Rx ESNR                        |  1   | 16.4     | 16.4     | 16.4     | dB      |
Rx CFO                         |  1   | 86       | 14       | 158      | MHz     |
Tx Power                       |  1   | -7.77    | -7.78    | -7.76    | dBm     |
Rx Input Optical Power         |  1   | -18.90   | -18.91   | -18.90   | dBm     |
Rx Input Optical Signal Power  |  1   | -19.18   | -19.19   | -19.18   | dBm     |
Rx SOPCR                       |  1   | 0        | 0        | 0        | krads/s |
Rx MER                         |  1   | 0.0      | 0.0      | 0.0      | dB      |
-------------------------------------------------------------------------------
Alarm Status                   |  1   | RLOLCD, RLOLD, RPF                    |
-------------------------------------------------------------------------------

-----------------------------------------------
               FEC Performance
-----------------------------------------------
       Attribute       | Lane |      Value     |
-----------------------------------------------
Rx Bits                |  1   | 462238792192   |
Rx Corrected Bits      |  1   | 1398045784     |
Rx Frames              |  1   | 902810141      |
Rx Uncorrected Frames  |  1   | 0              |
```

show qsfp-dd monitors module

Use this command to show QSFP-DD module monitors information.

Command Syntax

```
show qsfp-dd PORTNUM monitors module
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 monitors module

Codes: [HA : High Alarm], [LA : Low Alarm], [HW : High Warning], [LW : Low Warning]

Port Number                    : 0
-------------------------------------------------------------------------------------------------------------------
Attribute                    | Value        | High Alarm   | High Warning | Low Warning  | Low Alarm    | Units
-------------------------------------------------------------------------------------------------------------------
Voltage                      | 3.24         | 3.46         | 3.43         | 3.17         | 3.13         | Volt
Temperature                  | 42.0         | 80.0         | 75.0         | 15.0         | -5.0         | Celsius
TEC Current Magnitude        | 63.000       | 100.00       | 100.00       | -100.00      | -100.00      | %
Laser Temperature            | 43.000       | 80.00        | 75.00        | -40.00       | -80.00       | Celsius
```

show qsfp-dd state

Use this command to show QSFP-DD module current state information.

Command Syntax

```
show qsfp-dd PORTNUM state
```

Parameters

PORTNUM	QSFP-DD front panel port number

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Example

```
show qsfp-dd 0 state

Port Number                    : 0
Module Fault State             : No fault
Module State                   : Ready
Data Path State                : Activated [Starting On : Lane-1]
```

tx-input eq-target

Use this command to configure the Tx input equalizer target override value.

Use the no form of this command to remove the Tx input equalizer target override value.

Command Syntax

```
tx-input eq-target <1-15>
no tx-input eq-target
```

Parameters

<1-15>	Input equalizer target value

Default

None.

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#tx-input eq-target 1
(config-qsfp-dd)#commit
(config-qsfp-dd)#no tx-input eq-target
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 3
(config-qsfp-dd-host)#tx-input eq-target 5
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no tx-input eq-target
(config-qsfp-dd-host)#commit
```

tx cdr-bypass

Use this command to enable the Tx CDR bypass.

Use the no form of this command to disable the Tx CDR bypass.

Command Syntax

```
tx cdr-bypass
no tx cdr-bypass
```

Parameters

None

Command Mode

QSFP-DD and QSFP-DD host-lane modes

Applicability

This command was introduced before OcNOS version 6.5.1.

Example

```
#configure terminal
(config)#qsfp-dd 0
(config-qsfp-dd)#tx cdr-bypass
(config-qsfp-dd)#commit
(config-qsfp-dd)#no tx cdr-bypass
(config-qsfp-dd)#commit
(config-qsfp-dd)#host-lane 2
(config-qsfp-dd-host)#tx cdr-bypass
(config-qsfp-dd-host)#commit
(config-qsfp-dd-host)#no tx cdr-bypass
(config-qsfp-dd-host)#commit
```

EDFA Configuration Guide

CHAPTER 1 Erbium-Doped Fiber Amplifier (EDFA) Configuration

Overview

Before the development of optical amplifiers, optical signals had to be converted into electrical signals, then amplified, and subsequently transformed back into optical signals. This was a very complicated and expensive process. To avoid this complexity, optical amplifiers are developed, enabling the direct amplification of optical signals without the need for conversion. This streamlined approach significantly reduced costs.

Various types of optical amplifiers include:

- Semiconductor Optical Amplifier (SOA)
- Raman Amplifiers
- Brillouin Amplifiers
- Erbium-Doped Fiber Amplifier (EDFA)

Erbium-Doped Fiber Amplifier (EDFA) uses erbium-doped fiber as an amplification medium and are extensively deployed in Wavelength Division Multiplexing (WDM) systems. It can amplify multiple optical signals simultaneously and is commonly used in the C-band and L-band.

System Description

Basically, the system will be developed to combine the input signal with the pump light using a WDM coupler. This combined signal is then directed into the EDF. Within the EDF, the pump light initiates a process called population inversion, and the input signal undergoes amplification through stimulated emission.

To ensure stable signal amplification and prevent undesired back reflections from the output port, isolators are strategically placed at both the input and output ends. Additionally, the presence of isolators prevents the amplifier from functioning as a laser.

The wavelength of the pump LD is precisely controlled and maintained close to 980nm.

These optical and communication systems operate in two different modes.

APC (Automatic Power Control)

In APC mode, the microprocessor controls the output power by adjusting the pump laser to maintain a predefined reference output power level. This control mechanism ensures the output power remains constant, even when the input power fluctuates within the dynamic range.

AGC (Automatic Gain Control)

In AGC mode, the microprocessor controls the output power to maintain the specified gain relative to the input power. The expected output power cannot be guaranteed, if the input power falls below the minimum assured input power range.

© 2025 IP Infusion Inc. Proprietary

Objectives

The objective of this document is to provide the application of EDFA as a booster amplifier, Inline amplifier, and pre-amplifier.

- **Booster Amplifier:** The booster amplifier is placed just after the transmitter to increase the optical power launched to the transmission line. It's not always required in single-channel links but is an essential part of the DWDM link where the multiplexer attenuates the signal channels. It has high input power, high output power, and medium optical gain.
- **Inline Amplifier:** The inline amplifiers are placed in the transmission line, compensating for the attenuation induced by the optical fiber. The in-line EDFA is designed for optical amplification between two network nodes on the main optical link. In-line EDFAs are placed every 80-100 km to ensure that the optical signal level remains above the noise floor. It features medium to low input power, high output power, high optical gain, and a low noise figure.
- **Pre-Amplifier:** The pre-amplifier is placed just before the receiver, such that sufficient optical power is launched to the receiver. It has relatively low input power, medium output power, and medium gain.

Support added for the DDM parameters specific to the EDFA available in the QSFP28 form factor. This application supports the reading of In-power, Out-power, pump BIAS, and gain. Additionally, it will enable the configuration of the target out-power and the continuous monitoring of these attributes in accordance with the specified thresholds.

Topology

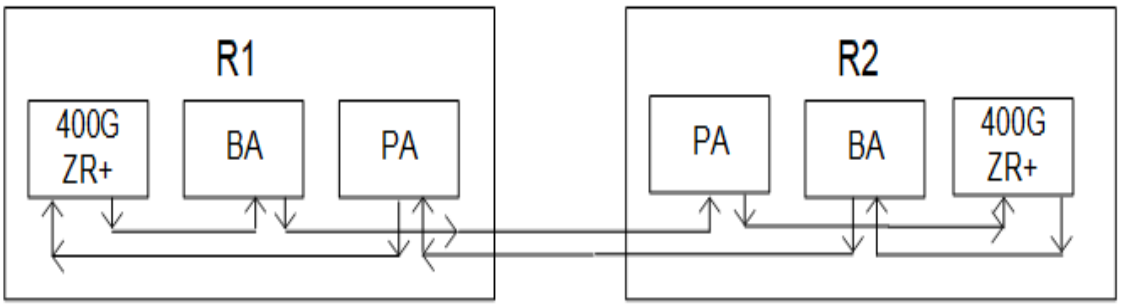


Figure 1-7: EDFA Sample Topology

Configuration

R1

`#configure terminal`	Enter into configure mode.
`(config)#interface ce15`	Enter into interface mode.
`(config-if)#edfa operating-mode agc`	Enable the EDFA operating mode AGC.
`(config-if)#edfa target-gain 5`	Specify the desired EDFA gain value.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config-if)#exit`	Exit the router mode.
`(config)#interface ce15`	Enter into interface mode.

(config-if)#edfa operating-mode apc	Enable the EDFA operating mode APC.
(config-if)# edfa target-outpwr 10	Specify the desired EDFA output power value.
(config-if)#commit	Commit the candidate configuration to the running configuration.
(config-if)#exit	Exit the router mode.

Validation

R1 - validation for AGC mode

```
#show running-config interface ce15
!
interface ce15
 edfa operating-mode agc
 edfa target-gain 5.000
verify is the gain value is applied after configuring.
ROUTER-1#show interface ce15 transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,  - Not
Applicable

Intf       DDM        InPwr      AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce15       Active*    -9.81      +5.00      +4.00      -20.97     -21.94

Intf       DDM        OutPwr     AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce15       Active*    -4.46      +20.00     +18.00     -10.00     -11.94

Intf       DDM        PumpBias   AlertMax   CritMax    CritMin    AlertMin
                      (Amp)      (Amp)      (Amp)      (Amp)      (Amp)
-------------------------------------------------------------------------
ce15       Active*    +0.05      +0.59      +0.53      +0.00      +0.00

Intf       DDM        Gain       AlertMax   CritMax    CritMin    AlertMin
                      (dB)       (dB)       (dB)       (dB)       (dB)
-------------------------------------------------------------------------
ce15       Active*    +3.67      +26.00     +25.00     +8.00      +7.00
```

R1 - validation for APC mode

```
#show running-config interface ce15
!
interface ce15
 edfa operating-mode apc
 edfa target-outpwr 10.000

R-1#show interface ce15 transceiver detail
```

```
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,  - Not
Applicable

Intf       DDM        InPwr      AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce15       Active*    -9.77      +5.00      +4.00      -20.97     -21.94

Intf       DDM        OutPwr     AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce15       Active*    +10.08     +20.00     +18.00     -10.00     -11.94

Intf       DDM        PumpBias   AlertMax   CritMax    CritMin    AlertMin
                      (Amp)      (Amp)      (Amp)      (Amp)      (Amp)
-------------------------------------------------------------------------
ce15       Active*    +0.13      +0.59      +0.53      +0.00      +0.00

Intf       DDM        Gain       AlertMax   CritMax    CritMin    AlertMin
                      (dB)       (dB)       (dB)       (dB)       (dB)
-------------------------------------------------------------------------
ce15       Active*    +19.85     +26.00     +25.00     +8.00      +7.00

*NOTE : after unconfiguring the edfa the value of output power and gain should be in
default value.
Provide the following:
o  Include a Topology diagram.
o  Document configuration steps. Ensure the topology and configuration steps match.
o  Request a show running-config for the new feature.
o  Provide verification steps to demonstrate that the configuration has taken effect.
o  Add a reference to any relevant information in the existing Configuration Guide.
Note:Request a "test report" before importing QA scenarios into your doc. Ensure you
only include configurations samples that "Pass".
```

EDFA Command Reference

CHAPTER 1 Erbium-doped Fiber Amplifier Commands

This chapter is a reference for Erbium-doped fiber amplifier (EDFA) commands:

- edfa operating-mode
- edfa target-gain
- edfa target-outpwr
- show edfa operating-mode
- show interface IFNAME transceiver
- show interface transceiver
- show interface IFNAME transceiver detail
- show interface transceiver detail
- show interface IFNAME transceiver threshold violations
- show interface transceiver threshold violations

© 2025 IP Infusion Inc. Proprietary

edfa operating-mode

Use this command to configure EDFA interface operating-mode.

Command Syntax

```
edfa operatingn-mode PARAM
```

Parameters

PARAM	Specifies the operating-mode Automatic Power Control (apc) and Automatic Gain Control (agc).

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS(config-if)#edfa operating-mode agc
OcNOS(config-if)#commit
```

edfa target-gain

Use this command to configure EDFA interface target gain.

Command Syntax

```
edfa target-gain VALUE
```

Parameters

VALUE	Target gain value.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Example

```
OcNOS(config-if)#edfa target-gain 15
OcNOS(config-if)#commit
```

edfa target-outpwr

Use this command to configure EDFA interface target output power.

Command Syntax

```
edfa target-outpwr VALUE
```

Parameters

VALUE	Target output power value.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS(config-if)#edfa target-outpwr 7
OcNOS(config-if)#commit
```

show edfa operating-mode

Use this command for a EDFA operating-mode summary.

Command Syntax

```
show edfa operating-mode
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS>show edfa operating-mode

Default Operating Mode     : AGC
Default Target OutPwr(BA)  : 17.000
Default Target OutPwr(PA)  : 7.000
Default Target Gain        : 17.000

--------------------------------------
Interface               Operating-Mode
--------------------------------------
ce5/1                          AGC
ce7/1                          AGC
ce11/1                         AGC
```

show interface IFNAME transceiver detail

Use this command to display EDFA attributes and their thresholds

Command Syntax

```
show interface IFNAME transceiver detail
```

Parameters

IFNAME	Interface name

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS>show interface ce9/1 transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable

...

Intf       DDM         InPwr      AlertMax   CritMax    CritMin    AlertMin
                       (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce9/1      Inactive*   -2.00      -7.00      -9.00      -30.97     -32.22

Intf       DDM         OutPwr     AlertMax   CritMax    CritMin    AlertMin
                       (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce9/1      Inactive*   -7.00      +10.00     +8.00      -20.00     -20.97

Intf       DDM         PumpBias   AlertMax   CritMax    CritMin    AlertMin
                      (Amp)      (Amp)      (Amp)      (Amp)      (Amp)
-------------------------------------------------------------------------
ce9/1      Inactive*   +0.35      +0.49      +0.45      +0.00      +0.00

Intf       DDM         Gain       AlertMax   CritMax    CritMin    AlertMin
                       (dB)       (dB)       (dB)       (dB)       (dB)
-------------------------------------------------------------------------
ce9/1      Inactive*   +12.00      +26.00     +25.00     +8.00      +7.00
```

Table 1-24 explains the output fields.

Table 1-24: show interface transceiver details output

Field	Description
Intf	Interface where the EDFA is present
DDM	Digital diagnostics monitor status for that particular interface
Inpwr	Input Power to the EDFA
OutPwr	Output Power from EDFA
PumpBias	Pump Bias
Gain	The total gain over the Input Power

show interface IFNAME transceiver threshold violations

Use this command to show EDFA module input power, output power, pump bias and gain thresholds violations from a specific port.

Command Syntax

```
show interface IFNAME transceiver threshold violations
```

Parameters

IFNAME	Interface Name

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS>show interface ce11/1 transceiver threshold violations
Intf       Lane       Timestamp            Type of alarm
----       ----       ---------            -------------
ce11/1     1          02-14-2019 12:39:04  Pump Bias low alarm, value 0.000A threshold 0.000A
                      02-14-2019 12:38:04  Gain low warning, value 7.500dB threshold 8.000dB
                      02-14-2019 12:38:04  Output power low warning, value -11.000dBm threshold -10.000dBm
                      02-14-2019 12:38:04  Input power low warning, value -21.000dBm threshold -20.969dBm
```

show interface IFNAME transceiver

Use this command to show EDFA module input power, output power, pump bias and gain current values from a specific port.

Command Syntax

```
show interface IFNAME transceiver
```

Parameters

IFNAME	Interface Name

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
Cassini-3>show interface ce9/1 transceiver
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,
- Not Applicable

Intf       DDM        InPwr      OutPwr     PumpBias   Gain
                      (dBm)      (dBm)      (Amp)       (dB)
-------------------------------------------------------------------------
ce9/1      Inactive*  -2.00      -7.00      +0.35      +12.00
OcNOS>show interface ce9/1 transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,
- Not Applicable

...

Intf       DDM        InPwr      AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce9/1      Inactive*  -2.00      -7.00      -9.00      -30.97     -32.22

Intf       DDM        OutPwr     AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce9/1      Inactive*  -7.00      +10.00     +8.00      -20.00     -20.97

Intf       DDM        PumpBias   AlertMax   CritMax    CritMin    AlertMin
                      (Amp)       (Amp)       (Amp)       (Amp)       (Amp)
-------------------------------------------------------------------------
ce9/1      Inactive*  +0.35      +0.49      +0.45      +0.00      +0.00

Intf       DDM        Gain       AlertMax   CritMax    CritMin    AlertMin
                      (dB)       (dB)       (dB)       (dB)       (dB)
-------------------------------------------------------------------------
```

```
ce9/1       Inactive*  +12.00      +26.00      +25.00      +8.00       +7.00
```

show interface transceiver

Use this command to show EDFA module input power, output power, pump bias and gain current values from all ports.

Command Syntax

```
show interface transceiver
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
Cassini-3>show interface transceiver
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No Power,  - Not
Applicable

Intf       DDM        Temp       Voltage    InPwr      OutPwr     PumpBias   Gain
                      (Celsius)  (volt)     (dBm)      (dBm)      (Amp)       (dB)
-------------------------------------------------------------------------------------
ce0        Inactive*  +33.10     +3.28      -8.12      +8.85      +0.11      +16.97
```

show interface transceiver detail

Use this command to show EDFA module input power, output power, pump bias and gain threshold and current values from all ports.

Command Syntax

```
show interface transceiver detail
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS>show interface transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable

...

Intf       DDM        InPwr      AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce0        Inactive*  -8.12      +5.00      +4.00      -20.97     -21.94

Intf       DDM        OutPwr     AlertMax   CritMax    CritMin    AlertMin
                      (dBm)      (dBm)      (dBm)      (dBm)      (dBm)
-------------------------------------------------------------------------
ce0        Inactive*  +8.83      +20.00     +18.00     -10.00     -11.94

Intf       DDM        PumpBias   AlertMax   CritMax    CritMin    AlertMin
                     (Amp)      (Amp)      (Amp)      (Amp)      (Amp)
-------------------------------------------------------------------------
ce0        Inactive*  +0.11      +0.59      +0.53      +0.00      +0.00

Intf       DDM        Gain       AlertMax   CritMax    CritMin    AlertMin
                      (dB)       (dB)       (dB)       (dB)       (dB)
-------------------------------------------------------------------------
ce0        Inactive*  +16.97     +26.00     +25.00     +8.00      +7.00
```

show interface transceiver threshold violations

Use this command to show EDFA EDFA module input power, output power, pump bias and gain thresholds violations.

Command Syntax

```
show interface transceiver threshold violations
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 6.3.0.

Example

```
OcNOS>show interface transceiver threshold violations
Intf       Lane       Timestamp            Type of alarm
----       ----       ---------            -------------
ce9/1      1          03-05-2019 08:53:31  Gain high alarm, value 100.000dB threshold 26.000dB
                      03-05-2019 08:53:31  Pump bias high alarm, value 100.000A threshold 0.579A
                      03-05-2019 08:53:31  Output power high alarm, value 100.000dBm threshold 20.000dBm
                      03-05-2019 08:53:31  Input power high alarm, value 100.000dBm threshold 5.000dBm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf       Lane       Timestamp            Type of alarm
----       ----       ---------            -------------
ce9/1      1          03-05-2019 08:57:09  Gain low alarm, value -100.000dB threshold 7.000dB
                      03-05-2019 08:57:09  Pump Bias low alarm, value -100.000A threshold 0.000A
                      03-05-2019 08:57:09  Output power low alarm, value -100.000dBm threshold -11.938dBm
                      03-05-2019 08:57:09  Input power low alarm, value -100.000dBm threshold -21.938dBm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf       Lane       Timestamp            Type of alarm
----       ----       ---------            -------------
ce9/1      1          03-05-2019 09:03:36  Gain high warning, value 25.500db threshold 25.000db
                      03-05-2019 09:03:36  Pump bias high warning, value 0.550A threshold 0.526A
                      03-05-2019 09:03:36  Output power high warning, value 19.000dbm threshold 18.000dbm
                      03-05-2019 09:03:36  Input power high warning, value 4.500dbm threshold 4.000dbm

OcNOS>show interface ce9/1 transceiver threshold violations
Intf       Lane       Timestamp            Type of alarm
----       ----       ---------            -------------
ce9/1      1          03-05-2019 09:07:05  Gain low warning, value 7.500dB threshold 8.000dB
                      03-05-2019 09:07:05  Pump Bias low alarm, value 0.000A threshold 0.000A
                      03-05-2019 09:07:05  Output power low warning, value -11.000dBm threshold -10.000dBm
                      03-05-2019 09:07:05  Input power low warning, value -21.000dBm threshold -20.969dBm
```

NetConf Configuration

CHAPTER 1 NetConf Call Home Configuration

By default, in the NetConf protocol (RFC 6241), a NetConf client application initiates the connection towards the NetConf server in the network element (OcNOS device). However, for certain use cases such as in the presence of firewalls or NAT, it is useful to have “call home” functionality where the connection process is reversed and the NetConf server initiates the connection to the NetConf client. This process, as shown in Figure 1-8, is standardized by IETF in RFC 8071.

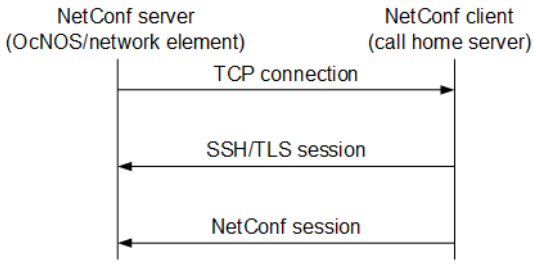


Figure 1-8: RFC 8071 NetConf call home functionality

OcNOS supports the call home feature (only for SSH) at the NetConf server side. You can use any standard NetConf client application which supports call home functionality. (Call home support in the NetConf client application [Yangcli] is not supported.)

Call home is generally useful for both the initial deployment and ongoing management of networking elements.

User Management VRF Configuration

`(config)#netconf callhome`	Enter call home mode
`(netconf-callhome)#feature netconf callhome enable`	Enable the call home feature
`(netconf-callhome)#reconnect enable`	Enable the reconnect feature
`(netconf-callhome)#retry-max-attempts 10`	Set the number of connect retries
`(netconf-callhome)#retry-interval 20`	Set the retry interval
`(netconf-callhome)#callhome server test-ch-server 192.168.56.1`	Configure the call home server
`(netconf-callhome)#management-port enp0s3`	Set the call home management port
`(netconf-callhome)#commit`	Commit the candidate configuration to the running configuration
`(netconf-callhome)#exit`	Exit call home mode

User Defined VRF Configuration

`(config)#netconf callhome`	Enter call home mode
`(netconf-callhome)# netconf callhome vrf user-vrf`	Netconf callhome for user defined vrf
`(netconf-callhome)#feature netconf callhome enable`	Enable the call home feature

(netconf-callhome)#reconnect enable	Enable the reconnect feature
(netconf-callhome)#retry-max-attempts 10	Set the number of connect retries
(netconf-callhome)#retry-interval 20	Set the retry interval
(netconf-callhome)#callhome server test- ch-server 192.168.56.1	Configure the call home server
(netconf-callhome)#management-port enp0s3	Set the call home management port (port will be part of user defined vrf)
(netconf-callhome)#commit	Commit the candidate configuration to the running configuration
(netconf-callhome)#exit	Exit call home mode

Validation

```
(config)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 management-port enp0s3
 reconnect enable
 retry-max-attempts 10
 retry-interval 20
 callhome server test-ch-server 192.168.56.1
!
(config)#
(config)#do show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User               Idle         Location/Session  PID     TYPE
Role

(#)(*) 130 vty 0    [C]root              0d00h00m     pts/0             2730    Local
network-admin

(config)#
```

Start the Call Home Server

After you start the call home server, the `show users` command displays a NetConf user.

```
2022 May 18 15:32:55.989 : OcNOS : CML : INFO : [CML_5]: Client [netconf (192.168.56.1)]
established connection with CML server

(config)#do show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
```

```
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

          Line       User                Idle         Location/Session  PID     TYPE
Role

(#)(*) 130 vty 0    [C]root              0d00h00m     pts/0             2730    Local
network-admin
       NA           [N]root              0d00h00m    192.168.56.1      2118    Local
network-admin

(config)#
```

NetConf sget Output

While the NetConf client is running, the `sget` command returns the session-specific data:

```
sget /netconf-state/sessions

<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <netconf-state xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">
      <sessions>
        <session>
          <session-id>1</session-id>
          <transport
           xmlns:ncm="urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring">ncm:netconf-
ssh</transport>
          <username>root</username>
          <source-host>192.168.56.1</source-host>
          <login-time>2022-05-18T15:32:55Z</login-time>
          <in-rpcs>0</in-rpcs>
          <in-bad-rpcs>0</in-bad-rpcs>
          <out-rpc-errors>0</out-rpc-errors>
          <out-notifications>0</out-notifications>
        </session>
      </sessions>
    </netconf-state>
  </data>
</rpc-reply>
```

Stop the Call Home Server

After you stop the call home server, the `show users` command no longer displays a NetConf user.

```
2022 May 18 15:33:20.028 : OcNOS : CML : NOTIF : [CML_4]: Client [netconf
(192.168.56.1)] has closed connection with CML server

(config)#
(config)#do show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
```

```
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

           Line       User                Idle         Location/Session  PID     TYPE
Role

(#)(*) 130 vty 0    [C]root               0d00h00m     pts/0             2730    Local
network-admin

(config)#
```

CHAPTER 2 NetConf Port Access Control

Overview

NetConf is a software tool that provides a mechanism to configure and manage remote network devices seamlessly. It uses a simple Remote Procedure Call (RPC) mechanism to facilitate communication between a client and a server.

During the OcNOS installation, the NetConf subsystem called “netconf” is installed. It runs on the default access port 830 over SSH and port 6513 over TLS.

Typically, these default access ports are not configurable and controlled. The NetConf port access control feature enhancement ensures that the Netconf-SSH and NetConf-TLS port access can be controlled and configurable.

Feature Characteristics

- This feature allows access control capabilities for the NetConf-SSH and NetConf-TLS ports.
- Enabling/disabling the port.
- Changing the default port.
- Accessing and controlling the NetConf services through Inband and Outband.
- Applying ACL rules to the NetConf port to control its access.

Benefits

This feature enables the user to control the NetConf port access and change the default port.

Configuration

To configure either NetConf-SSH port or the NetConf-TLS port, perform the following steps. After completing the steps you will be configured with a port for NetConf.

1. Disable `netconf-ssh` and `netconf-tls` feature
2. Configure port for `netconf-ssh` and `netconf-tls`
3. Enable `netconf-ssh` and `netconf-tls` feature

Topology

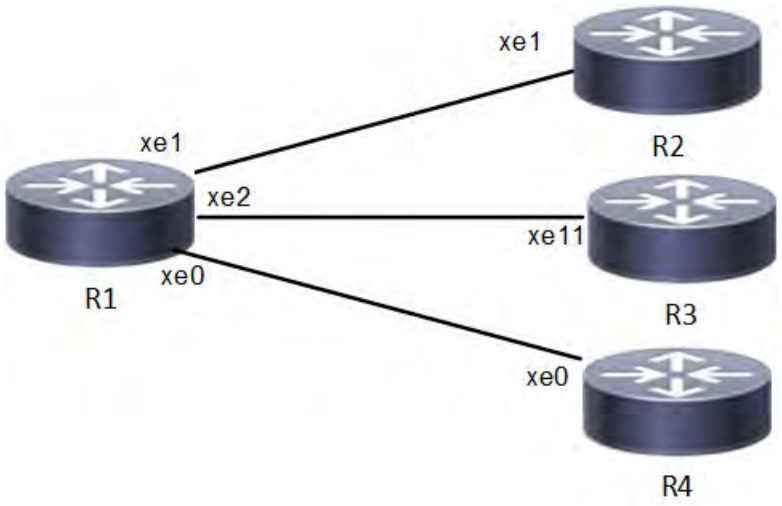


Figure 2-1: NetConf Access Port Topology

Enable Netconf-ssh on the default and vrf management port

R1

`#configure terminal`	Enter Configuration mode.
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port.
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port.
`R1(config)#commit`	Commit all the transactions.

Enable Netconf-tls on the default and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Execute the below commands to verify the NetConf port is enabled on VRF Management.

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 830
        Netconf TLS Server: Enabled
```

```
        TLS-Netconf Port : 6513
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 830
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 6513
```

Following is the output of NetConf server configurations.

```
#show running-config netconf-server
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
netconf server ssh-port 2000 vrf management
netconf server tls-port 60000 vrf management
feature netconf-ssh
feature netconf-tls
netconf server ssh-port 1060
netconf server tls-port 5000
!
```

Following is the output of the NetConf server configuration in XML format.

```
#show xml running-config
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-serve
r">
  <vrfs>
    <vrf>
      <vrf-name>default</vrf-name>
      <config>
        <vrf-name>default</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>1060</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>5000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
    <vrf>
      <vrf-name>management</vrf-name>
      <config>
        <vrf-name>management</vrf-name>
      </config>
      <netconf-ssh-config>
```

```
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>2000</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>60000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
  </vrfs>
</netconf-server>
<network-instances xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-network-insta
nce">
  <network-instance>
    <instance-name>default</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>default</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>default</vrf-name>
      </config>
    </vrf>
  </network-instance>
  <network-instance>
    <instance-name>management</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>management</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>management</vrf-name>
      </config>
    </vrf>
  </network-instance>
</network-instances>
<interfaces xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-interface">
```

Following is the output after login to the NetConf interface (YangCLI) on R1 node via the default NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=127.1 --user=ocnos --
password=ocnos
yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 127.1

NETCONF session established for ocnos on 127.1
……..
```

Disable netconf-ssh via default and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default port
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management
`R1(config)#commit`	Commit all the transactions

Disable netconf-tls via default port and vrf management port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Execute the below commands to verify the NetConf port is disabled on VRF Management.

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf Server: Disabled
VRF Default
        Netconf Server: Disabled
```

Configuring NetConf Port

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default port
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions

Validation

Following is the output of the NetConf server status and port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000
```

Following is the output after login to the NetConf interface (YangCLI) on R1 node via the user defined NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib1 yangcli --server=127.1 --user=ocnos --
password=ocnos ncport=2000
Warning: Revision date in the future (2022-08-30), further warnings are suppressed
ietf-netconf-notifications.yang:46.4: warning(421): revision date in the future

  yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 127.1

NETCONF session established for ocnos on 127.1
.......................
Checking Server Modules...

yangcli ocnos@127.1>
```

Ping between two nodes via Yang CLI

Perform the following configurations to verify the reachability among R1, R2 and R3 routers via NetConf-SSH and NetConf-TLS port.

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe1`	Enter interface mode
`R1(config)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`R1(config)#commit`	Commit all the transactions

R2

`#configure terminal`	Enter Configuration mode
`R2(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R2(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management
`R2(config)#no feature netconf-tls`	Disable netconf-tls via default

R2(config)#no feature netconf-tls vrf management	Disable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#netconf server ssh-port 1060	Configure port for netconf-ssh default
R2(config)#netconf server ssh-port 2000 vrf management	Configure port for netconf-ssh vrf management
R2(config)#netconf server tls-port 5000	Configure port for netconf-tls default
R2(config)#netconf server tls-port 60000 vrf management	Configure port for netconf-tls vrf management
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#feature netconf-ssh	Enable netconf-ssh via default port
R2(config)#feature netconf-ssh vrf management	Enable netconf-ssh via vrf management port
R2(config)#feature netconf-tls	Enable netconf-tls via default port
R2(config)#feature netconf-tls vrf management	Enable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#interface xe1	Enter interface mode
R2(config)#ip address 10.10.10.2/24	Configure ipv4 address on the interface xe1.
R2(config)#commit	Commit all the transactions

Validation

Following is the output of the configured NetConf port.

```
#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000

OcNOS#show running-config interface xe1
!
interface xe1
 ip address 10.10.10.1/24
!
OcNOS#ping 10.10.10.2
Press CTRL+C to exit
```

```
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.567 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.258 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.241 ms

--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 80ms
rtt min/avg/max/mdev = 0.241/0.355/0.567/0.150 ms
```

Following is the output after login to the NetConf interface (YangCLI) on R2 node through the user defined NetConf port:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=10.10.10.2 --user=ocnos --
password=ocnos ncport=1060
Warning: Revision date in the future (2022-08-30), further warnings are suppressed
ietf-netconf-notifications.yang:46.4: warning(421): revision date in the future

  yangcli version 2.5-5
  libssh2 version 1.8.0

  Copyright (c) 2008-2012, Andy Bierman, All Rights Reserved.
  Copyright (c) 2013-2015, Vladimir Vassilev, All Rights Reserved.
  Copyright (c) 2012-2016, OpenClovis Inc, All Rights Reserved.

  Type 'help' or 'help <command-name>' to get started
  Use the <tab> key for command and value completion
  Use the <enter> key to accept the default value in brackets

  These escape sequences are available when filling parameter values:

        ?       help
        ??      full help
        ?s      skip current parameter
        ?c      cancel current command

  These assignment statements are available when entering commands:

        $<varname> = <expr>     Local user variable assignment
        $$<varname> = <expr>    Global user variable assignment
        @<filespec> = <expr>    File assignment
val->res is NO_ERR.

yangcli: Starting NETCONF session for ocnos on 10.10.10.2

NETCONF session established for ocnos on 10.10.10.2
.........................
Checking Server Modules...

yangcli ocnos@10.10.10.2>
```

ACL Rule with IPv4 Configuration

Perform the following configurations to apply an ACL rule to allow or deny traffic from R1 to other nodes via NetConf port.

R1

`#configure terminal`	Enter Configuration mode
`R1(config)#no feature netconf-ssh`	Disable netconf-ssh via default
`R1(config)#no feature netconf-ssh vrf management`	Disable netconf-ssh via vrf management port
`R1(config)#no feature netconf-tls`	Disable netconf-tls via default port
`R1(config)#no feature netconf-tls vrf management`	Disable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#netconf server ssh-port 1060`	Configure port for netconf-ssh default
`R1(config)#netconf server ssh-port 2000 vrf management`	Configure port for netconf-ssh vrf management
`R1(config)#netconf server tls-port 5000`	Configure port for netconf-tls default
`R1(config)#netconf server tls-port 60000 vrf management`	Configure port for netconf-tls vrf management
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#feature netconf-ssh`	Enable netconf-ssh via default port
`R1(config)#feature netconf-ssh vrf management`	Enable netconf-ssh via vrf management port
`R1(config)#feature netconf-tls`	Enable netconf-tls via default port
`R1(config)#feature netconf-tls vrf management`	Enable netconf-tls via vrf management port
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe1`	Enter interface mode
`R1(config)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#interface xe2`	Enter interface mode
`R1(config)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`R1(config)#commit`	Commit all the transactions
`#configure terminal`	Enter Configuration mode
`R1(config)#ip access-list ACL1`	Create ip access list
`R1(config)#permit any host 10.1.1.1 any`	Create an acl rule to permit

R1(config)#deny any host 20.1.1.1 any	Create an acl rule to deny
R1(config)#commit	Commit all the transactions

R2

Perform the following configurations to apply an ACL rule to allow or deny traffic from R2 to other nodes via NetConf port

#configure terminal	Enter Configuration mode
R2(config)#no feature netconf-ssh	Disable netconf-ssh via default
R2(config)#no feature netconf-ssh vrf management	Disable netconf-ssh via vrf management
R2(config)#no feature netconf-tls	Disable netconf-tls via default
R2(config)#no feature netconf-tls vrf management	Disable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#netconf server ssh-port 1060	Configure port for netconf-ssh default
R2(config)#netconf server ssh-port 2000 vrf management	Configure port for netconf-ssh vrf management
R2(config)#netconf server tls-port 5000	Configure port for netconf-tls default
R2(config)#netconf server tls-port 60000 vrf management	Configure port for netconf-tls vrf management
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#feature netconf-ssh	Enable netconf-ssh via default port
R2(config)#feature netconf-ssh vrf management	Enable netconf-ssh via vrf management port
R2(config)#feature netconf-tls	Enable netconf-tls via default port
R2(config)#feature netconf-tls vrf management	Enable netconf-tls via vrf management port
R2(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R2(config)#interface xe1	Enter interface mode
R2(config)#ip address 10.10.10.2/24	Configure ipv4 address on the interface xe1.
R2(config)#commit	Commit all the transactions

R3

Perform the following configurations to apply an ACL rule to allow or deny traffic from R3 to other nodes via NetConf port.

#configure terminal	Enter Configuration mode
R3(config)#no feature netconf-ssh	Disable netconf-ssh via default

R3(config)#no feature netconf-ssh vrf management	Disable netconf-ssh via vrf management port
R3(config)#no feature netconf-tls	Disable netconf-tls via default port
R3(config)#no feature netconf-tls vrf management	Disable netconf-tls via vrf management port
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#netconf server ssh-port 1060	Configure port for netconf-ssh default
R3(config)#netconf server ssh-port 2000 vrf management	Configure port for netconf-ssh vrf management
R3(config)#netconf server tls-port 5000	Configure port for netconf-tls default
R3(config)#netconf server tls-port 60000 vrf management	Configure port for netconf-tls vrf management
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#feature netconf-ssh	Enable netconf-ssh via default port
R3(config)#feature netconf-ssh vrf management	Enable netconf-ssh via vrf management port
R3(config)#feature netconf-tls	Enable netconf-tls via default port
R3(config)#feature netconf-tls vrf management	Enable netconf-tls via vrf management port
R3(config)#commit	Commit all the transactions
#configure terminal	Enter Configuration mode
R3(config)#interface xe11	Enter interface mode
R3(config)#ip address 20.20.20.2/24	Configure ipv4 address on the interface xe11.
R3(config)#commit	Commit all the transactions

Validation

Following is the output to verify the user defined NetConf port.

```
R1#show running-config netconf-server
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
netconf server ssh-port 2000 vrf management
netconf server tls-port 60000 vrf management
feature netconf-ssh
feature netconf-tls
netconf server ssh-port 1060
netconf server tls-port 5000
!

R1#show netconf server
VRF Management
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 2000
```

```
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 60000
VRF Default
        Netconf SSH Server: Enabled
        SSH-Netconf Port : 1060
        Netconf TLS Server: Enabled
        TLS-Netconf Port : 5000
```

Following is the output of the show running-config in XML format.

```
R1#show xml running-config
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-serve
r">
  <vrfs>
    <vrf>
      <vrf-name>default</vrf-name>
      <config>
        <vrf-name>default</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>1060</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>5000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
    <vrf>
      <vrf-name>management</vrf-name>
      <config>
        <vrf-name>management</vrf-name>
      </config>
      <netconf-ssh-config>
        <config>
          <feature-netconf-ssh>true</feature-netconf-ssh>
          <ssh-port>2000</ssh-port>
        </config>
      </netconf-ssh-config>
      <netconf-tls-config>
        <config>
          <feature-netconf-tls>true</feature-netconf-tls>
          <tls-port>60000</tls-port>
        </config>
      </netconf-tls-config>
    </vrf>
```

```
  </vrfs>
</netconf-server>
<network-instances xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-network-insta
nce">
  <network-instance>
    <instance-name>default</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>default</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>default</vrf-name>
      </config>
    </vrf>
  </network-instance>
  <network-instance>
    <instance-name>management</instance-name>
    <instance-type>vrf</instance-type>
    <config>
      <instance-name>management</instance-name>
      <instance-type>vrf</instance-type>
    </config>
    <vrf xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-vrf">
      <config>
        <vrf-name>management</vrf-name>
      </config>
    </vrf>
  </network-instance>
</network-instances>
<interfaces xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-interface">
```

Implementation Examples

The below examples are based on the topology given in Topology section.

Accessing R1 from R2 with default port

Below is an example to access R1 from R2 with default port.

From OcNOS CLI:

```
feature netconf-ssh
feature netconf-ssh vrf management
feature netconf-tls
feature netconf-tls vrf management
```

From Yang CLI:

```
root@OcNOS:~# ip netns exec zebosfib0 yangcli --server=127.1 --user=ocnos --
password=ocnos
```

Accessing R1 from R2 with user defined port

Below is an example to access R1 from R2 via user defined port.

From OcNOS CLI:

```
netconf server ssh-port 1060
netconf server ssh-port 2000 vrf management
netconf server tls-port 5000
netconf server tls-port 60000 vrf management
```

From Yang CLI:

```
root@OcNOS:~#ip netns exec zebosfib1 yangcli --server=10.10.10.1 --user=ocnos --
password=ocnos ncport=2000
```

Applying ACL rule to permit or deny any Node

Below is an example to permit any traffic originating from IP address 10.1.1.1. and deny any traffic originating from 20.1.1.1.

From OcNOS CLI:

```
ip access-list ACL1
permit any host 10.1.1.1  any
deny any host   20.1.1.1 any
Permitting R2 and denying R3
```

From Yang CLI:

```
root@OcNOS:~# ip netns exec zebosfib1 yangcli --server=10.10.10.2 --user=ocnos --
password=ocnos ncport=2000
```

New CLI Commands

feature netconf-ssh

Use this command to enable or disable the netconf-ssh feature specific to the management VRF. When netconf feature-ssh is enabled, it allows the logins through the default netconf-ssh port or through default ssh port if feature SSH is also enabled.

Command Syntax

```
feature netconf-ssh (vrf management|)
no feature netconf-ssh (vrf management|)
```

Parameters

`vrf management` Specifies the management Virtual Routing and Forwarding

Default

Disabled by default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows you how to enable NetConf SSH on either the VRF management port or the default port. The no parameter disables the same.

```
(config)#feature netconf-ssh vrf management
(config)#feature netconf-ssh
(config)#no feature netconf-ssh vrf management
(config)#no feature netconf-ssh
#
```

feature netconf-tls

Use this command to enable or disable the NetConf TLS feature specific to a VRF. When netconf feature-ssh is enabled, it allows the logins through the default netconf-tls port and allows login through a default TLS port when the TLS feature is also enabled.

Command Syntax

```
feature netconf-tls (vrf management|)
no feature netconf-tls (vrf management|)
```

Parameters

`vrf management` Specifies management Virtual Routing and Forwarding.

Default

Disabled by default.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows how to execute the CLI:

```
(config)#feature netconf-tls vrf management
(config)#feature netconf-tls
(config)#no feature netconf-tls vrf management
```

```
(config)#no feature netconf-tls
```

If either NetConf SSH or NetConf TLS are disabled one after the other, the following error message will be displayed, `% Disabling this will stop the netconf service that is running in management vrf”` as shown below.

Management VRF Configuration

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no feature netconf-ssh vrf management
(config)#commit
(config)#no feature netconf-tls vrf management
(config)#commit
% Disabling this will stop the netconf service that is running in management vrf.
```

Default VRF Configuration

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#no feature netconf-ssh vrf management
(config)#commit
(config)#no feature netconf-tls vrf management
(config)#commit
% Disabling this will stop the netconf service that is running in defualt vrf.
```

netconf-ssh port

Use this command to either configure or unconfigure the custom NetConf SSH port.

Command Syntax

```
netconf-server ssh-port <1024-65535> (vrf management|)
no netconf-server ssh-port (vrf management|)
```

Parameters

`<1024-65535>`	Port range values
`Default`	By default, the netconf-ssh port value is 830.
`vrf`	Specifies the management Virtual Routing and Forwarding name

Command Mode

Config mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows how to execute the CLI:

```
(config)#netconf server ssh-port ?
```

```
  <1024-65535>  port
(config)#netconf server ssh-port 1024 vrf management
(config)#netconf server ssh-port 2000
(config)#no netconf server ssh-port
(config)#no netconf server ssh-port vrf management
```

netconf-tls port

Use this command to either configure or unconfigure the indicated NetConf TLS port.

Command Syntax

```
netconf-server tls-port <1024-65535> (vrf management|)
no netconf-server tls-port (vrf management|)
```

Parameters

`<1024-65535>`	Port range values
`Default`	By default, the netconf-tls port value is 6513.
`vrf`	Specifies the management Virtual Routing and Forwarding name

Command Mode

Config mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

```
(config)#netconf server tls-port ?
  <1024-65535>  port
(config)#netconf server tls-port 5000 vrf management
(config)#netconf server tls-port 3000
(config)#no netconf server tls-port vrf management
(config)#no netconf server tls-port
```

show netconf server

Use this command to display netconf server status.

Command Syntax

```
show netconf server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.4.1.

Examples

The following example shows the output of the CLI:

```
OcNOS#show netconf server
VRF MANAGEMENT
Netconf Server: Enabled
SSH-Netconf Port : 1000
TLS-Netconf Port : 7000
VRF DEFAULT
Netconf Server: Enabled
SSH-Netconf Port : 4500
TLS-Netconf Port : 3000
```

show running-config netconf server

Use this command to display the NetConf server settings that appear in the running configuration.

Command Syntax

```
show running-config netconf-server
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Examples

The following example shows the output of the CLI:

```
OcNOS#show running-config netconf-server
feature netconf vrf management
netconf server ssh-port 1000 vrf management
netconf server tls-port 7000 vrf management
feature netconf
netconf server ssh-port 4500
netconf server tls-port 3000
!
```

Revised CLI Commands

ip access-list tcp|udp

The existing `ip access-list tcp|udp` CLI is updated with the following two options to support the Access List (ACL) rules on the NetConf port. The ACL defines a set of rules to control network traffic and reduce network attacks.

`netconf-ssh` Secure Shell Network Configuration

`netconf-tls` Transport Layer Security Network Configuration

For the complete command reference, refer to ip access-list tcp|udp CLI in Access Control List Commands section.

Abbreviations

The following are some key abbreviations and their meanings relevant to this document:

Acronym	Description
ACL	Access control list
RPC	Remote Procedure Call
SSH	Secure Shell
TLS	Transport Layer Security

NetConf Command Reference

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 NetConf Call Home Commands

This chapter describes these commands:

- callhome server
- debug callhome
- feature netconf callhome
- management-port
- netconf callhome
- reconnect
- retry-interval
- retry-max-attempts
- show (xml|) running-config netconf-callhome

callhome server

Use this command to add a call home server. A maximum 5 servers can be configured.

Use the `no` form of this command to delete a call home server. If the specified call home server is already connected with the OcNOS NetConf server, deleting it will not disconnect it.

Command Syntax

```
callhome server WORD (A.B.C.D|X:X::X:X|HOSTNAME)
callhome server WORD (A.B.C.D|X:X::X:X|HOSTNAME) port <1-65535>
no callhome server WORD
```

Parameters

`WORD`	An arbitrary name for the NetConf listen endpoint. Any valid string with length 1-64 can be used.
`A.B.C.D`	IPv4 address of the call home server
`X:X::X:X`	IPv4 address of the call home server
`HOSTNAME`	Host name of the call home server
`<1-65535>`	Callhome server listening port

Note: The same address can be configured with different endpoint names, so use a different port number in those cases. For example:

```
callhome server name-1 1.1.1.1
callhome server name-3 1.1.1.1 port 5555
```

Avoid the redundant configuration: `callhome server name-2 1.1.1.1`

Default

Default value for the port is IANA assigned port 4334.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

The below configuration example illustrates how to define and manage callhome servers for NetConf communication.

1. Check the existing NetConf Callhome configuration usingthe `show running-config netconf-callhome` command.

```
(config)#netconf callhome
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
```

2. Configure the Callhome server.

```
(netconf-callhome)#callhome server name-1 169.154.45.12
(netconf-callhome)#callhome server name-2 192.168.56.1 port 12234
(netconf-callhome)#commit
```

3. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 callhome server name-1 169.154.45.12
 callhome server name-2 192.168.56.1 port 12234
!
```

4. Remove the configured `name-2` Callhome server.

```
(netconf-callhome)#no callhome server name-2
(netconf-callhome)#commit
```

5. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 callhome server name-1 169.154.45.12
!
(netconf-callhome)#exit
```

debug callhome

Use this command to enable debugging for the call home module. Once enabled, all debugging related information will be logged in the system logger file.

Use the `no` form of this command to disable debugging for the call home module.

Command Syntax

```
debug callhome
no debug callhome
```

Parameters

None

Default

By default, debugging is disabled (only critical message are enabled).

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

The below configuration example illustrates how to enable or disable debugging for the Callhome module.

1. Check the existing NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(config)#netconf callhome
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
!
```

2. Enable debug command for the Callhome module.

```
(netconf-callhome)#debug callhome
(netconf-callhome)#commit
```

3. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 debug callhome
!
```

4. Remove the configured debug command to disable debugging for the call home module.

```
(netconf-callhome)#no debug callhome
(netconf-callhome)#commit
```

5. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
!

(netconf-callhome)#exit
```

feature netconf callhome

Use this command to enable or disable the NetConf call home feature. When the feature is disabled, all other configurations are removed except debug callhome.

Enabling the call home feature is required before doing any other call home configurations.

Command Syntax

```
feature netconf callhome (enable|disable)
```

Parameters

`enable`	Enable the call home feature
`disable`	Disable the call home feature

Default

By default, the call home feature is disabled.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

The below configuration example illustrates how to enable or disable the NetConf Callhome feature.

1. Check the existing NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(config)#do show running-config netconf-callhome
(config)#
```

2. Enable the NetConf Callhome feature.

```
(config)#netconf callhome
(netconf-callhome)#feature netconf callhome enable
(netconf-callhome)#commit
```

3. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
```

4. Disable the NetConf callhome feature.

```
(netconf-callhome)#feature netconf callhome disable
(netconf-callhome)#commit
```

5. Check the current NetConf Callhome configurations using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
      !
      netconf callhome
      !
(netconf-callhome)#exit
```

management-port

Use this command to add an interface to use to connect to a call home server. This is useful when in-band (front panel) ports are used as management ports.

Use the `no` form of this command to use eth0 as the management port.

Command Syntax

```
management-port IFNAME
no management-port
```

Parameters

`IFNAME`	Interface used to connect to the call home server.

Default

By default, eth0 (out-of-band management port) is used as the management port.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

The below configuration example illustrates how to enable or disable the NetConf Callhome feature.

1. Check the existing NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
```

2. Using the management port command, add an interface `xe4` to connect to the call home server.

```
(netconf-callhome)#management-port xe4
(netconf-callhome)#commit
```

3. Check the current NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 management-port xe4
!
```

4. Remove the connected interface `xe4` using the no command, and by default, `eth0` is used as the management port.

```
(netconf-callhome)#no management-port
(netconf-callhome)#commit
```

5. Check the current NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
(netconf-callhome)#exit
```

netconf callhome

Use this command to enter NetConf call home configuration mode. All call home configurations are done in this mode.

Command Syntax

```
netconf callhome
```

Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

1. The below configuration example illustrates how to enter the NetConf Callhome configuration mode.

```
#configure terminal
(config)#netconf callhome
```

2. Check the NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
!
(netconf-callhome)#exit
```

reconnect

Use this command to enable or disable the reconnect feature in OcNOS, allowing users to control whether the system attempts to re-establish a connection if it fails. When enabled, OcNOS will make repeated connection attempts if the initial connection fails. If disabled, OcNOS will make only a single connection attempt; if it fails, it will not re-attempt the connection.

Command Syntax

```
reconnect (enable|disable)
```

Parameters

`enable`	Enable reconnect
`disable`	Disable reconnect

Default

By default, the reconnect feature is not enabled.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

1. Check the existing NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
```

2. Enable Reconnect:

```
(netconf-callhome)#reconnect enable
(netconf-callhome)#commit
```

3. Check the current NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
!
```

4. Configure Retry Attempts and Interval for the system to re-establish a connection after failing a maximum number of attempts with a specified time interval.

```
(netconf-callhome)#retry-max-attempts 10
```

```
(netconf-callhome)#retry-interval 30
(netconf-callhome)#commit
```

5. Check the current NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
 retry-max-attempts 10
 retry-interval 30
!
```

6. Disable Reconnect:

```
(netconf-callhome)#reconnect disable
(netconf-callhome)#commit
```

7. Check the current NetConf Callhome configuration using the `show running-config netconf-callhome` command.

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
!
(netconf-callhome)#
```

retry-interval

Use this command to specify the number of seconds to wait after a connect attempt to the call home server fails.

Use the `no` form of this command to reset the retry interval to its default (300 seconds).

Command Syntax

```
retry-interval <1-86400>
no retry-interval
```

Parameters

`<1-86400>`	Retry interval in seconds

Default

By default, when the reconnect feature is enabled, the default retry interval is 300 seconds.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

1. Enable the NetConf callhome feature and reconnect commands:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
!
```

2. Configure retry interval:

```
(netconf-callhome)#retry-interval 100
(netconf-callhome)#commit
(netconf-callhome)#
```

3. Check the NetConf callhome show output:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
 retry-interval 100
!
```

4. Reset the interval:

```
(netconf-callhome)#no retry-interval
(netconf-callhome)#commit
```

5. Check the NetConf callhome show output:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
!
(netconf-callhome)#exit
```

retry-max-attempts

Use this command to specify the number of retries the OcNOS should attempt to the call home server before giving up.

Use the `no` form of this command to reset the maximum attempts to its default value (3).

Command Syntax

```
retry-max-attempts <0-255>
no retry-max-attempts
```

Parameters

`<0-255>`	Number of retries; specify zero (0) to retry infinitely.

Default

By default, when the reconnect feature is enabled, 3 attempts will be made.

Mode

NetConf call home mode

Applicability

This command was introduced in OcNOS version 6.0.0.

When users update the reconnect parameters, note the following:

- Servers that haven't completed the configured retry count with the updated configurations will be included in the new count.
- Servers for which the configured retry count has already been completed will restart the retrial process with the new configuration.

Example

1. Enable the NetConf callhome feature and reconnect commands:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
!
```

2. Configure retry maximum attempts:

```
(netconf-callhome)#retry-max-attempts 10
(netconf-callhome)#commit
(netconf-callhome)#
```

3. Check the NetConf callhome show output:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
```

```
 retry-max-attempts 10
!
```

4. Reset the attempts to its default value:

```
(netconf-callhome)#no retry-max-attempts
(netconf-callhome)#commit
```

5. Check the NetConf callhome show output:

```
(netconf-callhome)#do show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 reconnect enable
!
(netconf-callhome)#exit
```

show (xml|) running-config netconf-callhome

Use this command to display call home configurations.

Command Syntax

```
show (xml|) running-config netconf-callhome
```

Parameters

xml	Display the output in XML format

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

The below show command displays the running configuration of the Netconf Callhome feature in a normal format.

```
#show running-config netconf-callhome
!
netconf callhome
 feature netconf callhome enable
 management-port xe10
 reconnect enable
 retry-max-attempts 10
 retry-interval 100
 callhome server local-nc 192.168.56.1
 debug callhome
!
```

The below show command displays the running configuration of the Netconf Callhome feature in XML format.

```
#show xml running-config netconf-callhome
<netconf-server xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-management-server">
  <callhome>
    <feature-enabled></feature-enabled>
    <management-port>xe10</management-port>
    <netconf-client>
      <name>local-nc</name>
      <address>192.168.56.1</address>
    </netconf-client>
    <reconnect>
      <enable></enable>
      <retry-max-attempts>10</retry-max-attempts>
      <retry-interval>100</retry-interval>
    </reconnect>
  </callhome>
  <debug>
    <callhome-debug></callhome-debug>
```

```
  </debug>
</netconf-server>
```

CHAPTER 2 NetConf Port Access Commands

This chapter describes NetConf Port Access commands.

- feature netconf-ssh
- feature netconf-tls
- netconf-ssh port
- netconf-tls port
- show netconf server
- show running-config netconf server

Security Management Configuration

© 2025 IP Infusion Inc. Proprietary

CHAPTER 1 Access Control Lists Configurations

This chapter contains a complete example of access control list (ACL) configuration.

Overview

An Access Control List is a list of Access Control Entries (ACE). Each ACE in ACL specifies the access rights allowed or denied.

Each packet that arrives at the device is compared to each ACE in each ACL in the order they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

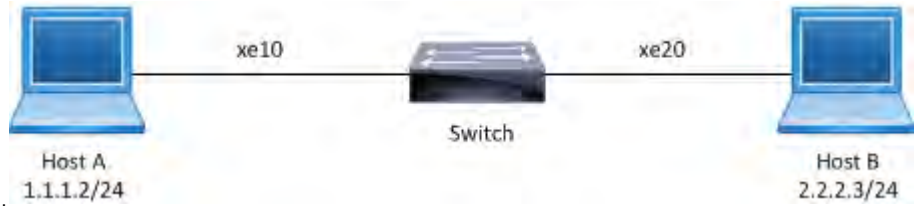


Figure 1-2: ACL sample topology

IPv4 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list T1`	Create an IP access list named T1.
`(config-ip-acl)#deny any host 1.1.1.1 any`	Create an access rule to deny IP packets with source address 1.1.1.1.
`(config-ip-acl)#permit any host 1.1.1.2 any`	Create an access rule to permit IP packets with source address 1.1.1.2.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group T1 in`	Apply access group T1 for inbound traffic to the interface.

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.1, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists T1
IP access list T1
        10 deny any host 1.1.1.1 any [match=200]
        20 permit any 1.1.1.2 any
        default deny-all
```

When inbound IP packets reach interface xe10 with a source address 1.1.1.2, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists T1
IP access list T1
    10 deny any host 1.1.1.1 any
    20 permit any 1.1.1.2 any [match=2000]
    default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

ICMP ACL Configuration

#configure terminal	Enter configure mode.
(config)#ip access-list icmp-acl-01	Create an IP access list named icmp-acl-01.
(config-ip-acl)#10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11	Create an access rule with sequence number 10 to deny ICMP packets from a specific source towards a specific destination with a DSCP value of af11. Note: The sequence number is optional.
(configip-acl)#20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash	Create an access rule with sequence number 20 to permit ICMP packets from a specific source towards a specific destination with precedence as flash.
(config-ip-acl)#exit	Exit access list mode.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface xe10	Enter interface mode.
(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#ip address 1.1.1.3/24	Assign an IP address.
(config-if)#ip access-group icmp-acl-01 in	Apply access group icmp-acl-01 for inbound traffic to the interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.X, destination address 2.2.2.X, DSCP value af11, and are fragmented, then the count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 [match=200]
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
    default deny-all
```

When inbound IP packets reach interface xe10 with source address as 1.1.1.X, destination address 2.2.2.X, and precedence value flash, then the count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash [match=200]
    default deny-all
```

Note: Use the command `clear ip access-list counters` to clear statistics of all ACLs configured or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

Access List Entry Sequence Numbering

You can change the sequence numbers of rules in an access list.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Enter access list mode for ACL icmp-acl-01.
`(config-ip-acl)#resequence 100 200`	Re-sequence the access list, starting with sequence number 100 and incrementing by 200.
`(config-ip-acl)#1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11`	Re-sequencing specific access rule 100 with sequence number 1000
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#commit`	Commit the candidate configuration to the running configuration

Validation

Before re-sequencing:

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
        20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
        default deny-all
```

After re-sequencing the access list, starting with sequence number 100 and incrementing by 200

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        100 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
        300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
```

```
        default deny-all
```

After re-sequencing specific access rule 100 with sequence number 1000

```
 #show access-lists icmp-acl-01
IP access list icmp-acl-01
300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
default deny-all
```

IPv6 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ipv6 access-list ipv6-acl-01`	Create an IPv6 access list named as icmp-acl-01.
`(config-ipv6-acl)#11 deny ipipv6 any any`	Create access rule sequence number 11 to deny IPv4 encapsulated packets in IPv6 with any source address to any destination address.
`(config-ipv6-acl)#default permit-all`	Update the default rule to permit all.
`(config-ipv6-acl)#exit`	Exit access list mode
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ipv6 address 1:1::1:3/64`	Assign an IPv6 address.
`(config-if)#ipv6 access-group ipv6-acl-01 in`	Apply access group ipv6-acl-01 for inbound traffic to the interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IPv6 packets reach interface xe10 with IPv4, then count for access rule 11 increases equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ipipv6 any any [match=1000]
    default permit all
```

For all other IPv6 packets, access rule 100 is invoked and the match counts increase equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ipipv6 any any
    default permit-all [match=2000]
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list <ipv6 access-list name> counters` to clear statistics of the particular IPv6 ACL.

IPv6 ACL Configuration for 128-Bit Support

Configuration for Physical, PO, SA and MLAG Interfaces

`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#ipv6 access-list test1`	Create an IPv6 access list named `test1`.
`(config-ipv6-acl)#permit any 2001::1/128 2002::1/128`	Create an access rule to permit any IPv6 packet from 2001::1/128 to 2002::1/128.
`(config-ipv6-acl)#commit`	Commit the candidate configuration to the running configuration.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#ipv6 access-group test1 in`	Attach IPv6 access list `test1` to the interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.

Validation

Use the commands below to verify the running configurations.

```
#show running-config ipv6 access-list
ipv6 access-list test1
 10 permit any 2001::1/128 2002::1/128
!
#show running-config interface xe1
!
interface xe1
 ipv6 access-group test1 in
!
#
```

Use the commands below to verify the match count.

```
#show ipv6 access-lists test1
IPv6 access list test1
        10 permit any 2001::1/128 2002::1/128  [match=1000]
        268435453 permit icmpv6 any any
        default deny-all
#
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list NAME counters` to clear statistics of the particular IPv6 ACL.

Configuration for VLAN Interfaces and L3 Subinterfaces

`(config)#commit`	Commit the candidate configuration to the running configuration.
`(config)#interface vlan1.20`	Enter interface mode.
`(config-if)#ipv6 access-group test1 in`	Attach IPv6 access list `test1` to the interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.
`(config)#interface xe1.2`	Enter interface mode.
`(config-if)#ipv6 access-group test1 in`	Attach IPv6 access list `test1` to the interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration.

Validation

Use the commands below to verify the running configurations.

```
#show running-config ipv6 access-list
ipv6 access-list test1
 10 permit any 2004::1/128 2005::1/128
!

#show running-config interface vlan1.20
!
interface vlan1.20
 ipv6 access-group test1 in
#

#show running-config interface xe1.2
interface xe1.2
 ipv6 access-group test1 in
!
```

Use the commands below to verify the match count.

```
#show ipv6 access-lists test1
IPv6 access list test1
        10 permit any 2004::1/128 2005::1/128 [match=1000]
        268435453 permit icmpv6 any any
        default deny-all
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list NAME counters` to clear statistics of a particular IPv6 ACL.

MAC ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#mac access-list mac-acl-01`	Create a MAC access list named mac-acl-01.

`(config-mac-acl)#22 permit host 0000.0011.1212 host 0000.1100.2222 vlan 2`	Create an access rule with sequence number 22 to permit packets from a host with a specific MAC towards a host with a specific MAC with VLAN 2.
`(config-mac-acl)#exit`	Exit access list mode.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#bridge 1 protocol rstp vlan-bridge`	Create a VLAN-aware RSTP bridge.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2.
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to trunk mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#mac access-group mac-acl-01 in`	Applies the MAC access list mac-acl-01 to ingress traffic.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound packets reach interface xe10 with the specific source and destination MAC with the VLAN as 2, then the count for access rule 22 increases equal to the number of packets sent.

```
#show mac access-lists
MAC access list mac-acl-01
    22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2 [match=3000]
    default deny-all
```

For all other packets, default rule is invoked and the match counts increases equal to the number of packets sent.

```
#show mac access-lists mac-acl-01
MAC access list mac-acl-01
    22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2
    default deny-all [match=2000]
```

Note: As per the present design, ARP/ND packets will be filtered based on the source MAC address only (host mac address).

Note: Use the command `clear mac access-list counters` to clear statistics of all MAC ACLs or `clear mac access-list <mac access-list name> counters` to clear statistics of a particular MAC ACL.

Management ACL Overview

Management Port ACL can be used to provide basic level of security for accessing the management network. ACLs can also be used to decide which types of management traffic to be forwarded or blocked at the management port.

When configuring access list on a router or a switch, each access list needs to be identified by a unique name or a number. Each access list entry can have permit or deny actions. Each entry will be associated with a sequence number in the range of <1-268435453>. Lower the sequence number, higher the priority.

User should be able to configure the system to allow certain IP address for a protocol and don't allow any other IP address matching for that protocol.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

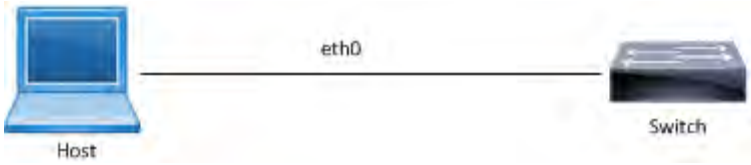


Figure 1-3: Management ACL Sample Topology

Management ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list mgmt`	Create an IP access list named mgmt
`(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh`	Create an access rule to permit TCP connection with source address 10.12.45.57 with destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet`	Create an access rule to permit TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq snmp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to SNMP.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq ntp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to NTP.
`(config-ip-acl)#permit udp host 10.12.29.49 any eq snmptrap`	Create an access rule to permit UDP packet with source address 10.12.29.49 with any Destination address on destination port equal to SNMPTrap.
`(config-ip-acl)#permit tcp host 10.12.29.49 eq ssh host 10.12.45.57`	Create an access rule to permit TCP connection with source address 10.12.29.49 on source port equal to ssh with Destination address 10.12.45.57 .
`(config-ip-acl)#deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh`	Create an access rule to deny TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet`	Create an access rule to deny TCP connection with source address 10.12.45.57 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 10.12.29.49/24`	Assign an IP address.

(config-if)#ip access-group mgmt in	Apply access group mgmt for inbound traffic to the interface.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When a TCP connection for Destination Port SSH reach interface eth0 with source address 10.12.45.57, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection for Destination Port Telnet reach interface eth0 with source address 10.12.45.58, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet [match=10]
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port SNMP reach interface eth0 with any source address, then the match count for access rule 30 increases equal to the number of packets sent. Prior to this SNMP should be configured on Device (10.12.29.49).

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

    #show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp [match=50]
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a UDP packet for Destination Port NTP reach interface eth0 with any source address, then the match count for access rule 40 increases equal to the number of packets sent. Prior to this NTP should be configured on Device (10.12.29.49).

```
    Example:
    ntp enable vrf management
    ntp authenticate vrf management
    ntp authentication-key 123 md5 swwx 7 vrf management
    ntp trusted-key 123 vrf management
    ntp server 10.12.45.36 vrf management
    ntp server 10.12.16.16 prefer vrf management
    ntp server 10.12.16.16 key 123 vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp [match=1]
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port SSH reach interface eth0 with source address 10.12.45.58, this should deny the connection and the match count for access rule 70 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh [match=1]
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When a TCP connection request for Destination Port Telnet reach interface eth0 with source address 10.12.45.57, this should deny the connection and the match count for access rule 80 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet[match=1]
            default deny-all
```

To enable SNMPTRAPS, apply the ACL outbound to the Management interface.

`#configure terminal`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#ip access-group mgmt out`	Apply access group mgmt for outbound traffic to the interface.
`(config-if)#commit`	Commit the candidate configuration to the running configuration
`(config-if)#end`	Exit interface and configure mode.

When a UDP packet for Destination Port SNMPTrap sends out of interface eth0 with any Destination address, then the match count for access rule 50 increases equal to the number of packets received. Prior to this SNMPTrap should be configured on Device (10.12.29.49) to listen to port 162.

```
    Example:
    snmp-server community SNMPTEST group network-admin vrf management
    snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-port 162 vrf
    management
    snmp-server enable snmp  vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap [match=5]
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

When an ACL is applied on interface eth0 outbound and inbound together, then we must configure an ACL to establish a TCP connection between source 10.12.29.49 with source Port SSH to destination address 10.12.45.57. When a TCP connection is established on port SSH, then the match count for access rule 10 and 60 increases equal to the number of packets sent and received.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57[match=9]
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

```
#show access-lists
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
```

```
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet


#show access-lists summary
     IPV4 ACL mgmt
           statistics enabled
           Total ACEs Configured: 8
           Configured on interfaces:
              eth0 - ingress (Router ACL)
           Active on interfaces:
              eth0 - ingress (Router ACL)

#show access-lists expanded
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet
            default deny-all [match=4]
```

ARP ACL Overview

ARP ACL can be used to permit or deny the ARP packets, based on the ARP request or response option configured.

Topology

Figure 1-4: ARP ACL Sample Topology

ARP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface ge4`	Enter interface mode
`(config-if)#ip address 11.11.11.11/24`	Assign IPv4 address.
`(config-if)#exit`	Exit access list mode.
`(config)#commit`	Commit the candidate configurations to the running configurations
`(config)#mac access-list m1`	Enter mac access list mode.
`(config-mac-acl)#permit any any vlan 6`	Create an access rule to permit any IPv6 packet
`(config-mac-acl)#permit 0000.0215.2151 0000.0000.0011 any vlan 3`	Create an access rule to permit specific ARP response.

(config-mac-acl)#exit	Exit access list mode.
(config)#commit	Commit the candidate configurations to the running configurations
(config)#interface ge4	Enter interface mode.
(config-if)#mac access-group m1 in	Apply access group mac1 for inbound traffic to the interface.
(config-if)#commit	Commit the candidate configurations to the running configurations
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to assign IP address on IXIA and ping from IXIA.

```
#show mac access-lists
    MAC access list mac1
            10 permit host 0000.3AE0.456D any arp request [match=1]
            20 permit host 0000.3AE0.456D any arp response [match=1]
            30 permit any any ipv4 [match=1]
            default deny-all
```

ACL over Loopback

The loopback interface ACL feature provides basic security for management applications accessible through In-band interfaces.

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

Topology

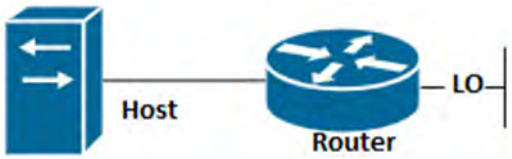


Figure 1-5: ACL Loopback Topology

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 3.3.3.3/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 4.4.4.4/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 5.5.5.5/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 6.6.6.6/32 secondary	Assign the IPv4 secondary address.
(config-if)#ip address 7.7.7.7/32 secondary	Assign the IPv4 secondary address.
(config-if)# exit	Exit interface mode.
(config)#commit	Commit the candidate configuration to the running configuration
(config)#ip access-list loopback	Create loopback access list
(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet	Permit telnet session from any source with specific destination.

(config-ip-acl)# 20 deny tcp any host 4.4.4.4 eq telnet	Deny telnet session from any source with specific destination.
(config-ip-acl)# 30 permit tcp any host 5.5.5.5 eq ssh	Permit ssh session from any source with specific destination.
(config-ip-acl)# 40 deny tcp any host 6.6.6.6 eq ssh	Deny ssh session from any source with specific destination.
(config-ip-acl)# 50 deny udp any host 6.6.6.6 eq snmp	Deny udp from any source with specific destination.
(config-ip-acl)# 60 deny udp any host 7.7.7.7 eq ntp	Deny udp from any source with specific destination.
(config-ip-acl)#exit	Exit interface acl mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#interface lo	Enter interface lo mode
(config-if)#ip access-group loopback in	Associate loopback acl over lo interface
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#exit	Exit config mode

Validation

```
#sh access-lists
IP access list loopback
        10 permit tcp any host 3.3.3.3 eq telnet [match=12]
        20 deny tcp any host 4.4.4.4 eq telnet [match=12]
        30 permit tcp any host 5.5.5.5 eq ssh
        40 deny tcp any host 6.6.6.6 eq ssh
        50 deny udp any host 6.6.6.6 eq snmp  [match=6]
        60 deny udp any host 7.7.7.7 eq ntp

#sh ip access-lists summary
 IPV4 ACL loopback
       statistics enabled
       Total ACEs Configured: 6
       Configured on interfaces:
          lo - ingress (Router ACL)
       Active on interfaces:
          lo - ingress (Router ACL)
       Configured on line vty:

#sh running-config aclmgr
ip access-list loopback
 10 permit tcp any host 3.3.3.3 eq telnet
 20 deny tcp any host 4.4.4.4 eq telnet
 30 permit tcp any host 5.5.5.5 eq ssh
 40 deny tcp any host 6.6.6.6 eq ssh
 50 deny udp any host 6.6.6.6 eq snmp
 60 deny udp any host 7.7.7.7 eq ntp
```

```
!
interface lo
 ip access-group loopback in
!
```

ACL OVER Virtual Terminal (VTY)

When a Telnet/SSH/NetConf connection is established in the OcNOS, it associates the connection with a virtual terminal (VTY) line. The ACL over VTY feature provides security for management features associated with VTY.

Users can create Standard and Extended ACL rules and attach them to a virtual teletype (VTY) command line interface. These ACL rules are applied on both Management and Default virtual routing forwarding (VRFs).

OcNOS supports both IPv4 and IPv6 access lists for VTY lines, providing flexibility for network configurations.

Applying a standard ACL rule on a VTY line permits or denies only management access protocols such as SSH, Telnet, and SSH-Netconf protocols (port numbers 22,23,830)).

Extended ACL rules are applied as configured by the user, and it is not limited to management protocols only, unlike Standard ACLs.

When a user configures a rule with 'deny any any any' and attaches it to the VTY, it effectively blocks only the Telnet, SSH, and NetConf protocols on the control plane

For example, when a user configures a rule as below and attach them to VTY, If the deny ACL rule includes ’any’ value in protocol, only Telnet/SSH/SSH-NetConf protocols are denied.

```
ip access-list ssh-access
10 permit tcp 10.12.43.0/24 any eq ssh
20 deny any any any
```

Note: To deny any protocols other than Telnet/SSH/SSH-Netconf, create a deny rule with the specific protocol access on VTY. For example: To deny OSPF protocol from all the source and destination address, apply the rule, `10 deny ospf any any`.

In general, the VTY ACLs are more specific to management protocols. Hence, the Extended ACL “any” rule translation is enhanced to allow management protocols as follows:

- If the **deny** ACL rule includes any value in protocol, only Telnet/SSH/SSH-Netconf protocols are denied.
- The **permit** ACL rule is unchanged. v

Note: Refer to the command reference section for limitations, default behavior, and unsupported features.

Topology

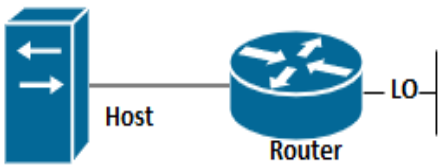


Figure 1-6: ACL VTY Topology

VTY ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 3.3.3.3/32 secondary`	Assign the IPv4 secondary address.
`(config-if)# exit`	Exit interface mode.
`(config)#ip access-list vty`	Create loopback access list
`(config-ip-acl)# 10 permit tcp any host 3.3.3.3 eq telnet`	Permit telnet session from any source with specific destination.
`(config-ip-acl)#exit`	Exit interface acl mode
`(config)#line vty`	Enter interface vty mode
`(config-all-line)#ip  access-group vty in`	Associate acl over
`(config-if)#exit`	Exit interface mode
`(config)#exit`	Exit config mode

Validation

```
OcNOS#sh access-lists
IP access list vty
       10 permit tcp any host 3.3.3.3 eq telnet

OcNOS#sh ip access-lists summary
IPV4 ACL vty
       statistics enabled
       Total ACEs Configured: 1
       Configured on interfaces:
       Active on interfaces:
       Configured on line vty:
       all vty lines - ingress

OcNOS#sh running-config access-list
ip access-list vty
10 permit tcp any host 3.3.3.3 eq telnet
!
line vty
ip access-group vty in
```

Implementation Examples

```
OcNOS#show running-config aclmgr
ip access-list ssh-access
 10 permit tcp 10.12.43.0/24 any eq ssh
 20 deny tcp 10.12.33.0/24 any eq 6513
 30 deny any 10.12.34.0/24 any
 40 deny any any any
!
line vty
 ip access-group ssh-access in
```

```
#####iptables o/p######

root@OcNOS:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  10.12.43.0/24        anywhere             tcp dpt:ssh
DROP       tcp  --  10.12.33.0/24        anywhere             tcp dpt:tls_netconf
DROP       tcp  --  10.12.34.0/24        anywhere             multiport dports
ssh,telnet,ssh_netconf
DROP       tcp  --  anywhere             anywhere             multiport dports
ssh,telnet,ssh_netconf
```

Timed ACL Configuration

The time range feature was introduced to be able to add a timing boundary for specified activities. The activity would start, end and repeat at the specific times set by the user. This time-range feature will enable creating "Timed ACLs". This will help service providers to customize the internet data to customers based on time to increase the video traffic during weekends and reduce data traffic, restrict the internet traffic in school or college non-working hours etc.

Topology

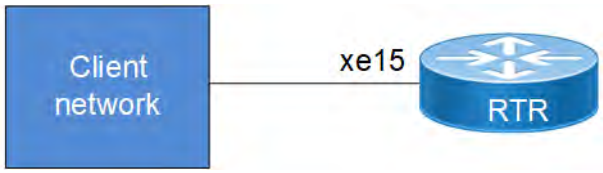


Figure 1-7: Timed ACL sample topology

Configuration with IPv4 Address

`#configure terminal`	Enter configure mode.
`(config)#time-range TIMER1`	Configure a timer
`(config-tr)#start-time 10:00 03 nov 2021`	Configure start time
`(config-tr)#end-time 18:00 03 nov 2021`	Configure end time
`(config-tr)#exit`	Exit timer
`(config)#ip access-list ACL1`	Create ip access list
`(config-ip-acl)# deny icmp host 10.1.1.1 host 10.1.2.2`	Create an acl rule to deny icmp
`(config-ip-acl)#exit`	Exit Acl mode
`(config)#commit`	Commit the candidate configuration to the running configuration
`(config)#int xe15`	Enter into the interface mode
`(config-if)#ip access-group ACL1 out time-range TIMER1`	Apply the acl along with the timer.

(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit

Configuration with IPv6 Address

(config)#ipv6 access-list ACL1v6	Create ipv6 access list
(config-ipv6-acl)# deny any any any	Create an acl rule to deny
(config-ipv6-acl)#exit	Exit Acl mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#int xe12	Enter into the interface mode
(config-if)# ipv6 access-group ACL1v6 in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit

Configuration with mac

(config)# mac access-list ACL1mac	Create ip access list
(config-mac-acl)# deny 0000.0000.0000 1111.2222.3333 0000.0000.0000 4444.5555.6666	Create an acl rule to deny icmp
(config-mac-acl)#exit	Exit Acl mode
(config)#commit	Commit the candidate configuration to the running configuration
(config)#int xe13	Enter into the interface mode
(config-if)# mac access-group ACL1mac in time-range TIMER1	Apply the acl along with the timer.
(config-if)#commit	Commit the candidate configuration to the running configuration
(config-if)#exit	Exit

Validation

```
#sh running-config in xe15
!
interface xe15
 ip access-group ACL1 out time-range TIMER1
!
#sh running-config in xe12
!
interface xe12
 ipv6 access-group ACL1v6 in time-range TIMER1
!
```

```
#sh running-config in xe13
!
interface xe13
 mac access-group ACL1mac in time-range TIMER1


#sh time-range
=====================================
TR handler interval: 10 seconds
=====================================
TR entries: 1
Entry: 0
 name: TIMER1
 state: Pending
 frequency: none
 start time: Wed Nov  3 10:00:00 2021
 end time: Wed Nov  3 18:00:00 2021
=====================================
RUNNING TR entries: 0
=====================================
COMPLETED TR entries: 0
```

ACL on IRB Interface over MPLS EVPN

Applying ACLs to an Integrated Routing and Bridging (IRB) interface or switchport enables control over packet flow, whether ingress or egress the interface. This capability is essential for maintaining security, managing bandwidth, and ensuring effective routing and bridging.

Topology

In this topology, PE1 and PE2 routers have IRB interfaces configured. The IRB interfaces bridge VLAN traffic and route between VLANs, enabling communication between Layer 2 and Layer 3.

ACLs are applied on the IRB interfaces to filter traffic, ensuring only authorized traffic passes through. The P1 router acts as a transit router, forwarding traffic between PE1 and PE2. The P1 router provides core functionality but does not handle IRB interfaces directly.

This configuration ensures that while traffic flows across the network, ACL policies can be enforced at both PE1 and PE2 over the IRB interfaces, securing communication between VLANs and controlling access between external networks.

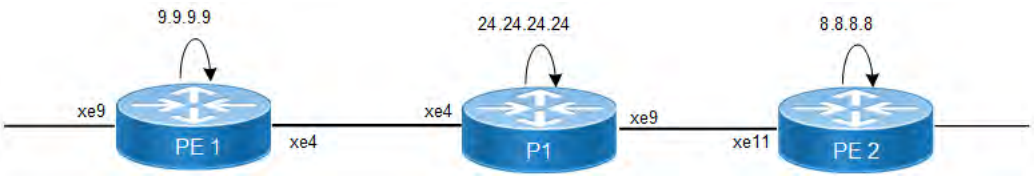


Figure 1-8: ACL on IRB sample topology

ACLs Configuration on IRB

Perform the following steps to enable EVPN MPLS on an IRB interface while applying ACLs to control ingress or egress traffic:

Note: The required configuration for ACL on IRB is added in the Configuration section, for the detailed configuration on IRB symmetric and asymmetric refer to the Configurations section in EVPN MPLS IRB Configuration.

1. Enable Hardware Profiles for both IPv4 and IPv6 traffic at the ingress and egress of the interface:

```
PE1(config)#hardware-profile filter ingress-ipv4-subif enable
PE1(config)#hardware-profile filter ingress-ipv6-ext-subif enable
PE1(config)#hardware-profile filter egress-ipv4-ext enable
PE1(config)#hardware-profile filter egress-ipv6 enable
PE1(config)#hardware-profile filter evpn-mpls-mh enable
PE1(config)#commit
```

2. Enable EVPN MPLS:

```
PE1(config)#evpn mpls enable
PE1(config)#evpn mpls irb
PE1(config)#evpn mpls multihoming enable  # Only if multihoming is required
PE1(config)#commit
```

3. Configure an anycast MAC address for the gateway in a multihoming scenario, allowing multiple devices to share the same MAC address for redundancy:

```
PE1(config)#evpn irb-forwarding anycast-gateway-mac 0011.3333.5555
PE1(config)#commit
```

4. Define a MAC VRF for isolating MAC address routing within the EVPN framework:

```
PE1(config)#mac vrf vrfirb
PE1(config-vrf)# rd 9.9.9.9:2001
PE1(config-vrf)# route-target both 2001:2001
```

Note: Ensure to provide `<RD value>` with a value different from PE1's RD of `9.9.9.9` to maintain proper routing table separation and avoiding conflicts between the two PE devices.

5. Define an IP VRF for routing L3 traffic within the EVPN framework:

```
PE1(config)#ip vrf ip_vrfirb
PE1(config-vrf)# rd 9.9.9.9:200
PE1(config-vrf)# route-target both 200:200
PE1(config-vrf)# l3vni 20000
PE1(config-vrf)#commit
```

Note: Ensure to provide `<rd value>` with a value different from PE1's RD of `9.9.9.9` to maintain proper routing table separation and avoiding conflicts between the two PE devices.

6. Configure EVPN MPLS for host reachability and specify the IRB interface:

```
PE1(config-evpn-mpls)#evpn mpls id 200
PE1(config-evpn-mpls)#host-reachability-protocol evpn-bgp vrfirb
PE1(config-evpn-mpls)#evpn irb irb100
PE1(config-evpn-mpls)#commit
```

7. Configure a po interface for VLAN encapsulation and map it to the EVPN instance:

```
PE1(config)#interface po1000.200 switchport
PE1(config-if)# encapsulation dot1q 200
PE1(config-if)# rewrite pop
PE1(config-if)# load-interval 30
PE1(config-if)# access-if-evpn
PE1(config-acc-if-evpn)#  map vpn-id 200
```

```
PE1(config-acc-if-evpn)#commit
```

8. Create ACL to filter outgoing traffic:

```
PE1(config)#ip access-list asy-egress
PE1(config-ip-acl)# 120 deny any host 70.70.1.2 80.80.1.0/24
PE1(config-ip-acl)#commit
```

9. Configure the IRB interface with IP addresses, associate it with the VRF, and apply the ACL:

```
PE1(config)#interface irb100
PE1(config-irb-if)# ip vrf forwarding ip_vrfirb
PE1(config-irb-if)# evpn irb-if-forwarding anycast-gateway-mac
PE1(config-irb-if)# ip address 80.80.1.1/24 anycast
PE1(config-irb-if)# ipv6 address 80:80::1/48 anycast
PE1(config-irb-if)# ip access-group asy-egress out
PE1(config-irb-if)#commit
```

Configuration Snapshot

PE1

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
hardware-profile filter ingress-ipv4-subif enable
hardware-profile filter ingress-ipv6-ext-subif enable
hardware-profile filter egress-ipv4-ext enable
hardware-profile filter evpn-mpls-mh enable
hardware-profile statistics voq-full-color enable
hardware-profile statistics cfm-ccm enable
!
qos enable
!
hostname 7009-PE1
no ip domain-lookup
ip domain-lookup vrf management
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
lldp run
```

```
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-description
!
ip access-list asy-egress
120 deny any host 70.70.1.2 80.80.1.0/24

!
evpn mpls enable
!
evpn mpls irb
!
evpn mpls multihoming enable
!
ip vrf management
!
mac vrf vrfirb
 rd 9.9.9.9:2001
 route-target both 2001:2001
!
ip vrf ip_vrfirb
 rd 9.9.9.9:200
 route-target both 200:200
 l3vni 20000
!
evpn irb-forwarding anycast-gateway-mac 0011.3333.5555
!
evpn mpls vtep-ip-global 9.9.9.9
!
evpn mpls id 200
 host-reachability-protocol evpn-bgp vrfirb
 evpn irb irb100
!
router ldp
 router-id 9.9.9.9
 targeted-peer ipv4 8.8.8.8
  exit-targeted-peer-mode
 transport-address ipv4 9.9.9.9
!
router rsvp
!
interface po1000
 switchport
 load-interval 30
 mtu 9216
!
interface po1000.200 switchport
 encapsulation dot1q 200
 rewrite pop
 load-interval 30
 access-if-evpn
```

```
   map vpn-id 200
 !
 interface eth0
  ip vrf forwarding management
  ip address dhcp
 !
 interface irb100
  ip vrf forwarding ip_vrfirb
  evpn irb-if-forwarding anycast-gateway-mac
  ip address 80.80.1.1/24 anycast
  ip access-group asy-egress out
 !
 interface lo
  ip address 127.0.0.1/8
  ip address 9.9.9.9/32 secondary
  ipv6 address ::1/128
  ip router isis ISIS-IGP
  enable-ldp ipv4
  enable-rsvp
 !
 interface lo.management
  ip vrf forwarding management
  ip address 127.0.0.1/8
  ipv6 address ::1/128
 !
 interface xe3
 !
 interface xe4
  description connected to 7024 P1
  speed 10g
  ip address 10.12.255.5/24
  mtu 9216
  label-switching
  ip router isis ISIS-IGP
  enable-ldp ipv4
  enable-rsvp
  exit
 !
interface xe9
channel-group 1000 mode active
 !
 router isis ISIS-IGP
  is-type level-1
  authentication mode md5 level-1
  ignore-lsp-errors
  lsp-gen-interval 5
  spf-interval-exp level-1 50 2000
  metric-style wide
  mpls traffic-eng router-id 9.9.9.9
  mpls traffic-eng level-1
```

```
 capability cspf
 dynamic-hostname
 fast-reroute terminate-hold-on interval 10000
 fast-reroute per-prefix level-1 proto ipv4 all
 fast-reroute per-prefix remote-lfa level-1 proto ipv4 tunnel mpls-ldp
 net 49.0001.0000.0000.0009.00
!
router bgp 65010
 neighbor 8.8.8.8 remote-as 65010
 neighbor 24.24.24.24 remote-as 65010
 neighbor 8.8.8.8 update-source lo
 neighbor 8.8.8.8 advertisement-interval 0
 neighbor 24.24.24.24 update-source lo
 neighbor 24.24.24.24 advertisement-interval 0
 !
 address-family l2vpn evpn
 neighbor 8.8.8.8 activate
 neighbor 24.24.24.24 activate
 exit-address-family
 !
 address-family ipv4 vrf ip_vrfirb
 redistribute connected
 exit-address-family
 !
 exit
!
rsvp-trunk PE1-PE3 ipv4
 to 8.8.8.8
!
!
end
```

PE2

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
hardware-profile filter ingress-ipv4-subif enable
hardware-profile filter ingress-ipv6-ext-subif enable
hardware-profile filter egress-ipv4-ext enable
hardware-profile filter egress-ipv6 enable
hardware-profile filter evpn-mpls-mh enable
hardware-profile statistics voq-full-color enable
hardware-profile statistics cfm-ccm enable
!
```

```
qos enable
!
hostname 7008-PE2
no ip domain-lookup
ip domain-lookup vrf management
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
lldp run
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-description
!
evpn mpls enable
!
evpn mpls irb
!
evpn mpls multihoming enable
!
ip vrf management
!
mac vrf vrfirb
 rd 8.8.8.8:2000
 route-target both 2000:2000
!
ip vrf ip_vrfirb
 rd 8.8.8.8:200
 route-target both 200:200
 l3vni 20000
!
evpn mpls vtep-ip-global 8.8.8.8
!
evpn mpls id 101
 host-reachability-protocol evpn-bgp vrfirb
 evpn irb irb100
!
router ldp
 router-id 8.8.8.8
 targeted-peer ipv4 9.9.9.9
  exit-targeted-peer-mode
 transport-address ipv4 8.8.8.8
!
router rsvp
```

```
!
interface po2000
 load-interval 30
 mtu 9216
!
interface po2000.200 switchport
 encapsulation dot1q 200
 rewrite pop
 load-interval 30
 mtu 9216
 access-if-evpn
  map vpn-id 101
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface irb100
 ip vrf forwarding ip_vrfirb
 ip address 70.70.1.1/24
!
interface lo
 ip address 127.0.0.1/8
 ip address 8.8.8.8/32 secondary
 ipv6 address ::1/128
 ip router isis ISIS-IGP
 enable-ldp ipv4
 enable-rsvp
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe11
 description connected to 7024-P1
 speed 10g
 ip address 10.12.121.5/24
 mtu 9216
 label-switching
 ip router isis ISIS-IGP
 enable-ldp ipv4
 enable-rsvp
!
interface xe26
 speed 10g
 channel-group 2000 mode active
!
interface xe27
!
```

```
 exit
!
router isis ISIS-IGP
 is-type level-1
 authentication mode md5 level-1
 ignore-lsp-errors
 lsp-gen-interval 5
 spf-interval-exp level-1 50 2000
 metric-style wide
 mpls traffic-eng router-id 8.8.8.8
 mpls traffic-eng level-1
 capability cspf
 dynamic-hostname
 fast-reroute terminate-hold-on interval 10000
 fast-reroute per-prefix level-1 proto ipv4 all
 fast-reroute per-prefix remote-lfa level-1 proto ipv4 tunnel mpls-ldp
 net 49.0001.0000.0000.0008.00
!
router bgp 65010
 neighbor 9.9.9.9 remote-as 65010
 neighbor 24.24.24.24 remote-as 65010
 neighbor 9.9.9.9 update-source lo
 neighbor 9.9.9.9 advertisement-interval 0
 neighbor 24.24.24.24 update-source lo
 neighbor 24.24.24.24 advertisement-interval 0
 !
 address-family l2vpn evpn
 neighbor 9.9.9.9 activate
 neighbor 24.24.24.24 activate
 exit-address-family
 !
 address-family ipv4 vrf ip_vrfirb
 redistribute connected
 exit-address-family
 !
 exit
!
rsvp-trunk PE3-PE1 ipv4
 to 9.9.9.9
!
!
end
```

P1

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
```

```
!
logging level nsm 4
logging level cmm 4
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
hardware-profile filter ingress-ipv4-subif enable
hardware-profile filter ingress-ipv6-ext-subif enable
hardware-profile filter egress-ipv4-ext enable
hardware-profile filter egress-ipv6 enable
hardware-profile filter evpn-mpls-mh enable
hardware-profile statistics voq-full-color enable
hardware-profile statistics cfm-ccm enable
!
qos enable
!
hostname 7024-P1
no ip domain-lookup
ip domain-lookup vrf management
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
lldp run
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt system-capabilities
lldp tlv-select basic-mgmt system-description
lldp tlv-select basic-mgmt management-address
lldp notification-interval 1000
fault-management enable
!
evpn mpls enable
!
evpn mpls multihoming enable
!
ip vrf management
!
router ldp
!
router rsvp
!
interface eth0
```

```
 ip vrf forwarding management
 ip address dhcp
!
interface ge25
!
interface lo
 ip address 127.0.0.1/8
 ip address 24.24.24.24/32 secondary
 ipv6 address ::1/128
 enable-ldp ipv4
 enable-rsvp
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe4
 description connected to 7009 PE1
 speed 10g
 ip address 10.12.255.4/24
 mtu 9216
 label-switching
 ip router isis ISIS-IGP
 enable-ldp ipv4
 enable-rsvp
!
interface xe9
 description connected to 7008-PE2
 speed 10g
 ip address 10.12.121.4/24
 mtu 9216
 label-switching
 ip router isis ISIS-IGP
 enable-ldp ipv4
 enable-rsvp
!
exit
!
router isis ISIS-IGP
 is-type level-1
 authentication mode md5 level-1
 ignore-lsp-errors
 lsp-gen-interval 5
 spf-interval-exp level-1 50 2000
 metric-style wide
 mpls traffic-eng router-id 24.24.24.24
 mpls traffic-eng level-1
 capability cspf
 dynamic-hostname
```

```
 fast-reroute terminate-hold-on interval 10000
 fast-reroute per-prefix level-1 proto ipv4 all
 fast-reroute per-prefix remote-lfa level-1 proto ipv4 tunnel mpls-ldp
 net 49.0001.0000.0000.0024.00
!
end
```

Validation

Verify that after applying ACL traffic is not egressing out:

```
7009-PE1#show interface counters rate mbps
+------------------+-------------+------------+-------------+------------+
|     Interface    |    Rx mbps  |    Rx pps  |    Tx mbps  |    Tx pps  |
+------------------+-------------+------------+-------------+------------+
 xe4                 6.53          6169          0.01          0
 xe9                 0.02          1             0.01          0

7009-PE1#show ip access-lists
IP access list asym-egress
        120 deny any host 70.70.1.2 80.80.1.0 0.0.0.255 [match=220847]
        default deny-all
```

Verify that the ACL rule is matching and counters are incremented accordingly:

```
7009-PE1#show ip access-lists
IP access list allow-1
       IP access list asym-egress
        120 deny any host 70.70.1.2 80.80.1.0 0.0.0.255 [match=242780]

7009-PE1#show ip access-lists
IP access list asym-egress
        120 deny any host 70.70.1.2 80.80.1.0 0.0.0.255 [match=257475]
        default deny-all

7009-PE1#show ip access-lists
IP access list asym-egress
        120 deny any host 70.70.1.2 80.80.1.0 0.0.0.255 [match=272097]
        default deny-all
```

ACL on IRB Interface over VXLAN EVPN

Applying ACLs to an Integrated Routing and Bridging (IRB) interface or switchport enables control over packet flow, whether ingress or egress the interface. This capability is essential for maintaining security, managing bandwidth, and ensuring effective routing and bridging.

Topology

In this topology, PE1 and PE2 routers have IRB interfaces configured. The IRB interfaces bridge VLAN traffic and route between VLANs, enabling communication between Layer 2 and Layer 3.

ACLs are applied on the IRB interfaces to filter traffic, ensuring only authorized traffic passes through. The P1 router acts as a transit router, forwarding traffic between PE1 and PE2. The P1 router provides core functionality but does not handle IRB interfaces directly.

This configuration ensures that while traffic flows across the network, ACL policies can be enforced at both PE1 and PE2 over the IRB interfaces, securing communication between VLANs and controlling access between external networks.

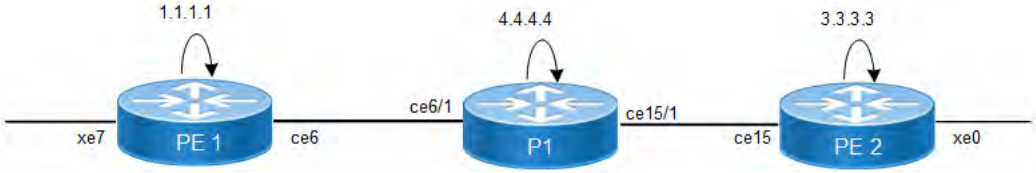


Figure 1-9: ACL on IRB sample topology

ACLs Configuration on IRB

Perform the following steps to enable EVPN VXLAN on an IRB interface while applying ACLs to control ingress or egress traffic:

Note: The required configuration for ACL on IRB is added in the Configuration section, for the detailed configuration on IRB symmetric and asymmetric refer to the Base Configuration - L2 VxLAN section in VxLAN-EVPN with IRB

1. Enable Hardware Profiles for both IPv4 and IPv6 traffic at the ingress and egress of the interface:

```
PE1(config)#hardware-profile filter ingress-ipv4-subif enable
PE1(config)#hardware-profile filter ingress-ipv6-ext-subif enable
PE1(config)#hardware-profile filter egress-ipv4-ext enable
PE1(config)#hardware-profile filter egress-ipv6 enable
PE1(config)#hardware-profile filter vxlan enable
PE1(config)#hardware-profile filter vxlan-mh enable
PE1(config)#commit
```

2. Enable EVPN VXLAN:

```
PE1(config)#nvo vxlan enable
PE1(config)#nvo vxlan irb
PE1(config)#evpn vxlan multihoming enable # Only if multihoming is required
PE1(config)#commit
```

3. Configure an anycast MAC address for the gateway in a multihoming scenario, allowing multiple devices to share the same MAC address for redundancy:

```
PE1(config)#evpn irb-forwarding anycast-gateway-mac 0000.0000.1111
PE1(config)#commit
```

4. Define a MAC VRF for isolating MAC address routing within the EVPN framework:

```
PE1(config)#mac vrf vxlan_l2_elan_sh
PE1(config-vrf)#rd 1.1.1.1:101
PE1(config-vrf)#route-target both 101:101
```

Note: Ensure to provide `<RD value>` with a value different from PE1's RD of `1.1.1.1` to maintain proper routing table separation and avoiding conflicts between the two PE devices.

5. Define an IP VRF for routing L3 traffic within the EVPN framework:

```
PE1(config)#ip vrf vxlan_l3_elan_mhsh
PE1(config-vrf)#rd 1111:701
PE1(config-vrf)#route-target both 701:701
```

```
PE1(config-vrf)#l3vni 10050
PE1(config-vrf)#commit
```

Note: Ensure to provide `<rd value>` with a value different from PE1's RD of `1.1.1.1` to maintain proper routing table separation and avoiding conflicts between the two PE devices.

6. Configure EVPN VXLAN for host reachability and specify the IRB interface:

```
PE1(config)#nvo vxlan id 100 ingress-replication
PE1(config-nvo)# vxlan host-reachability-protocol evpn-bgp vxlan_l2_elan_mhsh
PE1(config-nvo)# evpn irb100
```

7. Configure a po interface for VLAN encapsulation and map it to the EVPN instance:

```
PE1(config)#interface xe7.100 switchport
PE1(config-if)# encapsulation dot1q 100
PE1(config-if)# rewrite pop
PE1(config-if)# access-if-evpn
PE1(config-acc-if-evpn)# map vpn-id 100
PE1(config-acc-if-evpn)#commit
```

8. Create ACL to filter outgoing traffic:

```
PE1(config)#
PE1(config)#ip access-list irb_100_nw
PE1(config-ip-acl)# 50 permit any 100.1.1.0/24 any
PE1(config-ip-acl)# 51 permit any 101.1.1.0/24 any
PE1(config-ip-acl)# default deny-all
PE1(config-ip-acl)# exit
PE1(config-ip-acl)#ipv6 access-list irb_100_v6
PE1(config-ipv6-acl)# 150 permit any 1001::/48 any
PE1(config-ipv6-acl)# default permit-all
PE1(config-ipv6-acl)#commit
```

9. Configure the IRB interface with IP addresses, associate it with the VRF, and apply the ACL:

```
PE1(config)#interface irb100
PE1(config-irb-if)# ip vrf forwarding vxlan_l3_elan_mhsh
PE1(config-irb-if)# evpn irb-if-forwarding anycast-gateway-mac
PE1(config-irb-if)# ip address 100.1.1.1/24 anycast
PE1(config-irb-if)# ip address 101.1.1.1/24 secondary anycast
PE1(config-irb-if)# ipv6 address 1001::1/48 anycast
PE1(config-irb-if)# ipv6 address 1002::1/48 anycast
PE1(config-irb-if)# ip access-group irb_100_nw in
PE1(config-irb-if)# ipv6 access-group irb_100_v6 in
PE1(config-irb-if)#commit
```

Configuration Snapshot

PE1

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
logging console 5
logging monitor 5
logging level nsm 5
```

```
logging level ospf 5
logging level hsl 5
logging level rib 5
logging level bgp 5
logging level pserv 5
logging level cmm 5
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
snmp-server enable traps ospf
snmp-server enable traps bgp
!
load-balance enable
load-balance ipv4 protocol-id src-dest-ipv4
load-balance ipv6 src-dest-ipv6
load-balance src-dest-l4port
hardware-profile filter ingress-ipv4-subif enable
hardware-profile filter ingress-ipv6-ext-subif enable
hardware-profile filter egress-ipv4-ext enable
hardware-profile filter egress-ipv6 enable
hardware-profile filter vxlan enable
hardware-profile filter vxlan-mh enable
hardware-profile statistics voq-full-color enable
hardware-profile statistics cfm-ccm enable
!
bfd interval 3 minrx 3 multiplier 3
!
qos enable
qos statistics
qos profile dscp-to-queue default
 dscp 20 queue 4
!
hostname PE1
no ip domain-lookup
ip domain-lookup vrf management
ip name-server vrf management 10.12.3.24
bridge 1 protocol rstp vlan-bridge
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
username test role network-admin password encrypted
$1$bJoW4RH.$TPy.xPqFP4mOPALbPOX/b1
!
ip access-list irb_100_nw
```

```
 50 permit any 100.1.1.0/24 any
 51 permit any 101.1.1.0/24 any
 default deny-all
!
ipv6 access-list irb_100_v6
 150 permit any 1001::/48 any
 default permit-all
!
vlan database
 vlan 100 bridge 1
!
nvo vxlan enable
!
nvo vxlan irb
!
ip vrf management
!
mac vrf vxlan_l2_elan_mhsh
 rd 1.1.1.1:101
 route-target both 101:101
!
ip vrf vxlan_l3_elan_mhsh
 rd 1111:701
 route-target both 701:701
 l3vni 10050
!
evpn irb-forwarding anycast-gateway-mac 0000.0000.1111
!
nvo vxlan vtep-ip-global 1.1.1.1
!
nvo vxlan id 100 ingress-replication
 vxlan host-reachability-protocol evpn-bgp vxlan_l2_elan_mhsh
 evpn irb100
!
interface ce6
 description network_to_spine1
 load-interval 30
 ip address 11.1.1.1/24
 ip ospf cost 1
 ip router isis 1
!

interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface irb100
 ip vrf forwarding vxlan_l3_elan_mhsh
 evpn irb-if-forwarding anycast-gateway-mac
 ip address 100.1.1.1/24 anycast
```

```
 ip address 101.1.1.1/24 secondary anycast
 ipv6 address 1001::1/48 anycast
 ipv6 address 1002::1/48 anycast
 ip access-group irb_100_nw in
 ipv6 access-group irb_100_v6 in
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.1/32 secondary
 ipv6 address ::1/128
 ip router isis 1
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe7
 switchport
 load-interval 30
!
interface xe7.100 switchport
 encapsulation dot1q 100
 rewrite pop
 access-if-evpn
  map vpn-id 100
!

 exit
!
router ospf 1
 ospf router-id 1.1.1.1
 bfd all-interfaces
 network 1.1.1.1/32 area 0.0.0.0
 network 11.1.1.0/24 area 0.0.0.0
!
router bgp 1
 bgp router-id 1.1.1.1
 neighbor 3.3.3.3 remote-as 1
 neighbor 3.3.3.3 update-source lo
 !
 address-family ipv4 unicast
 max-paths ibgp 2
 exit-address-family
 !
 address-family l2vpn evpn
 neighbor 3.3.3.3 activate
 exit-address-family
 !
 address-family ipv4 vrf vxlan_l3_elan_mhsh
```

```
 max-paths ibgp 2
 redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf vxlan_l3_elan_mhsh
 max-paths ibgp 2
 redistribute connected
 exit-address-family
 !
 exit
!
line console 0
 exec-timeout 0 0
line vty 0 16
 exec-timeout 0 0
!
!
end
```

PE2

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
logging console 5
logging monitor 5
logging level nsm 5
logging level ospf 5
logging level hsl 5
logging level rib 5
logging level bgp 5
logging level pserv 5
logging level cmm 5
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
snmp-server enable traps ospf
snmp-server enable traps bgp
!
load-balance enable
load-balance ipv4 protocol-id src-dest-ipv4
load-balance ipv6 src-dest-ipv6
load-balance src-dest-l4port
hardware-profile filter ingress-ipv4-subif enable
hardware-profile filter ingress-ipv6-ext-subif enable
hardware-profile filter egress-ipv4-ext enable
hardware-profile filter egress-ipv6 enable
hardware-profile filter vxlan enable
hardware-profile statistics voq-full-color enable
```

```
hardware-profile statistics cfm-ccm enable
hardware-profile port-config mode3
!
bfd interval 3 minrx 3 multiplier 3
!
qos enable
qos statistics
qos profile dscp-to-queue default
 dscp 20 queue 4
!
hostname PE2
port ce2 breakout 4X10g
no ip domain-lookup
ip domain-lookup vrf management
ip name-server vrf management 10.12.3.24
ip name-server vrf management 10.12.3.23
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
username test role network-admin password encrypted
$1$bJoWADy.$LH9n3Skfe1mL7qQ6NTCrS/
lldp run
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
!
ip access-list irb_50_v4_ip
 150 permit any host 50.1.1.2 any
 151 permit any host 50.1.1.3 any
 152 permit any host 50.1.1.4 any
 default deny-all
!
ipv6 access-list irb_50_v6
 150 permit any 5000::/48 any
 default permit-all
!
nvo vxlan enable
!
nvo vxlan irb
!
ip vrf management
!
ip vrf vxlan_l3_elan_mhsh
 rd 6666:701
```

```
 route-target both 701:701
 l3vni 10050
!
mac vrf vxlan_l2_elan_mhsh2
 rd 6.6.6.6:50
 route-target both 50:50
!
evpn irb-forwarding anycast-gateway-mac 0000.0000.1111
!
nvo vxlan vtep-ip-global 3.3.3.3
!
nvo vxlan id 50 ingress-replication
 vxlan host-reachability-protocol evpn-bgp vxlan_l2_elan_mhsh2
 evpn irb50
!
interface ce15
 description network_to_spine1
 load-interval 30
 ip address 15.1.1.1/24
 ip ospf cost 1
 ip router isis 1
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface irb50
 ip vrf forwarding vxlan_l3_elan_mhsh
 evpn irb-if-forwarding anycast-gateway-mac
 ip address 50.1.1.1/24 anycast
 ip address 51.1.1.1/24 secondary anycast
 ipv6 address 5000::1/48 anycast
 ipv6 address 5001::1/48 anycast
 ip access-group irb_50_v4_ip in
 ipv6 access-group irb_50_v6 in
!
interface lo
 ip address 127.0.0.1/8
 ip address 3.3.3.3/32 secondary
 ipv6 address ::1/128
 ip router isis 1
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe0
 switchport
 load-interval 30
```

```
!
interface xe0.50 switchport
 encapsulation dot1q 50
 rewrite pop
 access-if-evpn
  map vpn-id 50
!
interface xe2
 switchport
!
interface xe3
!
 exit
!
router ospf 1
 ospf router-id 3.3.3.3
 bfd all-interfaces
 network 3.3.3.3/32 area 0.0.0.0
 network 15.1.1.0/24 area 0.0.0.0
!
router bgp 1
 bgp router-id 3.3.3.3
 neighbor 1.1.1.1 remote-as 1
 neighbor 1.1.1.1 update-source lo
 !
 address-family ipv4 unicast
 max-paths ibgp 2
 exit-address-family
 !
 address-family l2vpn evpn
 neighbor 1.1.1.1 activate
 exit-address-family
 !
 address-family ipv4 vrf vxlan_l3_elan_mhsh
 max-paths ibgp 2
 redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf vxlan_l3_elan_mhsh
 max-paths ibgp 2
 redistribute connected
 exit-address-family
 !
 exit
!
line console 0
 exec-timeout 0 0
line vty 0 16
 exec-timeout 0 0
!
```

```
!
end
```

P1

```
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
service password-encryption
!
logging console 5
logging monitor 5
logging level nsm 5
logging level ospf 5
logging level hsl 5
logging level rib 5
logging level bgp 5
logging level pserv 5
logging level cmm 5
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
qos enable
!
hostname P1
no ip domain-lookup
ip domain-lookup vrf management
ip name-server vrf management 10.12.3.24
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
lldp run
lldp tlv-select basic-mgmt port-description
lldp tlv-select basic-mgmt system-name
!
vlan database
 vlan-reservation 4063-4094
!
ip vrf management
!
interface ce6/1
```

```
 description network_to_vtep1
 load-interval 30
 ip address 11.1.1.2/24
 ip ospf cost 10
 ip router isis 1
!
interface ce14/4
!
interface ce15/1
 description network_to_vtep3
 load-interval 30
 ip address 15.1.1.2/24
 ip ospf cost 10
 ip router isis 1
!
interface ce32/4
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
 exit
!
router ospf 1
 ospf router-id 4.4.4.4
 bfd all-interfaces
 network 4.4.4.4/32 area 0.0.0.0
 network 11.1.1.0/24 area 0.0.0.0
 network 15.1.1.0/24 area 0.0.0.0
!
line console 0
 exec-timeout 0 0
line vty 0 16
 exec-timeout 0 0
!
!
end
```

Validation

Verify that after applying ACL traffic is not egressing out:

```
PE1#show interface counters rate mbps
+-------------------+-------------+-------------+-------------+-------------+
|     Interface     |    Rx mbps  |    Rx pps   |    Tx mbps  |    Tx pps   |
+-------------------+-------------+-------------+-------------+-------------+
 ce6                  312.62         224584        312.62         224583
 xe7                  229.97         224579        229.97         224579
 xe7.100              198.36         225410        230.79         225377
PE1#
PE1#show access-lists
IP access list irb_100_nw
        50 permit any 100.1.1.0/24 any [match=541906539]
        51 permit any 101.1.1.0/24 any
        default deny-all
IPv6 access list irb_100_v6
        150 permit any 1001::/48 any [match=180636075]
        268435453 permit icmpv6 any any [match=12]
        default permit-all
```

Verify that the ACL rule is matching and counters are incremented accordingly:

```
PE1#show ip access-lists
IP access list irb_100_nw
        50 permit any 100.1.1.0/24 any [match=563524977]
        51 permit any 101.1.1.0/24 any
        default deny-all
PE1#show ipv6 access-lists
IPv6 access list irb_100_v6
        150 permit any 1001::/48 any [match=188010307]
        268435453 permit icmpv6 any any [match=12]
        default permit-all
```

CHAPTER 2 Dynamic ARP Inspection

Overview

DAI (Dynamic ARP Inspection) is a security features that validates ARP packet in network by intercepting ARP packet and validating IP-to-MAC address binding learnt from DHCP SNOOP.

DAI (Dynamic ARP Inspection) is a security measures which allows user to intercept, log and discard ARP packets with invalid MAC address to IP address binding. Once the DAI feature is enabled on the system, ARP packets are re-directed to software and validated against the MAC to IP binding data base before getting forwarded. ARP coming on untrusted port is inspected, validated and forwarded/dropped appropriately.

Topology

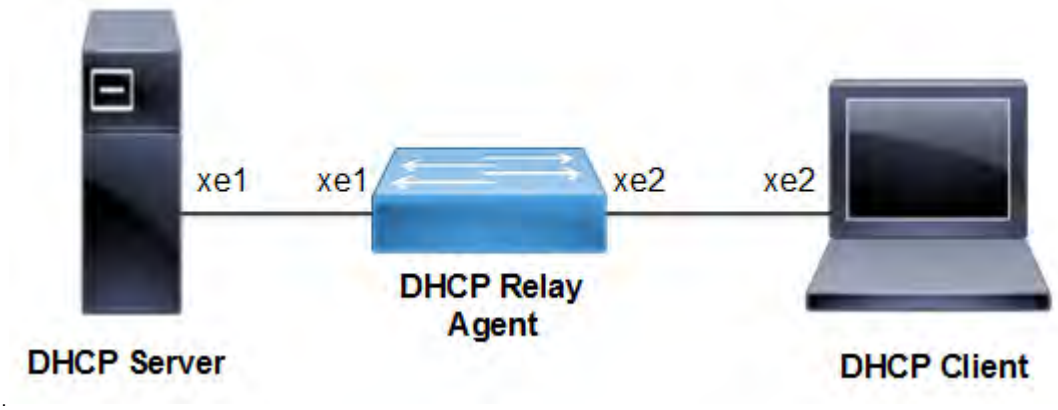


Figure 2-10: DAI Topology

Enable/Disable the Ingress DHCP-snoop TCAM group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop enable`	Enable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config
`(config)#hardware-profile filter dhcp-snoop disable`	Disable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config

Enable/Disable the Ingress DHCP-snoop-IPv6 TCAM group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop-ipv6 enable`	Enable the ingress DHCP-snoop-IPv6 TCAM group
`(config)#commit`	Commit Candidate config to running-config

(config)#hardware-profile filter dhcp-snoop-ipv6 disable	Disable the ingress DHCP-snoop-IPv6 TCAM group
(config)#commit	Commit Candidate config to running-config

Enable DHCP Snooping and DAI Globally

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol mstp	Create MSTP or IEEE VLAN-bridge.
(config)#ip dhcp snooping bridge 1	Enable DHCP Snooping on the bridge
(config)#ip dhcp snooping arp-inspection bridge 1	Enable DAI on bridge
(config)#commit	Commit Candidate config to running-config

Enable DHCP Snooping and DAI on a VLAN

#configure terminal	Enter Configure mode.
(config)#vlan 2 bridge 1	Configure a VLAN for the bridge.
(config)#ip dhcp snooping vlan 2 bridge 1	Enable DHCP Snooping on the VLAN 2
(config)#ip dhcp snooping arp-inspection vlan 2 bridge 1	Enable DAI on VLAN
(config)#commit	Commit Candidate config to running-config

Validation

```
OcNOS#show hardware-profile filters

Note: Shared count is the calculated number from available resources.
      Dedicated count provides allocated resource to the group.
      If group shares the dedicated resource with other groups, then dedicated
      count of group will reduce with every resource usage by other groups.

+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| Unit - TCAMS       | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
0 DHCP-SNOOP           5522      2     104       5626    1018        4608
0 DHCP-SNOOP-IPV6      5522      0     6         5528    920         4608
0 IPSG                 3327      0     1         3328    1024        2304
0 IPSG-IPV6            3327      0     1         3328    1024        2304
```

Enable/Disable IP DHCP Snooping ARP-inspection Validate

Use this command to enable validation of the source-MAC, destination-MAC, or IP address field in the ARP packet payload.

Note: The IP address in a payload is validated for not being a broadcast address, a reserved zero IP address, and multicast address.

`#configure terminal`	Enter Configure mode.
`(config)#ip dhcp snooping arp-inspection validate src-mac bridge 1`	Enable SRC-MAC validate
`(config)#commit`	Commit Candidate config to running-config
`(config)#no ip dhcp snooping arp-inspection validate src-mac bridge 1`	Disable SRC-MAC validate
`(config)#commit`	Commit Candidate config to running-config
`(config)#ip dhcp snooping arp-inspection validate dst-mac bridge 1`	Enable DST-MAC validate
`(config)#commit`	Commit Candidate config to running-config
`(config)#no ip dhcp snooping arp-inspection validate dst-mac bridge 1`	Disable DST-MAC validate
`(config)#commit`	Commit Candidate config to running-config
`(config)#ip dhcp snooping arp-inspection validate ip bridge 1`	Enable IP validate
`(config)#commit`	Commit Candidate config to running-config
`(config)#no ip dhcp snooping arp-inspection validate ip bridge 1`	Disable IP validate
`(config)#commit`	Commit Candidate config to running-config

Configuring the Ports Connected to DHCP Server and DHCP Client

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface xe1 to be configured, and Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface xe1 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface VLAN 2 to the port
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Specify interface xe2 to be configured connected to server.
`(config-if)#switchport`	Configure the interface as a switch port
`(config-if)#bridge-group 1`	Associate interface xe2 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#switchport access vlan 2`	Bind the interface VLAN 2 to the port
`(config-if)#exit`	Exit the config mode.
`(config)#commit`	Commit Candidate config to running-config
`(config)#exit`	Exit the config mode.

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as un-trusted port.

In this example, xe2 is connected to the DHCP client and xe1 is connected to the DHCP server.

- Configure xe2 connected to DHCP client as un-trusted port.
- Configure xe1 connected to the DHCP server as trusted port.

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config)#commit`	Commit Candidate config to running-config
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit Candidate config to running-config

Validation

```
OcNOS#show ip dhcp snooping arp-inspection statistics bridge 1
bridge     forwarded  dai dropped
------     ---------  -----------
1          0          10
```

CHAPTER 3 Proxy ARP and Local Proxy ARP

Overview

Proxy ARP (RFC 1027) is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address as destination. The captured traffic is then typically routed by the Proxy to the intended destination via another interface.

Use `no ip proxy-arp` to disable Proxy ARP, Proxy ARP is disabled by default.

Topology

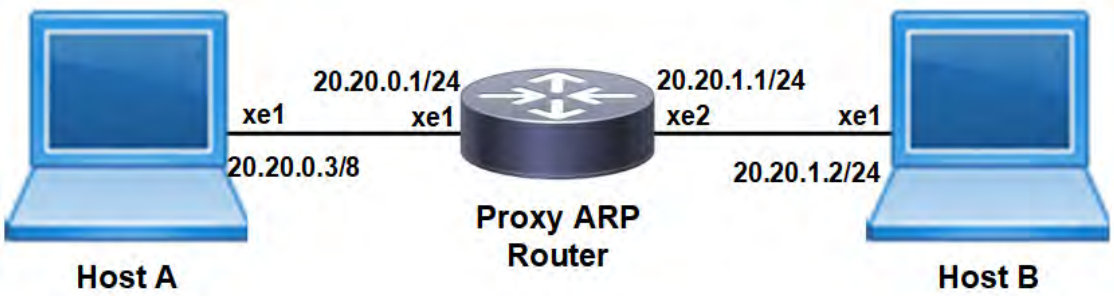


Figure 3-11: Sample topology

Host A

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured on Host A
`(config-if)#ip address 20.20.0.3/8`	Configure the IP address on the interface
`(config)# ip route 0.0.0.0/0 20.20.0.1`	Configure the default gateway
`(config)#commit`	Commit the candidate configuration to the running
`(config)#end`	Exit interface and configure mode

Host B

`#configure terminal`	Enter Configure mode
`(config)#interface xe1`	Specify the interface to be configured on Host B
`(config-if)#ip address 20.20.1.2/24`	Configure the ip address on the interface
`(config)# ip route 0.0.0.0/0 20.20.1.1`	Configure the default gateway
`(config)#commit`	Commit the candidate configuration to the running
`(config)#end`	Exit interface and configure mode

Enable Proxy ARP

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface connected to Host A
`(config-if)#ip address 20.20.0.1/24`	Configure the ip address on the interface
`(config-if)#interface xe2`	Specify the interface connected to Host B
`(config-if)#ip address 20.20.1.1/24`	Configure the ip address on the interface
`(config-if)#interface xe1`	Specify the interface to configure Proxy ARP
`(config-if)#ip proxy-arp`	Enable Proxy ARP
`(config)#commit`	Commit the candidate configuration to the running
`(config)#end`	Exit interface and configure mode

Validation

```
Router#show running-config arp
!
interface xe1
ip proxy-arp
!
```

The `show arp` command on the hosts shows the ARP table entries to reach different subnets. Host B is reachable from host A and the necessary configurations should be present. Ping Host A from Host B. The ARP table should have the router's xe1 interface MAC address to reach Host A. Execute the below command at Host B:

```
HostB#show arp

Flags: D - Static Adjacencies attached to down interface
IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State
20.20.0.3      00:02:39      ecf4.bbc0.3d71      xe1       STALE.
```

Local Proxy ARP Overview

Local Proxy ARP feature is used to enable local proxy support for ARP requests per interface level. Activation will make the router answer all ARP requests on configured subnet, even for clients that should not normally need routing. Local proxy ARP means that the traffic comes in and goes out the same interface.

The local proxy ARP feature allows responding to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

Topology

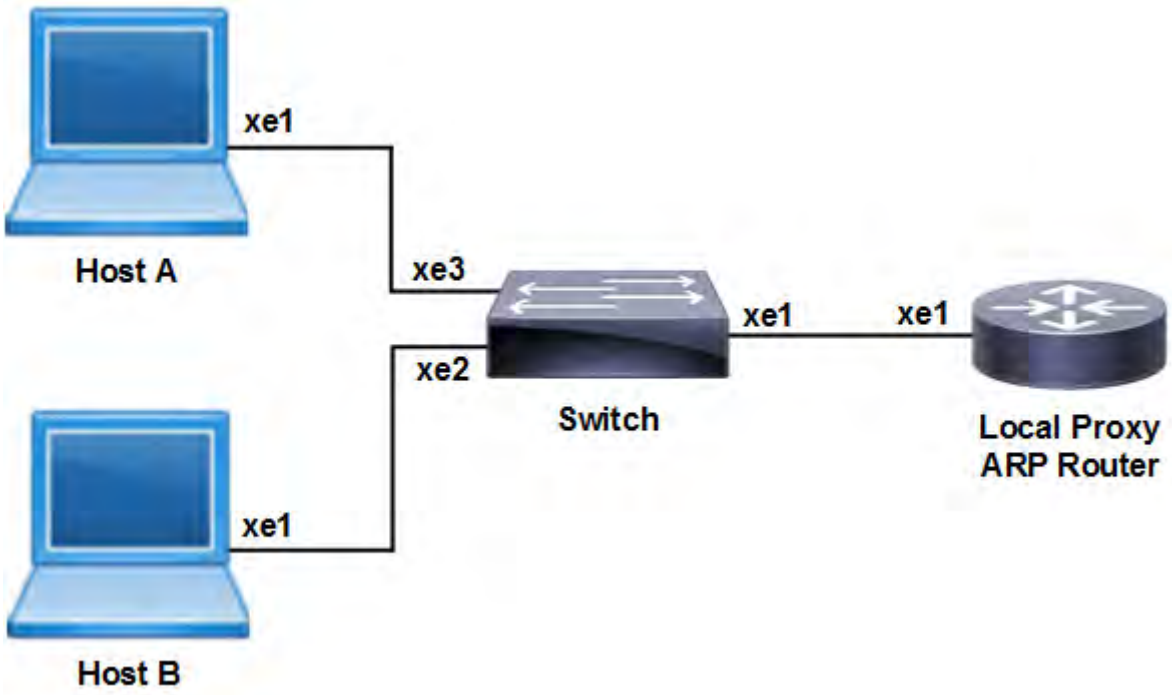


Figure 3-12: Sample topology

Host A

#configure terminal	Enter Configure mode.
(config)#interface xe1	Specify the interface to be configured on Host A
(config-if)#ip address 20.20.0.2/24	Configure the ip address on the interface
(config)#commit	Commit the candidate configuration to the running
(config)#end	Exit interface and configure mode

Host B

#configure terminal	Enter Configure mode
(config)#interface xe1	Specify the interface to be configured on Host B
(config-if)#ip address 20.20.0.3/24	Configure the ip address on the interface
(config)#commit	Commit the candidate configuration to the running
(config)#end	Exit interface and configure mode

Private Vlan Configuration on Switch

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create ieee vlan-bridge on switch for pvlan configuration
(config)#vlan database	Enter into the vlan database
(config-vlan)#vlan 100-101 bridge 1 state enable	Create vlans 100 and 101 as part of bridge 1
(config-vlan)#private-vlan 100 primary bridge 1	Configure vlan 100 as a primary vlan
(config-vlan)#private-vlan 101 isolated bridge 1	Configure vlan 101 as a isolated vlan
(config-vlan)#private-vlan 100 association add 101 bridge 1	Associate secondary vlan 101 to primary vlan 100
(config-vlan)#exit	Exit from the vlan database
(config)#commit	Commit the candidate configuration to the running
(config)#interface xe1	Specify the interface to be configured
(config-if)#switchport	Configure xe1 as a layer2 interface.
(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary vlan to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe1 interface as a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running
(config)#interface xe2	Specify the interface to be configured
(config-if)#switchport	Configure xe2 as a layer2 interface.
(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)#bridge-group 1	Associate the interface to the bridge

(config-if)#switchport access vlan 100	Associate primary vlan to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe2 interface as a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running
(config)#interface xe3	Specify the interface to be configured
(config-if)#switchport	Configure xe3 as a layer2 interface.
(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary VLAN to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe2 interface as a promiscuous port
(config-if)#switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)#exit	Exit interface mode
(config)#commit	Commit the candidate configuration to the running

Enable Local Proxy ARP on Router

#configure terminal	Enter Configure mode
(config)#interface xe1	Specify the interface to be configured on router
(config-if)#ip address 20.20.0.1/24	Configure the ip address on the interface
(config-if)#ip local-proxy-arp	Enable Local Proxy ARP
(config)#commit	Commit the candidate configuration to the running
(config)#end	Exit interface and configure mode

Validation

ARP cache on Host A and Host B

The show arp command on hosts shows the arp table entries to reach different subnets. Ping from Host A to random destination ip with same network (20.20.0.7) and then Ping Host B from Host A.Host A ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
Host-A#ping 20.20.0.7
Press CTRL+C to exit
PING 20.20.0.7 (20.20.0.7) 100(128) bytes of data.
From 20.20.0.3 icmp_seq=1 Destination Host Unreachable


Host-A#ping 20.20.0.3
Press CTRL+C to exit
PING 20.20.0.3 (20.20.0.3) 100(128) bytes of data.
108 bytes from 20.20.0.3: icmp_seq=1 ttl=64 time=0.509 ms
108 bytes from 20.20.0.3: icmp_seq=2 ttl=64 time=0.447 ms
```

```
Host-A#sh arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age      MAC Address     Interface  State
20.20.0.3        00:00:05 f88e.a1d6.6619  xe1        REACHABLE
20.20.0.7        00:10:12 f88e.a1d6.6619  xe1        STALE
```

CHAPTER 4 DHCP Snooping

Overview

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. It is a security feature that acts like a fire wall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in 'man-in the middle' or 'Denial of Service' attacks from malicious purpose. Similarly DHCP clients (rogue) can also cause 'Denial of Service' attacks by continuously requesting for IP addresses causing address depletion in the DHCP server.

The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from un-trusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and un-trusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about un-trusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from un-trusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Topology

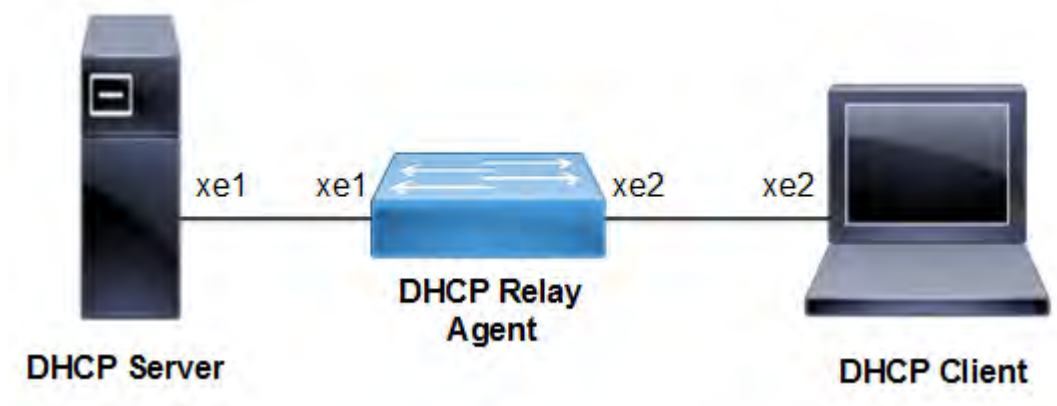


Figure 4-13: DHCP Snooping topology

Configuration Guidelines

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP snooping globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the device acting as the DHCP server is configured and enabled.

- If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as un-trusted by entering the `no ip dhcp snooping trust` interface configuration command.

Procedures

The following subsections provide examples of how to enable and configure DHCP Snooping.

Enable the Ingress DHCP-snoop TCAM group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop enable`	Enable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config

Disable the Ingress DHCP-snoop TCAM group

`#configure terminal`	Enter Configure mode.
`(config)# hardware-profile filter dhcp-snoop disable`	Disable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config

Enable the Ingress DHCP-snoop-IPv6 TCAM group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop-ipv6 enable`	Enable the ingress DHCP-snoop-IPv6 TCAM group
`(config)#commit`	Commit Candidate config to running-config

Disable the Ingress DHCP-snoop-IPv6 TCAM group

`#configure terminal`	Enter Configure mode.
`(config)# hardware-profile filter dhcp-snoop-ipv6 disable`	Disable the ingress DHCP-snoop-IPv6 TCAM group
`(config)#commit`	Commit Candidate config to running-config

Enable DHCP Snooping Globally

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Create MSTP or IEEE VLAN-bridge.
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge
`(config)#commit`	Commit Candidate config to running-config

Enable DHCP Snooping on a VLAN

`#configure terminal`	Enter Configure mode.
`(config)#vlan 2 bridge 1`	Configure a VLAN for the bridge.
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the VLAN 2
`(config)#commit`	Commit Candidate config to running-config

Validation

```
OcNOS#show hardware-profile filters

Note: Shared count is the calculated number from available resources.
      Dedicated count provides allocated resource to the group.
      If group shares the dedicated resource with other groups, then dedicated
      count of group will reduce with every resource usage by other groups.

+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| Unit - TCAMS       | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
0 DHCP-SNOOP           9717      0     5         9722    1018        8704
0 DHCP-SNOOP-IPV6      9717      0     6         9723    1019        8704
```

Configuring the Ports Connected to DHCP Server and DHCP Client

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface xe1 to be configured, and Enter interface mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface xe1 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface VLAN 2 to the port
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Specify interface xe2 to be configured connected to server.
`(config-if)#switchport`	Configure the interface as a switch port
`(config-if)#bridge-group 1`	Associate interface xe2 with bridge-group 1.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#switchport access vlan 2`	Bind the interface VLAN 2 to the port
`(config-if)#exit`	Exit the config mode.
`(config)#commit`	Commit Candidate config to running-config
`(config)#exit`	Exit the config mode.

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as un-trusted port.

In this example, xe2 is connected to the DHCP client and xe1 is connected to the DHCP server.

- Configure xe2 connected to DHCP client as un-trusted port.
- Configure xe1 connected to the DHCP server as trusted port.

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config)#commit`	Commit Candidate config to running-config
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit Candidate config to running-config

DHCP Snooping Operation

1. Configure DHCP server that is connected to DHCP Snooper through trusted port.
2. Request an IP address from the DHCP client connected through the un-trusted port.
3. DHCP client broadcast the DHCP DISCOVER message to the switch.
4. DHCP server responds to the DHCP DISCOVER message with DHCP offer message to the client.
5. Once the DHCP OFFER is received by the client, it sends an DHCP REQUEST to the server.
6. DHCP server validates the request from the client and sends DHCP ACK with the offered IP address to the client with the lease time.
7. DHCP Snooper creates an entry for the above operation into the binding table which includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.
8. DHCP Snooper clears the entry in the binding table once the client sends the DHCP RELEASE query.

Validation

The `show running-config ip dhcp snooping` command displays the DHCP snooping commands configured on the device in question

```
#show running-config ip dhcp snooping
!
!
ip dhcp snooping bridge 1
ip dhcp snooping vlan 2 bridge 1
interface xe1
 ip dhcp snooping trust
!
```

The `show ip dhcp snooping bridge 1` command displays the configured information about DHCP Snooping.

```
#show ip dhcp snooping bridge 1
```

```
Bridge Group : 1
DHCP snooping is : Enabled
DHCP snooping option82 is : Disabled
Verification of hwaddr field is : Disabled
Rate limit(pps) : 100
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2


DHCP snooping IP Source Guard is configured on the following Interface


Interface       Trusted
--------------- -------
xe2             Yes
```

The `show ip dhcp snooping binding bridge 1` command displays the binding table entries associated with un-trusted interfaces.

```
#show ip dhcp snooping bridge 1

Bridge Group : 1
DHCP snooping is : Enabled
DHCP snooping option82 is : Disabled
Verification of hwaddr field is : Disabled
Rate limit(pps) : 100
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface  Trusted
--------   -------
 Xe1       Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface       Source Guard
-------         ------------
```

CHAPTER 5 DHCP Snooping IP Source Guard

Overview

IPSG is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database. Use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor. Enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP DHCP snooping binding table and denies all other traffic.

Topology

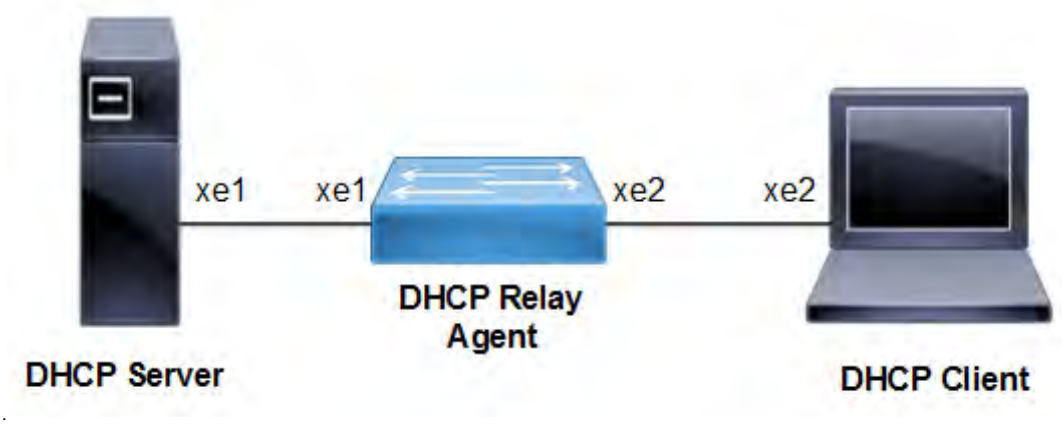


Figure 5-14: IP Source Guard Topology

Enable/Disable the Ingress DHCP-snoop TCAM Group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop enable`	Enable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config
`(config)#hardware-profile filter dhcp-snoop disable`	Disable the ingress DHCP-snoop TCAM group
`(config)#commit`	Commit Candidate config to running-config

Enable/Disable the Ingress DHCP-snoop-IPv6 TCAM Group

`#configure terminal`	Enter Configure mode.
`(config)#hardware-profile filter dhcp-snoop-ipv6 disable`	Disable the ingress DHCP-snoop-IPv6 TCAM group
`(config)#commit`	Commit Candidate config to running-config

© 2025 IP Infusion Inc. Proprietary

(config)#hardware-profile filter dhcp-snoop-ipv6 disable	Disable the ingress DHCP-snoop-IPv6 TCAM group
(config)#commit	Commit Candidate config to running-config

Enable/Disable the Ingress IPSG TCAM group

#configure terminal	Enter Configure mode.
(config)#hardware-profile filter ipsg enable	Enable the ingress IPSG TCAM group
(config)#commit	Commit Candidate config to running-config
(config)#hardware-profile filter ipsg disable	Disable the ingress IPSG TCAM group
(config)#commit	Commit Candidate config to running-config

Enable/Disable the Ingress IPSG-IPV6 TCAM group

#configure terminal	Enter Configure mode.
(config)#hardware-profile filter ipsg-ipv6 enable	Enable the ingress IPSG-IPv6 TCAM group
(config)#commit	Commit Candidate config to running-config
(config)#hardware-profile filter ipsg-ipv6 disable	Disable the ingress IPSG-IPv6 TCAM group
(config)#commit	Commit Candidate config to running-config

Validation

```
OcNOS#show hardware-profile filters

Note: Shared count is the calculated number from available resources.
      Dedicated count provides allocated resource to the group.
      If group shares the dedicated resource with other groups, then dedicated
      count of group will reduce with every resource usage by other groups.

+---------------------+---------+---------------+-----------------------------+
|                     | Free    |     Used      |       Total Entries         |
| Unit - TCAMS        | Entries |---------------|-----------------------------|
|                     |         |  %  | Entries | Total | Dedicated | shared  |
+---------------------+---------+-----+---------+-------+-----------+---------+
0 DHCP-SNOOP            5620      0     6         5626    1018        4608
0 DHCP-SNOOP-IPV6       5620      0     6         5626    1018        4608
0 IPSG                  3327      0     1         3328    1024        2304
0 IPSG-IPV6             3327      0     1         3328    1024        2304
```

Configuring the Ports Connected to DHCP Server and DHCP Client

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create IEEE VLAN bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2

(config)#ip dhcp snooping bridge 1	Configure DHCP snooping for bridge 1
(config)#ip dhcp snooping information option bridge 1	Configure DHCP snooping information option 82
(config)#ip dhcp snooping vlan 2 bridge 1	Configure DHCP snooping for VLAN 2 for bridge 1
(config)#ip dhcp snooping verify mac-address bridge 1	Configure DHCP snooping verify MAC-address
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe2	Configure IPv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and VLAN configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe2	Configure IPv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and VLAN configured
(config)#commit	Commit Candidate config to running-config
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge:

```
#sh ip dhcp snooping bridge 1
Bridge Group : 1
DHCP snooping is : Enabled
DHCP snooping option82 is : Enabled
Verification of hwaddr field is : Enabled
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface       Trusted
--------------- -------
xe1             Yes
```

```
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface       Source Guard
--------------- ------------
xe2             Yes
```

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as un-trusted port.

In this example, xe2 is connected to the DHCP client and xe1 is connected to the DHCP server.

- Configure xe2 connected to DHCP client as un-trusted port.
- Configure xe1 connected to the DHCP server as trusted port.

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured
`(config-if)#ip dhcp snooping trust`	Enable the port as trusted.
`(config)#commit`	Commit Candidate config to running-config
`(config)#interface xe2`	Specify the interface to be configured
`(config-if)#no ip dhcp snooping trust`	Disable the port as trusted.
`(config-if)#exit`	Exit interface mode
`(config)#commit`	Commit Candidate config to running-config

Validation

Verify that static DHCP snooping entries are configured for the bridge:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries : 1
Total number of dynamic IPV4 entries : 0
Total number of static IPV6 entries : 1
Total number of dynamic IPV6 entries : 0

MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- ---------------
0011.1111.2222     1.1.1.1         0          static        2    xe2
0022.2222.3333     3ffe::1         0          static        2    xe2
```

Configuring IP Source Guard on LAG Port

In this example, the LAG port (sa2) is created, then physical interfaces are added.

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2
`(config)#ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)#ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)#ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for VLAN 2 for bridge 1
`(config)#ip dhcp snooping verify mac-address bridge 1`	Configure DHCP snooping verify MAC-address

(config)#interface sa2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#ip verify source dhcp-snooping-vlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#static-channel-group 2	Configure Static Channel LAG on the interface
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe1	Configure IPv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and VLAN configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe2	Configure IPv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and VLAN configured
(config)#commit	Commit Candidate config to running-config
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Validation

Verify that DHCP snooping is enabled on the bridge with the static LAG interface:

```
#sh ip dhcp snooping bridge 1
Bridge Group : 1
DHCP snooping is : Enabled
DHCP snooping option82 is : Enabled
Verification of hwaddr field is : Enabled
DHCP snooping is configured on following VLANs : 2
DHCP snooping is operational on following VLANs : 2
DHCP snooping trust is configured on the following Interfaces
Interface       Trusted
--------------- -------
Xe1             Yes
```

```
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface       Source Guard
--------------- ------------
sa2             Yes
```

Verify that static DHCP snooping or source guard entries are configured for the bridge with the LAG interface:

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries : 1
Total number of dynamic IPV4 entries : 0
Total number of static IPV6 entries : 1
Total number of dynamic IPV6 entries : 0
MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- -------------
-
----
0011.1111.2222     1.1.1.1         0          static        2    sa2
0022.2222.3333     3ffe::1         0          static        2    sa2
```

CHAPTER 6 No IP Unreachable

Overview

The "no ip unreachable" feature in networking devices is a configuration used to enhance network security and efficiency by disabling the generation of Internet Control Message Protocol (ICMP) unreachable messages. Normally, these messages are sent by routers and other network devices in response to packets that cannot be delivered to their intended destination for various reasons.

When the "no ip unreachable" command is enabled, the network device stops sending these ICMP unreachable messages.

The supported ICMP Unreachable Codes

Table 1 shows the codes used in ICMPv6 Unreachable.

Table P-1: ICMP Unreachable Codes

Code	Message	Description
0	Destination network unreachable	
1	Destination host unreachable	
2	Destination protocol unreachable	
3	Destination port unreachable	The destination network is not reachable from the current router.
4	Fragmentation needed and DF flag set	The specific destination host within a reachable network is not accessible.
5	Source Route Failed	The protocol specified in the packet is not supported by the destination.
6	Destination Network Unknown	The destination port is not open or not listening on the destination device.
7	Destination Host Unknown	NA
8	Source Host Isolated	NA
9	Network Administratively Prohibited	NA
10	Network Administratively Prohibited	NA
11	Network Unreachable for TOS	NA
12	Host Unreachable for TOS	NA
13	Communication Administratively Prohibited	NA
14	Host Precedence Violation	NA

Table P-1: ICMP Unreachable Codes

Code	Message	Description
15	Precedence Cutoff in Effect	NA

The supported ICMPv6 Unreachable Codes

Table 2 shows the codes used in ICMPv6 Unreachable.

Table P-2: ICMPv6 Unreachable Codes

Codes	Description
0	No route to destination
1	Communication with destination administratively prohibited
2	Beyond scope of source address
3	Address unreachable
4	Port unreachable
5	Source address failed ingress/egress policy
6	Reject route to destination

Feature Characteristics

The "no ip unreachable" feature is used to prevent a device from sending ICMP unreachable messages. These messages are typically generated when a router cannot forward a packet because the destination is unreachable. Disabling these messages can enhance network performance and security.

Benefits

The advantages of utilizing a No IP Unreachables:

- Enhanced Security
- Performance Optimization
- Simplified Troubleshooting.

Configuration

To configure "no ip unreachable," enter interface configuration mode on the device, select the outgoing interface, and apply the "no ip unreachable" command. This prevents the device from sending ICMP unreachable messages for packets sent through that interface, thereby enhancing network security.

Example for Suppressing the ICMP Destination Host Unreachable Message

With the configuration shown in the diagram, R2 is set to drop ICMP unreachable messages for packets exiting from interface ge10. The following steps describe how it operates. The procedures in this section use the topology in Figure 6-15

Figure 6-15: No IP Unreachable

1. **Packet Reception**: R2 receives a packet that it needs to forward to a destination.
2. **Routing Decision**: R2 checks its routing table to determine the next hop for the packet.
3. **Unreachable Destination**: If there is no valid route to reach the destination 20.1.1.3, R2 would normally generate an ICMP unreachable message, indicating Destination Host Unreachable.
4. **Suppression of ICMP Message**: With the "no ip unreachable" command enabled on R2's interface ge10, R2 suppresses outgoing ICMP messages from interface ge10, effectively dropping the packet without notifying the sender. In this case, R2 drops the Destination Host Unreachable message.

Example for Suppressing the ICMP Destination Network Unreachable Message

With the configuration shown in the diagram, R2 is set to drop ICMP unreachable messages for packets going out from interface ge10. The following steps describe how it operates. The procedures in this section use the topology in Figure 6-15

1. **Packet Reception**: R2 receives a packet that it needs to forward to a destination.
2. **Routing Decision**: R2 checks its routing table to determine the next hop for the packet.
3. **Unreachable Destination**: If there is no valid route to reach the destination network 30.1.1.1, R2 would normally generate an ICMP unreachable message, indicating Destination Network Unreachable.
4. **Suppression of ICMP Message**: With the "no ip unreachable" command enabled on R2's interface ge10, R2 suppresses outgoing ICMP messages from interface ge10, effectively dropping the packet without notifying the sender. In this case, R2 drops the "Destination Network Unreachable" message.

Example for Suppressing the ICMP Fragmentation Needed Message

With the configuration shown in the diagram, R2 is set to drop ICMP unreachable messages for packets going out from interface ge10. The following steps describe how it operates. The procedures in this section use the topology in Figure 6-15

1. **Packet Reception**: R2 receives a packet that it needs to forward to a destination.
2. **Routing Decision**: R2 checks the data size of the packet to transmit to the next hop. In this case, the data size is 1328 bytes.
3. **Unreachable Destination**: Since the maximum transmission unit (MTU) on R2 is set to 1200 bytes, R2 would normally generate an ICMP unreachable message, indicating "Fragmentation needed but DF is set."

4. **Suppression of ICMP Message**: With the "no ip unreachable" command enabled on R2's interface ge10, R2 suppresses outgoing ICMP messages from interface ge10, effectively dropping the packet without notifying the sender. In this case, R2 drops the "Fragmentation needed" message.

Topology

The procedures in this section use the topology in Figure 6-16

Figure 6-16: No IPv6 Unreachable

Configurations

This configuration suppresses ICMP messages from being sent out of the interface. Perform the following steps to configure no ip unreachable functionality for R2.

No IP Unreachable Configuration

- Supports all type of nodes.

Configuring No IP/IPv6 Unreachable

1. Enter the interface configuration mode.
   ```
   R2(config)#interface ge10
   ```
   - Assign an IPv6 address to the interface using the ipv6 address command followed by the desired IPv6 address and subnet mask.
     (ipv6 address 1000::1/64)
2. Disable the No IP/IPv6 Unreachable.
   ```
   R2(config-if)#no ip unreachable
   R2(config-if)#no ipv6 unreachable
   ```
3. To commit the changes exit.
   ```
   R2(config)#commit
   R2(config)#exit
   ```

Snippet configuration on R1 router is as follows:

```
!
interface ge10
 ip address 10.1.1.1/24
!
```

Snippet configuration on R2 router is as follows:

```
!
interface ge10
```

```
 ip address 10.1.1.2/24
 no ip unreachable
!
```

Validation

To verify that the no ip unreachables command has been applied to the interface, you can use the following command:.

R1:

```
OcNOS#ping 20.1.1.3
Press CTRL+C to exit
PING 20.1.1.3 (20.1.1.3) 100(128) bytes of data.
From 10.1.1.2 icmp_seq=1 Destination Host Unreachable
From 10.1.1.2 icmp_seq=2 Destination Host Unreachable
From 10.1.1.2 icmp_seq=3 Destination Host Unreachable
From 10.1.1.2 icmp_seq=4 Destination Host Unreachable
From 10.1.1.2 icmp_seq=5 Destination Host Unreachable
From 10.1.1.2 icmp_seq=6 Destination Host Unreachable

--- 20.1.1.3 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 142ms
pipe 3
OcNOS#
```

No IP Unreachable Unconfiguration

To revert the suppression of ICMP messages to the original configuration, follow the steps.

1. Enter the global configuration mode.

   ```
   R2#configure terminal
   ```

2. Configure the interface ge10.

   ```
   R2(config)#interface ge10
   ```

3. Re-enable ICMP unreachable messages.

   ```
   R2(config-if)#ip unreachable
   ```

4. To commit the changes exit.

   ```
   R2(config)#commit
   ```

   ```
   R2(config)#exit
   ```

Validation

R1:

```
OcNOS#ping 20.1.1.3
Press CTRL+C to exit
PING 20.1.1.3 (20.1.1.3) 100(128) bytes of data.

--- 20.1.1.3 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 167ms
```

```
OcNOS#
```

No IPv6 Unreachable Unconfiguration

To revert the suppression of ICMPv6 messages to the original configuration, follow the steps.

1. Enter the global configuration mode.
   ```
   R2#configure terminal
   ```
2. Configure the interface ge10.
   ```
   R2(config)#interface ge10
   ```
3. Re-enable ICMP unreachable messages.
   ```
   R2(config-if)#ipv6 unreachable
   ```
5. To commit the changes exit.
   ```
   R2(config)#commit
   R2(config)#exit
   ```

CLI Commands

The no ip unreachable introduces the following configuration commands:

- no ip unreachable
- no ipv6 unreachable

no ip unreachable

This command to suppress the ICMP messages going out from the interface.

Remove the no form of this command to allow ICMP messages going out from the interface.

Command Syntax

```
no ip unreachable
ip unreachable
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.5.2.

Examples

```
#configure terminal
(config)# interface ge0
(config-if)#no ip unreachable
```

no ipv6 unreachable

This command to suppress the ICMPv6 messages going out from the interface.

Remove the no form of this command to allow ICMPv6 messages going out from the interface.

Command Syntax

```
no ipv6 unreachable
ipv6 unreachable
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.5.2.

Examples

```
#configure terminal
(config)# interface ge0
(config-if)#no ipv6 unreachable
```

Glossary

The following provides definitions for key terms or abbreviations and their meanings used throughout this document:

Key Terms/Acronym	Description
ICMP	Internet Control Message Protocol (ICMP) is a fundamental protocol used in networking to relay error messages and operational information.

Security Management Command Reference

CHAPTER 1 Access Control List Commands

This chapter is a reference for the Access Control List (ACL) commands:

- arp access-group
- arp access-list
- arp access-list default
- arp access-list remark
- arp access-list request
- arp access-list resequence
- arp access-list response
- clear access-list
- clear arp access-list
- clear ip access-list
- clear ipv6 access-list
- clear mac access-list
- ip access-group
- ip access-list
- ip access-list default
- ip access-list filter
- ip access-list icmp
- ip access-list remark
- ip access-list resequence
- ip access-list tcp|udp
- ipv6 access-group in
- ipv6 access-list
- ipv6 access-list default
- ipv6 access-list filter
- ipv6 access-list icmpv6
- ipv6 access-list remark
- ipv6 access-list resequence
- ipv6 access-list sctp
- ipv6 access-list tcp|udp
- mac access-group
- mac access-list
- mac access-list default
- mac access-list filter
- mac access-list remark
- mac access-list resequence

© 2025 IP Infusion Inc. Proprietary

- show access-lists
- show arp access-lists
- show ip access-lists
- show ipv6 access-lists
- show mac access-lists
- show running-config access-list
- show running-config aclmgr
- show running-config ipv6 access-list

arp access-group

Use this command to attach an ARP access list to an interface to filter incoming ARP packets.

When you attach an ARP access list to a LAG interface as well as to a physical interface that is a member of that LAG interface, the priority order is:

1. LAG interface
2. Physical interface

Use the `no` form of this command to detach an ARP access group.

Note: An ARP access-list is supported only on switch ports.

Note: To attach an ARP access-group to an interface, the `ingress-arp` TCAM group should be enabled. See the hardware-profile filter (Qumran1) command for details.

Command Syntax

```
arp access-group NAME in
no arp access-group NAME in
```

Parameters

`NAME`	ARP access list name

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#permit ip any mac any
(config-arp-acl)#exit

(config)#interface xe1
(config-if)#arp access-group arp1 in
(config-if)#exit

(config)#interface xe1
(config-if)#no arp access-group arp1 in
(config-if)#exit
```

arp access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop the ARP packets, based on the ARP request or response option configured.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. A single-entry ACL with only one deny specification is the same as denying all traffic. You must have at least one permit specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Note: An ARP access list is supported only on switch ports.

Command Syntax

```
arp access-list NAME
no arp access-list NAME
```

Parameters

`NAME`	ARP access list name

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#arp access-list arp1
```

arp access-list default

Use this command to modify the default rule action of an access list.

The default rule is applicable only when an access list is attached to an interface. The default rule will have the lowest priority and only ARP packets not matching any of the user defined rules match the default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

The default rule is `deny-all` when an access list is attached to an interface.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#default permit-all
```

arp access-list remark

Use this command to add a description to a named ARP access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)# remark Permit arp request packets
```

arp access-list request

Use this command to configure ARP access control entry in an ARP access control list (ACL).

This command determines whether to accept or drop a packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring the same filter again with a change of sequence number or change of action will result in updating the sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit)(request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | ((XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
  (XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(request |) ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) mac (any | ((XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
  (XX-XX-XX-XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (vlan <1-4094>|) (inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	ARP ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`request`	ARP request.
`ip`	Internet Protocol (IP).
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.
`mac`	MAC address configuration.
`any`	Match any source mac address.
`XX-XX-XX-XX-XX-XX`	Source MAC address (Option 1).
`XX:XX:XX:XX:XX:XX`	Source MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source MAC address (Option 3).
`XX-XX-XX-XX-XX-XX`	Source wildcard (Option 1).
`XX:XX:XX:XX:XX:XX`	Source wildcard (Option 2).
`XXXX.XXXX.XXXX`	

Source wildcard (Option 3).

`host (XX-XX-XX-XX-XX-XX)`

A single source host MAC address.

`vlan <1-4094>` VLAN identifier.

`inner-vlan <1-4094>`

Inner VLAN identifier.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#10 permit request ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
(config-arp-acl)#no 10
```

arp access-list resequence

Use this command to modify the sequence numbers of an ARP access list.

Note: IP Infusion Inc. recommends to use a non-overlapping sequence space for a new sequence number set to avoid unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#resequence 15 15
```

arp access-list response

Use this command to configure an ARP access control entry in an ARP access control list (ACL).

This command determines whether to accept or drop an ARP response packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring the same filter again with a change of sequence number or change of action will result in updating the sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | ((XX-XX-XX-
  XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) -XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (any | ((XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)))(vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit) response ip (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) mac (any | ((XX-XX-XX-
  XX-XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) -XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))) (any | ((XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) | (host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)))(vlan <1-4094>|) (inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	ARP ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`response`	ARP response
`A.B.C.D/M`	Source/destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source/destination IP address and mask.
`host A.B.C.D`	A single source/destination host IP address.
`any`	Match any source/destination IP address.
`mac`	MAC address configuration.
`any`	Match any source/destination MAC address.
`XX-XX-XX-XX-XX-XX`	Source/destination MAC address (Option 1).
`XX:XX:XX:XX:XX:XX`	Source/destination MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source/destination MAC address (Option 3).

`XX-XX-XX-XX-XX-XX`
: Source/destination wildcard (Option 1).

`XX:XX:XX:XX:XX:XX`
: Source/destination wildcard (Option 2).

`XXXX.XXXX.XXXX` Source/destination wildcard (Option 3).

`vlan <1-4094>` VLAN identifier.

`inner-vlan <1-4094>`
: Inner VLAN identifier.

Command Mode

ARP access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#arp access-list arp1
(config-arp-acl)#10 permit response ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
(config-arp-acl)#no 10
```

clear access-list

Use this command to clear the access-list counters.

Command Syntax

```
clear access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear access-list counters
```

clear arp access-list

Use this command to clear the ARP access-list counters.

Command Syntax

```
clear arp access-list (NAME|) counters
```

Parameters

NAME	ARP access list name

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#clear arp access-list counters
```

clear ip access-list

Use this command to clear the IP access-list counters.

Command Syntax

```
clear ip access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ip access-list counters
```

clear ipv6 access-list

Use this command to clear the IPv6 access-list counters.

Command Syntax

```
clear ipv6 access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear ipv6 access-list counters
```

clear mac access-list

Use this command to clear the MAC access-list counters.

Command Syntax

```
clear mac access-list (NAME|) counters
```

Parameters

NAME	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clear mac access-list counters
```

ip access-group

Use this command to attach an IP access list to an interface or terminal line to filter incoming or outgoing IP packets.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: An egress IP ACL is supported on physical and lag interfaces only. An egress IP ACL will match only routed traffic and not switched traffic. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

Command Syntax

```
ip access-group NAME (in|out) (time-range TR_NAME|)
no ip access-group NAME (in|out) (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets
`out`	Filter outgoing packets.
`TR_NAME`	Time range name set with the time-range command.

Command Mode

Line mode

Interface mode

Applicability

This command was introduced before OcNOS version 3.0. The `time-range` parameter was added in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#hardware-profile filter ingress-ipv4-ext enable

(config)#interface xe3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#no ip access-group mylist in time-range TIMER1
(config-if)#exit
```

```
(config)#line vty
(config-all-line)#no ip access-group mylist in
```

Usage: VLANs and LAGs

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Usage: TCAM Groups

An access-group in the egress direction uses the TCAM group used by the QoS output service policy. Therefore, actions are unpredictable when conflicting matches are configured on same interface. IP Infusion Inc. recommends to avoid such a configuration. Otherwise, you need to configure the priority (in QoS) or the sequence number (in ACL) carefully to handle such cases.

To attach an IP ACL in the ingress direction the `ingress-ipv4` or `ingress-ipv4-ext` TCAM group needs to be enabled and to attach an IP ACL in the egress direction the `egress-ipv4` TCAM group needs to be enabled. See the hardware-profile filter (Qumran1) commands for details.

Usage: VTY Interfaces

You can create ACLs for VTY interfaces to filter packets from management applications such as SSH, Telnet, NTP, SNMP, and SNMP traps. TCP, UDP, and ICMP are supported.

For an ACL for VTY, you create the ACL, configure it with rules, and associate the ACL to the terminal line in line mode.

VTY ACLs do not support the following:

- The default rule `deny all`. You must explicitly set up a `deny all` rule based on your requirements.
- VLAN-specific rules.
- Rules with TCP flags.
- Rules with `dscp`, `fragments`, `log`, `precedence`, and `sample` parameters.
- Rules with ICMP code and message types.

Usage: Timed ACL on interfaces

You create a timer range that is identified by a name and configured with a start time, end time, and frequency. Once you create the time range, you can tie the ACL configuration to the time-range object. This allows you to create an access group that is enabled when the timer has started and disabled when the timer ends. You can also disassociate an access group from the timer if needed.

ip access-list

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming IP packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL.

Command Syntax

```
ip access-list NAME
no ip access-list NAME
```

Parameters

`NAME`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
```

ip access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the IP packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#default permit-all
```

ip access-list filter

Use this command to configure access control entry in an access control list (ACL).

This determines whether to accept or drop an IP packet based on the configured match criteria.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring the same filter again with change of sequence number or change of action results in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip|ipcomp|ipv6ip
  |ospf|pim|rsvp|vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D|host A.B.C.D|any) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (precedence (<0-7>| critical| flash | flashoverride| immediate|
  internet| network| priority| routine))|) (vlan <1-4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(<0-255> |ahp | any | eigrp | esp | gre | ipip |
  ipcomp | ipv6ip | ospf | pim | rsvp| vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D | host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63> |af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef )|) (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`<0-255>`	IANA assigned protocol number.
`any`	Any protocol packet.
`ahp`	Authentication Header packet.
`eigrp`	Enhanced Interior Gateway Routing Protocol packet.
`esp`	Encapsulating Security Payload packet.
`gre`	Generic Routing Encapsulation packet.
`ipip`	IPv4 over IPv4 encapsulation packet.
`ipcomp`	IP Payload Compression Protocol packet.
`ipv6ip`	IPv6 over IPv4 encapsulation packet.
`ospf`	Open Shortest Path First packet.
`pim`	Protocol Independent Multicast packet
`rsvp`	Resource Reservation Protocol packet.
`vrrp`	Virtual Router Redundancy Protocol packet.
`A.B.C.D/M`	Source IP prefix and length.

A.B.C.D A.B.C.D	
	Source IP address and mask.
host A.B.C.D	A single source host IP address.
any	Match any source IP address.
A.B.C.D/M	Destination IP prefix and length.
A.B.C.D A.B.C.D	
	Destination IP address and mask.
host A.B.C.D	A single destination host IP address.
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).

`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`vlan`	Match packets with given vlan value.
`<1 - 4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner vlan value.
`<1 - 4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#11 permit any 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
(config-ip-acl)#no 11
```

ip access-list icmp

Use this command to permit or deny ICMP packets based on the given source and destination IP address. Even DSCP, precedence, vlan ID and inner vlan ID can be configured to permit or deny with the given values.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) ((dscp (<0-63>|af11| af12| af13|
  af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6|
  cs7| default| ef ))| (precedence (<0-7>| critical| flash |
  flashoverride|immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>| critical| flash |
  flashoverride|immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|) (inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`icmp`	Internet Control Message Protocol packet.
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.
`A.B.C.D/M`	Destination IP prefix and length.
`A.B.C.D A.B.C.D`	Destination IP address and mask.
`host A.B.C.D`	A single destination host IP address.
`any`	Match any destination IP address.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.

`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.
`af43`	AF43 DSCP (100110) decimal value 38.
`cs1`	CS1 (precedence 1) DSCP (001000) decimal value 8.
`cs2`	CS2 (precedence 2) DSCP (010000) decimal value 16.
`cs3`	CS3 (precedence 3) DSCP (011000) decimal value 24.
`cs4`	CS4 (precedence 4) DSCP (100000) decimal value 32.
`cs5`	CS5 (precedence 5) DSCP (101000) decimal value 40.
`cs6`	CS6 (precedence 6) DSCP (110000) decimal value 48.
`cs7`	CS7 (precedence 7) DSCP (111000) decimal value 56.
`default`	Default DSCP (000000) decimal value 0.
`ef`	EF DSCP (101110) decimal value 46.
`precedence`	Match packets with given precedence value.
`<0-7>`	Enter precedence value 0-7.
`critical`	Match packets with critical precedence (5).
`flash`	Match packets with flash precedence (3).
`flashoverride`	Match packets with flash override precedence (4).
`immediate`	Match packets with immediate precedence (2).
`internet`	Match packets with internetwork control precedence (6).
`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner-vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-icmp
(config-ip-acl)#200 permit icmp any any
```

ip access-list remark

Use this command to add a description to a named IPv4 access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#remark permit the inside admin address
(config-ip-acl)#exit

(config)#ip access-list mylist
(config-ip-acl)#no remark
(config-ip-acl)#exit
```

ip access-list resequence

Use this command to modify sequence numbers of the IP access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Default

None

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#resequence 5 5
(config-ip-acl)#end
```

ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming TCP or UDP IP packet based on the specified match criteria. This form of command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: TCP flags options and range options like neq, gt, lt and range are not supported by hardware in egress direction.

Note: Both ACK and established flag in TCP have same functionality in hardware.

Note: `neq` option from IPv4 access list configuration should removed for Qumran2 Series Platform.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
  |exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
  uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
  |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www|netconf-ssh|netconf-tls) | range <0-65535> <0-65535>|)
  ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) |(precedence (<0-7>|
  critical| flash | flashoverride| immediate| internet| network| priority|
  routine)) |) ({ack|established|fin|psh|rst|syn|urg}|) vlan <1-4094>|)(inner-vlan
  <1-4094>|)
(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535>|biff|bootpc|bootps|discard|dnsix|domain|
  echo|isakmp|mobile-ip |nameserver | netbios-dgm | netbios-ns| netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp
  |time|who|xdmcp) | range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) ((eq|gt |lt|neq)(<0-65535> |biff |bootpc |bootps| discard| dnsix|
  domain| echo| isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp |ntp|pim-auto- rp| rip| snmp| snmptrap| sunrpc| syslog| tacacs|
  talk| tftp| time| who| xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11|
  af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine))|) (vlan <1-
  4094>|)(inner-vlan <1-4094>|)
no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
  domain| drip| echo|exec|finger|ftp |ftp-data |gopher |hostname| ident| irc|
  klogin| kshell|login|lpd|nntp|pim-auto-rp |pop2 |pop3 |smtp| ssh| sunrpc| tacacs
  |talk|telnet|time|uucp|whois|www|netconf-ssh|netconf-tls) | range <0-65535> <0-
  65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>
  |bgp |chargen |cmd |daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data|
  gopher| hostname| ident| irc| klogin| kshell| login| lpd| nntp| pim-auto-rp |
```

```
  pop2| pop3| smtp |ssh |sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-
  65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31|
  af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) |
  (precedence (<0-7>| critical| flash | flashoverride| immediate| internet|
  network| priority| routine)) |) ({ack|established|fin|psh|rst|syn|urg}|)(vlan <1-
  4094>|)(inner-vlan <1-4094>|)
no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
  domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|
  tftp|time|who|xdmcp) | range <0-65535> <0-65535>|)(A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D| any) ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix|
  domain|echo| isakmp|mobile- ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp| ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|
  tacacs|talk|tftp|time|who|xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>|
  af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2|
  cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash |
  flashoverride| immediate| internet| network| priority| routine)) |)(vlan <1-
  4094>|)(inner-vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`A.B.C.D/M`	Source or destination IP prefix and length.
`A.B.C.D A.B.C.D`	Source or destination IP address and mask.
`host A.B.C.D`	Source or destination host IP address.
`any`	Any source or destination IP address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.

domain	Domain Name Service.
drip	Dynamic Routing Information Protocol.
echo	Echo.
exec	EXEC.
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections.
gopher	Gopher.
hostname	NIC hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login.
lpd	Printer service.
nntp	Network News Transport Protocol.
pim-auto-rp	PIM Auto-RP.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
smtp	Simple Mail Transport Protocol.
ssh	Secure Shell.
sunrpc	Sun Remote Procedure Call.
tacacs	TAC Access Control System.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	WHOIS/NICNAME
www	World Wide Web.
netconf-ssh	Secure Shell Network Configuration
netconf-tls	Transport Layer Security Network Configuration
nntp	Range of source or destination port numbers:
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.

af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34.
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Precedence.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.

`echo`	Echo.
`isakmp`	Internet Security Association and Key Management Protocol.
`mobile-ip`	Mobile IP registration.
`nameserver`	IEN116 name service.
`netbios-dgm`	Net BIOS datagram service.
`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`rip`	Routing Information Protocol.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.
`syslogS`	ystem Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`vlan`	Match packets with given vlan value.
`<1-4094>`	VLAN identifier.
`inner-vlan`	Match packets with given inner vlan value.
`<1-4094>`	VLAN identifier.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end
```

ipv6 access-group in

Use this command to attach an IPv6 access list to an interface to filter incoming IPv6 packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: To attach IPv6 ACL in the ingress direction ingress-ipv6 TCAM group needs to be enabled. See the hardware-profile filter (Qumran1) command for details.

Command Syntax

```
ipv6 access-group NAME in (time-range TR_NAME|)
no ipv6 access-group NAME in (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`TR_NAME`	Time range name set with the time-range command.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#permit ipv6 any any
(config-ipv6-acl)#exit
(config)#hardware-profile filter ingress-ipv6 enable

(config)#interface xe3
```

```
(config-if)#ipv6 access-group mylist in

(config)#interface xe3
(config-if)#no ipv6 access-group mylist in

(config)#interface xe3
(config-if)#ipv6 access-group mylist in time-range TIMER1

(config)#interface xe3
(config-if)#no ipv6 access-group mylist in time-range TIMER1
```

ipv6 access-list

Use this command to define a IPv6 access control list (ACL) that determines whether to accept or drop an incoming IPv6 packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Note: IPv6 routing protocols need neighbor discovery to establish sessions. Applying IPv6 ACLs implicitly drops all the ICMPv6 packets, thereby affecting the protocol sessions. To overcome this problem, an implicit ICMPv6 permit rule is added to the IPv6 ACLs.

If required behavior is to deny the icmpv6, the implicit rule can be deleted. For example, create an IPv6 ACL:

```
(config)#ipv6 access-list ipv6-acl

#show ipv6 access-lists
IPv6 access list ip1
268435453 permit icmpv6 any any
```

To delete this rule:

```
(config)#ipv6 access-list ipv6-acl

(config-ipv6-acl)#no 268435453 permit icmpv6 any any

#show ipv6 access-lists
IPv6 access list ip1
```

Use the `no` form of this command to remove the ACL.

Command Syntax

```
ipv6 access-list NAME
no ipv6 access-list NAME
```

Parameters

`NAME`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#exit
```

ipv6 access-list default

Use this command to modify the default rule action of IPv6 access-list. Default rule is applicable only when IPv6 access-list is attached to interface. Default rule will have the lowest priority and only the IPv6 packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ipv6-acl-01
(config-ipv6-acl)#default permit-all
```

ipv6 access-list filter

Use this command to define an access-control entry in an access control list (ACL) that determines whether to accept or drop an IPv6 packet based on the criteria specified. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address
- DSCP value
- VLAN identifier

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: For IPv6 source and destination address filters, only the network part from the address (upper 64 bits) is supported due to hardware restriction. If the address length is more than 64 bits, it cannot be applied on the interfaces but it can be used with distributed lists in control plane protocols.

Command Syntax

```
(<1-268435453>|) (deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22| af23|
  af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef
  )|) (vlan <1-4094>|)
no (<1-268435453>|)(deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) (dscp (<0-63>|af11| af12| af13| af21| af22| af23|
  af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef
  )|) (vlan <1-4094>|)
no (<1-268435453>)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`<0-255>`	IANA assigned protocol number.
`any`	Any protocol packet.
`ahp`	Authentication Header packet.
`eigrp`	Enhanced Interior Gateway Routing Protocol packet.
`esp`	Encapsulating Security Payload packet.
`gre`	Generic Routing Encapsulation packet.
`ipipv6`	IPv4 over IPv6 Encapsulation packet.
`ipcomp`	IP Payload Compression Protocol packet.
`ipv6ipv6`	IPv6 over IPv6 Encapsulation packet.

ospf	Open Shortest Path First packet.
pim	Protocol Independent Multicast packet
rsvp	Resource Reservation Protocol packet.
vrrp	Virtual Router Redundancy Protocol packet.
X:X::X:X/M	Source Address with network mask length.
X:X::X:X X:X::X:X	Source Address with wild card mask.
any	Any source address.
X:X::X:X/M	Destination address with network mask length.
X:X::X:X X:X::X:X	Destination address with wild card mask.
any	Any destination address
any	Match any destination IP address.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#permit ipipv6 any any
(config-ipv6-acl)#end
```

ipv6 access-list icmpv6

Use this command to permit or deny IPv6 ICMP packets with the given source and destination IPv6 address, DSCP value and VLAN ID.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/ M|X:X::X:X X:X::X:X|any) ((dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef)|) (vlan <1-4094>|)
```

```
no (<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) ((dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`icmpv6`	Internet Control Message Protocol packet.
`X:X::X:X/M`	Source Address with network mask length.
`X:X::X:X X:X::X:X`	Source Address with wild card mask.
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X X:X::X:X`	Destination address with wild card mask.
`any`	Any destination address
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.

af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit icmpv6 any any
```

ipv6 access-list remark

Use this command to add a description to an IPv6 access control list (ACL).

Use the `no` form of this command to remove an access control list description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)# remark Permit the inside admin address
```

ipv6 access-list resequence

Use this command to modify sequence numbers of the IPv6 access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting Sequence number.
`INCREMENT`	Sequence number increment steps.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#resequence 15 15
```

ipv6 access-list sctp

Use this command to allow ACL to permit or deny SCTP packets based on the given source and destination IPV6 address. Even DSCP and vlan ID can be configured to permit or deny with the given values.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Range options like neq, gt, lt and range are not supported by hardware in egress direction.

Note: `neq` option from IPv6 access list configuration should removed for Qumran2 Series Platform.

Command Syntax

```
(<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <0-
  65535>)|  } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33|
  af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) (vlan <1-
  4094>|)
no (<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535>
  <0-65535>)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33|
  af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|) (vlan <1-
  4094>|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`sctp`	Stream Control Transmission Protocol packet.
`X:X::X:X/M`	Source address with network mask length.
`X:X::X:X`	Source address with wild card mask.
`X:X::X:X`	Source address's wild card mask (ignored bits).
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X`	Destination address with wild card mask.
`X:X::X:X`	Destination address's wild card mask (ignored bits).
`any`	Any destination address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.

<0-65535>	Highest value in the range.
dscp	Match packets with given DSCP value.
<0-63>	DSCP value.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value 20.
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit sctp any any
```

ipv6 access-list tcp|udp

Use this command to define a IPv6 access control list (ACL) specification that determines whether to accept or drop an incoming IPv6 packet based on the criteria that you specify. This form of this command filters packets based on source and destination IPv6 address along with protocol (TCP or UDP) and port.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Range options such as neq, gt, lt and range are not supported by the hardware in the egress direction.

Note: `neq` option from IPv6 access list configuration should removed for Qumran2 Series Platform.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>|)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any)((eq|gt|lt|neq) <0-65535>|bgp|chargen|cmd|daytime|discard|domain
  |drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk| telnet|time
  |uucp|whois|www) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12| af13|
  af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
  cs6| cs7| default| ef)) (vlan <1-4094>|)

(<1-268435453>|) (deny|permit) udp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain
  |echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk
  |tftp|time|who|xdmcp) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix
  |domain|echo|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-
  ss|non500-isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk
  |tftp|time|who|xdmcp) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef) (vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X
  X:X::X:X|any) ((eq|gt|lt|neq) <0-65535>|bgp|chargen|cmd|daytime|discard|domain|
  drip|echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin
  |kshell|login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | (range <0- 65535> <0-65535>)|) (dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef) | (vlan <1-4094>|)

no (<1-268435453>|) (deny|permit) udp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain|echo
  |isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
  isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time
```

```
|who|xdmcp) | (range <0-65535> <0-65535>)|)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
((eq|gt|lt|neq) <0-65535>|biff|bootpc|bootps|discard|dnsix|domain|echo
|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-
isakmp|ntp|pim-auto-rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time
|who|xdmcp) | (range <0-65535> <0-65535>)|) (dscp (<0-63>| af11| af12| af13|
af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|
cs6| cs7| default| ef) | (vlan <1-4094>|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`tcp`	Transmission Control Protocol.
`udp`	User Datagram Protocol.
`X:X::X:X/M`	Source or destination IPv6 prefix and length.
`X:X::X:X X:X::X:X`	Source or destination IPv6 address and mask.
`any`	Any source or destination IPv6 address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.
`lt`	Source or destination port less than.
`neq`	Source or destination port not equal to.
`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`ftp`	File Transfer Protocol (21).
`ssh`	Secure Shell (22).
`telnet`	Telnet (23).
`www`	World Wide Web (HTTP 80).
`tftp`	Trivial File Transfer Protocol (69).
`bootp`	Bootstrap Protocol (BOOTP) client (67).
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.
`exec`	EXEC.

`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nnt`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.
`ssh`	Secure Shell.
`sunrpc`	Sun Remote Procedure Call.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`telnet`	Telnet.
`time`	Time.
`uucp`	UNIX-to-UNIX Copy Program.
`whois`	WHOIS/NICNAME
`www`	World Wide Web.
`nntp`	Range of source or destination port numbers:
`dscp`	Match packets with given DSCP value.
`<0-63>`	DSCP value.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.
`af21`	AF21 DSCP (010010) decimal value 18.
`af22`	AF22 DSCP (010100) decimal value 20.
`af23`	AF23 DSCP (010110) decimal value 22.
`af31`	AF31 DSCP (011010) decimal value 26.
`af32`	AF32 DSCP (011100) decimal value 28.
`af33`	AF33 DSCP (011110) decimal value 30.
`af41`	AF41 DSCP (100010) decimal value 34
`af42`	AF42 DSCP (100100) decimal value 36.

af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.
mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.
netbios-ns	Net BIOS name service.
netbios-ss	Net BIOS session service.
non500-isakmp	Non500-Internet Security Association and Key Management Protocol.
ntp	Network Time Protocol.
pim-auto-rp	PIM Auto-RP.
rip	Routing Information Protocol.
snmp	Simple Network Management Protocol.
snmptrap	SNMP Traps.
sunrpc	Sun Remote Procedure Call.
syslog	System Logger.
tacacs	TAC Access Control System.
talk	Talk.
tftp	Trivial File Transfer Protocol.
time	Time.
who	Who service.
xdmcp	X Display Manager Control Protocol.
vlan	Match packets with given vlan value.
<1-4094>	VLAN identifier.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#deny udp any eq tftp any
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fdf2:860a:746a:e49c::/64 eq ssh
```

mac access-group

Use this command to attach a MAC access list to an interface to filter incoming packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

The `time-range` parameter is optional. If used, the access-group is tied to the timer specified.

After the access-group has been configured with the time-range, to detach the access-group from the time-range, use the `no` form of this command with a time-range parameter as shown in the syntax and examples below.

To delete the access-group, use the `no` form of this command without a time-range.

Note: To attach a MAC ACL in the ingress direction ingress-l2 or ingress-l2-ext TCAM group needs to be enabled and to attach a MAC ACL in the egress direction egress-l2 TCAM group needs to be enabled. See the hardware-profile filter (Qumran1) command for details.

Note: An egress ACL is supported on physical and lag interfaces only. VLAN and inner-VLAN options in ACL rules will match incoming packet VLANs even when ACL attached at egress.

Command Syntax

```
mac access-group NAME (in|out) (in|out) (time-range TR_NAME|)
no mac access-group NAME (in|out) (time-range TR_NAME|)
```

Parameters

`NAME`	Access list name.
`in`	Filter incoming packets.
`out`	Filter outgoing packets.
`TR_NAME`	Time range name set with the time-range command.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3. The `time-range` parameter was added in OcNOS version 5.0.

Examples

```
#configure terminal
```

```
(config)#mac access-list mylist
(config-mac-acl)#permit any any
(config-mac-acl)#exit

(config)#hardware-profile filter ingress-l2-ext enable

(config)#interface xe3
(config-if)#mac access-group mylist in
(config-if)#exit

(config)#interface xe3
(config-if)#mac access-group mylist in time-range TIMER1
(config-if)#exit

(config)#interface xe3
(config-if)#no mac access-group mylist in time-range TIMER1
(config-if)#exit

(config)#interface xe3
(config-if)#no mac access-group mylist in
(config-if)#exit
```

mac access-list

Use this command to define a MAC access control list (ACL) that determines whether to accept or drop an incoming packet based on specifications configured under the ACL. An ACL is made up of one or more ACL specifications.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied by default. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied deny specification for traffic that is not permitted. Implied specification can be updated to permit if the use-case is to deny a certain set of traffic.

Use the `no` form of this command to remove an ACL.

Command Syntax

```
mac access-list NAME
no mac access-list NAME
```

Parameters

`NAME`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#exit
```

mac access-list default

Use this command to modify the default rule action of mac access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax

```
default (deny-all|permit-all)
```

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#default permit-all
```

mac access-list filter

Use this command to define an access control entry (ACE) in a mac access control list (ACL) that determines whether to permit or deny packets with the given source and destination MAC, ether type, cos and VLAN values.

Use the `no` form of this command to remove an ACL specification. ACL specification can be removed using the sequence number as well.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Note: Ether type option is not supported by hardware in egress direction

Command Syntax

```
(<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))(aarp|appletalk|decnet-iv|diagnostic|etype-
  6000|etype-8042|ipv4|ipv6|mpls|lat|lavc-sca|mop-console|mop-dump|vines-
  echo|<0x600-0xFFF>))(cos <0-7>|)(vlan <1-4094>|) (inner-vlan <1-4094>|<0x600-
  0xFFF>)
no (<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX))(aarp|appletalk|decnet-iv|diagnostic|etype-
  6000|etype-8042|ipv4|ipv6|mpls|lat|lavc-sca|mop-console|mop-dump|vines-
  echo|<0x600-0xFFF>|))(cos <0-7>|)(vlan <1-4094>|) (inner-vlan <1-4094>|<0x600-
  0xFFF>)
no (<1-268435453>)
```

Parameters

`ETHTYPE`	Any Ethertype value (0x600 - 0xffff)
`deny`	Drop the packet.
`permit`	Accept the packet.
`<1-268435453>`	IPv4 ACL sequence number.
`any`	Source/Destination any.
`XX-XX-XX-XX-XX-XX`	Source/Destination MAC address (Option 1)
`XX-XX-XX-XX-XX-XX`	Source/Destination MAC address (Option 2).
`XXXX.XXXX.XXXX`	Source/Destination MAC address (Option 3).
`XX-XX-XX-XX-XX-XX`	Source/Destination wildcard (Option1).
`XX:XX:XX:XX:XX:XX`	Source/Destination wildcard (Option2).
`XXXX.XXXX.XXXX`	Source/Destination wildcard (Option3).

`host`	A single source/destination host.
`aarp`	Ethertype - 0x80f3.
`appletalk`	Ethertype - 0x809b.
`decnet-iv`	Ethertype - 0x6003
`diagnostic`	Ethertype - 0x6005
`etype-6000`	Ethertype - 0x6000
`etype-8042`	Ethertype - 0x8042
`ip4`	Ethertype - 0x0800
`ip6`	Ethertype - 0x86dd
`mpls`	Ethertype - 0x8847
`lat`	Ethertype - 0x6004
`lavc-sca`	Ethertype - 0x6007
`mop-console`	Ethertype - 0x6002
`mop-dump`	Ethertype - 0x6001
`vines-echo`	Ethertype - 0x0baf
`WORD`	Any Ethertype value
`cos <0-7>`	Cos value
`vlan <1-4094>`	VLAN identifier
`inner-vlan <1 - 4094>`	Inner-VLAN identifier

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#permit 0000.1234.1234 0000.0000.0000 any
```

mac access-list remark

Use this command to add a description to a MAC access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax

```
remark LINE
no remark
```

Parameters

`LINE`	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)# remark Permit the inside admin address
```

mac access-list resequence

Use this command to modify sequence numbers of mac access list specifications.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax

```
resequence <1-268435453> INCREMENT
```

Parameters

`<1-268435453>`	Starting sequence number.
`INCREMENT`	Sequence number increment steps.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#resequence 15 15
```

show access-lists

Use this command to display a list of access list

Command Syntax

```
show access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show access-lists expanded
IP access list Iprule1
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
default deny-all
MAC access list Macrule1
10 permit host 0000.1234.1234 any
default deny-all
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
default deny-all

#show access-lists summary
IPV4 ACL Iprule1
statistics enabled
Total ACEs Configured: 1
Configured on interfaces:
xe3/1 - egress (Router ACL)
Active on interfaces:
xe1/3 - ingress (Router ACL)
MAC ACL Macrule1
statistics enabled
Total ACEs Configured: 0
Configured on interfaces:
Active on interfaces:
IPV6 ACL ipv6-acl-01
```

```
statistics enabled
Total ACEs Configured: 2
Configured on interfaces:
xe7/1 - ingress (Router ACL)
Active on interfaces:
```

show arp access-lists

Use this command to display ARP access lists.

Note: Broadcast ARP request packets are counted twice.

Command Syntax

```
show arp access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	ARP access-list name.
expanded	Expanded access-list.
summary	Access-list summary.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show arp access-lists
ARP access list arp1
        10 permit ip 1.1.1.0/24 mac 0000.0000.0001 FFFF.FFFF.FFF0
        20 deny ip 2.2.2.0/24 mac any
        default deny-all

#show arp access-lists summary
ARP ACL arp1
       statistics enabled
       Total ACEs Configured: 2
       Configured on interfaces:
          xe1 - ingress (Port ACL)
       Active on interfaces:
          xe1 - ingress (Port ACL)
```

© 2025 IP Infusion Inc. Proprietary

show ip access-lists

Use this command to display IP access lists.

Note: In Qumran devices, when both ip access-list and mac access-list configured on the same interface with rules from both access-lists matching the packet, the match packet statistics is incremented only for the access-list whose hardware-profile filter is configured at the last. Also, when qos is configured on the same interface, along with ingress-acl statistics profile, ingress-qos statistics profile need to be enabled in order to get statistics for both qos entries and acl entries.

Note: See hardware-profile filter (Qumran1) for filter groups and hardware-profile statistics.

Command Syntax

```
show ip access-lists (NAME|) (expanded|summary|)
```

Parameters

`NAME`	Access-list name.
`expanded`	Expanded access-list.
`summary`	Access-list summary.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip access-lists
IP access list Iprule2
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
default deny-all

#show ip access-lists summary
IPV4 ACL Iprule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa1 - ingress (Port ACL)
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

```
xe3/1 - egress (Router ACL)
Active on interfaces:
sa1 - ingress (Port ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

show ipv6 access-lists

Use this command to display IPv6 access lists.

Command Syntax

```
show ipv6 access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 access-lists
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
20 permit ahp 78fe::1/48 68fe::1/48
30 permit ahp 3333::1/64 4444::1/48 fragments
40 permit ahp 5555::1/64 4444::1/48 dscp af23
default deny-all

#show ipv6 access-lists summary
IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
vlan1.3 - ingress (Router ACL)
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

© 2025 IP Infusion Inc. Proprietary

show mac access-lists

Use this command to display MAC access lists.

Note: In Qumran devices, when both ip access-list and mac access-list configured on the same interface with rules from both access-lists matching the packet, match packet statistics is incremented only for the access-list whose hardware-profile filter is configured at the last. Also, when qos is configured on the same interface, along with ingress-acl statistics profile, ingress-qos statistics profile need to be enabled in order to get statistics for both qos entries and acl entries.

Note: See hardware-profile filter (Qumran1) for filter groups and hardware-profile statistics.

Command Syntax

```
show mac access-lists (NAME|) (expanded|summary|)
```

Parameters

NAME	Access-list name.
expanded	Expanded access-list.
summary	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show mac access-lists
MAC access list Macrule2
default deny-all
MAC access list Macrule3
10 permit host 0000.1234.1234 any
20 deny host 1111.1111.AAAA any 65535
30 permit host 2222.2222.AAAA any 65535
40 permit 0000.3333.3333 0000.0000.FFFF 4444.4444.4444 0000.0000.FFFF
default deny-all [match=1126931077]

# show mac access-lists summary
MAC ACL Macrule3
statistics enabled
Total ACEs Configured: 4
Configured on interfaces:
sa3 - ingress (Router ACL)
sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL)
```

```
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router ACL)
xe1/3 - ingress (Router ACL)
```

show running-config access-list

Use this command to show the running system status and configuration details for MAC and IP access lists.

Command Syntax

```
show running-config access-list
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config access-list
ip access-list abd
10 deny any any any
!
mac access-list abc
remark test
10 deny any any
!
```

show running-config aclmgr

Use this command to display the entire access list configurations along with the attachment to interfaces.

Command Syntax

```
show running-config aclmgr (all|)
```

Parameters

`all`	Show running config with defaults

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config aclmgr
ip access-list ip-acl-01
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
12 deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24
mac access-list mac-acl-01
10 permit host 0000.1234.1234 any
20 permit host 0000.1111.AAAA any ipv4 cos 3 vlan 3
!
ipv6 access-list ipv6-acl-01
10 deny ipv6 3ffe::/64 4ffe::/64 dscp af43
20 permit ipv6 78fe::/64 68fe::/64 dscp cs3
!
interface xe1/1
ip access-group ip-acl-01 in
!
```

© 2025 IP Infusion Inc. Proprietary

show running-config ipv6 access-list

Use this command to show the running system status and configuration details for IPv6 access lists.

Command Syntax

```
show running-config ipv6 access-list
```

Parameters

None

Default

None

Command Mode

Privileged exec mode, configure mode, and route-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config ipv6 access-list
ipv6 access-list test
10 permit any any any
```

CHAPTER 2 Access Control List Commands (Standard)

This chapter is a reference for the standard Access Control List (ACL) commands:

- ip access-list standard
- ip access-list standard filter
- Ipv6 access-list standard
- ipv6 access-list standard filter

ip access-list standard

Use this command to define a standard IP access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IP packet based on the source IP address, either an exact match or a range of prefixes.

Standard ACL can be used by L3 and SNMP protocols to permit or deny IP packets from a host or a range of prefixes.

Use the `no` form of this command to remove the ACL.

Note: Standard access-lists are not allowed to be attached on interfaces and are used for protocol level filtering purposes.

Command Syntax

```
ip access-list standard NAME
no ip access-list standard NAME
```

Parameters

`NAME`	Standard IP access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#ip access-list standard ip-acl-01
(config-ip-acl-std)#exit
(config)#no ip access-list standard ip-acl-01
```

ip access-list standard filter

Use this command to configure access control entry in an access control list (ACL).

This command determines whether to accept or drop a packet based on the configured source IP address.

Use the `no` form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
no (deny|permit) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.
`any`	Match any source IP address.

Default

No default value is specified

Command Mode

Standard IP access-list mode

Applicability

This command was introduced in OcNOS version 3.0

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl-std)#permit 30.30.30.0/24
(config-ip-acl-std)#no permit 30.30.30.0/24
```

Ipv6 access-list standard

Use this command to define a standard IPv6 access control list (ACL) in which multiple specifications can be configured. A specification determines whether to accept or drop an incoming IPv6 packet based on the source IPv6 address, either an exact match or a range of prefixes.

Standard IPv6 ACL can be used by L3 protocols to permit or deny IPv6 packets from a host or a range of prefixes.

Use the `no` form of this command to remove the ACL.

Note: Standard access-lists are not allowed to be attached on interfaces and are used for protocol level filtering purposes.

Command Syntax

```
ipv6 access-list standard NAME
no ipv6 access-list standard NAME
```

Parameters

`NAME`	Standard IPv6 access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#exit
(config)#no ipv6 access-list standard ipv6-acl-01
```

ipv6 access-list standard filter

Use this command to configure access control entry in an access control list (ACL).This determines whether to accept or drop a packet based on the configured IPv6 prefix.

Use the `no` form of this command to remove an ACL specification.

Command Syntax

```
(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
no(deny|permit)(X:X::X:X/M|X:X::X:X X:X::X:X|any)
```

Parameters

`deny`	Drop the packet.
`permit`	Accept the packet.
`X:X::X:X/M`	Source address with network mask length.
`X:X::X:X X:X::X:X`	Source address with wild card mask.
`any`	Any source address.

Default

No default value is specified

Command Mode

Standard IPv6 access-list mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#ipv6 access-list standard ipv6-acl-01
(config-ipv6-acl-std)#permit 2000::0/64
(config-ipv6-acl-std)#no permit 2000::0/64
```

CHAPTER 3 DHCP Snooping Commands

This chapter describe the commands for DHCP snooping.

- debug ip dhcp snooping
- hardware-profile filter dhcp-snoop
- hardware-profile filter dhcp-snoop-ipv6
- ip dhcp packet strict-validation bridge
- ip dhcp snooping arp-inspection bridge
- ip dhcp snooping arp-inspection vlan
- ip dhcp snooping arp-inspection validate
- ip dhcp snooping bridge
- ip dhcp snooping database
- ip dhcp snooping information option bridge
- ip dhcp snooping trust
- ip dhcp snooping verify mac-address
- ip dhcp snooping vlan
- renew ip dhcp snooping binding database
- show debugging ip dhcp snooping
- show debugging ip dhcp snooping
- show ip dhcp snooping bridge
- show ip dhcp snooping binding bridge

© 2025 IP Infusion Inc. Proprietary

debug ip dhcp snooping

Use this command to enable the debugging DHCP snooping.

Use the `no` parameter to disable the debug options.

Command Syntax

```
debug ip dhcp snooping (event|rx|tx|packet|all)
no debug ip dhcp snooping (event|rx|tx|packet|all)
```

Parameters

`event`	Enable event debugging
`rx`	Enable receive debugging
`tx`	Enable transmit debugging
`packet`	Enable packet debugging
`all`	Enable all debugging

Default

By default all debugging options are disabled.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#debug ip dhcp snooping all
#no debug ip dhcp snooping packet
```

© 2025 IP Infusion Inc. Proprietary

hardware-profile filter dhcp-snoop

Use this command to enable or disable the ingress dhcp-snoop TCAM group.

Command Syntax

```
hardware-profile filter dhcp-snoop (disable | enable)
```

Parameters

`enable`	Enable the ingress dhcp-snoop group
`disable`	Disable the ingress dhcp-snoop group

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
configure terminal
(config)#hardware-profile filter dhcp-snoop enable
```

hardware-profile filter dhcp-snoop-ipv6

Use this command to enable or disable the ingress dhcp-snoop-ipv6 TCAM group.

Command Syntax

```
hardware-profile filter dhcp-snoop-ipv6 (disable | enable)
```

Parameters

`enable`	Enable the ingress dhcp-snoop-ipv6 group
`disable`	Disable the ingress dhcp-snoop-ipv6 group

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
configure terminal
(config)#hardware-profile filter dhcp-snoop-ipv6 enable
```

ip dhcp packet strict-validation bridge

Use this command to enable strict validation of DHCP packets. Strict validation checks that the DHCP option field in the packet is valid including the magic cookie in the first four bytes of the options field. The device drops the packet if validation fails.

Use the `no` form of this command to disable strict validation.

Command Syntax

```
ip dhcp packet strict-validation bridge <1-32>
no ip dhcp packet strict-validation bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default, strict validation of DHCP packets is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
configure terminal
(config)#bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#ip dhcp packet strict-validation bridge 1
```

ip dhcp snooping arp-inspection bridge

Use this command to enable/disable arp-inspection on the bridge.

Note: You must enable dhcp snooping before enabling ARP inspection.

Command Syntax

```
ip dhcp snooping arp-inspection bridge <1-32>
no ip dhcp snooping arp-inspection bridge <1-32>
```

Parameter

<1-32>	Bridge number

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#ip dhcp snooping arp-inspection bridge 1
```

ip dhcp snooping arp-inspection vlan

Use this command to enable ARP inspection on the VLAN in a bridge.

Use the no form of this command to disable ARP inspection on the VLAN in a bridge.

Command Syntax

```
ip dhcp snooping arp-inspection vlan VLAN_RANGE2 bridge <1-32>
no ip dhcp snooping arp-inspection vlan VLAN_RANGE2 bridge <1-32>
```

Parameters

VLAN_RANGE2	VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19
<1-32>	Bridge number

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
configure terminal
(config)#bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#ip dhcp snooping arp-inspection bridge 1
(config)#vlan 2 bridge 1 state enable
(config)#ip dhcp snooping vlan 2 bridge 1
(config)#ip dhcp snooping arp-inspection vlan 2 bridge 1
```

ip dhcp snooping arp-inspection validate

Use this command to enable validation of the source-mac, destination-mac, or IP address field in the ARP packet payload.

Note: The IP address in a payload is validated for not being a broadcast address, a reserved zero IP address, and multicast address.

Use the `no` form of this command to disable validation of the source-mac, destination-mac, or IP address field in the ARP packet payload

Command Syntax

```
ip dhcp snooping arp-inspection validate (dst-mac | ip | src-mac) bridge <1-32>
no ip dhcp snooping arp-inspection validate (dst-mac | ip | src-mac) bridge <1-32>
```

Parameters

`dst-mac`	Destination MAC validation
`ip`	ARP IP address validation
`src-mac`	Source MAC validation
`<1-32>`	Bridge number

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
configure terminal
(config)# bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#ip dhcp snooping arp-inspection bridge 1
(config)#ip dhcp snooping arp-inspection validate dst-mac bridge 1
(config)#no ip dhcp snooping arp-inspection validate dst-mac bridge 1
(config)#ip dhcp snooping arp-inspection validate src-mac bridge 1
(config)#no ip dhcp snooping arp-inspection validate src-mac bridge 1
(config)#ip dhcp snooping arp-inspection validate ip bridge 1
(config)#no ip dhcp snooping arp-inspection validate ip bridge 1
```

ip dhcp snooping bridge

Use this command to enable DHCP snooping on a bridge.

Use the `no` form of this command to disable DHCP snooping on a bridge.

Command Syntax

```
ip dhcp snooping bridge <1-32>
no ip dhcp snooping bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default DHCP snooping is disabled on a bridge.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
```

ip dhcp snooping database

Use this command to write the entries in the binding table to persistent storage.

Command Syntax

```
ip dhcp snooping database bridge <1-32>
```

Parameters

<1-32>	Bridge number

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#ip dhcp snooping database bridge 1
```

ip dhcp snooping information option bridge

Use this command to insert interface and VLAN name in the option 82 field in DHCP packets.

Use the `no` form of this command to disable inserting option 82 information in DHCP packets.

Command Syntax

```
ip dhcp snooping information option bridge <1-32>
no ip dhcp snooping information option bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default option 82 information insertion is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
configure terminal
(config)# bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#vlan 2 bridge 1 state enable
(config)#ip dhcp snooping vlan 2 bridge 1
(config)#ip dhcp information option bridge 1
```

ip dhcp snooping trust

Use this command to mark an interface as trusted. All DHCP servers must be connected to the trusted interface.

Use the `no` form of this command to remove an interface from the list of trusted interfaces.

Command Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Parameters

None

Default

By default all interfaces are untrusted.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
configure terminal
(config)#bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#vlan 2 bridge 1 state enable
(config)#ip dhcp snooping vlan 2 bridge 1
(config)#interface xe1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode access
(config-if)#switchport access vlan 2
(config-if)#ip dhcp snooping trust
```

© 2025 IP Infusion Inc. Proprietary

ip dhcp snooping verify mac-address

Use this command to enable MAC address verification. If the device receives a DHCP request packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, the device drops the packet.

Use the `no` form of this command to disable address verification.

Command Syntax

```
ip dhcp snooping verify mac-address bridge <1-32>
no ip dhcp snooping verify mac-address bridge <1-32>
```

Parameters

`<1-32>`	Bridge number

Default

By default MAC address verification is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
configure terminal
(config)# bridge 1 protocol mstp
(config)#ip dhcp snooping bridge 1
(config)#ip dhcp snooping verify mac-address bridge 1
```

ip dhcp snooping vlan

Use this command to enable DHCP snooping for the given VLAN.

Use the `no` form of this command to disable the DHCP snooping for aVLAN.

Command Syntax

```
ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32>
no ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32>
```

Parameters

`VLAN_RANGE2`	VLAN identifier <1-4094> or range such as 2-5,10 or 2-5,7-19
`<1-32>`	Bridge number

Default

By default DHCP snooping is disabled for all VLANs.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
configure terminal
(config)#vlan 2 bridge 1 state enable
(config)#ip dhcp snooping vlan 2 bridge 1
```

renew ip dhcp snooping binding database

Use this command to populate the binding table by fetching the binding entries from persistent storage.

Command Syntax

```
renew ip dhcp snooping (source|) binding database bridge <1-32>
```

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#renew ip dhcp snooping binding database bridge 1
```

show debugging ip dhcp snooping

Use this command to display the enabled debugging options.

Command Syntax

```
show debugging ip dhcp snooping
```

Parameters

None

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show debugging ip dhcp snooping
DHCP snoop debugging status:
DHCP snoop event debugging is on
DHCP snoop tx debugging is on
```

show ip dhcp snooping arp-inspection statistics bridge

Use this command to show dhcp dynamic ARP inspection related statistics on bridge.

Command Syntax

```
show ip dhcp snooping arp-inspection statistics bridge <1-32>
```

Parameters

`<1-32>`	Bridge number.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#show ip dhcp snooping arp-inspection statistics bridge 1

bridge      forwarded  dai dropped
------      ---------  -----------
1           9          1
```

Table 3-1 explains the fields in the output.

Table 3-1: show ip dhcp snooping arp-inspection statistics bridge fields

Field	Description
`bridge`	Bridge number.
`forwarded`	Number of forwarded packets.
`dai dropped`	Number of dropped packets.

show ip dhcp snooping bridge

Use this command to display the DHCP configuration, including trusted ports, configured VLAN, active VLAN, and strict validation status.

Command Syntax

```
show ip dhcp snooping bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Strict validation of DHCP packet is                   : Disabled
DB Write Interval(secs)                               : 300
DHCP snooping is configured on following VLANs        : 20,30
DHCP snooping is operational on following VLANs       : 20,30

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted
---------------         -------
xe1                     Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------
```

Table 3-2 explains the fields in the output.

Table 3-2: show ip dhcp snooping bridge fields

Field	Description
Bridge Group	Bridge number
DHCP snooping is	Whether DHCP snooping is enabled

Table 3-2: show ip dhcp snooping bridge fields (Continued)

Field	Description
DHCP snooping option82 is	Whether DHCP snooping option 82 is enabled
Verification of hwaddr field is	Whether verification of hwaddr field is enabled
Strict validation of DHCP packet is	Whether strict validation of DHCP packets is enabled
DB Write Interval(secs)	Database write interval in seconds
DHCP snooping is configured on following VLANs	VLANs on which DHCP snooping is enabled
DHCP snooping is operational on following VLANs	VLANs on which DHCP snooping is operating
Interface	Interface name
Trusted	Whether DHCP snooping trust is enabled on the interface
Source Guard	Whether DHCP snooping IP source guard is enabled on the interface

show ip dhcp snooping binding bridge

Use this command to display the DHCP snooping binding table.

Command Syntax

```
show ip dhcp snooping binding bridge <1-32>
```

Parameters

<1-32>	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                    : 0
Total number of dynamic IPV4 entries                   : 2
Total number of static IPV6 entries                    : 0
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   --------------
3cfd.fe0b.06e0       12.12.12.10       30         dhcp-snooping   20     xe12

3cfd.fe0b.06e0       30.30.30.30       480        dhcp-snooping   30     xe12
```

Table 3-3 explains the output .

Table 3-3: show ip dhcp snooping binding bridge fields

Field	Description
Total number of static IPV4 entries	Number of static IPV4 entries.
Total number of dynamic IPV4 entries	Number of dynamic IPV4 entries.
Total number of static IPV6 entries	Number of static IPV6 entries.
Total number of dynamic IPV6 entries	Number of dynamic IPV6 entries .
MacAddress	MAC address of the interface.
IP Address	IP address of the peer device.
Lease (sec)	DHCP lease time in seconds provided to untrusted IP addresses.
Type	Configured either statically or dynamically by the DHCP server.

Table 3-3: show ip dhcp snooping binding bridge fields

Field	Description
VLAN	Identifier of the number.
Interface	Interface is being snooped.

CHAPTER 4 IP Source Guard Commands

This chapter describes the commands for IP Source Guard (IPSG):

- hardware-profile filter ipsg
- hardware-profile filter ipsg-ipv6
- ip verify source dhcp-snooping-vlan

hardware-profile filter ipsg

Use this command to enable or disable the ingress IPSG TCAM group for IPv4.

Command Syntax

```
hardware-profile filter ipsg (disable | enable)
```

Parameters

`enable`	Enable the ingress IPSG TCAM group
`disable`	Disable the ingress IPSG TCAM group

Default

N/A

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)# hardware-profile filter ipsg enable
```

hardware-profile filter ipsg-ipv6

Use this command to enable or disable the ingress IPSG TCAM group for IPv6.

Command Syntax

```
hardware-profile filter ipsg-ipv6 (disable | enable)
```

Parameters

`enable`	Enable the ingress IPSG TCAM group
`disable`	Disable the ingress IPSG TCAM group

Default

N/A

Command Mode

Config mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)# hardware-profile filter ipsg-ipv6 disable
```

ip verify source dhcp-snooping-vlan

Use this command to enable the IPSG feature at the interface level.

Use the no form of this command to disable the IPSG on an interface.

Command Syntax

```
ip verify source dhcp-snooping-vlan
no ip verify source dhcp-snooping-vlan
```

Parameters

None

Default

N/A

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip verify source dhcp-snooping-vlan

(config-if)#no ip verify source dhcp-snooping-vlan
```

CHAPTER 5 OSPFv3 IPSec Authentication Commands

This chapter is a reference for the Internet Protocol Security (IPsec) commands for OSPFv3 authentication.

- crypto ipsec transform-set
- crypto map
- set peer
- set session-key
- set transform-set
- sequence
- show crypto ipsec transform-set

crypto ipsec transform-set

Use this command to configure a transform set that defines protocols and algorithm settings to apply to IPSec protected traffic.

During the IPSec security association negotiation, the peers agree to use a particular transform-set to be used for protecting a particular data flow.

Several transform-sets can be specified and associated with a crypto map entry.

A transform set defines the IPSec security protocols: Encapsulation Security Protocol (ESP) or Authentication Header (AH), and also specifies which algorithms to use with the selected security protocol.

Command Syntax

```
crypto ipsec transform-set NAME ah (none|ah-md5|ah-sha1|ah-sha256|ah-sha384|ah-sha512)
crypto ipsec transform-set NAME esp-auth (none|esp-md5|esp-sha1|esp-sha256|espsha384|esp-sha512) esp-enc (esp-null|esp-3des|esp-aes|esp-aes192|esp-aes256|espblf|esp-blf192|esp-blf256|esp-cast)
crypto ipsec transform-set NAME mode (transport)
no crypto ipsec transform-set NAME mode
no crypto ipsec transform-set NAME
```

Parameters

NAME	Name of the transform set.
mode	Change the transform-set mode to tunnel or transport.
transport	The payload (data) of the original IP packet is protected.
ah	Authentication Header protocol provides data authentication.
none	No authentication.
ah-md5	Authentication Header with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
ah-sha1	Authentication Header with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.
ah-sha256	Authentication Header with Secure Hash Algorithm 256 (SHA-256) Hashed Message Authentication Code (HMAC) variant.
ah-sha384	Authentication Header with Secure Hash Algorithm 384 (SHA-384) Hashed Message Authentication Code (HMAC) variant.
ah-sha512	Authentication Header with Secure Hash Algorithm 512 (SHA-512) Hashed Message Authentication Code (HMAC) variant.
esp-auth	Encapsulating Security Payload authentication protocol provides data authentication.
none	No authentication.
esp-md5	Encapsulating Security Payload with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
esp-sha1	Encapsulating Security Payload with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.

esp-sha256	Encapsulating Security Payload with Secure Hash Algorithm 256 (SHA-256) Hashed Message Authentication Code (HMAC) variant.
esp-sha384	Encapsulating Security Payload with Secure Hash Algorithm 384 (SHA-384) Hashed Message Authentication Code (HMAC) variant.
esp-sha512	Encapsulating Security Payload with Secure Hash Algorithm 512 (SHA-512) Hashed Message Authentication Code (HMAC) variant.
esp-enc	Encapsulating Security Payload encryption protocol
esp-null	Encapsulating Security Payload null encryption.
esp-3des	Encapsulating Security Payload with 168-bit DES encryption (3DES or Triple DES).
esp-aes	Alternative AES.
esp-aes192	Alternative AES192.
esp-aes256	Alternative AES256.
esp-blf	Alternative Blowfish.
esp-blf192	Alternative Blowfish192.
esp-blf256	Alternative Blowfish256.
esp-cast	Alternative Cast (IKEv1 not supported).

Command Mode

Configure mode

Example

```
#configure terminal
(config)#crypto ipsec transform-set TEST_ESP esp-auth esp-md5 esp-enc esp-3des
(config)#crypto ipsec transform-set TEST_AH ah ah-sha512
```

crypto map

Use this command to create or change a crypto map entry and enter crypto map configuration mode.

Use the `no` form of this command to delete a crypto map entry or set.

Command Syntax

```
crypto map MAP-NAME ipsec-manual
no crypto map MAP-NAME
```

Parameters

`MAP-NAME`	Name of the crypto map set (maximum length 127).
`ipsec-manual`	Do not use IKE to establish IPSec security associations.

Command Mode

Configure mode

Example

```
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#
```

set peer

Use this command to specify an IPSec peer IPv4 or IPv6 for a crypto map.

Use the `no` form of this command to remove an IPSec peer from a crypto map entry.

Command syntax

```
set peer (A.B.C.D | X:X::X:X) (spi (<0-4096>)|)
no set peer (A.B.C.D | X:X::X:X)
```

Parameters

`A.B.C.D`	IPv4 peer address
`X:X:X:X`	IPv6 peer address
`spi`	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association.
`<0-4096>`	Security parameter index (SPI) range

Default

None

Command Mode

Crypto map sequence mode

Applicability

This command is introduced in OcNOS version 6.0.0

Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set transform-set TEST_ESP
(config-crypto-seq)#set peer fe80::3617:ebff:fe0e:1222 spi 200
```

set session-key

Use this command to define IPSec keys for security associations via ipsec-manual crypto map entries.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map.

Session keys at one peer must match the session keys at the remote peer.

Command syntax

```
set session-key (inbound|outbound) esp SPI cipher HEX-KEY-DATA authenticator HEX-
  KEY-DATA
no set session-key (inbound|outbound) esp SPI
```

Parameters

`inbound`	Sets the inbound IPSec session key. Both inbound and outbound keys must be set.
`outbound`	Sets the outbound IPSec session key. Both inbound and outbound keys must be set.
`esp`	Sets the IPSec session key for the Encapsulation Security Protocol.
`SPI`	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association.
`cipher`	Indicates that the key string is to be used with the ESP encryption.
`HEX-KEY-DATA`	Specifies the session key in hexadecimal format.
`authenticator`	Indicates that the key string is to be used with the ESP authentication.

Default

None

Command Mode

Crypto map sequence mode

Applicability

This command is introduced in OcNOS version 6.0.0

Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set session-key outbound esp 200 cipher
12345678123456781234567812345678123456781234567812345678 authenticator
123456781234567812345678
(config-crypto-seq)#set session-key inbound esp 200 cipher
12345678123456781234567812345678123456781234567812345678  authenticator
123456781234567812345678
```

set transform-set

Use this command to specify which transform sets to include in a crypto map entry.

Use no form of this command to unset the transform set.

Command syntax

```
set transform-set NAME
no set transform-set NAME
```

Parameters

NAME	Transform-set name

Default

None

Command Mode

Crypto map sequence mode

Applicability

This command is introduced in OcNOS version 6.0.0

Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#set transform-set TEST_ESP
```

sequence

The number you assign to the seq-num will be used to rank multiple crypto map entries within a crypto map set. This number defines the priority of crypto-map evaluation within a crypto map set.

Command syntax

```
sequence <1-65535>
no sequence <1-65535>
```

Parameters

<1-65535>	Value for crypto map sequence number

Default

None

Command Mode

Crypto map mode

Applicability

This command is introduced in OcNOS version 6.0.0

Examples

```
#configure terminal
(config)#crypto map MAP1 ipsec-manual
(config-crypto)#sequence 1
(config-crypto-seq)#
```

show crypto ipsec transform-set

Use this command to show the IPsec transform-set entries.

Command syntax

```
show crypto ipsec transform-set NAME
```

Parameters

NAME	Transform-set name

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command is introduced in OcNOS version 6.0.0

Examples

```
#show crypto ipsec transform-set TEST_ESP
Transform set t3
  Mode is Transport
  Algorithm none esp-3des esp-md5
```

Port Breakout Configuration

CHAPTER 1 Port Breakout (100G) on Qumran2

Overview

Port breakout enables 100GbE ports to be broken out into 4x10GbE, 4x25GbE, and 2x50GbE ports through a secure, highly reliable breakout cabling solution. Networks require a mix of 10Gb, 25Gb, 40Gb, and 100Gb Ethernet interface speeds able to utilize the widest range of flexible connectivity options and it require a variety of cost-effective cabling options for both addressing connectivity and allowing for simple migrations as network speeds and density requirements evolve.

Port breakout feature provides flexibility in splitting 100G to 4X10G, 4X25G, 2X50G, and vice-versa. 100G splittable ports are called control ports. Ports which are members of a control port are called subsidiary ports. When you do port breakout on 100g (ce3) port into 4X10g, the original port (ce3) will be removed and four 10g ports will be added as ce3/1, ce3/2, ce3/3, and ce3/4. On this breakout port you can do the all L2 and L3 features like on a normal port.

When port breakout is un-configured, the breakout ports (ce3/1, ce3/2, ce3/3, ce3/4) will be removed and the original port (ce3) will be added back.

Limitations

- Port Breakout is supported on all 100g interfaces except the ports having an external phy. These external phy ports can be seen using command `show hsl extphy status`.
- You cannot change one port breakout mode (4X10G, 4X25G) to the other mode (4X10G, 4X25G) directly. You must remove the breakout configuration to change the mode.
- Port breakout is not supported on ports which contains sub-interfaces or any other services running over it. To breakout, all services on the interfaces need to be un-configured. After breakout, all the services can be configured on breakout ports.
- While configuring port-breakout, you need to reduce the speed of some interface if this error message is displayed: “%% Max egress credit limit reached”. This is due to hardware limitation.

Topology

© 2025 IP Infusion Inc. Proprietary

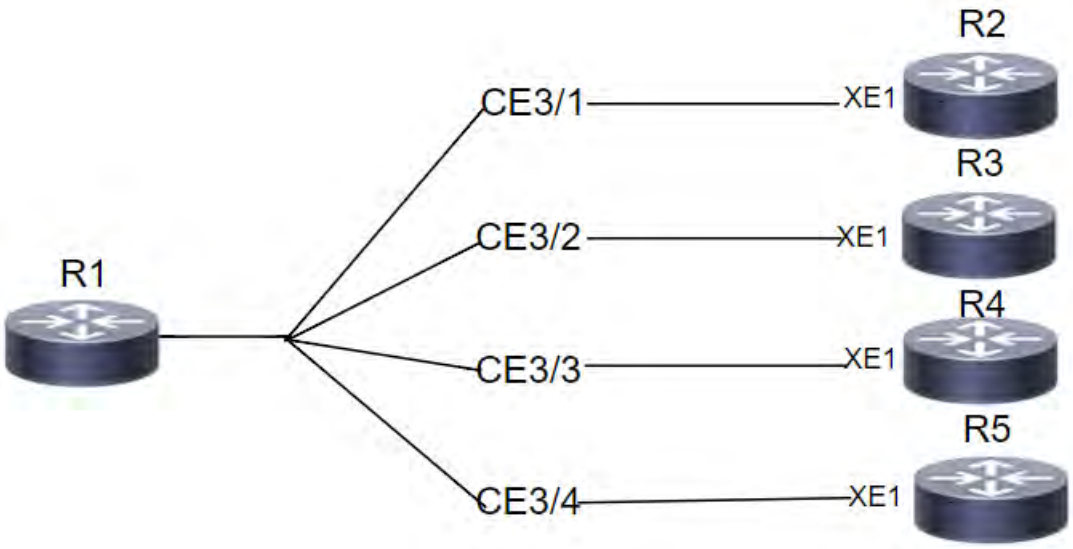


Figure 1-17: Sample Port Breakout Topology

Port Breakout 4X10g

Breakout 100g port (ce3) into 4X10g as (ce3/1, ce3/2, ce3/3, ce3/4).

Configuration

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#port ce3 breakout 4X10g`	Breakout 100g port ce3 into 4X10g as (ce3/1, ce3/2, ce3/3, ce3/4).
`OcNOS(config)#commit`	Commit the configuration.

Validation

```
OcNOS#sh run int ce3
% Can't find interface ce3.
OcNOS#sh run int ce3/1
!
interface ce3/1
!
OcNOS#sh run int ce3/2
!
interface ce3/2
!
OcNOS#sh run int ce3/3
!
interface ce3/3
!
OcNOS#sh run int ce3/4
!
interface ce3/4
```

```
!

OcNOS#sh int br

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                              Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    40g   --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
ce3/1         ETH           --    routed           down    PD      10g   --       No  No
ce3/2         ETH           --    routed           down    PD      10g   --       No  No
ce3/3         ETH           --    routed           down    PD      10g   --       No  No
ce3/4         ETH           --    routed           down    PD      10g   --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
ce6           ETH           --    routed           down    PD      100g  --       No  No
ce7           ETH           --    routed           down    PD      100g  --       No  No
ce8           ETH           --    routed           down    PD      100g  --       No  No
ce9           ETH           --    routed           down    PD      100g  --       No  No
ce10          ETH           --    routed           down    PD      100g  --       No  No
ce11          ETH           --    routed           down    PD      100g  --       No  No
ce12          ETH           --    routed           down    PD      100g  --       No  No
ce13          ETH           --    routed           down    PD      100g  --       No  No
ce14          ETH           --    routed           up      none    40g   --       No  No
ce15          ETH           --    routed           up      none    40g   --       No  No
ce16          ETH           --    routed           down    PD      100g  --       No  No
ce17          ETH           --    routed           down    PD      100g  --       No  No
ce18          ETH           --    routed           down    PD      100g  --       No  No
ce19          ETH           --    routed           down    PD      100g  --       No  No
ce20          ETH           --    routed           down    PD      100g  --       No  No
ce21          ETH           --    routed           down    PD      100g  --       No  No
ce22          ETH           --    routed           down    PD      100g  --       No  No
ce23          ETH           --    routed           down    PD      100g  --       No  No
ce24          ETH           --    routed           down    PD      100g  --       No  No
ce25          ETH           --    routed           down    PD      100g  --       No  No
ce26          ETH           --    routed           down    PD      100g  --       No  No
ce27          ETH           --    routed           down    PD      100g  --       No  No
```

```
ce28          ETH           --    routed           down    PD      100g  --       No  No
```

Port Breakout 4X25g

Breakout 100g port (ce3) into 4X25g as (ce3/1, ce3/2, ce3/3, ce3/4).

Configuration

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#port ce3 breakout 4X25g`	Breakout 100g port ce3 into 4X25g as (ce3/1, ce3/2, ce3/3, ce3/4).
`OcNOS(config)#commit`	Commit the configuration.

Validation

```
OcNOS#sh run int ce3
% Can't find interface ce3.
OcNOS#sh run int ce3/1
!
interface ce3/1
!
OcNOS#sh run int ce3/2
!
interface ce3/2
!
OcNOS#sh run int ce3/3
!
interface ce3/3
!
OcNOS#sh run int ce3/4
!
interface ce3/4
!

OcNOS#sh int br

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
```

```
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
-------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    40g   --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
ce3/1         ETH           --    routed           down    PD      25g   --       No  No
ce3/2         ETH           --    routed           down    PD      25g   --       No  No
ce3/3         ETH           --    routed           down    PD      25g   --       No  No
ce3/4         ETH           --    routed           down    PD      25g   --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
ce6           ETH           --    routed           down    PD      100g  --       No  No
ce7           ETH           --    routed           down    PD      100g  --       No  No
ce8           ETH           --    routed           down    PD      100g  --       No  No
ce9           ETH           --    routed           down    PD      100g  --       No  No
ce10          ETH           --    routed           down    PD      100g  --       No  No
ce11          ETH           --    routed           down    PD      100g  --       No  No
ce12          ETH           --    routed           down    PD      100g  --       No  No
ce13          ETH           --    routed           down    PD      100g  --       No  No
ce14          ETH           --    routed           up      none    40g   --       No  No
ce15          ETH           --    routed           up      none    40g   --       No  No
ce16          ETH           --    routed           down    PD      100g  --       No  No
ce17          ETH           --    routed           down    PD      100g  --       No  No
ce18          ETH           --    routed           down    PD      100g  --       No  No
ce19          ETH           --    routed           down    PD      100g  --       No  No
ce20          ETH           --    routed           down    PD      100g  --       No  No
ce21          ETH           --    routed           down    PD      100g  --       No  No
ce22          ETH           --    routed           down    PD      100g  --       No  No
ce23          ETH           --    routed           down    PD      100g  --       No  No
ce24          ETH           --    routed           down    PD      100g  --       No  No
ce25          ETH           --    routed           down    PD      100g  --       No  No
ce26          ETH           --    routed           down    PD      100g  --       No  No
ce27          ETH           --    routed           down    PD      100g  --       No  No
```

Port Breakout 2X50g

Breakout 100g port (ce3) into 2X50g as (ce3/1, ce3/2).

Configuration

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#port ce3 breakout 2X50g`	Breakout 100g port ce3 into 2X50g as (ce3/1, ce3/2).
`OcNOS(config)#commit`	Commit the configuration.

Validation

```
OcNOS#sh run int ce3
% Can't find interface ce3.
OcNOS#sh run int ce3/1
!
interface ce3/1
!
OcNOS#sh run int ce3/2
!
interface ce3/2
!

OcNOS#sh int br

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                                 Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    40g   --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
ce3/1         ETH           --    routed           down    PD      50g   --       No  No
ce3/2         ETH           --    routed           down    PD      50g   --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
ce6           ETH           --    routed           down    PD      100g  --       No  No
ce7           ETH           --    routed           down    PD      100g  --       No  No
ce8           ETH           --    routed           down    PD      100g  --       No  No
ce9           ETH           --    routed           down    PD      100g  --       No  No
ce10          ETH           --    routed           down    PD      100g  --       No  No
ce11          ETH           --    routed           down    PD      100g  --       No  No
ce12          ETH           --    routed           down    PD      100g  --       No  No
ce13          ETH           --    routed           down    PD      100g  --       No  No
ce14          ETH           --    routed           up      none    40g   --       No  No
ce15          ETH           --    routed           up      none    40g   --       No  No
ce16          ETH           --    routed           down    PD      100g  --       No  No
ce17          ETH           --    routed           down    PD      100g  --       No  No
ce18          ETH           --    routed           down    PD      100g  --       No  No
```

```
ce19          ETH           --    routed           down    PD      100g  --       No  No
ce20          ETH           --    routed           down    PD      100g  --       No  No
ce21          ETH           --    routed           down    PD      100g  --       No  No
ce22          ETH           --    routed           down    PD      100g  --       No  No
ce23          ETH           --    routed           down    PD      100g  --       No  No
ce24          ETH           --    routed           down    PD      100g  --       No  No
ce25          ETH           --    routed           down    PD      100g  --       No  No
ce26          ETH           --    routed           down    PD      100g  --       No  No
ce27          ETH           --    routed           down    PD      100g  --       No  No
ce28          ETH           --    routed           down    PD      100g  --       No  No
ce29          ETH           --    routed           down    PD      100g  --       No  No
ce30          ETH           --    routed           down    PD      100g  --       No  No
ce31          ETH           --    routed           down    PD      100g  --       No  No
```

Un-configure Port Breakout

Combine the breakout port back to original port as (ce3).

Configuration

`OcNOS#configure terminal`	Enter configure mode.
`OcNOS(config)#no port ce3 breakout`	Combine the breakout port back to original port as (ce3).
`OcNOS(config)#commit`	Commit the configuration.

Validation

```
OcNOS#sh run int ce3
!
interface ce3
!
OcNOS#sh run int ce3/1
% Can't find interface ce3/1.
OcNOS#sh run int ce3/2
% Can't find interface ce3/2.
OcNOS#sh run int ce3/3
% Can't find interface ce3/3.
OcNOS#sh run int ce3/4
% Can't find interface ce3/4.

OcNOS#sh int br

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
```

```
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                              Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    40g   --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
ce3           ETH           --    routed           down    PD      100g  --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
ce6           ETH           --    routed           down    PD      100g  --       No  No
ce7           ETH           --    routed           down    PD      100g  --       No  No
ce8           ETH           --    routed           down    PD      100g  --       No  No
ce9           ETH           --    routed           down    PD      100g  --       No  No
ce10          ETH           --    routed           down    PD      100g  --       No  No
ce11          ETH           --    routed           down    PD      100g  --       No  No
ce12          ETH           --    routed           down    PD      100g  --       No  No
ce13          ETH           --    routed           down    PD      100g  --       No  No
ce14          ETH           --    routed           up      none    40g   --       No  No
ce15          ETH           --    routed           up      none    40g   --       No  No
```

CHAPTER 2 Port Breakout (100G) on Qumran AX and MX

Port Breakout (100G) for AS5916-54XKS (Qumran-MX) Platform

Overview

The port breakout system AS5916-54XKS device offers support for 48 ports (1-48) with 10GbE SFP+ interfaces, and 6 ports (0-5) with 100GbEQSFP28 interfaces. Port breakout allows the flexibility to divide each 100G QSFP28 port (ce0, ce1, ce2, ce3, ce4, ce5) into (4X25G) configurations.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The advantages of utilizing a 100G port breakout:

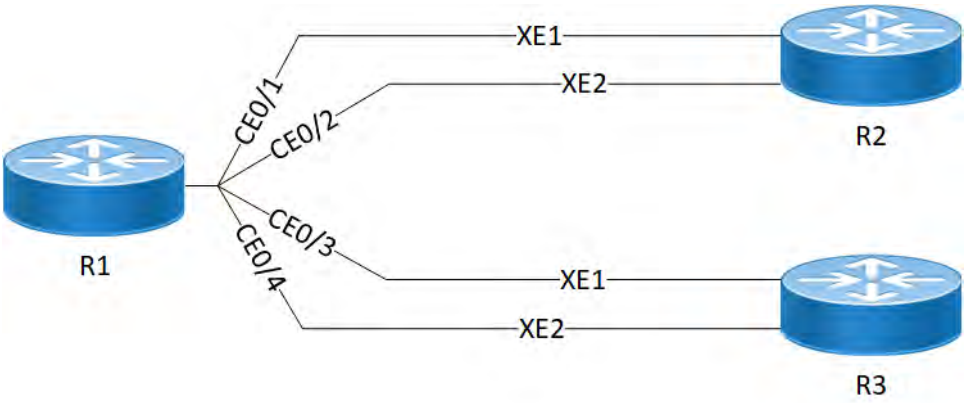
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS5916-54XKS(QMX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce0/1, ce0/2, ce0/3, ce0/4 as shown in the Topology section.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
ce2/1         ETH           --    routed           down    PD      25g   --       No  No
ce2/2         ETH           --    routed           down    PD      25g   --       No  No
ce2/3         ETH           --    routed           down    PD      25g   --       No  No
ce2/4         ETH           --    routed           down    PD      25g   --       No  No
ce3/1         ETH           --    routed           up      none    25g   --       No  No
ce3/2         ETH           --    routed           down    AD      25g   --       No  No
ce3/3         ETH           --    routed           up      none    25g   --       No  No
ce3/4         ETH           --    routed           up      none    25g   --       No  No
ce4/1         ETH           --    routed           down    PD      25g   --       No  No
ce4/2         ETH           --    routed           down    PD      25g   --       No  No
ce4/3         ETH           --    routed           down    PD      25g   --       No  No
ce4/4         ETH           --    routed           down    PD      25g   --       No  No
ce5/1         ETH           --    routed           down    PD      25g   --       No  No
ce5/2         ETH           --    routed           down    PD      25g   --       No  No
ce5/3         ETH           --    routed           down    PD      25g   --       No  No
ce5/4         ETH           --    routed           down    PD      25g   --       No  No

--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
--------------------------------------------------------------------------------
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
Interface                                          Status      Description
--------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --

--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.2      down     PD
```

After reloading the interfaces ce0, ce1, ce2, ce3, ce4, and ce5, the 100G ports are subdivided into four 25G ports, as indicated below.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce0 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           down    PD      100g  --       No  No
ce1           ETH           1     trunk            up      none    100g  --       No  No
ce2           ETH           --    routed           down    PD      100g  --       No  No
ce3           ETH           --    routed           down    PD      100g  --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
```

After reloading the interfaces ce0, ce1, ce2, ce3, ce4, and ce5, all the 4x25G sub-ports will be deleted, and the 100G ports ce0, ce1, ce2, ce3, ce4, and ce5 will be added.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

```
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform

Overview

The AS7315-27X device accommodates a combination of port breakout options with hybrid port speeds. On this device, configure 4 ports (port 1-4) with 25G Ethernet SFP28 interfaces, 20 ports (port 5-24) with 10GbE SFP+ interfaces, and 3 ports (port 25-27) with 100G Ethernet QSFP28 interfaces. Using port breakout, divide the 100G QSFP28 ports (ce0, ce1, and ce2) into 4X25G configurations if desired.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

Enabling breakout mode on network equipment such as switches, routers, and servers introduces innovative approaches for network operators to meet the ever-growing need for higher bandwidth. By incorporating high-speed ports that support breakout functionality, operators can enhance faceplate port density and enable a gradual transition to higher data rates, effectively adapting to evolving bandwidth requirements.

Benefits

The advantages of utilizing a 100G port breakout:

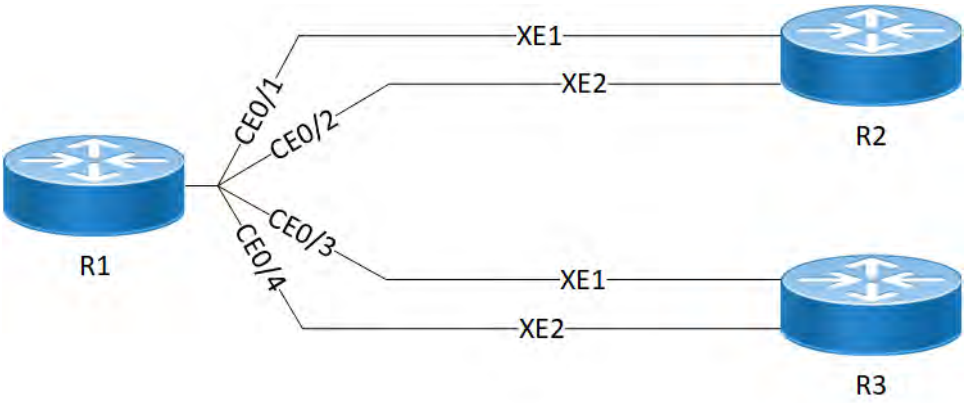
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS7315-27X(QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce/1, ce/2, ce/3, ce/4 as shown in the Topology section.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
```

```
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
ce2/1         ETH           --    routed           up      none    25g   --       No  No
ce2/2         ETH           --    routed           down    PD      25g   --       No  No
ce2/3         ETH           --    routed           up      none    25g   --       No  No
ce2/4         ETH           --    routed           up      none    25g   --       No  No
```

After reloading the interfaces ce/1, ce/2, ce/3, and ce/4, the 100G ports are subdivided into four 25G ports, as indicated below.

```
 ce0 - ce0/1,ce0/2,ce0/3,ce0/4
 ce1 - ce1/1,ce1/2,ce1/3,ce1/4
 ce2 - ce2/1,ce2/2,ce21/3,ce2/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce49 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    100g  --       No  No
ce2           ETH           --    routed           up      none    100g  --       No  No
```

After reloading the interfaces ce/1, ce/2, ce/3, and ce/4, all the 4x25G sub-ports will be deleted, and the 100G ports ce/1, ce/2, ce/3, and ce/4 will be added.

```
ce0/1,ce0/2,ce0/3,ce0/4
ce1/1,ce1/2,ce1/3,ce1/4
ce2/1,ce2/2,ce21/3,ce2/4
```

Port Breakout (100G) for 26XAS7316-26XB (Qumran-AX) Platform

Overview

The AS7316-26XB supports 16 (port 1-16) 10GbE SFP+ ports, 8 (port 17-24) 25GbE SFP28 ports and 2 (25-26) 100 GbE QSFP28 ports. We can split only the 100G QSFP28 (ce0,ce1)ports into 4X25G. Breakout not supported for other ports.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The advantages of utilizing a 100G port breakout:

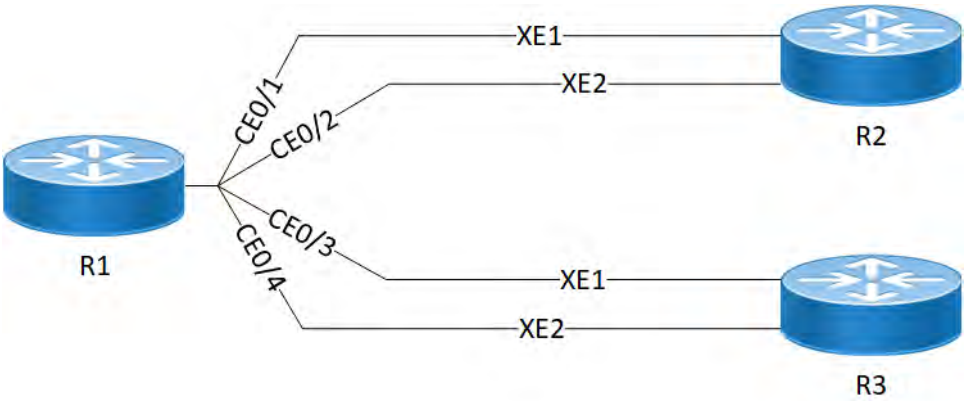
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



AS7316-26XB (QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce0/1, ce0/2, ce0/3, ce0/4 as shown in the Topology section.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
```

```
-------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
-------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No

-------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
-------------------------------------------------------------------------------
eth0          METH             up      --      1g


-------------------------------------------------------------------------------
Interface                                          Status      Description
-------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --

-------------------------------------------------------------------------------
Interface    Status   Reason
-------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.2      down     PD
```

After reloading the interfaces ce0 and ce1 the 100G ports are subdivided into four 25G ports, as indicated below.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce0 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           down    PD      100g  --       No  No
ce1           ETH           1     trunk            up      none    100g  --       No  No
```

After reloading the interfaces ce0/1, ce0/2, ce0/3, and ce0/4 all the 4x25G sub-ports will be deleted, and the 100G ports ce0 and ce1 will be added.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform

Overview

The S9500-30XS supports 20 (port 1-20) 10GbE SFP+ ports, 8 (port 21-28) 25GbE SFP28 ports and 2 (29-30) 100 GbE QSFP28 ports. We can split only the 100G QSFP28 (ce0,ce1)ports into 4X25G. Breakout not supported for other ports.

Note: The port breakout functionality is not supported on ports other than these designated ports.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

Enabling breakout mode on network equipment such as switches, routers, and servers introduces innovative approaches for network operators to meet the ever-growing need for higher bandwidth. By incorporating high-speed ports that support breakout functionality, operators can enhance faceplate port density and enable a gradual transition to higher data rates, effectively adapting to evolving bandwidth requirements.

Benefits

The advantages of utilizing a 100G port breakout:

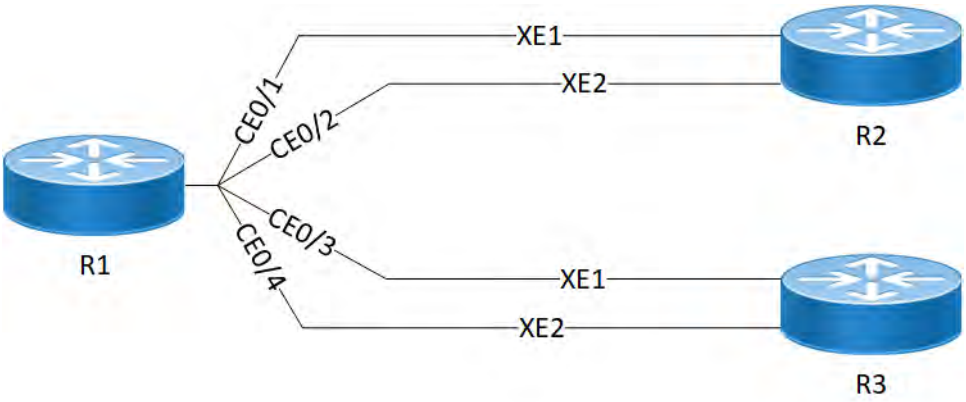
- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades.

Configuration

By default, mode 1 designates the board with 100G ports. If you switch it to mode 2, all 100G ports will be divided into 4x25G ports. To split a 100G port into 4x25G ports, use the following command, save the configuration, and then reload the device.

Topology

The platform supports splitting a single 100G QSFP28 port into the following 4x25G ports.



SP9500-30XS (QAX) 100G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`R1#configure terminal`	Enter Configuration mode.

`R1(config)#hardware-profile port-config mode2`	Breakout 100G ports into 4x25G ports called as ce1/1, ce1/2, ce1/3, ce1/4 as shown in the Topology section.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
OcNOS#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0/1         ETH           --    routed           down    PD      25g   --       No  No
ce0/2         ETH           --    routed           down    PD      25g   --       No  No
ce0/3         ETH           --    routed           down    PD      25g   --       No  No
ce0/4         ETH           --    routed           down    PD      25g   --       No  No
ce1/1         ETH           --    routed           up      none    25g   --       No  No
ce1/2         ETH           --    routed           up      none    25g   --       No  No
ce1/3         ETH           --    routed           up      none    25g   --       No  No
ce1/4         ETH           --    routed           up      none    25g   --       No  No
```

After reloading the interfaces ce0 and ce1, the 100G ports are subdivided into four 25G ports, as indicated below.

```
 ce0 - ce0/1,ce0/2,ce0/3,ce0/4
 ce1 - ce1/1,ce1/2,ce1/3,ce1/4
```

Unconfigure Port Breakout

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce49 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

R1

The following table outlines the unconfiguration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)#hardware-profile port-config mode1`	Combine the breakout port to its original port throughput capabilities.
`R1(config)#commit`	Commit the configuration.

Validation

Use this command to validate the port breakout unconfiguration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed            up      none    100g  --       No  No
ce1           ETH           --    routed            up      none    100g  --       No  No
```

After reloading the interfaces ce1/1, ce1/2, ce1/3, and ce1/4, all the 4x25G sub-ports will be deleted, and the 100G ports ce0, ce1, will be added.

```
 ce0/1,ce0/2,ce0/3,ce0/4-ce0
 ce1/1,ce1/2,ce1/3,ce1/4-ce1
```

CHAPTER 3 Port Breakout (400G) on Qumran2

Overview

The port breakout capability offers a robust and secure solution for divide 400GbE ports into multiple port, ensuring a reliable network infrastructure. In today's networks, there's a demand for a diverse range of Ethernet interface speeds, including 10GbE, 25GbE, 40GbE, and 100GbE. It is essential to have a variety of cost-effective cabling options. This flexibility is crucial to address connectivity requirements and facilitate seamless migrations as network speeds and density needs continue to evolve.

Each 400GbE port (QSFP-DD) has the capacity to support up to eight SERDES, with each SERDES capable of delivering 50G of bandwidth. This capability allows for the following port configurations. The default SERDES mode operates at 50G.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The 400G platforms empower data centers and high-performance computing environments to meet the increasing demand for greater bandwidth at a reduced cost and power consumption per gigabit. Some key benefits of these platforms include:

• Upgrades from 100G to 400G systems increases the available switching bandwidth by a factor of 4, effectively addressing the need for higher data throughput.

• Enables the use of optical or copper breakouts to create higher density 100G ports, providingmore options for data connectivity and transmission.

• Reduces the number of optical fiber links, connectors, and patch panels required, achieving a fourfold reduction in infrastructure components when compared to 100G platforms with the same aggregate bandwidth. This reduction contributes to cost savings and simplifies network management.

Configuration

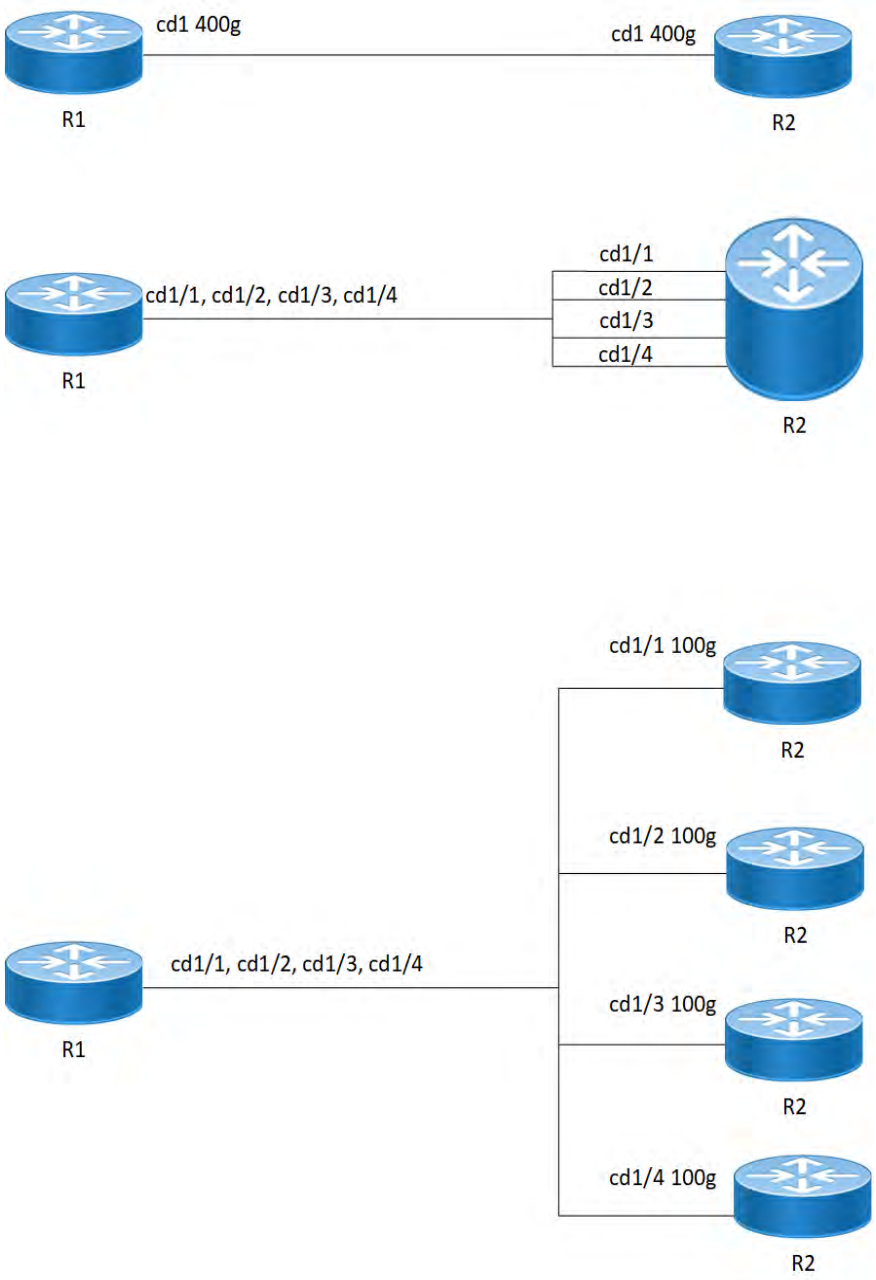
Use the `config# qsfp dd application` command to select the application ID to be configured for this QSFP-DD module.

Note: Only 400G application modes are supported.

Use the `show qsfp ddport no > advertisement applications` command to check the application modes.

Topology

The platform supports splitting a single 400G (QSFP-DD) port into any of the following ports.



400G Port Breakout Configuration

R1

The following table outlines the configuration steps for dividing a single port into multiple ports through channelization.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`R1(config-qsfp-dd)#application 3`	Select the application ID to be configured for this QSFP-DD module.
`R1(config)#commit`	Commit the configuration.

EEPROM Details for ZR+ Optics

The below show command displays output for “SO-TQSFPDD4CCZRP” optics.

Execute the “`show qsfp-dd 3 eeprom`” command in the terminal window.

```
Port Number                    : 3
Identifier                     : QSFP-DD Double Density 8X Pluggable Transceiver
Name                           : SmartOptics
OUI                            : 0x0 0x53 0x4f
Part No                        : SO-TQSFPDD4CCZRP
Revision Level                 : A
Serial_Number                  : 223950575
Manufacturing Date             : 220926   (yymmddvv, v=vendor specific)
Module Power Class             : 8
Module Max Power               : 23.75 Watt
Cooling Implemented            : Yes
Module Temperature Max         : 80 Celsius
Module Temperature Min         : 0 Celsius
Operating Voltage Min          : 3.12 Volt
Optical Detector               : PIN
Rx Power Measurement           : Average Power
Tx Disable Module Wide         : No
Cable Assembly Link Length     : Separable Media
Connector Type                 : LC (Lucent Connector)
Media Interface Technology     : 1550 nm DFB
CMIS Revision                  : 4.1
Memory Model                   : Paged
MCI Max Speed                  : 1000 kHz
Active Firmware Revision       : 61.20
Inactive Firmware Revision     : 61.20
Hardware Revision              : 1.2
Media Type                     : Optical SMF
Max SMF Link Length            : 630.0 Kilometer
Wavelength Nominal             : 1547.70 nm
Wavelength Tolerance           : 166.55 nm
```

Port Breakout Configuration

Use this command to configure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

R1#configure terminal	Enter Configuration mode.
R1(config)# qsfp-dd 49	Enter the QSFP-DD mode.
R1(config-qsfp-dd)#application 3	Configure the required application number. The supported range is from <2 to 15>.
R1(config-qsfp-dd)#commit	Commit the configuration.
R1(config-qsfp-dd)#exit	Exit from the QSFP-DD configuration mode.
R1(config)#port cd49 breakout 4X100g	Enable port breakout
R1(config)# commit	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
R1#show qsfp-dd 49 application

Port Number                     : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 3  |   Application 3

R1#show qsfp-dd 49 advertisement applications

Port Number                    : 49
> Application 1:
    | Host |
         Interface             : 400GAUI-8 C2M
         Application BR        : 425.00
         Lane Count            : 8
         Lane Sig BR           : 26.5625
         Modulation Format     : PAM4
         Bits Per Unit Intvl   : 2.000000
         Lane Assigned         : Lane-1
    | Media |
         Interface             : 400ZR, DWDM, Amplified
         Application BR        : 478.75
         Lane Count            : 1
         Lane Sig BR           : 59.84375
         Modulation Format     : DP-16QAM
         Bits Per Unit Intvl   : 8.000000
         Lane Assigned         : Lane-1
  Application 2:
    | Host |
         Interface             : 400GAUI-8 C2M
         Application BR        : 425.00
```

```
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
    | Media |
        Interface            : 400ZR, Single Wavelen., Unamp.
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 3:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : 400ZR, DWDM, Amplified
        Application BR       : 478.75
        Lane Count           : 1
        Lane Sig BR          : 59.84375
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
        Lane Assigned        : Lane-1
Application 4:
    | Host |
        Interface            : 400GAUI-8 C2M
        Application BR       : 425.00
        Lane Count           : 8
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-1
    | Media |
        Interface            : ZR400-OFEC-16QAM
        Application BR       : 481.108374
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-16QAM
        Bits Per Unit Intvl  : 8.000000
```

```
       Lane Assigned        : Lane-1
Application 5:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR400-OFEC-16QAM
       Application BR       : 481.108374
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-16QAM
       Bits Per Unit Intvl  : 8.000000
       Lane Assigned        : Lane-1
Application 6:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR300-OFEC-8QAM
       Application BR       : 360.831281
       Lane Count           : 1
       Lane Sig BR          : 60.1385468
       Modulation Format    : DP-8QAM
       Bits Per Unit Intvl  : 6.000000
       Lane Assigned        : Lane-1
Application 7:
  | Host |
       Interface            : 100GAUI-2 C2M
       Application BR       : 106.25
       Lane Count           : 2
       Lane Sig BR          : 26.5625
       Modulation Format    : PAM4
       Bits Per Unit Intvl  : 2.000000
       Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
  | Media |
       Interface            : ZR200-OFEC-QPSK
```

```
        Application BR       : 240.554187
        Lane Count           : 1
        Lane Sig BR          : 60.1385468
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
  Application 8:
    | Host |
        Interface            : 100GAUI-2 C2M
        Application BR       : 106.25
        Lane Count           : 2
        Lane Sig BR          : 26.5625
        Modulation Format    : PAM4
        Bits Per Unit Intvl  : 2.000000
        Lane Assigned        : Lane-7/Lane-5/Lane-3/Lane-1
    | Media |
        Interface            : ZR100-OFEC-QPSK
        Application BR       : 120.277094
        Lane Count           : 1
        Lane Sig BR          : 30.069273
        Modulation Format    : DP-QPSK
        Bits Per Unit Intvl  : 4.000000
        Lane Assigned        : Lane-1
```

Port Breakout Interfaces

Use this command to configure the to see the interfaces after the port breakout.

```
R1#show interface brief | include cd49
cd49/1        ETH           --    routed           up      none    100g  --       No  No
cd49/2        ETH           --    routed           up      none    100g  --       No  No
cd49/3        ETH           --    routed           up      none    100g  --       No  No
cd49/4        ETH           --    routed           up      none    100g  --       No  No
```

Port Breakout Unconfiguration

Use this command to unconfigure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`R1(config-qsfp-dd)#no application`	Remove the application.

R1(config-qsfp-dd)#commit	Commit the configuration.
R1(config-qsfp-dd)#exit	Exit from the QSFP-DD configuration mode.
R1(config)#no port cd49 breakout	Remove the port breakout. Your port will revert to functioning as a 400G port.
R1(config)# commit	Commit the configuration.

```
R1#show qsfp-dd 49 application

Port Number                    : 49
----------------------------------
   User Config    |   H/W Config
----------------------------------
   Application 1  |   Application 1

R1#show interface brief | include cd49
cd49        ETH           --    routed            up      none    400g  --       No  No
```

Port Breakout Configuration with serdes 25g

Use this command to configure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

R1#configure terminal	Enter Configuration mode.
R1(config)# qsfp-dd 49	Enter the QSFP-DD mode.
R1(config-qsfp-dd)#application 12	Configure the required application number. The accepted range is from 2 to 15.
R1(config-qsfp-dd)#commit	Commit the configuration.
R1(config-qsfp-dd)#exit	Exit from the QSFP-DD configuration mode.
R1(config)#port cd49 breakout 2X100g serdes 25g	Configure port breakout with 25G Serdes.
R1(config)# commit	Commit the configuration.

Validation

Use this command to validate the port breakout configuration.

```
R1#show qsfp-dd 49 application

Port Number                    : 49
----------------------------------
   User Config    |   H/W Config
----------------------------------
   Application 12  |   Application 12
```

Port Breakout Interfaces

Use this command to configure the to see the interfaces after the port breakout.

```
R1#show interface brief | include cd49
cd49/1        ETH           --    routed           up      none    100g  --       No  No
cd49/2        ETH           --    routed           up      none    100g  --       No  No
```

Port Breakout Unconfiguration with serdes 25g

Use this command to unconfigure the port breakout on the QSFP-DD module.

R1

The following table outlines the configuration steps for port breakout.

`R1#configure terminal`	Enter Configuration mode.
`R1(config)# qsfp-dd 49`	Enter the QSFP-DD mode.
`R1(config-qsfp-dd)#no application`	Remove the application
`R1(config-qsfp-dd)#commit`	Commit the configuration.
`R1(config-qsfp-dd)#exit`	Exit from the QSFP-DD configuration mode.
`R1(config)#no port cd49 breakout`	Remove the port breakout. Your port will revert to functioning as a 400G port.
`R1(config)# commit`	Commit the configuration.

```
R1#show qsfp-dd 49 application

Port Number                    : 49
-----------------------------------
   User Config    |   H/W Config
-----------------------------------
   Application 1  |   Application 1

R1#show interface brief | include cd49
cd49        ETH           --    routed           up      none    400g  --       No  No
```

CHAPTER 4 Dynamic Port Breakout (100G) on Qumran AX and MX

Overview

Dynamic port breakout is a feature in networking equipment, particularly in switches and routers, that allows for the dynamic allocation of physical ports to different speeds and protocols based on the connected devices requirements. It enhances the network flexibility, scalability, and cost-efficiency by dynamically adapting switch port configurations to meet the evolving demands of modern networking environments.

The port breakout functionality supports the division of 100GbE ports into distinct configurations, such as 4x10GbE, 4x25GbE, and 2x50GbE, using a secure and highly reliable breakout cabling solution. Networks today demand a combination of interface speeds, including 10Gb, 25Gb, 40Gb, and 100Gb Ethernet, to accommodate a diverse range of flexible connectivity options. Additionally, cost-effective cabling solutions are crucial to address connectivity needs and facilitate smooth migrations as network speeds and density requirements evolve.

The port breakout feature offers the flexibility to split a 100G port into 4X10G, 4X25G, 2X50G, and vice versa. When performing a port breakout on the 100G port (ce1), the original port (ce1) is replaced by four 10G ports, namely ce1/1, ce1/2, ce1/3, and ce1/4. All Layer 2 (L2) and Layer 3 (L3) features applicable to normal ports can be executed on these breakout ports.

In the event of un-configuring the port breakout, the breakout ports (ce1/1, ce1/2, ce1/3, ce1/4) will be removed, and the original 100G port (ce1) will be reinstated. This seamless process allows for efficient management and adaptation of network configurations based on evolving needs.

Feature Characteristics

Breakout configurations facilitate the connection between network devices with varying port speeds, allowing for the optimal utilization of port bandwidth.

The breakout mode on network equipment, such as switches, routers, and servers, opens up new possibilities for network operators to keep up with the pace of bandwidth demand. By adding high-speed ports that support breakout mode, network operators can increase the front port density and incrementally enable an upgrade to higher data rates.

Benefits

The advantages of utilizing a 100G port breakout:

- Boosts port density and saves on rack space
- Reduces power consumption
- Facilitates future upgrades
- No reload is necessary after performing the dynamic port breakout.

Prerequisites

- The board must be up and running with the appropriate build.

Limitations

- Port Breakout is supported on all 100g interfaces except the ports having an external phy. These external phy ports can be seen using command show hsl extphy status.
- You cannot change one port breakout mode (4X10G, 4X25G) to the other mode (4X10G, 4X25G) directly. You must remove the breakout configuration to change the mode.
- Port breakout is not supported with ports hosting sub-interfaces or other active services. To enable breakout, all services on the interfaces must be un-configured first. After breakout, services can be reconfigured on the breakout ports.

Configuration

By default, the device is supported with 100G ports interfaces such as ce0, ce1, ce2, and ce3. Following a breakout, all 100G ports will be divided into 4x10G, 4x25G, and 2x50G ports. The following configuration steps outlines for dividing a single port into multiple ports through channelization.

1. To break a port into multiple ports, execute the following command in the config mode.
   ```
   R1#configure terminal
   R1(config)#port ce1 breakout 4X10g
   ```
   Breakout 100G ports into 4x10G ports called as ce1/1, ce1/2, ce1/3, ce1/4 as shown in the Configuration section.

Sample running configuration

Use this command for the sample running configuration.

```
OcNOS#show running-config
!
! Software version: EC_AS5916-54X-OcNOS-CSR-6.5.1.55-EFT 04/23/2024 05:04:43
!
!Last configuration change at 16:38:03 UTC Thu Apr 11 2019 by ocnos
!
feature netconf-ssh vrf management
feature netconf-tls vrf management
no feature netconf-ssh
no feature netconf-tls
no service password-encryption
!
logging console 5
logging monitor 5
logging cli
logging level all 2
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
!
hardware-profile filter qos-ext enable
hardware-profile statistics voq-full-color enable
hardware-profile statistics ingress-acl disable
hardware-profile statistics cfm-ccm enable
!
```

```
ip vrf management
!
qos enable
qos statistics
!
port ce1 breakout 4X10g
no ip domain-lookup
ip domain-lookup vrf management
ip name-server vrf management 10.12.3.23
bridge 1 protocol rstp vlan-bridge
tfo Disable
errdisable cause stp-bpdu-guard
no feature telnet vrf management
no feature telnet
feature ssh vrf management
no feature ssh
no aaa local authentication password-policy
feature dns relay
ip dns relay
ipv6 dns relay
feature ntp vrf management
ntp enable vrf management
feature rsyslog vrf management
lldp run
lldp tlv-select basic-mgmt system-name
lldp tlv-select basic-mgmt management-address
!
class-map type qos match-all c2
 match cos 2
!
policy-map type qos p1
 class type qos c2
  police cir 8 gbps
  exit
!
vlan database
 vlan 2-100 bridge 1 state enable
!
interface ce0
!
interface ce1/1
!
interface ce1/2
!
interface ce1/3
!
interface ce1/4
!
interface ce2
!
```

```
interface ce3
 shutdown
!
interface ce4
!
interface ce5
!
interface eth0
 ip vrf forwarding management
 ip address dhcp
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface lo.management
 ip vrf forwarding management
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
interface xe0
!
interface xe1
!
interface xe2
!
interface xe3
!
interface xe4
 shutdown
!
interface xe5
!
interface xe6
!
interface xe7
!
interface xe8
 shutdown
!
interface xe9
 load-interval 30
!
interface xe10
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
 service-policy type qos input p1
```

```
!
interface xe11
!
interface xe12
!
interface xe13
!
interface xe14
!
interface xe15
!
interface xe16
!
interface xe17
!
interface xe18
!
interface xe19
!
interface xe20
!
interface xe21
 switchport
 bridge-group 1
 switchport mode trunk
 switchport trunk allowed vlan all
 load-interval 30
!
interface xe22
!
interface xe23
!
interface xe24
!
interface xe25
!
interface xe26
 speed 1g
!
interface xe27
 speed 1g
!
interface xe28
!
interface xe29
!
interface xe30
!
interface xe31
!
```

```
interface xe32
!
interface xe33
!
interface xe34
!
interface xe35
!
interface xe36
!
interface xe37
!
interface xe38
!
interface xe39
!
interface xe40
!
interface xe41
!
interface xe42
!
interface xe43
!
interface xe44
!
interface xe45
!
interface xe46
!
interface xe47
!
 exit
!
!
end
```

Validation

Use this command to validate the port breakout configuration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
```

```
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                                  Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1/1         ETH           --    routed           down    PD      10g   --       No  No
ce1/2         ETH           --    routed           down    PD      10g   --       No  No
ce1/3         ETH           --    routed           down    PD      10g   --       No  No
ce1/4         ETH           --    routed           down    PD      10g   --       No  No
ce2           ETH           --    routed           down    PD      40g   --       No  No
ce3           ETH           --    routed           up      none    100g  --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No

--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
--------------------------------------------------------------------------------
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
Interface                                          Status      Description
--------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --


--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.100    down     PD
vlan1.200    down     PD


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                                  Ch #
--------------------------------------------------------------------------------
xe0           ETH           --    routed           up      none    10g   --       No  No
xe1           ETH           --    routed           down    PD      10g   --       No  No
xe2           ETH           --    routed           down    PD      10g   --       No  No
xe3           ETH           --    routed           down    PD      10g   --       No  No
xe4           ETH           --    routed           up      none    10g   --       No  No
```

```
xe5          ETH          --    routed          down    PD      10g   --       No  No
xe6          ETH          --    routed          down    PD      10g   --       No  No
xe7          ETH          --    routed          down    PD      10g   --       No  No
xe8          ETH          --    routed          up      none    1g    --       No  No
xe9          ETH          --    routed          up      none    1g    --       No  No
xe10         ETH          --    routed          down    PD      10g   --       No  No
xe11         ETH          --    routed          down    PD      10g   --       No  No
xe12         ETH          --    routed          down    PD      10g   --       No  No
xe13         ETH          --    routed          down    PD      10g   --       No  No
xe14         ETH          --    routed          down    PD      10g   --       No  No
xe15         ETH          --    routed          down    PD      10g   --       No  No
xe16         ETH          --    routed          down    PD      10g   --       No  No
xe17         ETH          --    routed          down    PD      10g   --       No  No
xe18         ETH          --    routed          down    PD      10g   --       No  No
xe19         ETH          --    routed          down    PD      10g   --       No  No
xe20         ETH          --    routed          down    PD      10g   --       No  No
xe21         ETH          --    routed          down    PD      10g   --       No  No
xe22         ETH          --    routed          down    PD      10g   --       No  No
xe23         ETH          --    routed          down    PD      10g   --       No  No
xe24         ETH          --    routed          down    PD      10g   --       No  No
xe25         ETH          --    routed          down    PD      10g   --       No  No
xe26         ETH          --    routed          down    PD      10g   --       No  No
xe27         ETH          --    routed          down    PD      10g   --       No  No
xe28         ETH          --    routed          down    PD      10g   --       No  No
xe29         ETH          --    routed          down    PD      10g   --       No  No
xe30         ETH          --    routed          down    PD      10g   --       No  No
xe31         ETH          --    routed          down    PD      10g   --       No  No
xe32         ETH          --    routed          down    PD      10g   --       No  No
xe33         ETH          --    routed          down    PD      10g   --       No  No
xe34         ETH          --    routed          down    PD      10g   --       No  No
xe35         ETH          --    routed          down    PD      10g   --       No  No
xe36         ETH          --    routed          down    PD      10g   --       No  No
xe37         ETH          --    routed          down    PD      10g   --       No  No
xe38         ETH          --    routed          down    PD      10g   --       No  No
xe39         ETH          --    routed          down    PD      10g   --       No  No
xe40         ETH          --    routed          down    PD      10g   --       No  No
xe41         ETH          --    routed          down    PD      10g   --       No  No
xe42         ETH          --    routed          down    PD      10g   --       No  No
xe43         ETH          --    routed          down    PD      10g   --       No  No
xe44         ETH          --    routed          down    PD      10g   --       No  No
xe45         ETH          --    routed          down    PD      10g   --       No  No
xe46         ETH          --    routed          down    PD      10g   --       No  No
xe47         ETH          --    routed          down    PD      10g   --       No  No
```

The interfaces ce0, ce1, ce2, ce3, ce4, and ce5, the 100G ports are subdivided into four 10G ports, as indicated below.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
```

```
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

Unconfiguration

Combine a port that has been previously split into multiple smaller ports. This command allows you to revert the port to its original combined state. For example, if port ce0 was a 100G port that was broken into four 25G ports, this command will allow you to revert the port to its original state as a 100G port.

1. To revert the breakout of multiple ports to the original configuration, execute the following command in the config mode.
   ```
   R1#configure terminal
   R1(config)#no port ce1 breakout
   ```

Validation

Use this command to validate the dynamic port breakout unconfiguration.

```
R1#show interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down
Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       LBG - Link Bonding Group, MODEM - Link Bonding Modem
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)
       HD  - ESI Hold Timer Down

--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
ce0           ETH           --    routed           up      none    100g  --       No  No
ce1           ETH           --    routed           up      none    100g  --       No  No
ce2           ETH           --    routed           down    PD      40g   --       No  No
ce3           ETH           --    routed           up      none    100g  --       No  No
ce4           ETH           --    routed           down    PD      100g  --       No  No
ce5           ETH           --    routed           down    PD      100g  --       No  No
```

```
--------------------------------------------------------------------------------
Interface     Type             Status  Reason  Speed
--------------------------------------------------------------------------------
eth0          METH             up      --      1g


--------------------------------------------------------------------------------
Interface                                          Status      Description
--------------------------------------------------------------------------------
lo                                                 up          --
lo.management                                      up          --


--------------------------------------------------------------------------------
Interface    Status   Reason
--------------------------------------------------------------------------------
vlan1.1      down     PD
vlan1.100    down     PD
vlan1.200    down     PD


--------------------------------------------------------------------------------
Ethernet   Type          PVID  Mode             Status  Reason  Speed Port    Ctl Br/Bu
Loopbk
Interface                                                          Ch #
--------------------------------------------------------------------------------
xe0           ETH           --    routed           up      none    10g   --       No  No
xe1           ETH           --    routed           down    PD      10g   --       No  No
xe2           ETH           --    routed           down    PD      10g   --       No  No
xe3           ETH           --    routed           down    PD      10g   --       No  No
xe4           ETH           --    routed           up      none    10g   --       No  No
xe5           ETH           --    routed           down    PD      10g   --       No  No
xe6           ETH           --    routed           down    PD      10g   --       No  No
xe7           ETH           --    routed           down    PD      10g   --       No  No
xe8           ETH           --    routed           up      none    1g    --       No  No
xe9           ETH           --    routed           up      none    1g    --       No  No
xe10          ETH           --    routed           down    PD      10g   --       No  No
xe11          ETH           --    routed           down    PD      10g   --       No  No
xe12          ETH           --    routed           down    PD      10g   --       No  No
xe13          ETH           --    routed           down    PD      10g   --       No  No
xe14          ETH           --    routed           down    PD      10g   --       No  No
xe15          ETH           --    routed           down    PD      10g   --       No  No
xe16          ETH           --    routed           down    PD      10g   --       No  No
xe17          ETH           --    routed           down    PD      10g   --       No  No
xe18          ETH           --    routed           down    PD      10g   --       No  No
xe19          ETH           --    routed           down    PD      10g   --       No  No
xe20          ETH           --    routed           down    PD      10g   --       No  No
xe21          ETH           --    routed           down    PD      10g   --       No  No
xe22          ETH           --    routed           down    PD      10g   --       No  No
```

```
xe23          ETH           --    routed           down    PD      10g   --       No  No
xe24          ETH           --    routed           down    PD      10g   --       No  No
xe25          ETH           --    routed           down    PD      10g   --       No  No
xe26          ETH           --    routed           down    PD      10g   --       No  No
xe27          ETH           --    routed           down    PD      10g   --       No  No
xe28          ETH           --    routed           down    PD      10g   --       No  No
xe29          ETH           --    routed           down    PD      10g   --       No  No
xe30          ETH           --    routed           down    PD      10g   --       No  No
xe31          ETH           --    routed           down    PD      10g   --       No  No
xe32          ETH           --    routed           down    PD      10g   --       No  No
xe33          ETH           --    routed           down    PD      10g   --       No  No
xe34          ETH           --    routed           down    PD      10g   --       No  No
xe35          ETH           --    routed           down    PD      10g   --       No  No
xe36          ETH           --    routed           down    PD      10g   --       No  No
xe37          ETH           --    routed           down    PD      10g   --       No  No
xe38          ETH           --    routed           down    PD      10g   --       No  No
xe39          ETH           --    routed           down    PD      10g   --       No  No
xe40          ETH           --    routed           down    PD      10g   --       No  No
xe41          ETH           --    routed           down    PD      10g   --       No  No
xe42          ETH           --    routed           down    PD      10g   --       No  No
xe43          ETH           --    routed           down    PD      10g   --       No  No
xe44          ETH           --    routed           down    PD      10g   --       No  No
xe45          ETH           --    routed           down    PD      10g   --       No  No
xe46          ETH           --    routed           down    PD      10g   --       No  No
xe47          ETH           --    routed           down    PD      10g   --       No  No
```

The interfaces ce0/1, ce0/2, ce0/3, ce0/4, all the 4x10G sub-ports will be deleted, and the 100G ports ce0, ce1, ce2, ce3, ce4, and ce5 will be added.

```
ce0 - ce0/1,ce0/2,ce0/3,ce0/4
ce1 - ce1/1,ce1/2,ce1/3,ce1/4
ce2 - ce2/1,ce2/2,ce2/3,ce2/4
ce3 - ce3/1,ce3/2,ce3/3,ce3/4
ce4 - ce4/1,ce4/2,ce4/3,ce4/4
ce5 - ce5/1,ce5/2,ce5/3,ce5/4
```

System Management Command Reference

CHAPTER 1 Basic Commands

This chapter describes basic commands.

- banner motd
- banner motd file URL
- cli timestamp
- clock set
- clock timezone
- configure terminal
- configure terminal force
- copy empty-config startup-config
- copy running-config startup-config
- copy backup-config FILE running-config replace-mode
- crypto pki generate rsa common-name ipv4
- debug nsm
- debug vm-events
- disable
- do
- enable
- enable password
- end
- exec-timeout
- exit
- help
- history
- hostname
- line console
- line vty (all line mode)
- line vty (line mode)
- logging cli
- logout
- max-session
- ping
- ping (interactive)
- port breakout
- quit
- reload
- service advanced-vty

© 2025 IP Infusion Inc. Proprietary

- service password-encryption
- service terminal-length
- show clock
- show cli
- show cli history
- show cli list
- show cli list all
- show cli modes
- show crypto csr
- show debugging nsm
- show debugging vm-events
- show logging cli
- show nsm client
- show process
- show running-config
- show running-config switch
- show startup-config
- show tcp
- show timezone
- show users
- show version
- sys-reload
- sys-shutdown
- terminal width
- terminal length
- terminal monitor
- traceroute
- watch static-mac-movement
- write
- write terminal

© 2025 IP Infusion Inc. Proprietary

banner motd

Use this command to set the message of the day (motd) at login.

After giving this command, you must write to memory using the terminal monitor command. If you do not write to memory, the new message of the day is not available after the device reboots.

Use the `no` parameter to not display a banner message at login. To configure multi-line banner message, see banner motd file URL command.

Command Syntax

```
banner motd LINE
banner motd default
banner motd file URL
no banner motd
```

Parameters

`LINE`	Custom message of the day.
`default`	Default message of the day.
`file`	A file input to set a custom message of the day.
`URL`	The file path and name containing the banner message.

Default

By default, the following banner is displayed after logging in:

```
OcNOS version 1.3.4.268-DC-MPLS-ZEBM 09/27/2018 13:44:22
```

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#banner motd default

#configure terminal
(config)#no banner motd
```

© 2025 IP Infusion Inc. Proprietary

cli timestamp

Use this command to enable timestamp print after every show command line interfaces.

Use the `no` form of this command disable the timestamp print.

Command Syntax

```
cli timestamp
```

Parameters

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.5.2.

Example

```
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#cli timestamp
OcNOS(config)#commit
OcNOS(config)#exit
OcNOS#
OcNOS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
OcNOS(config)#no cli timestamp
OcNOS(config)#commit
OcNOS(config)#exit
```

Validation Example:

```
Virgo-6#show ip ospf neighbor
! [execution timestamp : 2024 May 14 08:57:44]
Virgo-6#
Virgo-6#show mpls forwarding-table
! [execution timestamp : 2024 May 14 08:57:49]
Codes: > - installed FTN, * - selected FTN, p - stale FTN, ! - using backup
       B - BGP FTN, K - CLI FTN, (t) - tunnel, P - SR Policy FTN, (b) -
bypass,
       L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, I - IGP-Shortcut,
       U - unknown FTN, O - SR-OSPF FTN, i - SR-ISIS FTN, k - SR-CLI FTN
       (m) - FTN mapped over multipath transport, (e) - FTN is ECMP

FTN-ECMP LDP: Disabled
Code  FEC  FTN-ID  Nhlfe-ID  Tunnel-ID Pri Out-Label Out-Intf ELC  Nexthop
UpTime
```

clock set

Use this command to set the system time manually.

Command Syntax

```
clock set HH:MM:SS <1-31> MONTH <2000-2099>
```

Parameters

`HH:MM:SS`	Time of day: hour, minutes, seconds
`<1-31>`	Day of month
`MONTH`	Month of the year (january-december)
`<2000-2099>`	Year

Default

N/A

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#clock set 18:30:00 13 january 2021
18:30:00 UTC Wed Jan 13 2021
```

clock timezone

Use this command to set the system time zone.

Use `no` form of this command to set the default system time zone (UTC).

Command Syntax

```
clock timezone (WORD)
no clock timezone
```

Parameters

`WORD`	Timezone name. Use 'show timezone' to get the list of city names.

Default

By default, system time zone is UTC

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#clock timezone Los_Angeles
```

configure terminal

Use this command to enter configure mode.

When multiple CLI sessions are enabled with the cmlsh multiple-config-session command, `configure terminal` will not acquire a running datastore lock.

Command Syntax

```
configure terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering configure mode (note the change in the command prompt).

```
#configure terminal
(config)#
```

configure terminal force

Use the configure terminal force command to kick out the configure command mode to privileged EXEC mode, iff there is any session already in configure command mode.

Note: Configure terminal force with option 0 or without any option indicates immediate kick out the session which is locked to configure command mode. similarly, configure terminal force with option of any value indicates session locked to configure command mode will be exited to privileged Exec mode after the specified number of seconds completed.

When multiple CLI sessions are enabled with the cmlsh multiple-config-session command, `configure terminal force` has no effect because configuration mode is allowed for multiple users simultaneously.

Command Syntax

```
configure terminal force <0-600|>
```

Parameters

`<0-600>`	Timeout value in seconds for the session in config mode to exit to Privileged

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal force 0
#
```

copy empty-config startup-config

Use this command to clear the contents of the startup configuration.

Command Syntax

```
copy empty-config startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy empty-config startup-config
#
```

copy running-config startup-config

Use this command to a write the configuration to the file used at startup. This is the same as the terminal monitor command.

Command Syntax

```
copy running-config startup-config
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```

copy backup-config FILE running-config replace-mode

Use this command to backup the configuration to the file currently running configuration to the server.

Command Syntax

```
copy backup-config FILE running-config replace-mode
```

Parameters

`copy`	Copy configuration contents from file (replace existing config).
`file`	Copy local config file to running-config.
`FILE`	File path and name.
`running-config`	Copy to system running-config.
`replace-mode`	Include parsing errors for incorrect CLIs.

Default

No default value is specified

Command Mode

Replace mode

Applicability

This command was introduced before OcNOS version 6.4.1.

Example

```
#copy backup-config FILE running-config replace-mode
Building configuration...
[OK]
#
```

crypto pki generate rsa common-name ipv4

Use this command to generate a private key and Certificate Signing Request (CSR) which are required for OcNOS to establish a Transport Layer Security (TLS) connection with a NetConf client.

Command Syntax

```
crypto pki generate rsa common-name ipv4 IPv4ADDR
```

Parameters

IPv4ADDR	IPv4 address for the Common Name field of the CSR

Default

N/A

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+lEF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagtfh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVdOZ5yxQsLY8604ONL7Upl766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCNn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoXHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwXkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPaM
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSIteZv9cYyKhNuO07okwr67c2Ea
1lB7Pcu1tOb4wj3xjqaO/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fA1OyVgfvg/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoOMQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
#
```

debug nsm

Use this command to enable NSM debugging.

Use the `no` form of this command or the `undebug` command to disable NSM debugging.

Command Syntax

```
debug nsm (all|)
no debug nsm (all|)
undebug nsm (all|)

debug nsm bfd
no debug nsm bfd
undebug nsm bfd

debug nsm events
no debug nsm events
undebug nsm events

debug nsm hal (all|) debug
debug nsm hal events
no debug nsm hal (all|)
no debug nsm hal events
undebug nsm hal events

debug nsm packet (recv|send|) (detail|)
no debug nsm packet (recv|send|) (detail|)
undebug nsm packet (recv|send|) (detail|)
```

Parameters

`all`	Enable all debugging.
`bfd`	Debug BFD events.
`events`	Debug NSM events.
`hal`	Debug HAL.
`events`	Debug HAL events.
`packet`	Debug packet events.
`recv`	Debug received packets.
`send`	Debug sent packets.
`detail`	Show detailed packet information.

Default

By default, debugging is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#debug nsm all
#
#debug nsm bfd
#
#debug nsm events
#
#debug nsm hal all
#
#debug nsm packet
#
#debug nsm packet recv detail
```

debug vm-events

Use this command to enable debug logs for Guest VM events

Use the no form of this command to disable debug logs for Guest VM events

Command Syntax

```
debug vm-events
no debug vm-events
```

Parameters

None

Default

No default value specified.

Command Mode

Configure mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0

Examples

```
#configure terminal
(config)#debug vm-events
```

disable

Use this command from to exit privileged exec mode and return to exec mode. This is the only command that allows you to go back to exec mode. The exit or quit commands in privileged exec mode end the session without returning to exec mode.

Command Syntax

```
disable
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#disable
>
```

do

Use this command to run several exec mode or privileged exec mode commands from configure mode. The commands that can be run from configure mode using `do` are: `show`, `clear`, `debug`, `ping`, `traceroute`, `write`, and `no debug`.

Command Syntax

```
do LINE
```

Parameters

`LINE`	Command and its parameters.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
#(config)#do show interface
Interface lo
  Hardware is Loopback index 1 metric 1 mtu 16436 duplex-half arp ageing
timeout 25
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
  inet 4.4.4.40/32 secondary
  inet 127.0.0.1/8
  inet6 ::1/128
  Interface Gifindex: 3
  Number of Data Links: 0
  GMPLS Switching Capability Type:
    Packet-Switch Capable-1 (PSC-1)
  GMPLS Encoding Type: Packet
  Minimum LSP Bandwidth 0
    input packets 10026, bytes 730660, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 10026, bytes 730660, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
#
```

enable

Use this command to enter privileged exec command mode.

Command Syntax

```
enable
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering the Privileged Exec mode (note the change in the command prompt).

```
>enable
#
```

enable password

Use this command to change or create a password to use when entering enable mode.

Note: Only network administrators can execute this command. For more, see the username command.

There are two methods to enable a password:

- Plain Password: a clear text string that appears in the configuration file.
- Encrypted Password: An encrypted password does not display in the configuration file; instead, it displays as an encrypted string. First, use this command to create a password. Then, use the service password-encryption command to encrypt the password.

Use the `no` parameter to disable the password.

Command Syntax

```
enable password LINE
no enable password
no enable password LINE
```

Parameters

`LINE`	Password string, up to 8 alpha-numeric characters, including spaces. The string cannot begin with a number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#enable password mypasswd
```

end

Use this command to return to privileged exec command mode from any other advanced command mode.

Command Syntax

```
end
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows returning to privileged exec mode directly from interface mode.

```
#configure terminal
(config)#interface eth0
(config-if)#end
#
```

exec-timeout

Use this command to set the interval the command interpreter waits for user input detected. That is, this sets the time a telnet session waits for an idle VTY session before it times out. A value of zero minutes and zero seconds (0 and 0) causes the session to wait indefinitely.

Use the `no` parameter to disable the wait interval.

Command Syntax

```
exec-timeout <0-35791> (<0-2147483>|)
no exec-timeout
```

Parameters

`<0-35791>`	Timeout value in minutes.
`<0-2147483>`	Timeout value in seconds.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the telnet session will timeout after 2 minutes, 30 seconds if there is no response from the user.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#exec-timeout 2 30
```

exit

Use this command to exit the current mode and return to the previous mode. When used in exec mode or privileged exec mode, this command terminates the session.

Command Syntax

```
exit
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows exiting interface mode and returning to configure mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
(config)#
```

help

Use this command to display help for the OcNOS command line interface.

Command Syntax

```
help
```

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#help
CLI provides advanced help feature. When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)
```

history

Use this command to set the maximum number of commands stored in the command history.

Use the `no` parameter to remove the configuration.

Command Syntax

```
history max <0-2147483647>
no history max
```

Parameters

`<0-2147483647>` Number of commands.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#line vty 12 77
(config-line)#history max 123

(config-line)#no history max
```

hostname

Use this command to set the network name for the device. OcNOS uses this name in system prompts and default configuration filenames.

Setting a host name using this command also sets the host name in the kernel.

Note: After giving the `hostname` command, you must write to memory using the terminal monitor command. If you do not write to memory, the change made by this command (the new host name) is not set after the device reboots.

Use the `no` parameter to disable this function.

Command Syntax

```
hostname WORD
no hostname (WORD|)
```

Parameter

`WORD`	Network name for a system. Per RFC 952 and RFC 1123, a host name string can contain only the special characters period (“.”) and hyphen (“-”). These special characters cannot be at the start or end of a host name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#hostname ABC
(config)#

(config)#no hostname
(config)#exit
```

line console

Use the this command to move or change to the line console mode.

Command Syntax

```
line console <0-0>
```

Parameters

<0-0>	First line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example enters line mode (note the change in the prompt).

```
#configure terminal
(config)#line console 0
(config-line)#
```

line vty (all line mode)

Use this command to move or change to all line VTY mode.

Note: line vty is just a mode changing command, and it can't exist without sub attributes being configured. i.e exec-timeout.

Command Syntax

```
line vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

The following example shows entering all line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty
(config-all-line)#exit
(config)#
```

line vty (line mode)

Use this command to move or change to VTY mode. This command is used to connect to a protocol daemon. This configuration is necessary for any session. This configuration should be in the daemon's config file before starting the daemon.

Use the `no` parameter to disable this command.

Note: line vty is just a mode changing command, and it can't exist without sub attributes being configured. i.e exec-timeout.

Command Syntax

```
line vty <0-871> <0-871>
no line vty <0-871> (<0-871>|)
```

Parameters

`<0-871>`	Specify the first line number.
`<0-871>`	Specify the last line number.

Note: Configurations (exec-timeout) performed under this mode, affects only the current VTY session.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example shows entering line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty 9
(config-line)#exit
(config)no line vty 9
```

logging cli

Use this command to enable logging commands entered by all users.

Use the `no` parameter to disable logging commands entered by all users.

Command Syntax

```
logging cli
no logging cli
```

Parameter

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#logging cli
(config)#no logging cli
```

logout

Use this command to exit the OcNOS shell.

Command Syntax

```
logout
```

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>logout
OcNOS login:

>enable
en#logout
>
```

max-session

Use this command to set maximum VTY session limit.

Use `no` form of this command to unset session-limit.

User can configure session-limit for Telnet and SSH sessions separately but this max-session parameter value takes the precedence to restrict the maximum number of sessions. If user configured this max-session to be 4, then the device would allow only maximum of 4 SSH and Telnet sessions collectively irrespective of the individual SSH and Telnet max-session configuration. Active sessions won't be disturbed even if the configured max-session limit is lesser than the current active sessions.

Command syntax

```
max-session <1-40>
```

Parameters

`<1-40>`	Number of sessions

Default

By default, 40 sessions are allowed.

Command Mode

Line mode

Applicability

This command is introduced in OcNOS version 5.0

Example

In the following example max-session is configured as 4, thus the device would allow only 4 management sessions of SSH and Telnet collectively.

```
#configure terminal
(config)#line vty
(config-all-line)#max-session 5
(config-all-line)#commit
(config-all-line)#exit
(config)#exit
```

ping

Use this command to send echo messages to another host.

Note: When data packets copied to cpu due to destination lookup fail, both data packets and icmp echo request packets processed in cpu through same cpu queue and it may happen that ping fails due to congestion. In such cases, to check connectivity, please use interactive ping command and update tos value 192. Refer ping (interactive) for the interactive ping command.

Command Syntax

```
ping WORD (broadcast | count <1-2147483647> | datasize <36-18024> |interface
  IFNAME| source-ip A.B.C.D | interval <0-3600>  | timeout <0-3600>|) (vrf
  (NAME|management)|)
ping ip WORD (broadcast | count <1-2147483647> | datasize <36-18024> | interface
  IFNAME| source-ip A.B.C.D | interval <0-3600>  | timeout <0-3600>|) (vrf
  (NAME|management)|)
ping ipv6 WORD (broadcast | count <1-2147483647> | datasize <36-18024> |interface
  IFNAME| source-ip X:X::X:X | interval <0-3600>  | timeout <0-3600>|) (vrf
  (NAME|management)|)
```

Parameters

WORD	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
ip	IPv4 echo.
WORD	Destination address in A.B.C.D format or host name.
ipv6	IPv6 echo.
WORD	Destination address in X:X::X:X format or host name.
interface	Interface name through which the ICMP packets to be sent.
IFNAME	Interface's name
source-ip	Source IP to be used in ICMP packet.
A.B.C.D	Source IPv4 address in the ping.
X:X::X:X	Source IPv6 address in the ping.
vrf	Virtual Routing and Forwarding instance.
NAME	VRF instance name.
management	Management VRF.
broadcast	Allow broadcast
count	Ping repeat count
<1-2147483647>	Repeat count value
datasize	Datagram size
<36-18024>	Data size in bytes (Default value is 100)
interval	Interval between sending each packet
<0-3600>	Interval value (Default value is 1)
timeout	Response timeout
<0-3600>	Timeout in seconds (Default value is 2)

Default

No default value is specified

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping 20.20.20.1 vrf management
Press CTRL+C to exit
PING 20.20.20.1 (20.20.20.1) 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=64 time=0.036 ms

--- 20.20.20.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
rtt min/avg/max/mdev = 0.032/0.034/0.036/0.006 ms

#ping ipv6 3001:db8:0:1::129 vrf management
Press CTRL+C to exit
PING 3001:db8:0:1::129(3001:db8:0:1::129) 56 data bytes
64 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=8 ttl=64 time=0.048 ms

--- 3001:db8:0:1::129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms

#ping 11.11.11.1 source-ip 11.11.11.2  count 5 timeout 1
Press CTRL+C to exit
PING 11.11.11.1 (11.11.11.1) from 11.11.11.2 : 100(128) bytes of data.
108 bytes from 11.11.11.1: icmp_seq=1 ttl=64 time=0.437 ms
108 bytes from 11.11.11.1: icmp_seq=2 ttl=64 time=0.359 ms
108 bytes from 11.11.11.1: icmp_seq=3 ttl=64 time=0.314 ms
108 bytes from 11.11.11.1: icmp_seq=4 ttl=64 time=0.340 ms
108 bytes from 11.11.11.1: icmp_seq=5 ttl=64 time=0.299 ms

--- 11.11.11.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 97ms
rtt min/avg/max/mdev = 0.299/0.349/0.437/0.053 ms
```

```
#ping 9.2.27.17 source-ip 1.1.17.12 count 10 timeout 5 interval 10 broadcast
vrf management
Press CTRL+C to exit
PING 9.2.27.17 (9.2.27.17) from 1.1.17.12 : 100(128) bytes of data.
108 bytes from 9.2.27.17: icmp_seq=1 ttl=64 time=0.211 ms
108 bytes from 9.2.27.17: icmp_seq=2 ttl=64 time=0.171 ms
108 bytes from 9.2.27.17: icmp_seq=3 ttl=64 time=0.182 ms
108 bytes from 9.2.27.17: icmp_seq=4 ttl=64 time=0.183 ms
108 bytes from 9.2.27.17: icmp_seq=5 ttl=64 time=0.182 ms
108 bytes from 9.2.27.17: icmp_seq=6 ttl=64 time=0.175 ms
108 bytes from 9.2.27.17: icmp_seq=7 ttl=64 time=0.186 ms
108 bytes from 9.2.27.17: icmp_seq=8 ttl=64 time=0.173 ms
108 bytes from 9.2.27.17: icmp_seq=9 ttl=64 time=0.163 ms
108 bytes from 9.2.27.17: icmp_seq=10 ttl=64 time=0.197 ms

--- 9.2.27.17 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 331ms
rtt min/avg/max/mdev = 0.163/0.182/0.211/0.016 ms
#
```

© 2025 IP Infusion Inc. Proprietary

ping (interactive)

Use this command to send echo messages to another host interactively. You are prompted with options supported by the command.

Command Syntax

```
ping
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#ping
Protocol [ip]:
Target IP address: 20.20.20.1
Name of the VRF : management
Repeat count [5]: 6
Time Interval in Sec [1]: 2.2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Ping Broadcast? Then -b [n]:
PING 20.20.20.1 (20.20.20.1) 100(128) bytes of data.
108 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.037 ms
108 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.034 ms

--- 20.20.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11000ms
rtt min/avg/max/mdev = 0.034/0.036/0.038/0.007 ms

#ping
Protocol [ip]: ipv6
Target IP address: 3001:db8:0:1::129
Name of the VRF : management
Repeat count [5]:
Time Interval in Sec [1]:
Datagram size [100]:
```

```
Timeout in seconds [2]:
Extended commands [n]:
PING 3001:db8:0:1::129(3001:db8:0:1::129) 100 data bytes
108 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.050 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.042 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.048 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.051 ms

--- 3001:db8:0:1::129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.042/0.047/0.051/0.008 ms
```

The input prompts are described in Table 1-4:

Table 1-4: ping output fields

Protocol [ip]	IPv4 or IPv6. The default is IPv4 if not specified.
Target IP address	IPv4 or IPv6 address or host name.
Name of the VRF	Name of the Virtual Routing and Forwarding instance.
Repeat count [5]	Number of ping packets to send. The default is 5 if not specified.
Time Interval in Sec [1]	Time interval between two ping packets. The default is 1 second if not specified.
Datagram size [100]	Ping packet size. The default is 100 bytes if not specified.
Timeout in seconds [2]	Time to wait for ping reply. The default is 2 seconds if not specified.
Extended commands [n]	Options for extended ping. The default is “no”.
Source address or interface	Source address or interface.
Type of service [0]	Types of service. The default is 0 if not specified.
Set DF bit in IP header? [no]	Do not fragment bit. The default value is “no” if not specified.
Data pattern [0xABCD]	Specify a pattern.
Ping Broadcast? Then -b [n]	Broadcast ping. The default is “no”. For a broadcast address, the value should be “y”.

port breakout

Use this command for the port breakout configuration.

Note: Application and related breakout types will differ for transceivers based on the make or vendor. Check the related applications and breakout type using the command "`#show qsfp-dd <port no> advertisement applications`" and configure application, corresponding breakout type as network needed.

Note: `serdes` command is applicable only for 1X100g and 1X200g breakout modes. If we configure serdes 25g then each lane will be configured with 25g.

Note: The 100g (ce) ports support 4X10g, 4X25g, and 2X50g breakout modes only.

Command Syntax

```
port IFNAME breakout (4X10g|4X25g|2X50g)
port IFNAME breakout
  (1X100g|1X200g|2X100g|2X200g|2X50g|3X100g|4X100g|4X10g|4X25g|4X50g|8X10g|8X25g|8
  X50g)
port IFNAME breakout (2X100g|1X100g) (serdes (25g)|)
no port IFNAME breakout
```

Parameters

`IFNAME`	Interface Name.
`1X100g`	split to 1X100g(default serdes is 50G).
`1X200g`	split to 1X200g.
`2X100g`	split to 2X100g(default serdes is 50G).
`2X200g`	split to 2X200g.
`2X50g`	split to 2X50g.
`3X100g`	split to 3X100g.
`4X100g`	split to 4X100g.
`4X10g`	split to 4X10g.
`4X25g`	split to 4X25g.
`4X50g`	split to 4X50g.
`8X10g`	split to 8X10g.
`8X25g`	split to 8X25g.
`8X50g`	split to 8X50g.
`Serdes 25g`	configure serdes 25g.

Default

No default value is specified

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 6.4.

Example

```
#Configuring port breakout:
OcNOS(config)#port cd2 breakout 1X100g
OcNOS(config)#port cd3 breakout 1X200g
OcNOS(config)#port cd4 breakout 2X100g
OcNOS(config)#port cd5 breakout 2X200g
OcNOS(config)#port cd6 breakout 2X50g
OcNOS(config)#port cd7 breakout 3X100g
OcNOS(config)#port cd8 breakout 4X100g
OcNOS(config)#port cd9 breakout 4X10g
OcNOS(config)#port cd10 breakout 4X25g
OcNOS(config)#port cd11 breakout 4X50g
OcNOS(config)#port cd12 breakout 8X10g
OcNOS(config)#port cd13 breakout 8X25g
OcNOS(config)#port cd14 breakout 8X50g

Configuring port-breakout with serdes option:
OcNOS(config)#port cd15 breakout 1X100g serdes 25g
OcNOS(config)#port cd16 breakout 2X100g serdes 25g

Unconfiguring the port-breakout:
OcNOS(config)#no port cd5 breakout
```

© 2025 IP Infusion Inc. Proprietary

quit

Use this command to exit the current mode and return to the previous mode. When this command is executed in one of the exec modes, it closes the shell and logs you out.

Command Syntax

```
quit
```

Parameters

None

Default

No default value is specified

Command Mode

All modes

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#

>enable
#quit
[root@TSUP-123 sbin]#
```

reload

Use this command to shut down the device and perform a cold restart. You call this command when:

- You detect a configuration issue such as `show running-config` displaying a configuration but when you try to remove that configuration, you get a message that it is not configured.
- You have replaced the start-up configuration file (in this case you specify the `flush-db` parameter).

Command Syntax

```
reload (flush-db|)
```

Parameters

`flush-db`	Delete the database file and recreate it from the start-up configuration file.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows replacing a start-up configuration file and then synchronizing it to the configuration database:

```
#copy file /home/TEST.conf startup-config
Copy Success
#
#reload flush-db
The system has unsaved changes.
Would you like to save them now? (y/n): n

Configuration Not Saved!
Are you sure you would like to reset the system? (y/n): y
```

For both of these prompts, you must specify whether to save or discard the changes. Abnormal termination of the session without these inputs can impact the system behavior.

For the `unsaved changes` prompt:

```
Would you like to save them now?
```

You should always say “no” to this prompt because otherwise the command takes the current *running configuration* and applies it to the current start-up configuration.

service advanced-vty

Use this command to set multiple options to list when the tab key is pressed while entering a command. This feature applies to commands with more than one option.

Use the `no` parameter to not list options when the tab key is pressed while entering a command.

Command Syntax

```
service advanced-vty
no service advanced-vty
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#service advanced-vty
(config)#no service advanced-vty
```

service password-encryption

Use this command to encrypt passwords created with the enable password command. Encryption helps prevent observers from reading passwords.

Use the `no` parameter to disable this feature.

Command Syntax

```
service password-encryption
no service password-encryption
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#enable password mypasswd
(config)#service password-encryption
```

service terminal-length

Use this command to set the number of lines that display at one time on the screen for the current terminal session.

Use the `no` parameter to disable this feature.

Command Syntax

```
service terminal-length <0-512>
no service terminal-length (<0-512>|)
```

Parameters

`<0-512>`	Number of lines to display. A value of 0 prevents pauses between screens of output.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#service terminal-length 60
```

show clock

Use this command to display the current system time.

Command Syntax

```
show clock
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show clock
12:54:02 IST Fri Apr 29 2016
```

show cli

Use this command to display the command tree of the current mode.

Command Syntax

```
show cli
```

Parameters

None

Default

None

Command Mode

All command modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
        +-domain
          +-DOMAIN_NAME [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
        +-level
          +-LEVEL_ID [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
      +-maintenance-points
        +-remote
          +-domain
            +-DOMAIN_NAME [clear ethernet cfm maintenance-points remote(domain
D
--More--
```

show cli history

Use this command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

Command Syntax

```
show cli history
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show cli history
   1 en
   2 show ru
   3 con t
   4 show spanning-tree
   5 exit
```

show cli list

Use this command to display the commands relevant to the current mode.

Command Syntax

```
show cli list
```

Parameters

None

Default

None

Command Mode

All command modes except IPv4 access-list and IPv6 access-list mode.

Applicability

This command was introduced before OcNOS version 6.4.

Example

```
> show cli list
  cat LINE
  cd (WORD|)
  clear aaa local user lockout username USERNAME
  clear access-list NAME counters
  clear access-list counters
  clear arp access-list NAME counters
  clear arp access-list counters
  clear arp-cache
  clear bgp *
  clear bgp * in
  clear bgp * in prefix-filter
  clear bgp * l2vpn vpls
  clear bgp * out
  clear bgp * soft
  clear bgp * soft in
  clear bgp * soft out
  clear bgp <1-4294967295>
  clear bgp <1-4294967295>
```

show cli list all

Use this command to display all the cli's present in OcNOS device.

Command Syntax

```
show cli list all
```

Parameters

None

Default

None

Command Mode

Exec mode.

Applicability

This command was introduced before OcNOS version 6.4.

Example

```
> show cli list all
  cat LINE
  cd (WORD|)
  clear aaa local user lockout username USERNAME
  clear access-list NAME counters
  clear access-list counters
  clear arp access-list NAME counters
  clear arp access-list counters
  clear arp-cache
  clear bgp *
  clear bgp * in
  clear bgp * in prefix-filter
  clear bgp * l2vpn vpls
  clear bgp * out
  clear bgp * soft
  clear bgp * soft in
  clear bgp * soft out
  clear bgp <1-4294967295>
  clear bgp <1-4294967295> in
  clear bgp <1-4294967295> in prefix-filter
  clear bgp <1-4294967295> l2vpn vpls
  clear bgp <1-4294967295> out
  clear bgp <1-4294967295> soft
  clear bgp <1-4294967295> soft in
  clear bgp <1-4294967295> soft out
  clear bgp (A.B.C.D|X:X::X:X|WORD)
  clear bgp (A.B.C.D|X:X::X:X) in
  clear bgp (A.B.C.D|X:X::X:X) in prefix-filter
  clear bgp (A.B.C.D|X:X::X:X) l2vpn vpls
  clear bgp (A.B.C.D|X:X::X:X) out
  clear bgp (A.B.C.D|X:X::X:X) soft
```

```
clear bgp (A.B.C.D|X:X::X:X) soft in
clear bgp X:X::X:X soft out
clear bgp all *
```

show cli modes

Use this command to display cli modes present in OcNOS.

Command Syntax

```
show cli modes
```

Parameters

None

Default

None

Command Mode

Execution mode.

Applicability

This command was introduced before OcNOS version 6.4.

Example

```
> Mode(4) Exec  []
Mode(5) Configure  [(config)]
Mode(6) Line configuration  [(config-line)]
Mode(12) Key-chain configuration  [(config-keychain)]
Mode(13) Key-chain key configuration  [(config-keychain-key)]
Mode(14) Virtual-router instance configuration  [(config-vr)]
Mode(15) IP VPN Routing/Forwarding instance configuration  [(config-vrf)]
Mode(16) Interface configuration  [(config-if)]
Mode(24) VPLS configuration  [(config-vpls)]
Mode(26) Router configuration  [(config-router)]
Mode(27) Router Address Family configuration  [(config-router-af)]
Mode(28) Router Address Family configuration  [(config-router-af)]
Mode(29) Router Address Family configuration  [(config-router-af)]
Mode(30) Router Address Family configuration  [(config-router-af)]
Mode(31) Router Address Family configuration  [(config-router-af)]
Mode(32) Router configuration  [(config-router)]
Mode(33) Router Address Family configuration  [(config-router-af)]
Mode(34) Router configuration  [(config-router)]
Mode(35) Router configuration  [(config-router)]
Mode(36) Router configuration  [(config-router)]
Mode(37) Router configuration  [(config-router)]
Mode(38) Router Address Family configuration  [(config-router-af)]
Mode(46) Router configuration  [(config-router)]
Mode(48) Router configuration  [(config-router)]
Mode(51) Router configuration  [(config-router)]
Mode(52) MPLS Path configuration  [(config-path)]
Mode(53) MPLS Trunk configuration  [(config-trunk)]
Mode(56) IP Prefix-List configuration  [(config-ip-prefix-list)]
Mode(61) IPv6 Prefix-List configuration  [(config-ipv6-prefix-list)]
Mode(63) Route Map configuration  [(config-route-map)]
Mode(71) MSTI configuration  [(config-mst)]
```

```
Mode(96) Crypto Map configuration  [(config-crypto)]
Mode(99) RSVP Bypass Tunnel configuration  [(config-bypass)]
--More--
```

show crypto csr

Use this command to display the Certificate Signing Request (CSR) created with the crypto pki generate rsa common-name ipv4 command.

Command Syntax

```
show crypto csr
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#crypto pki generate rsa common-name ipv4 7.7.7.7
#show crypto csr
-----BEGIN CERTIFICATE REQUEST-----
MIICVzCCAT8CAQAwEjEQMA4GA1UEAwwHNy43LjcuNzCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMkzIZaxNYPd8PW0hexecUFKq9pJn5IJzJkOQDtoVFOT
zeLPRxBaOt1NVd+lEF+wy3AgnGMw004g4AP7qaE+S5X1vKGAjagtfh/gfDAPDUtM
CpYLMCACM7n76OmyP9eUpkMbOSPkZDIBZfjUMxDTFwkzCBH+BF6SkSxtA24NUA9z
5heCIb1ArXYjdlIeB+9FfiVdOZ5yxQsLY8604ONL7Upl766SArGQo6oZ1dJ+bc91
sQVCEpF40SdCNn+Uw3R0cPfQF81BJD4H0EHf1VnHtYJwQ1yax6qc5ghT9R/rABDa
BFB3R09QpjV4Ihd/MyrdQmEIoXHeNNvSGDj9+eiEpksCAwEAAaAAMA0GCSqGSIb3
DQEBCwUAA4IBAQAwXkQmNf3yiL+pmpwvE+gU8KVp3i4cvD13Vjh7IQMkCT47WPaM
DUiYgwk+dPVAI+iWZq4qTvUNn6xahOyN5rnkTz9eipsQ1YHPpZB7hj5fimWwzJws
m4Tun0GZieEBCROqUpbuW+6QDvtR3XSzHhdGGSIteZv9cYyKhNuO07okwr67c2Ea
1lB7Pcu1tOb4wj3xjqaO/ENDG+nmdUPaIKZrAwf2fEOarOaHgKwcl1AHHbusbJWL
qH0fA1OyVgfvg/WuCPP6Peg/Cpla7bDWqeGYt9vFTtekKoOMQLzJwl6oINbtBCcw
DZJpeaQpUhFm+ZOjwibZ5NGPBRSTuYncp5xJ
-----END CERTIFICATE REQUEST-----
```

show debugging nsm

Use this command to display debugging information.

Command Syntax

```
show debugging nsm
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
```

show debugging vm-events

Use this command to display the vm-events debugging information

Command Syntax

```
show debugging events
```

Parameters

None

Default

No default value specified.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.1.0

Examples

```
#show debugging vm-events#
```

show logging cli

Use this command to display command history for all users.

Command Syntax

```
show logging cli ((logfile LOGFILENAME)|) (match-pattern WORD |)
show logging cli last <1-9999>
show logging logfile list
```

Parameters

`LOGFILENAME`	Name of a saved command history log file. The default path is `/var/log/messages`, but you can specify a full path to override the default.
`WORD`	Display only lines with this search pattern.
`<1-9999>`	Number of lines to display from the end of the command history.
`logfile list`	Display a list of command history files.

Default

LOGFILENAME Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh logging cli
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#sh logging cli logfile ipi match-pattern root
2017 Mar 01 16:30:59 : OcNOS : User root@/dev/pts/1 : CLI : 'exit'
2017 Mar 01 16:31:06 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging logfile list'
#show logging cli last 2
2017 Mar 1 16:34:26.302 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging info'
2017 Mar 1 16:34:37.317 : OcNOS : User root@/dev/pts/1 : CLI : 'sh logging cli last 2'
#show logging logfile list
file1
file2
```

show nsm client

Use this command to display NSM client information including the services requested by the protocols, statistics and the connection time

Command Syntax

```
show nsm client
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
 IMI, socket 23
  Service: Interface Service, Router ID Service, VRF Service
  Messsage received 1, sent 58
  Connection time: Thu Jul 22 11:03:12 2010
  Last message read: Service Request
  Last message write: Link Up
NSM client ID: 25
 ONMD, socket 24
  Service: Interface Service, Bridge service, VLAN service
  Messsage received 2, sent 74
  Connection time: Thu Jul 22 11:03:15 2010
  Last message read: OAM  LLDP msg
  Last message write: Link Up
#
```

show process

Use this command to display the OcNOS daemon processes that are running.

Command Syntax

```
show process
```

Parameters

None

Command Mode

Exec modes

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show process
 PID NAME             TIME     FD
   1 nsm          00:56:29     7
   2 ripd         00:56:29     11
   3 ripngd       00:56:29     12
   4 ospfd        00:56:29     9
   5 ospf6d       00:56:29     10
   6 bgpd         00:56:29     14
   9 isisd        00:56:29     8
#
```

Table 1-5 explains the output fields.

Table 1-5: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S)—Number of system and user CPU seconds that the process has used. (None, D, and E)—Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.

show running-config

Use this command to show the running system status and configuration.

Command Syntax

```
show running-config
show running-config full
```

Parameters

`full`	Display the full configuration information.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config
no service password-encryption
!
no service dhcp
ip domain-lookup
!
mpls propagate-ttl
!
vrrp vmac enable
spanning-tree mode provider-rstp
no data-center-bridging enable
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.1.2.173/24
 no shutdown
!
interface eth1
 shutdown

!
line con 0
 login
!
end
(config)#
```

show running-config switch

Use this command to display the running system switch configuration.

Command Syntax

```
show running-config switch bridge
show running-config switch dot1x
show running-config switch gmrp
show running-config switch gvrp
show running-config switch lacp
show running-config switch lmi
show running-config switch mstp
show running-config switch radius-server
show running-config switch rpsvt+
show running-config switch rstp
show running-config switch ptp
show running-config switch stp
show running-config switch synce
show running-config switch vlan
```

Parameters

`bridge`	Display Bridge group information.
`dot1x`	Display 802.1x port-based authentication information.
`gmrp`	Display GARP Multicast Registration Protocol (GMRP) information.
`gvrp`	Display GARP VLAN Registration Protocol (GVRP) information.
`lacp`	Display Link Aggregation Control Protocol (LACP) information.
`lmi`	Display Ethernet Local Management Interface Protocol (LMI) information.
`mstp`	Display Multiple Spanning Tree Protocol (MSTP) information.
`radius-server`	Display RADIUS server information.
`rpvst+`	Display Rapid Per-VLAN Spanning Tree (rpvst+) information.
`rstp`	Display Rapid Spanning Tree Protocol (RSTP) information.
`ptp`	Display Precision time Protocol (PTP)
`stp`	Display Spanning Tree Protocol (STP) information.
`synce`	Display synce information.
`vlan`	Display values associated with a single VLAN.

Default

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#show running-config switch stp
!
bridge 6 ageing-time 45
bridge 6 priority 4096
bridge 6 max-age 7
```

show startup-config

Use this command to display the startup configuration.

Command Syntax

```
show startup-config
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show startup-config
!   2001/04/21 11:38:52
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 redistribute connected
 network 10.10.10.0/24
 network 10.10.11.0/24
!
line vty
 exec-timeout 0 0
```

show tcp

Use this command to display the Transmission Control Protocol (TCP) connection details.

Command Syntax

```
show tcp
```

Parameters

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show tcp
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp        0      0 127.0.0.1:25          0.0.0.0:*              LISTEN
tcp        0      1 10.12.44.1:57740      127.0.0.1:705          CLOSE_WAIT
tcp       52      0 10.12.44.21:22        10.12.7.89:705         ESTABLISHED
tcp       85      0 10.12.44.21:57742     10.12.44.21:57738      ESTABLISHED
```

Table 1-6: Show tcp output

Entry	Description
Proto	Protocol – TCP
Recv-Q	Number of TCP packets in the Receive Queue.
Send-Q	Number of TCP packets in the Send-Q.
Local Address and port number	Local IP address and the port number.

Table 1-6: Show tcp output (Continued)

Entry	Description
Foreign Address and port number	Foreign (received) IP address and the port number.
State	Current state of TCP connections: ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2 TIME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING UNKNOWN

show timezone

Use this command to display the list of timezone names.

Command Syntax

```
show timezone
  (all|africa|america|antarctica|arctic|asia|atlantic|australia|brazil|canada|chil
  e|europe|indian|mexico|pacific|us)
```

Parameters

`africa`	Africa timezone list
`all`	All timezone list
`l2-profile-three`	L2 profile Three (default); the size of the l2 table (Mac address table) and l3 table (Host table) is almost equal
`l3-profile`	L3 profile
`america`	America timezone list
`antarctica`	Antarctica timezone list
`asia`	Asia timezone list
`atlantic`	Atlantic timezone list
`australia`	Australia timezone list
`brazil`	Brazil timezone list
`canada`	Canada timezone list
`chile`	Chile timezone list
`europe`	Europe timezone list
`indian`	Indian timezone list
`mexico`	Mexico timezone list
`pacific`	Pacific timezone list
`us`	US timezone list

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show timezone asia
Asia:
Kuwait
```

```
Samarkand
Novosibirsk
Hebron
Singapore
Dushanbe
Rangoon
Riyadh
Thimphu
Shanghai
Phnom_Penh
Taipei
Qyzylorda
Ho_Chi_Minh
Urumqi
Chita
Khandyga
Nicosia
Jerusalem
Ashkhabad
Gaza
Tel_Aviv
Baghdad
Anadyr
Tehran
Ashgabat
Saigon
Damascus
Sakhalin
Yekaterinburg
Baku
Bangkok
Kashgar
Macao
Seoul
Jakarta
Aden
Katmandu
Amman
Ujung_Pandang
Kuching
Hong_Kong
Ulan_Bator
Dhaka
Macau
Omsk
Vientiane
Pyongyang
Ust-Nera
Manila
Srednekolymsk
Tbilisi
Kamchatka
Magadan
Istanbul
Chongqing
Jayapura
Yerevan
```

```
Makassar
Colombo
Karachi
Hovd
Novokuznetsk
Krasnoyarsk
Irkutsk
Kabul
Kolkata
Dacca
Brunei
Calcutta
Kathmandu
Bishkek
Qatar
Tashkent
Aqtau
Oral
Kuala_Lumpur
Pontianak
Harbin
Aqtobe
Bahrain
Muscat
Vladivostok
Dubai
Tokyo
Chungking
Almaty
Choibalsan
Thimbu
Beirut
Dili
Yakutsk
Ulaanbaatar
```

© 2025 IP Infusion Inc. Proprietary

show users

Use this command to display information about current users.

Command Syntax

```
show users
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

      Line      User     Idle     Location/Session      PID     TYPE        Role
(*) 130 vty 0 [C]root   00:00:36      pts/0            20872    Local    network-admin
(#)   NA      [N]root     NA           1                NA       NA      network-admin
      NA      [N]root     NA           2                NA       NA      network-admin
    131 vty 1 [C]joyce  00:00:26     pts/1             17593    Remote   network-admin
```

Table 1-7 explains the output fields.

Table 1-7: show users fields

Entry	Description
Current users	
CLI user	
Location	
Session	
Lock acquired by user	
Netconf users	
Line	
User	User name.

Table 1-7: show users fields

Entry	Description
Idle	How long the user has been idle.
Location/Session	
PID	Process identifier name.
Type	
Role	

show version

Use this command to display OcNOS version information.

Command Syntax

```
show version
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show version
Software version: EC_AS5812-54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0 09/27/2018
13:44:22
 Copyright (C) 2018 Coriant. All rights reserved

 Software Product: OcNOS, Version: 1.3.4.268
 Hardware Model: Edgecore 5812-54X-O-AC-F
 Software Feature Code: DC-MPLS-ZEBM
 System Configuration Code: S0
 Package Configuration Code: P0
 Software Baseline Version: 1.3.4.208

Installation Information:
 Image Filename: EC_AS5812_54X-OcNOS-1.3.4.268-DC_MPLS_ZEBM-S0-P0-installer
 Install method: http
 ONIE SysInfo: x86_64-accton_as5812_54x-r0
#
```

Table 1-8: Show version output

Entry	Description
Software version	The software version including hardware device name and date.
Software Product	Product name and version.
Hardware Model	Hardware platform.
Software Feature Code	SKU that specifies the capabilities of this version of the software.
System Configuration Code	System configuration number.

Table 1-8: Show version output (Continued)

Entry	Description
Package Configuration Code	ONIE package installer versions.
Software Baseline Version	Version from which this release branch is created.
Installation Information	Information about the installation.
Image Filename	The file name of the installed image.
Install method	The type of server (or USB stick) from which the software was installed.
ONIE SysInfo	ONIE version.

sys-reload

Use this command to cold restart the device.

Note: This command is an alias for the reload command.

Command Syntax

```
sys-reload
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Example

```
>sys-reload
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to reset the system? (y/n): n
```

sys-shutdown

Use this command to shut down the device gracefully. After giving this command, you can remove the device power cable.

Note: Some of the switch hardwares doesn't support system shutdown. On such devices this command will make the switch to go for a reboot.

Command Syntax

```
sys-shutdown
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 1.3.7.

Example

```
>sys-shutdown
The system has unsaved changes.
Would you like to save them now? (y/n): y
Building Configuration...
[OK]
Are you sure you would like to shutdown the system? (y/n): y
For both of these prompts, you must specify whether to save or discard the
changes.
For the unsaved changes prompt:
Would you like to save them now?
```

terminal width

Use this command to set the number of characters to be displayed in one line on the screen. Use the no option to unset the number of characters on the screen.

Note: If user wants to have a fixed terminal length and width, then terminal length should not be set to 0. i.e. CLI “terminal length 0“ should not be used, and only non-zero length to be used.

Command Syntax

```
terminal width <24-511>
terminal no width <24-511>
```

Parameters

<24-511>	Number of lines on screen

Default

Default width value 80 is optionally overridden by kernel.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
host#terminal width 120
```

terminal length

Use this command to set the number of lines displayed on the screen.

Use the `no` option to unset the number of lines on a screen.

Note: If user wants to have a fixed terminal length and width, then terminal length should not be set to 0. i.e. CLI “terminal length 0“ should not be used, and only non-zero length to be used.

Command Syntax

```
terminal length <0-511>
terminal no length <0-511>
```

Parameters

`<0-511>`	Number of lines on screen. Specify 0 for no pausing.

Default

Default length value 24 is optionally overridden by kernel.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
>enable
#terminal length 0
```

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

terminal monitor

Use this command to display debugging output on a terminal.

Use one of the optional parameters to display debugging output for the OcNOS user. When the command is used without a parameter, it can be used by a OcNOS user to display the debug output on the terminal for the user local OcNOS. When used with a parameter, it may be used only by a OcNOS user.

The `no` form of the command terminates the debug output on the terminal. The OcNOS user can use this command. In addition, the OcNOS user can cancel a debug output from a specific VR or all VRs.

Command Syntax

```
terminal monitor
terminal monitor (all|WORD|)
terminal no monitor
terminal no monitor (WORD|)
```

Parameters

`WORD`	Used in the PVR context, and contains the VR name to be included in the debugging session.
`all`	Used the PVR context to include all VR in a PVR debugging session.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>Enable
#terminal monitor
#terminal no monitor
```

traceroute

Use this command to trace an IPv4/v6 route to its destination.

Command Syntax

```
traceroute WORD
traceroute WORD (vrf (NAME|management)|)
traceroute ip WORD
traceroute ip WORD (vrf (NAME|management)|)
traceroute ipv6 WORD
traceroute ipv6 WORD (vrf (NAME|management)|)
```

Parameters

`WORD`	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
`vrf`	Virtual Routing and Forwarding instance.
`NAME`	Virtual Routing and Forwarding name.
`management`	Virtual Routing and Forwarding name.
`ip`	IPv4 echo.
`WORD`	Destination address in A.B.C.D format or host name.
`ipv6`	IPv6 echo.
`WORD`	Destination address in X:X::X:X format or host name.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#traceroute ip 10.10.100.126 vrf management
traceroute to 10.10.100.126 (10.10.100.126), 30 hops max, 38 byte packets
 1  10.1.2.1 (10.1.2.1)  0.386 ms  0.315 ms  0.293 ms
 2  10.10.100.126 (10.10.100.126)  1.944 ms  1.497 ms  1.296 ms
#
```

watch static-mac-movement

Use this command to watch if any MAC movement is detected over static MAC entries for a time period. A notification will display if static MAC movement happens before the timer expires.

The counters can be validated with show interface counters queue-stats for the L2 movement queue (`Tx pkts` and `Dropped pkts` columns).

Without enabling `watch static-mac-movement`, the statistics are reflected in the `Rx EGR Port Unavail` of show interface counters queue-drop-stats.

For VXLAN, `watch static-mac-movement` applies to all the MAC entries learned from the remote peer (remote dynamic or static remote), as these learned MACs are installed as static MAC entries in the hardware.

Command Syntax

```
watch static-mac-movement (<1-300>|)
```

Parameters

`<1-300>`	Timer value in seconds.

Default

By default, the timer is 10 seconds

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#watch static-mac-movement
```

write

Use this command to a write the running configuration to the file used at startup or to a specified file. This is the same as the copy running-config startup-config command.

Command Syntax

```
write
write file FILE
write memory
write WORD
```

Parameters

FILE	Write to a given path and file. If you do not give a file path, the file is added to /root.
memory	Write to non-volatile memory.
WORD	Write to running configuration file path.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows writing the running configuration to the startup configuration file:

```
#write
Building configuration...
[OK]
```

This example shows writing the running configuration to a specified file:

```
#write file /home/test.txt
Building configuration...
[OK]
```

write terminal

Use this command to display the current configuration.

Command Syntax

```
write terminal
```

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#write terminal

Current configuration:
!
hostname ripd
password zebra
log stdout
!
debug rip events
debug rip packet
!
interface lo
!
interface eth0
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth1
 ip rip send version 1 2
 ip rip receive version 1 2
!
!
router rip
 network 10.10.10.0/24
 network 10.10.11.0/24
 redistribute connected
!
line vty
 exec-timeout 0 0
```

CHAPTER 2 Multi-Line Banner Support

Overview

Multi-Line Banner support enables you to configure banner messages spanning multiple lines.

Options to Configure Multi-Banner Message

Two options to facilitate the configuration of multi-line banner messages:

- Use escape character sequences within the CLI to format the banner message with appropriate line breaks and indentation. Supported escape character sequences enable flexible alignment and multi-line message display.

  The supported escape characters are:

Characters	Description
\"	double quote
\'	single quote
\‘	forward quote
\\	backslash
\f	form feed
\n	newline
\r	carriage return
\t	horizontal tab
\v	vertical tab

- Specify a local file containing the banner message. The content of the file is retrieved and displayed as the banner message

Multi-Banner Message Commands

The Multi-Banner Message uses the following configuration command.

banner motd file URL

Use this optional command to set the multi-line banner messages of the day (motd) at login. To set a customized or default message of the day, use banner motd command.

Use the `no` parameter to not display a banner message at login.

Note:

- Users are responsible for aligning the text of the banner. For instance, when using the "banner motd LINE" or "banner motd FILE" options, the alignment of the banner message output matches the alignment of the banner message input provided by the user.
- There is a restriction on the character count for banner messages, with a maximum limit of 1024 characters.
  - When using the FILE option to input a banner message, only the first 1024 characters from the file will be read and displayed as the banner output.
  - If the LINE option is used to input a banner message, only 1024 characters are allowed from the command line interface (CLI). If the user tries to include more than that, an error message such as "% Invalid input (Allowed length 1 - 1024):" will be displayed.
- When using the banner motd file option, consider the following:
  - The file must be available locally, and users must specify the file name along with the path during configuration.
  - Users are responsible for ensuring the correct file type, as there are no restrictions regarding the type of file allowed.
  - If the file content is empty, a notification log will be displayed to alert the user, and the default banner message will be shown.
  - If the file is removed or cannot be opened, an error log will be displayed to notify the user, and the default banner message will be shown.
- During a downgrade to a lower version that does not support the banner motd file option, if the banner motd file option is configured, the default banner message will be used.

Command Syntax

```
banner motd file URL
no banner motd
```

Parameters

`file`	A file input to set a custom message of the day.
`URL`	The file path and name containing the banner message

Default

Disabled

Command Mode

Configure mode

Applicability

Introduced before OcNOS version 1.3.

Examples

Example for LINE option with escape character sequence:

```
#configure terminal
(config)#banner motd Welcome\n To \n OcNOS
(config)#commit
(config)#exit
```

Example for using a specific file:

```
#configure terminal
(config)#banner motd file /home/ocnos/banner.txt
(config)#commit
(config)#exit
```

CHAPTER 3 Common Management Layer Commands

This chapter is a reference for the Common Management Layer (CML) commands.

Transaction are enabled by default. You can disable the feature by using the cmlsh transaction command outside of configuration mode, but IP Infusion Inc. does *not* recommend this.

These are the steps to follow to use transactions:

- When transactions are enabled, any changes done in configure mode are stored in a separate *candidate* configuration that you can view with the show transaction current command.
- When a configuration is complete, apply the candidate configuration to the running configuration with the commit command.
- If a commit fails, no configuration is applied as the entire transaction is considered failed. You can continue to change the candidate configuration and then retry the commit.
- Discard the candidate configuration with the abort transaction command.
- Check the last aborted transaction with the show transaction last-aborted command.

This chapter describes these commands:

- abort transaction
- cancel-commit
- cml force-unlock config-datastore
- cml lock config-datastore
- cml logging
- cml notification
- cml unlock config-datastore
- cmlsh cli-format
- cmlsh multiple-config-session
- cmlsh notification
- cmlsh transaction
- cmlsh transaction limit
- commit
- commit dry-run
- Commit Rollback
- confirm-commit
- debug cml
- module notification
- netconf translation openconfig
- save cml commit-history WORD
- show cml auto-config-sync state
- show cml bulk limit cpu state
- show cml cli-error status
- show cml commit-history state

- show cml commit-id rollover state
- show cml config-sync detail
- show cml database-dump
- show cmlsh multiple-config-session status
- show cmlsh notification status
- show json/xml commit config WORD
- show json/xml commit diff WORD WORD
- show max-transaction limit
- show module-info
- show running-config notification
- show system restore failures
- show transaction current
- show transaction last-aborted
- show (xml|json) running-config|candidate-config|startup-config

abort transaction

Use this command to end a configuration session and discard all uncommitted changes.

Command Syntax

```
abort transaction
```

Parameters

None

Default

N/A

Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#
(config)#interface eth2
(config-if)#ip address 10.12.3.4/24
(config-if)#exit
(config)#abort transaction
(config)#exit
#show running-config interface eth2
!
interface eth2
!
#
```

cancel-commit

Use this command to revert configuration changes immediately before the timeout in a “confirmed commit” operation.

Note: This command does not support the <persist-id> parameter as specified in RFC 6241.

Command Syntax

```
cancel-commit
```

Parameters

None

Default

N/A

Mode

All configuration modes

Applicability

This command was introduced in OcNOS version 6.3.0.

Example

```
(config)#router ospf 1
(config-router)#router ospf 2
(config-router)#commit confirmed timeout 100 description This is a test for confirmed
commit
(config-router)#
(config-router)#cancel-commit
```

cml force-unlock config-datastore

Use this command to release a configuration lock previously obtained with the cml lock config-datastore command by a *different* user.

This command is available only to users with the `network-admin` role.

A notification message is sent to the lock holder when forced out.

Command Syntax

```
cml force-unlock config-datastore (running|startup|candidate) (<0-600>|)
```

Parameters

`<0-600>`	Timeout interval to force out lock acquired by another user session. Zero (0) is immediate and is the default.
`running`	Release the lock on the running datastore.
`startup`	Release the lock on the startup datastore.
`candidate`	Release the lock on the candidate datastore.

Default

The default timeout is zero (0) which is immediate.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#cml force-unlock config-datastore running
```

cml lock config-datastore

Use this command to lock the entire configuration datastore of a device. Such locks are intended to be short-lived and allow you to make a change without fear of interaction with other users.

When the lock is acquired, the server prevents any changes to the locked resource other than those requested by this session.

The duration of the lock is defined as beginning when the lock is acquired and lasting until either the lock is released or the user session closes. The session closure can be explicitly performed by the user, or implicitly performed by the server based on criteria such as failure of the underlying transport, simple inactivity timeout, or detection of abusive behavior on the part of the client.

A lock will not be granted if any of the following conditions is true:

- A lock is already held by any user session or another entity.
- The target configuration is candidate, it has already been modified, and these changes have not been committed or rolled back.
- The target configuration is running, and another user session has an ongoing confirmed commit.

Command Syntax

```
cml lock config-datastore (running|startup|candidate)
```

Parameters

`running`	Lock on this datastore will not allow other sessions to perform operations with the target as running like commit, copy candidate to running and so on.
`startup`	Lock on this datastore will not allow other sessions to perform operations like copy-config and delete-config with the target startup
`candidate`	Lock on this datastore will not allow other sessions to perform operations with the target as candidate like edit-config, copy file candidate and so on. (Not supported in OcNOS version 5.1.)

Default

All three datastores are in the unlocked state.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#cml lock config-datastore running
#
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

           Line        User               Idle         Location/Session  PID     TYPE   Role

(#)(*) 130 vty 0    [C]ocnos              0d00h00m     pts/0             10732   Local  network-admin
```

cml logging

Use this command to enable or disable CML logging. The logging level and debug cml should also be configured.

Command Syntax

```
cml logging (enable | disable)
```

Parameters

`enable`	Enable CML logging
`disable`	Disable CML logging

Default

By default CML Logging is enabled.

Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#cml logging disable
```

cml notification

Use this command to enable or disable notification for a given CML client.

Command Syntax:

```
cml notification (enable|disable) (netconf|snmp|cmlsh|all)
```

Parameters

`disable`	Disable notification subscription
`enable`	Enable notification subscription
`all`	All CML clients
`cmlsh`	CML client CMLSH
`netconf`	CML client NETCONF
`snmp`	CML client SNMP

Default

By default, notification is enabled for all CML clients.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To enable notification for NETCONF client:

```
#cml notification enable netconf
```

To disable notification for NETCONF client:

```
#cml notification disable netconf
```

cml unlock config-datastore

Use this command to release a configuration lock previously obtained with the cml lock config-datastore command.

An unlock operation will not succeed if either of the following conditions is true:

- The specified lock is not currently active.
- The session calling tis command is not the same session that obtained the lock.

Command Syntax

```
cml unlock config-datastore (running|startup|candidate)
```

Parameters

`running`	Release the lock on the running datastore.
`startup`	Release the lock on the startup datastore.
`candidate`	Release the lock on the candidate datastore.

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#cml unlock config-datastore running
#
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

           Line        User               Idle         Location/Session  PID     TYPE   Role

   (*) 130 vty 0    [C]ocnos              0d00h00m     pts/0             10732   Local  network-admin

#
```

cmlsh cli-format

Use this command to display command strings in CLI error messages. By default, OcNOS displays error messages with Xpaths (path notation for navigating through the hierarchical structure of an XML document) which is not very clear for users.

Command Syntax

```
cmlsh cli-format (enable | disable)
```

Parameters

`enable`	Display command strings in CLI error messages.
`disble`	Display Xpaths in CLI error messages.

Default

Display Xpaths in CLI error messages

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.3.0.

Example

This is the default behavior where an Xpath is displayed:

```
>en
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ospf 10
(config-router)#area 3.3.3.3 interface xe1
(config-router)#commit
% Configuration " /ospfv2/processes/process[ospf-id='10']/areas/area[area-id='3.3.3.3']/interfaces/interface[name='xe1']/
vrf-name" depends on "/ospfv2/global/config/area-interface-config-mode"
% Failed to commit .. As error(s) encountered during commit operation…
```

If you enable this feature, the Xpath is replaced with the respective command string:

```
>en
#cmlsh cli-format enable
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ospf 10
(config-router)#area 3.3.3.3 interface xe1
(config-router)#commit
% Configuration "   area <value-option>  interface <value-option>" depends on "  ospf area-interface-config-mode"
% Failed to commit .. As error(s) encountered during commit operation…
```

cmlsh multiple-config-session

Use this command to enable or disable multiple CLI sessions to enter into configuration mode simultaneously.

With this support, multiple CLI users can enter into configuration mode simultaneously and do configurations in parallel and commit into the running datastore. This is similar to NetConf multiple session support described in RFC 6241.

When multiple configuration mode sessions are disabled, only one user can enter configuration mode and it will lock the running datastore.

If any CLI session is already there in configuration mode, error will be given when user tries to enable this mode.

A datastore lock can be acquired using the cml lock config-datastore command if you want to do configuration without fear of interaction with other user sessions.

This command is available only to users with the `network-admin` role.

This configuration is retained across reboots.

Command Syntax

```
cmlsh multiple-config-session (enable|disable)
```

Parameters

`enable`	Enable multiple configuration mode sessions.
`disable`	Disable multiple configuration mode sessions.

Default

By default, multiple CLI sessions are disabled.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#cmlsh multiple-config-session enable
#
#show cmlsh multiple-config-session status
CMLSh multiple configuration session mode : Enabled
#
```

Usage

Multiple users can enter into configuration mode simultaneously and do configurations in parallel and commit into the running datastore. Examples of when you need this feature are:

- Migrating to replace an existing device. If an existing device has a large configuration and it is only done by one person, it will take more time to configure. If multiple users can configure at same time, it will take less time.
- Troubleshooting and operating. Sometimes a single device has 2 or more links to troubleshoot. If only one user only can do configuration, it will take more time to resolve the problem.

When multiple sessions are doing parallel configurations, there is a chance that one user's configuration might conflict with another user's configuration.

If you do not lock the datastore before doing a configuration, a parallel candidate datastore can be created and will be allowed to commit to the datastore. So the datastore can change while the previous user is still having the configuration in its candidate. Now when the previous user tries to commit, if the configurations conflict, it will fail.

For example, if the previous user was adding a BGP neighbor and the BGP router itself is removed from the datastore via the parallel transaction, when this user tries to commit, it will fail. The reason is when commands are added to candidate, it only checks the running datastore at that point and allows them to be added to candidate configuration datastore. But later if the running datastore itself is changed, these configurations can be irrelevant and will cause an error on commit. So the user will have to abort the transaction.

cmlsh notification

Use this command to enable or disable notification for the current CMLSH session.

Command Syntax

```
cmlsh notification (enable|disable)
```

Parameters

`disable`	Disable notification subscription for current CMLSH session
`enable`	Enable notification subscription for current CMLSH session

Default

By default, notification is enabled for the CMLSH session.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To enable notification for current CMLSH session:

```
#cmlsh notification enable
```

To disable notification for current CMLSH session:

```
#cmlsh notification disable
```

cmlsh transaction

Use this command to enable or disable the transaction-based command-line interface.

Note: IP Infusion Inc. recommends that you do *not* disable transactions.

Command Syntax

```
cmlsh transaction (enable | disable)
```

Parameters

`enable`	Enable transaction-based command-line interface
`disable`	Disable transaction-based command-line interface

Default

The transaction-based command-line interface is enabled by default.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
>en
#cmlsh transaction disable
% Deprecated CLI. Disabling transaction mode is not recommended
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ipv6 ospf test
(config-router)#exit
(config)#show running-config router ipv6 ospf
!
router ipv6 ospf test
!
(config)#
```

cmlsh transaction limit

Use this command to set the maximum number of transactions.

To verify, give the show max-transaction limit command in exec mode.

Command Syntax

```
cml transaction limit <0-300000>
```

Parameters

<0-300000>	Maximum number of transactions with zero (0) indicating unlimited transactions.

Default

300,000 transactions

Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#cml transaction limit 1500
(config)#exit
#show max-transaction limit
Max-Transaction Limit is 1500
```

commit

Use this command to commit the candidate configuration to the running configuration.

Note: After a successful `commit` command, you must give the write command to save the running configuration to the startup configuration.

Note: Multiple configurations cannot be removed with a single `commit`. You must remove each configuration followed by a `commit`.

Optionally with “confirmed commit”, you can commit the configuration on a trial basis for a time specified in seconds. If you do not confirm within the specified time, the configuration will be reverted after the timeout.

- To revert the configuration before timeout, then give the cancel-commit command.
- To retain the configuration before timeout, then give the confirm-commit command.

See RFC 6241 “Confirmed Commit Capability”.

Note: A `commit` command without any parameters is treated as permanent and an explicit confirm-commit command is not required to confirm the commit.

Note: Multiple confirmed commits in the same session or different sessions are not supported. The `commit` command does not support the <persist-id> parameter as specified in RFC 6241.

Command Syntax

```
commit (confirmed (timeout <1-500>|)|) (description LINE|)
```

Parameters

`confirmed`	Commits the configuration on a trial basis.
`<1-500>`	Timeout in seconds after which configuration should be reverted if a confirmation is not given with confirm-commit. If not specified, the default timeout is 300 seconds.
`LINE`	Commit description up to 65 characters

Default

The default timeout is 300 seconds.

Mode

All configuration modes

Applicability

This command was introduced in OcNOS version 5.0 and the `confirmed` clause added in OcNOS version 6.3.0.

Example

```
(config)#router ospf 1
(config-router)#exit
(config)#router isis 3
(config-router)#commit
(config-router)#exit
(config)#show running-config ospf
!
router ospf 1
```

```
!
(config)#show running-config isis
!
router isis 3
!
(config)#
```

If you try to `exit` or `end`, you are prompted to commit or abort first:

```
(config)#router bgp 10
(config-router)#bgp as-local-count 34
(config-router)#exit
(config)#exit
% Un-committed transactions present. Please do commit or abort before exiting.
(config)#end
% Un-committed transactions present. Please do commit or abort before exiting.
(config)#commit
(config)#show running-config bgp
!
router bgp 10
 bgp as-local-count 34
!
(config)#
```

This is an example of a “confirmed commit”:

```
(config)#router ospf 1
(config-router)#router ospf 2
(config-router)#commit confirmed timeout 100 description This is Test for confirmed
commit
```

Usage

OcNOS validates dependencies when you commit. In this example, bridge 1 must exist before you can create a VLAN on it:

```
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
(config-vlan)#exit
(config)commit
```

Because of the unmet dependency, you get an error when you try to commit.

If you also create the bridge, the commit succeeds:

```
(config)#bridge 1 protocol mstp
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
(config-vlan)#exit
(config)commit
```

In a single transaction, dependent configurations can be given in any order. Using the same example as before, you can create the bridge *after* the VLAN:

```
(config)#vlan database
(config-vlan)#vlan 10 bridge 1
```

```
(config-vlan)#exit
(config)#bridge 1 protocol mstp
(config)commit
```

OcNOS supports “hitless merges” and does not write to the candidate configuration if you make the same configuration in separate transactions. In this example, subinterface xe1.1 is not created the second time because it already exists:

```
(config)#interface xe1.1
(config-if)#commit
(config)#interface xe1.1
(config-if)#commit
```

OcNOS does not write to the candidate configuration if you create and delete the same entity in the same transaction. You must create the entity and delete it with separate commits.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by the show transaction current command.

confirm-commit

Use this command to commit configuration changes before the timeout in a “confirmed commit” operation.

Note: This command does not support the <persist-id> parameter as specified in RFC 6241.

Command Syntax

```
confirm-commit
```

Parameters

None

Default

N/A

Mode

All configuration modes

Applicability

This command was introduced in OcNOS version 6.3.0.

Example

```
(config)#router ospf 1
(config-router)#router ospf 2
(config-router)#commit confirmed timeout 100 description This is a test for confirmed
commit
(config-router)#
(config-router)#confirm-commit
```

commit dry-run

Use this command to validate the current candidate configuration without committing.

Command Syntax

```
commit dry-run
```

Parameters

None

Default

N/A

Mode

All configuration modes

Applicability

This command was introduced in OcNOS version 6.3.0.

Example

```
OcNOS(config)#commit dry-run
```

debug cml

Use this command to enable or disable CML sub-module logging.

Command Syntax

```
debug cml (enable | disable) (events | engine | transaction | database | replace |
  smi | notification | all)
```

Parameters

`enable`	Enable debugging.
`disable`	Disable debugging.
`events`	Enable/disable events debugging
`engine`	Enable/disable engine debugging
`transaction`	Enable/disable transaction debugging
`database`	Enable/disable database debugging
`replace`	Enable/disable replace debugging
`smi`	Enable/disable SMI debugging
`notification`	Enable/disable notification debugging
`all`	Enable/disable all debugging

Default

By default, CML sub-module logging is disabled for all sub-modules.

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 4.2 and the `notification` parameter added in OcNOS version 6.1.0.

Example

```
#debug cml enable transaction
```

module notification

Use this command to enable or disable notification for a given protocol at a given notification severity level.

Command Syntax

```
module PROTOCOL_NAME notification (enable|disable) (severity
  (all|info|warning|minor|major|critical)|)
```

Parameters

`PROTOCOL_NAME`	Protocol name. Specify `all` for all protocols.
`enable`	Enable notification subscription
`disable`	Disable notification subscription
`severity`	If notification is enabled, then all notifications having severity higher than or equal to this severity allowed. If notification disabled then all the notifications having severity lower than or equal to this severity not allowed.
`all`	Notification severity all
`critical`	Notification severity critical
`info`	Notification severity info
`major`	Notification severity major
`minor`	Notification severity minor
`warning`	notification severity warning

Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To enable notification for NSM for all severity levels:

```
#module nsm notification enable
```

To disable notifications for NSM for all severity levels:

```
#module nsm notification disable
```

To enable notifications for NSM for severity levels higher than or equal to major (major and critical):

```
#module nsm notification enable severity major
```

To disable notifications for NSM for severity levels lower than or equal to minor (info, warning, and minor):

```
#module nsm notification disable severity minor
```

netconf translation openconfig

Use this command to enable or disable Netconf OpenConfig translation.

Use the `no` form of this command to Netconf translation.

Command Syntax

```
netconf translation openconfig
```

Parameters

`openconfig`	Translate NetConf to YANG
`no`	Disable OpencConfig translation

Default

Netconf OpenConfig translation is disabled.

Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 6.4.

Example

```
OcNOS# configure terminal
OcNOS(config)# netconf translation openconfig
OcNOS(config)# commit
```

save cml commit-history WORD

Use this command to save a specific commit entry mentioned by its commit ID.

Prerequisites

The `<cml commit-history>` functionality must be enabled for commit records to be stored in the commit history list to display the commit configuration.

Command Syntax

```
save cml commit-history WORD
```

Parameters

`WORD`	Specifies the commit ID of the commit entry to be saved. You can find the commit ID in the commit history list using the command `show commit list`.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.0.

Example

The following example shows the sequence of the commands to be performed to save the commit list and view it:

```
OcNOS#show commit list

S.No.         ID           User    Client         TimeStamp
Commit Status                    Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1703839538291276    root    cmlsh    29-12-2023 08:45:38
Confirmed                       NA
  2    1703849659767186    root    cmlsh    29-12-2023 11:34:19
Confirmed                       NA
  3    1703849669076279    root    cmlsh    29-12-2023 11:34:29
Confirmed                       NA

OcNOS#save cml commit-history
OcNOS#save cml commit-history ?
  WORD  Commit-id of commit entry to be saved

OcNOS#save cml commit-history 1703839538291276
OcNOS#show commit saved list

S.No.         ID           User    Client         TimeStamp
Commit Status                    Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

```
      1    1703839538291276    root    cmlsh    29-12-2023 08:45:38
    Confirmed                          NA

    OcNOS#show commit list

    S.No.          ID            User    Client         TimeStamp
    Commit Status                      Description
    ~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
      1    1703839538291276    root    cmlsh    29-12-2023 08:45:38
    Confirmed                          NA
      2    1703849659767186    root    cmlsh    29-12-2023 11:34:19
    Confirmed                          NA
      3    1703849669076279    root    cmlsh    29-12-2023 11:34:29
    Confirmed                          NA

OcNOS#
```

show cml auto-config-sync state

Use this command to inspect the status and functionality of automatic configuration synchronization in a CML environment.

Command Syntax

```
show cml auto-config-sync state
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

```
#Disable auto db sync:
OcNOS#cml auto-config-sync disable

#Configure the CLI that is causing the issue

#Do the config check manually:
OcNOS#cml config-sync check

#Compare the tables in both running and temporary databases:
sqlite3 /cfg/usr/local/etc/CML_RD.db
sqlite> select * from ipiCMLSEPifCMLSEPip_ipv4;
cmlAutoDummy4097|name|cmlAutoDummy3073
4097|lo.management|3073
4097|lo|3073

sqlite3 /tmp/.CML_TMP_DB.db
sqlite> select * from ipiCMLSEPifCMLSEPip_ipv4;
cmlAutoDummy4097|name|cmlAutoDummy3073
4097|lo.management|3073
4097|eth0|3073
4097|lo|3073
```

show cml bulk limit cpu state

Use this command to enable or disable CPU limitation when applying bulk configurations and should be used to prevent CPU spikes and system degradation during the apply process.

Command Syntax

```
show cml bulk limit cpu state
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.5.1.

Example

```
OcNOS#show cml bulk ?
  limit  limitation

OcNOS#show cml bulk limit ?
  cpu  cpu

OcNOS#show cml bulk limit cpu ?
  state  status (enabled | disabled)

OcNOS#show cml bulk limit cpu state ?
  |  Output modifiers
  >  Output redirection
  <cr>

OcNOS#show cml bulk limit cpu state
bulk timeout prompt config status is disabled

# show cml bulk limit cpu state
bulk timeout prompt config status is enabled
```

show cml cli-error status

Use this command to know the status of the cli-error feature.

Command Syntax

```
show cml cli-error status
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

```
OcNOS#show cml cli-error status
cmlsh cli-error feature disabled
OcNOS#
OcNOS#cmlsh cli-format enable
OcNOS#show cml cli-error status
cmlsh cli-error feature enabled
```

show cml commit-history state

Use this command to verify whether the CMLSH commit confirmed and commit rollback feature is enabled or disabled.

Command Syntax

```
show cml commit-history state
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

```
OcNOS#
OcNOS#show cml commit-history state
cml commit-history feature is enabled
```

show cml commit-id rollover state

Use this command to check commit-id rollover is enabled or not. If it is enabled after max commit-history count, old commit entry gets deleted and it adds new commit entry to the commit-history list.

Command Syntax

```
show cml commit-id rollover state
```

Parameters

None

Default

Enabled

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

```
OcNOS#show cml commit-id rollover state
cml commit-id rollover feature is enabled
```

show cml config-sync detail

Use this command to check information on database sync issue, if there is mismatch in database and show running config, it will display information of invalid config with table name and values.

Command Syntax

```
show cml config-sync detail
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

```
OcNOS#show cml config-sync detail
CREATE: it indicates that mentioned config is removed from DB but present in 'show
running-config' output
DELETE: it indicates that mentioned config is present in DB but does not exist in 'show
running-config' output
UPDATE1: it indicates incorrectly modified attribute value in DB. Attribute value needs
to modify as present in UPDATE2
UPDATE2: it indicates correct attribute value present in 'show running-config' output


Config datastore check done at 08-Jan-2024 at 15:31:13;


[Invalid Config from DB]:  UPDATE1:INSERT INTO
"ipiCMLSEPtimeCMLSEPrange_timeCMLSEPranges_timeCMLSEPrange_endCMLSEPtimeCMLSEPoptions_c
onfig" VALUES(135688,135687
,'1',135681,'2:53 15 sep 2023','?');


[    Running Config    ]:  UPDATE2:INSERT INTO
"ipiCMLSEPtimeCMLSEPrange_timeCMLSEPranges_timeCMLSEPrange_endCMLSEPtimeCMLSEPoptions_c
onfig" VALUES(135688,135687
,'1',135681,'02:53 15 sep 2023','?');
```

show cml database-dump

Use this command to display information such as the status, size, creation date, and other relevant details about the specified database dump.

Command Syntax

```
show cml database-dump (WORD|) (candidate|)
```

Parameters

Field	Description
WORD	Refers to the specific name or identifier of the database dump you want to inspect.
candidate	Indicates that querying information about a candidate database dump.

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.4.

Example

Ocnos# show cml database-dump my_database_dump candidate

Database dump "my_database_dump" details:

- Name: my_database_dump
- Type: Candidate
- Status: Complete
- Size: 512 MB
- Creation Time: 2024-05-03 10:15:00
- Location: /var/cml/database_dumps/my_database_dump

show cml notification status

Use this command to display notification status (enabled or disabled) for all CML clients.

Command Syntax

```
show cml notification status
```

Parameters

None

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To show notification status for all clients:

```
#show cml notification status
NETCONF notification enabled
CMLSH notification enabled
SNMP notification enabled
```

show cmlsh multiple-config-session status

Use this command to display the multiple configuration mode session setting.

Command Syntax

```
show cmlsh multiple-config-session status
```

Parameters

None

Default

N/A

Mode

Privileged exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
#cmlsh multiple-config-session enable
#
#show cmlsh multiple-config-session status
CMLSh multiple configuration session mode : Enabled
#
```

show cmlsh notification status

Use this command to display the notification status (enabled or disabled) for the current CMLSH session.

Command Syntax

```
show cmlsh notification status
```

Parameters

None

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To show notification status for the CMLSH session.

```
# OcNOS#show cmlsh notification status
CMLSH notification enabled.
```

show json/xml commit config WORD

Use this command to display the full running system configurations of the specified commit ID in JSON or XML format.

Prerequisites

The `<cml commit-history>` functionality must be enabled for commit records to be stored in the commit history list to display the commit configuration.

Command Syntax

```
show json/xml commit config WORD
```

Parameters

`WORD`	Specifies the commit ID of the recorded commit operations that is found in the commit-history list. You can find the commit ID in the commit history list using the command `show commit list`.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.0.

Example

The following example shows the sequence of the commands to be performed to view the running configuration in JSON format:

```
OcNOS#show commit list

S.No.          ID           User    Client         TimeStamp
Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1703839538291276    root    cmlsh    29-12-2023 08:45:38
Confirmed                          NA

OcNOS#show json commit ?
  config  Full snapshot of a system configurations
  diff    Difference of two different commit id

OcNOS#show json commit config ?
  WORD  Commit-id of a commit record from commit histroy list

OcNOS#show json commit config
```

show json/xml commit diff WORD WORD

Use this command to display configuration changes from the 1st commit operation to the 2nd commit operation.

Prerequisites

The `<cml commit-history>` functionality must be enabled for commit records to be stored in the commit history list to display the commit configuration.

Command Syntax

```
show json/xml commit diff WORD WORD
```

Parameters

`WORD`	Specifies the starting commit ID from which you want to see the difference in recorded commit operations. You can find the commit ID in the commit history list using the command `show commit list`.
`WORD`	Specifies the starting commit ID to which you want to see the difference in recorded commit operations. You can find the commit ID in the commit history list using the command `show commit list`.

Default

None

Command Mode

Exec mode

Applicability

Introduced in OcNOS version 6.5.0.

Example

The following example shows the sequence of the commands to be performed to view difference between the commits in JSON format:

```
OcNOS#show commit list

S.No.         ID           User    Client         TimeStamp
Commit Status                    Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~
  1    1703839538291276    root    cmlsh    29-12-2023 08:45:38
Confirmed                       NA
  2    1703849659767186    root    cmlsh    29-12-2023 11:34:19
Confirmed                       NA
  3    1703849669076279    root    cmlsh    29-12-2023 11:34:29
Confirmed                       NA

OcNOS#show json commit diff 1703849659767186 1703849669076279
@@ -153,6 +153,14 @@
             "vrf-name":"default",
             "router-id":"2.2.2.2"
```

```
            }
+         },
+         {
+           "ospf-id":"3",
+           "config":{
+             "ospf-id":"3",
+             "vrf-name":"default",
+             "router-id":"3.3.3.3"
+           }
          }
        ]
      }
OcNOS#
```

show max-transaction limit

Use this command to display the maximum number of transactions.

Command Syntax

```
show max-transaction limit
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#show max-transaction limit
Max-Transaction Limit is 30000
```

show module-info

Use this command to display module's config and state configuration for any top-level object in the data model. This command can be used to display module configuration in XML or JSON format. This command is equivalent to a NETCONF GET operation.

Command Syntax

```
show module-info OBJECT_NAME format (xml|json)
```

Parameters

`OBJECT_NAME`	Name of the object, such as ISIS or OSPF
`xml`	XML output format
`json`	JSON output format

Mode

All modes

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To display the user-session module's config and state configuration in XML format:

```
#show module-info user-session format xml
<user-session xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-user-session-management">
  <sessions>
    <session>
      <id>pts/0</id>
      <state>
        <id>pts/0</id>
        <user-role>network-admin</user-role>
        <type>Local</type>
        <process-identifier>1099</process-identifier>
        <idle-time>0d00h00m</idle-time>
        <client-type>CLI</client-type>
        <user-name>root</user-name>
        <line>130 vty 0</line>
      </state>
    </session>
  </sessions>
</user-session>
```

To display the user-session module's config and state configuration in JSON format:

```
#show module-info user-session format json
{
  "user-session":{
    "sessions":{
      "session":[
```

```
        {
          "id":"pts/0",
          "state":{
            "id":"pts/0",
            "user-role":"network-admin",
            "type":"Local",
            "process-identifier":"1099",
            "idle-time":"0d00h00m",
            "client-type":"CLI",
            "user-name":"root",
            "line":"130 vty 0"
          }
        }
      ]
    }
  }
}
```

show running-config notification

Use this command to display the notification status (enabled or disabled) and notification severity levels.

Command Syntax:

```
show running-config notification
```

Parameters

None

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.0.0.

Example

To display the notification status and notification severity levels.

```
#show running-config notification
!
module nsm notification enable severity major
!
```

show system restore failures

Use this command to display configuration restoration status after save reload device.

Command Syntax

```
show system restore failures
```

Parameters

None

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

Configuration restoration successful status information after save reload device:

```
#show system restore failures
Configuration restore from DB is completed.
Total no. of failed configuration objects = 0
```

Configuration restoration failure status information after save reload device:

```
#show system restore failures
Configuration restore from DB is completed.
Total no. of failed configuration objects = 1.

Failed Protocols information :
Protocol Name=ipi-interface, Protocol Id=3 :
Failed configuration object information :
Total no. of failed configuration objects = 1.
  Object Name = config, DN = cmlAutoDummy3074=3074,name=eth0,cmlAutoDummy3073=3073 :
  Error Information :
  Total no. of configuration errors = 1.
    ErrorCode = -16946, ErrorMessage = % No such VRF, ErrorXpath =  /interfaces/
interface[name='eth0']/config.
```

show transaction current

Use this command to display the current transaction.

Mode changes, action items (such as `clear interface counters`), and `show` commands are not part of a transaction and are not displayed by this command.

Command Syntax

```
show transaction current
```

Parameters

None

Default

N/A

Mode

Exec mode and configure mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#interface eth3
(config-if)#description testing
(config-if)#mtu 664
(config-if)#exit
(config)#show transaction current
interface eth3
description testing
mtu 664
```

show transaction last-aborted

Use this command to display the last aborted transaction.

Command Syntax

```
show transaction last-aborted
```

Parameters

None

Default

N/A

Mode

Exec mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#router isis 4
(config-router)#isis wait-timer 45
(config-router)#net 11.22.33
(config-router)#exit
(config)#commit
%% Invalid NET length -  /isis/isis-instance[instance='4']/config
(config)#show running-config isis
!
!
(config)#abort transaction
(config)#exit
#show transaction last-aborted
router isis 4
isis wait-timer 45
net 11.22.33
#
```

show (xml|json) running-config|candidate-config|startup-config

Use this command to display the running or candidate or startup system configuration for any top-level object in the data model. This CLI can also be used for display full running or candidate or startup system configuration for all protocol modules. This command can be used to display running or candidate or startup system configuration in xml or json format. This command is equivalent to a NETCONF GET-CONFIG operation.

Command Syntax

```
show (xml|json) (running-config | candidate-config | startup-config) OBJECT_NAME
```

Parameters

`xml`	XML output format
`json`	JSON output format
`candidate-config`	Candidate system configuration
`running-config`	Running system configuration
`startup-config`	Startup system configuration
`OBJECT_NAME`	Name of the object, such as ISIS or OSPF

Mode

All modes

Applicability

This command was introduced before OcNOS version 4.2 and updated in OcNOS version 6.0.0.

Example

To display the top level objects:

```
#show xml running-config
arp                 bfd                 bgp                 dhcp                evpn                evpn-mpls
interfaces          ip-global           isis                key-chains          lacp                layer2-global
ldp                 lldp                logging             mpls                neighbor-discovery  network-instances
ospfv2              pcep                ping                prefixes            routemaps           routing
rsvp-te             segment-routing     system-info         tacacs              time-ranges         vlan-classifier
vpls                vpws                vxlan
```

To display the ISIS running configuration in XML format:

```
#show xml running-config isis
<isis xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
  <isis-instance xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
  <instance>1</instance>
  <config xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-isis">
    <instance>1</instance>
    <vrf-name>default</vrf-name>
  </config>
  </isis-instance>
</isis>
```

To display the logging running configuration in XML format:

```
#show xml running-config logging
<logging xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-logging">
  <rsyslog>
    <vrf>default</vrf>
    <config>
      <vrf>default</vrf>
      <enable-rsyslog>rsyslog</enable-rsyslog>
    </config>
  </rsyslog>
</logging>
```

To display the logging running configuration in JSON format:

```
#show json running-config logging
{
   "logging":{
      "rsyslog":[
         {
            "vrf":"default",
            "config":{
            "vrf":"default",
            "enable-rsyslog":"rsyslog"
            }
         }
      ]
   }
}
```

To display the OSPFv2 candidate configuration in XML format:

```
#show xml candidate-config ospfv2
<ospfv2 xmlns="http://www.ipinfusion.com/yang/ocnos/ipi-ospf">
  <processes>
    <process>
      <ospf-id>1</ospf-id>
      <config>
        <ospf-id>1</ospf-id>
        <vrf-name>default</vrf-name>
      </config>
    </process>
  </processes>
</ospfv2>
```

To display the OSPFv2 candidate configuration in JSON format:

```
#show json candidate-config ospfv2
{
  "ospfv2":{
    "processes":{
      "process":[
        {
          "ospf-id":"1",
          "config":{
            "ospf-id":"1",
```

```
              "vrf-name":"default"
            }
          }
        ]
      }
    }
}
```

CHAPTER 4 Remote Management Commands

This chapter is a reference for commands that copy these types of files:

- Start-up configuration and running configuration
- System files such as boot files, core dumps, and debug logs

Users can use these commands to copy files locally or to copy between the local device and a remote system.

The commands in this chapter use the techniques in Table 4-9 to remotely transfer files:

Table 4-9: File transfer techniques

Trivial File Transfer Protocol (TFTP)	No authentication or encryption; dangerous to use over the Internet, but might be acceptable in a trusted environment Address format: `tftp:[//server[:port]][/path]`
File Transfer Protocol (FTP)	Authenticates, but does not encrypt Address format: `ftp:[//server][/path]`
Secure copy (SCP)	Authenticates and encrypts using Secure Shell (SSH1) Address format: `scp:[//server][/path]`
SSH File Transfer Protocol (SFTP)	Authenticates and encrypts using Secure Shell (SSH2); this is the most secure technique Address format: `sftp:[//server][/path]`
Hyper text Transfer Protocol (HTTP)	Address format: `http:[//server][/path]` For download of running and startup configurations

This chapter contains these commands.

- copy running-config
- copy running-config (interactive)
- copy startup-config
- copy startup-config (interactive)
- copy system file
- copy system file (interactive)
- copy ftp startup-config
- copy scp filepath
- copy scp startup-config
- copy sftp startup-config
- copy tftp startup-config
- copy http startup-config
- copy ftp startup-config (interactive)
- copy scp startup-config (interactive)
- copy tftp startup-config (interactive)
- copy http startup-config (interactive)
- copy file startup-config
- load-config

copy running-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http HTTP-URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp sftp://sftp.mysite.com/running_conf vrf management
```

copy running-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy running-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy running-config sftp vrf management
```

copy startup-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL|http
  HTTP_URL) (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`HTTP-URL`	Destination: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp sftp://sftp.mysite.com/start-up_conf vrf management
```

copy startup-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, a TFTP server or an HTTP server.

Command Syntax

```
copy startup-config (ftp|tftp|scp|sftp|http) (vrf (NAME|management)|)
```

Parameters

`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`http`	Destination: HTTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy startup-config sftp vrf management
```

copy system file

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy core myFile sftp sftp://sftp.mysite.com/dst_filename vrf management

#copy techsupport tech_support_23_Feb_2001_18_27_00.tar.gz scp scp://
10.12.16.17/home/satya/tech_support_23_Feb_2001_18_27_00.tar.gz vrf management
Enter Username:root
Enter Password:
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
100 72368 0 0 0 72368 0 147k -::- -::- -::- 147k
Copy Success
```

copy system file (interactive)

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log|techsupport|filepath) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-
  URL|sftp SFTP-URL)(vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to `/var/log/`
`techsupport`	Copy techsupport log files to remote machine
`filepath`	Copy device file to remote machine
`FILE`	Source file name
`TFTP-URL`	Destination: `tftp://server[:port]][/path]`
`FTP-URL`	Destination: `ftp://server][/path]`
`SCP-URL`	Destination: `scp://server][/path]`
`SFTP-URL`	Destination: `sftp://server][/path]`
`ftp`	Destination: FTP server
`tftp`	Destination: TFTP server
`scp`	Destination: SCP server
`sftp`	Destination: SFTP server
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy log myFile sftp sftp://sftp.mysite.com/dst_filename vrf management
```

copy ftp startup-config

Use this command to copy the start up configuration from an FTP server to the local device.

Command Syntax

```
copy ftp FTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`FTP-URL`	Configuration source: `ftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename startup-config vrf management
```

copy scp filepath

Use this command to copy the remote system file using SCP to the local device.

Note: OcNOS has a dedicated partition called `/cfg` for storing system level configurations, OcNOS configurations and license data. This is persistent across reboots and upgrades and consists of directories `/cfg/` and `/usr/local/etc`. Copying `user/general` files under `/cfg` partition is discouraged because the size of this partition is very small and impacts normal system operations like `bootup/upgrades` and important system files copy when it doesn't have enough space. Users are recommended to use `/home` to copy the general files. Please note that the contents placed in `/home` directory are deleted upon software upgrade.

Command Syntax

```
copy scp SCP-URL (filepath FILEPATH) (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`FILEPATH`	Enter the local filesystem path with filename
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#copy scp scp://10.12.65.89/root/cmlsh filepath /root/cmlsh vrf management
```

copy scp startup-config

Use this command to copy the start up configuration from a SCP server to the local device.

Command Syntax

```
copy scp SCP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`SCP-URL`	Configuration source: `scp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp scp://scp.mysite.com/scr filename startup-config vrf management
```

copy sftp startup-config

Use this command to copy the start up configuration from a SFTP server to the local device.

Command Syntax

```
copy sftp SFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`SFTP-URL`	Configuration source: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp sftp://sftp.mysite.com/scr filename startup-config vrf management
```

copy tftp startup-config

Use this command to copy the start up configuration from a TFTP server to the local device.

Command Syntax

```
copy tftp TFTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`TFTP-URL`	Configuration source: `tftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename startup-config vrf management
```

copy http startup-config

Use this command to copy the start up configuration from an HTTP server to the local device.

Command Syntax

```
copy http HTTP-URL startup-config (vrf (NAME|management)|)
```

Parameters

`HTTP-URL`	Configuration source: `http:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http http://http.mysite.com/scr filename startup-config vrf management
```

copy ftp startup-config (interactive)

Use this command to copy the start up confguration from an FTP server to the local device.

Command Syntax

```
copy ftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy ftp startup-config vrf management
```

copy scp startup-config (interactive)

Use this command to copy the start up confguration from a SCP server to the local device.

Command Syntax

```
copy scp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy scp startup-config vrf management
```

copy sftp startup-config (interactive)

Use this command to copy the start up confguration from an SFTP server to the local device.

Command Syntax

```
copy sftp startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy sftp startup-config vrf management
```

copy tftp startup-config (interactive)

Use this command to copy the start-up confguration from a TFTP server to the local device.

Command Syntax

```
copy tftp startup-config (vrf (NAME|management)|)
```

Parameters

`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy tftp startup-config vrf management
```

copy http startup-config (interactive)

Use this command to copy the start-up confguration from an HTTP server to the local device.

Command Syntax

```
copy http startup-config (vrf (NAME|management)|)
```

Parameters

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy http startup-config vrf management
```

copy file startup-config

Use this command to copy and store a local file into the startup configuration.

Command Syntax

```
copy file FILE startup-config
```

Parameters

FILE	File name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#copy file myFile startup-config
```

load-config

Use this command to copy a configuration file from either the remote or local file system and apply it to the running-config.

Command Syntax

```
load-config ((scp SCP-URL) | (filepath FILEPATH))
```

Parameters

SCP-URL	Configuration source in the format `scp:[//server][/path]`
FILEPATH	Enter the local file system path with the filename.

Command Mode

Privileged Exec mode

Applicability

This command was introduced in OcNOS version 6.4.1.

Example

For instance, when retrieving a configuration from a remote source, the command might be used as follows:

Remote:

```
Remote#cat /home/config.txt
interface eth2
 ip address 3.3.3.5/24
```

Device:

```
OcNOS#load-config scp scp://10.12.43.155/home/config.txt
Enter Username:root
Enter Password:
Enter configuration commands, one per line.  End with CNTL/Z.
Please wait. System is restoring previous saved configs..
This may take sometime. Please don't abort....
 50% [||||||||||||||||||||||||                         ]
Please wait. Starting commit operation..
This may take sometime. Please don't abort....
100% [||||||||||||||||||||||||||||||||||||||||||||||||||]
```

CHAPTER 5 Interface Commands

This chapter is a reference for each of the interface commands.

- admin-group
- bandwidth
- bandwidth-measurement static uni-available-bandwidth
- bandwidth-measurement static uni-residual-bandwidth
- bandwidth-measurement static uni-utilized-bandwidth
- clear hardware-discard-counters
- clear interface counters
- clear interface cpu counters
- clear interface fec
- clear ip prefix-list
- clear ipv6 neighbors
- clear ipv6 prefix-list
- debounce-time
- delay-measurement dynamic twamp
- delay-measurement a-bit-min-max-delay-threshold
- delay-measurement static
- delay-measurement a-bit-delay-threshold
- description
- duplex
- fec
- flowcontrol
- hardware-profile port-config
- hardware-profile portmode
- if-arbiter
- interface
- ip address A.B.C.D/M
- ip address dhcp
- ip forwarding
- ip prefix-list
- ip proxy-arp
- ip remote-address
- ip unnumbered
- ip vrf forwarding
- ipv6 address
- ipv6 forwarding

© 2025 IP Infusion Inc. Proprietary

- ipv6 prefix-list
- ipv6 unnumbered
- link-debounce-time
- loopback
- loss-measurement dynamic
- loss-measurement uni-link-loss
- mac-address
- mac-address secondary peer-mlag
- monitor speed
- monitor queue-drops
- monitor speed threshold
- mtu
- multicast
- show flowcontrol
- show hardware-discard-counters
- show interface
- show interface capabilities
- show interface counters
- show interface counters drop-stats
- show interface counters error-stats
- show interface counters (indiscard-stats|outdiscard-stats)
- show interface counters protocol
- show interface counters queue-drop-stats
- show interface counters queue-stats
- show interface counters speed
- show interface counters summary
- show interface fec
- show ip forwarding
- show ip interface
- show ip prefix-list
- show ip route
- show ip vrf
- show ipv6 forwarding
- show ipv6 interface brief
- show ipv6 route
- show ipv6 prefix-list
- show hosts
- show running-config interface
- show running-config interface ip

© 2025 IP Infusion Inc. Proprietary

- show running-config interface ipv6
- show running-config ip
- show running-config ipv6
- show running-config prefix-list
- shutdown
- speed
- switchport
- switchport allowed ethertype
- switchport protected
- transceiver
- tx cdr-bypass
- rx cdr-bypass

admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in configure mode, then interfaces are added to the group in interface mode.

Use the `no` parameter with this command to disable this command.

Command Syntax

```
admin-group NAME
no admin-group NAME
```

Parameters

`NAME`	Name of the admin group to add.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

In the following example, the `eth3` interface is added to the group `myGroup`:

```
#configure terminal
(config)#interface eth3
(config-if)#admin-group myGroup
```

bandwidth

Use this command to specify a discrete, maximum bandwidth value for the interface.

Use the `no` parameter resets the interface's bandwidth to the default value.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameter

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

Default bandwidth is the link speed of the interface. For LAG, default bandwidth will be collective bandwidth of its member ports. For VLAN interface, default bandwidth is 1 gigabits/sec.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface xe4
(config-if)#bandwidth 100m
```

bandwidth-measurement static uni-available-bandwidth

Use this command to advertise the available bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset available bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement static uni-available-bandwidth BANDWIDTH
no bandwidth-measurement static uni-available-bandwidth
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement static uni-available-bandwidth 10k
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement static uni-available-bandwidth
(config-if)#commit
```

bandwidth-measurement static uni-residual-bandwidth

Use this command to advertise the residual bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset residual bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement static uni-residual-bandwidth BANDWIDTH
no bandwidth-measurement static uni-residual-bandwidth
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#interface ethernet 2
(config-if)#bandwidth-measurement static uni-residual-bandwidth 10g
(config-if)#commit

(config)#interface ethernet 2
(config-if)#no bandwidth-measurement static uni-residual-bandwidth
(config-if)#commit
```

bandwidth-measurement static uni-utilized-bandwidth

Use this command to advertise the utilized bandwidth between two directly connected OSPF/ISIS neighbors.

Use the `no` parameter with this command to unset utilized bandwidth on the current interface.

Command Syntax

```
bandwidth-measurement static uni-utilized-bandwidth BANDWIDTH
no bandwidth-measurement static uni-utilized-bandwidth
```

Parameter

`BANDWIDTH`	<0-999>k for 0 to 999 kilo bits/s
	<0-999>m for 0 to 999 mega bits/s
	<0-100>g for 0 to 100 giga bits/s

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#int eth2
(config-if)#bandwidth-measurement static uni-utilized-bandwidth 10m
(config-if)#commit

(config)#int eth2
(config-if)#no bandwidth-measurement static uni-utilized-bandwidth
(config-if)#commit
```

clear hardware-discard-counters

Use this command to clear device level discard counters.

Command Syntax

```
clear hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Examples

```
#clear hardware-discard-counters
```

clear interface counters

Use this command to clear the statistics on a specified interface or on all interfaces.

Note: This command is not supported on loopback interfaces or the out-of-band management (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) counters
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface xe0 counters
```

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax

```
clear interface cpu counters
```

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface cpu counters
```

clear interface fec

Use this command to clear FEC (forward error correction) statistics on a specified interface or on all interfaces.

Note: This command is not supported on loop-back interfaces or the out-of-band (OOB) management interface.

Command Syntax

```
clear interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear interface ce1/1 fec
```

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

Command Syntax

```
clear ip prefix-list
clear ip prefix-list WORD
clear ip prefix-list WORD A.B.C.D/M
```

Parameters

WORD	Name of the prefix-list.
A.B.C.D/M	IP prefix and length.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ip prefix-list List1
```

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Command Syntax

```
clear ipv6 neighbors
```

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 neighbors
```

clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

Command Syntax

```
clear ipv6 prefix-list
clear ipv6 prefix-list WORD
clear ipv6 prefix-list WORD X:X::X:X/M
```

Parameters

`WORD`	Name of the prefix-list.
`X:X::X:X/M`	IP prefix and length.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#clear ipv6 prefix-list List1
```

debounce-time

Use this command to set the debounce time for a interface.

The debounce timer avoids frequent updates (churn) to higher layer protocol during interface flapping. If the status of a link changes quickly from up to down and then back to up, the port debounce timer suppresses the link status notification. If the link transitions from up to down, but does not come back up, the port debounce timer delays the link status notification.

Note: Keep the following in mind when using the debounce timer:

- Debounce is not applicable for admin down operations.
- Debounce timer is supported only for physical L2 and L3 interfaces.
- The debounce flap-count refers to the number of flaps OcNOS receives while the debounce timer is running:
  - The flap-count is only updated if the timer is still running and OcNOS receives a link status event for the interface.
  - The flap-count is reset at the subsequent start of the debounce timer.
- Protocol-specific timers such as BFD which depend on the link status should be configured to a minimum of 1.5 times the value of the debounce timer. Otherwise it could affect the protocol states if the debounce timer is still running.

Use the `no` form of this command to turn-off the debounce timer on a interface.

Command Syntax

```
debounce-time <250-5000>
no debounce-time
```

Parameters

`<250-5000>`	Timer value in milliseconds.

Default

By default, disabled.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 1.3.8.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#debounce-time 4000
```

delay-measurement dynamic twamp

This command will start the measurement on the interface by using the "interfaces" profile.

The user should be aware that the IP used as a reflector IP must be a directly connected IP.

In case hostname needs to be used, the user must be sure about the hostnames configured in the network.

In case the user configures the delay-measurement with a certain hostname and then the hostname entry in the DNS changes, the delay-measurement must be unconfigured and configured again for the new configuration to take effect (a clear command would not be sufficient in this situation)

Use the `no` form of this command to stop the delay measurement.

Command Syntax

```
delay-measurement dynamic twamp reflector-ip (HOSTNAME | X:X::X:X | A.B.C.D)
  (reflector-port <1025-65535>|) (sender-ip (HOSTNAME | X:X::X:X | A.B.C.D)|) (dscp
  WORD|)
no delay-measurement dynamic twamp reflector-ip (HOSTNAME | X:X::X:X | A.B.C.D)
```

Parameters

`twamp`	This parameter specifies the protocol to be used to do the measurement. It is the only protocol available in this implementation. The subsequent parameters in this command are specific to the protocol chosen (TWAMP).
`reflector-ip`	Specify the reflector ip/hostname used to send the TWAMP packets to
`HOSTNAME`	The hostname of the reflector
`X:X::X:X`	The ip address of the reflector
`A.B.C.D`	The ip address of the reflector
`reflector-port`	specify the UDP port of the TWAMP reflector
`<1025-65535>`	The reflector port value
`sender-ip`	Specify the IP used to send the TWAMP packets from (must be an IP configured on the current interface)
`HOSTNAME`	The hostname of the reflector
`X:X::X:X`	The ip address of the reflector
`A.B.C.D`	The ip address of the reflector
`dscp`	Specify the dscp value used during this measurement
`WORD`	The dscp value

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.1.

Example

```
(config)#
(config)#interface xe7
```

```
(config-if)#delay-measurement dynamic twamp reflector-ip 23.1.1.2 sender-ip
23.1.1.1 dscp 24
(config-if)#commit


(config-if)#no delay-measurement dynamic twamp reflector-ip 23.1.1.2
(config-if)#commit
```

delay-measurement a-bit-min-max-delay-threshold

Use this command to advertise the minimum and maximum delay values between two directly connected IS-IS/OSPF neighbors.

The A bit is set when one or more measured values exceed a configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset a-bit-min-max-delay-threshold on the current interface.

Command Syntax

```
delay-measurement a-bit-min-max-delay-threshold min <1-16777215> <1-16777215> max
  <1-16777215> <1-16777215>)
no delay-measurement a-bit-min-max-delay-threshold
```

Parameter

`min`	Reuse threshold
`<1-16777215>`	Reuse threshold value of Min-Delay in microseconds
`<1-16777215>`	Reuse threshold value of Max-Delay in microseconds
`a-bit-threshold`	Threshold values to set/clear A-bit
`max`	Maximum threshold
`<1-16777215>`	Maximum threshold value of Min-Delay in microseconds
`<1-16777215>`	Maximum threshold value of Max-Delay in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
 (config-if)#delay-measurement a-bit-min-max-delay-threshold min 11 22 max 33
44
(config-if)#no delay-measurement a-bit-min-max-delay-threshold
```

delay-measurement static

Use this command to advertise static the minimum and maximum delay values or average link delay variation or average link delay values between two directly connected IS-IS/OSPF neighbors.

Use the `no` parameter with this command to unset min-max-uni-link-delay, uni-delay-variation and uni-link-delay static values on the current interface.

Command Syntax

```
delay-measurement static (min-max-uni-link-delay <1-16777215> <1-16777215> |  uni-
  delay-variation  <0-16777215> |  uni-link-delay <1-16777215>)
no delay-measurement static (min-max-uni-link-delay | uni-delay-variation | uni-
  link-delay)
```

Parameter

`min-max-uni-link-delay` Min/Max Unidirectional Link Delay

`<1-16777215>` Minimum Unidirectional Link Delay in microseconds

`<1-16777215>` Maximum Unidirectional Link Delay in microseconds

`uni-delay-variation` Unidirectional Delay Variation

`<0-16777215>` Value in microseconds

`uni-link-delay` Unidirectional Link Delay

`<1-16777215>` Value in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement uni-delay-variation static 12
(config-if)#no delay-measurement uni-delay-variation static
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement static uni-link-delay 12
(config-if)#no delay-measurement static uni-link-delay
(config-if)#delay-measurement static min-max-uni-link-delay 1 3
config-if)#no delay-measurement static min-max-uni-link-delay
```

delay-measurement a-bit-delay-threshold

Use this command to advertise average link delay between two directly connected IS-IS/OSPF neighbors.

a-bit-threshold represents the Anomalous (A) bit. The A bit is set when the static value exceeds its configured maximum threshold. The A bit is cleared when the static value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-delay on the current interface.

Command Syntax

```
delay-measurement a-bit-delay-threshold min <1-16777215> max <1-16777215>))
no delay-measurement a-bit-delay-threshold
```

Parameter

`min` Reuse threshold

`<1-16777215>` Reuse threshold value in microseconds

`max` Maximum threshold

`<1-16777215>` Maximum threshold value in microseconds

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#delay-measurement a-bit-delay-threshold min 11 max 22
(config-if)#no delay-measurement a-bit-delay-threshold
```

description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

Command Syntax

```
description LINE
no description
```

Parameter

`LINE`	Interface description. Avoid the special characters “?”, “,”, “>”, “|”, and “=” in the description.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router#configure terminal
Router(config)#interface eth1
Router(config-if)#description Connected to Zenith's fas2/0
```

duplex

Use this command to set the duplex mode for each interface.

Use the `no` parameter to remove the duplex mode.

Note: Interface duplex setting is not supported on Management interface `eth0`.

Command Syntax

```
duplex (half|full)
no duplex
```

Parameter

`half`	Half-duplex mode.
`full`	Full-duplex mode.

Default

By default, duplex mode is full duplex.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#duplex full

(config-if)#no duplex
```

fec

Use this command to force/auto configure forward error correction (FEC) on a physical port.

Use the `no` parameter to enable automatic FEC configuration provisioning based on medium.

Command Syntax

```
fec (on (cl74|cl91)|off|auto)
no fec
```

Parameter

`on`	Enable FEC.
`on cl74`	Enable Base-R FEC if H/W supports it
`on cl91`	Enable RS-528 FEC is H/W supports it
`off`	Disable FEC.
`auto`	Automatically apply FEC for the below transceiver Ethernet compliance codes. Transceiver compliance codes can be fetched via the "show interface controller" command. Also, "fec auto" behavior is the same as no fec. 100G AOC (Active Optical Cable) or 25GAUI C2M AOC 100G ACC (Active Copper Cable) or 25GAUI C2M ACC 100G ACC or 25GAUI C2M ACC 100G AOC or 25GAUI C2M AOC 100GBASE-SR4 or 25GBASE-SR 100G AOC (Active Optical Cable) or 25GAUI C2M AOC

Default

By default, FEC mode is set to auto.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 4.1. The CLI is updated for options `cl74|cl91` in OcNOS version 6.3.1

Examples

```
(config)#interface eth3
(config-if)#fec on
(config-if)#fec off
(config-if)#fec auto
(config-if)#fec on cl74
(config-if)#fec on cl91
```

flowcontrol

Use this command to enable or disable flow control.

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

Use the `no` parameter with this command to disable flow control.

Command Syntax

```
flowcontrol both
flowcontrol send on
flowcontrol send off
flowcontrol receive on
flowcontrol receive off
no flowcontrol
```

Parameters

`both`	Specify flow control mode for sending or receiving.
`send`	Specify flow control mode for sending.
`receive`	Specify the flow control mode for receiving.
`off`	Turn off flow control.
`on`	Turn on flow control.

Default

The flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive off

#configure terminal
(config)#interface eth1
(config-if)#flowcontrol receive on
```

```
(config)#interface eth1
(config-if)#no flowcontrol
```

hardware-profile port-config

To use the four SFP28 ports UFIS9600-32X model, the new command is being introduced to breakout the first 100G port 0 and initialize the first four SFP28 ports as either 4X1G or 4X10G or 4X25G. By default, port 0 is being used as 100G and the four SFP28 ports are not available to OcNOS, as these ports are inactive in HW

Command Syntax

```
hardware-profile port-config (mode1 | mode2 |mode3|mode4 )
```

Parameter

mode1	32X100G (Default) ALL 100G ports will be present
mode2	4X1G + 31X100G 100G port 0 and initialize the first four SFP ports 4X1G
mode3	4X10G + 31X100G 100G port 0 and initialize the first four SFP+ ports 4X10G
mode4	4X25G + 31X100G 100G port 0 and initialize the first four SFP28 ports 4X25G

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.0.0

Examples

```
OcNOS(config)#hardware-profile port-config ?
  mode1  32X100G (Default)
  mode2  4X1G  + 31X100G (ce0 breakout to 4X1G)
  mode3  4X10G + 31X100G (ce0 breakout to 4X10G)
  mode4  4X25G + 31X100G (ce0 breakout to 4X25G)

OcNOS(config)#hardware-profile port-config mode2
OcNOS(config)#comm
OcNOS(config)#
```

hardware-profile portmode

Use this command to set the global port mode.

Command Syntax

```
hardware-profile portmode (4X10g|40g)
```

Parameter

`4X10g`	Split all the 40G flex ports on the system
`40g`	Disable splitting on all flex ports and make all ports 40G

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#hardware-profile portmode 40g
```

if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the OcNOS database.

This command starts the arbiter to check interface information periodically. OcNOS dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when OcNOS is already running, this command polls and updates the kernel information periodically.

Use the `no` parameter with this command to revert to default.

Command syntax

```
if-arbiter (interval <1-65535>|)
no if-arbiter
```

Parameter

`interval`	Interval (in seconds) after which NSM sends a query to the kernel.

Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of OcNOS (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `noif-arbiter` command.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#if-arbiter interval 5
```

interface

Use this command to select an interface to configure, and to enter the `Interface` command mode.

Use the `no` parameter with this command to remove this configuration.

Command Syntax

```
interface IFNAME
no interface IFNAME
```

Parameter

`IFNAME`	Name of the interface.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

```
#configure terminal
(config)#interface eth3
(config-if)#
```

ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address A.B.C.D/M label LINE
ip address A.B.C.D/M (secondary|)
ip address A.B.C.D/M secondary label LINE
no ip address A.B.C.D/M label LINE
no ip address A.B.C.D/M secondary label LINE
no ip address (A.B.C.D/M (secondary|)|)
```

Parameters

`LINE`	Label of this address.
`secondary`	Make the IP address secondary.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```

ip address dhcp

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax

```
ip address dhcp
no ip address dhcp
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

© 2025 IP Infusion Inc. Proprietary

ip forwarding

Use this command to turn on IP forwarding.

Use the `no` parameter with this command to turn off IP forwarding.

Command Syntax

```
ip forwarding
ip forwarding vrf NAME
no ip forwarding
no ip forwarding vrf NAME
```

Parameters

`NAME`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ip forwarding
```

ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

Use the parameters `ge` and `le` specify the range of the prefix length to be matched. When setting these parameters, set `le` to be less than 32 and `ge` to be less than `le` value.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ip prefix-list WORD
 (deny|permit) (A.B.C.D/M|any)
 (deny|permit) A.B.C.D/M eq <0-32>
 (deny|permit) A.B.C.D/M ge <0-32>
 (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
 (deny|permit) A.B.C.D/M le <0-32>
 (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
 seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
 seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32>
 seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32>
 description LINE
 no seq <1-4294967295> (deny|permit) (A.B.C.D/M|any)
 no description LINE
 no description
no ip prefix-list WORD
ip prefix-list sequence-number
no ip prefix-list sequence-number
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`A.B.C.D/M`	IP address mask and length of the prefix list mask.
`eq`	Exact prefix length to be matched
`le`	Maximum prefix length to be matched
`ge`	Minimum prefix length to be matched

`<0-32>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`any`	Take all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for `A.B.C.D/M`.
`sequence-number`	To suppress sequence number generation, give the `no ip prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ip prefix-list` command. To enable sequence number generation, give the `ip prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

IP prefix-list mode

Applicability

This command was introduced before OcNOS Version SP 4.0.

Examples

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
(config-router)#neighbor 10.6.5.3 prefix-list mylist out
(config-router)#exit
(config)#ip prefix-list mylist
(config-ip-prefix-list)#seq 5 deny 76.2.2.0/24
(config-ip-prefix-list)#seq 10 permit 0.0.0.0/0
```

ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the `no` parameter to disable the proxy ARP feature on an interface.

Command Syntax

```
ip proxy-arp
no ip proxy-arp
```

Parameters

None

Default

By default, the ip proxy-arp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip proxy-arp
```

ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the `no` parameter to disable this function.

Command Syntax

```
ip remote-address A.B.C.D/M
no ip remote-address
```

Parameter

`A.B.C.D/M`	IP address and prefix length of the link remote address.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```

ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link. Moreover, this command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-to-point interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax

```
ip unnumbered IFNAME
no ip unnumbered
```

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example creates a tunnel on `eth1`.

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

ip vrf forwarding

This command associates an interface with a VRF.

Use the `no` parameter with this command to unbind an interface.

Note: When you give this command in interface configuration or subinterface configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving this command, the IP attributes must then be configured in the context of the VRF.

Note: The Out Of Band (OOB) management port is part of the “management” VRF. Also, this port cannot be moved out of “management” VRF.

Command Syntax

```
ip vrf forwarding WORD
no ip vrf forwarding WORD
```

Parameter

`WORD`	Name of the VRF.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#exit
(config)#interface eth1
(config-if)#ip vrf forwarding myVRF
```

ipv6 address

Use this command to set the IPv6 address of an interface.

Use the `no` form of this command to disable this function.

Note: This command is also used to configure an IPv6 link-local address for an interface.

Command Syntax

```
ipv6 address X:X::X:X/M
ipv6 address X:X::X:X/M anycast
no ipv6 address X:X::X:X/M
```

Parameters

`X:X::X:X/M`	IP destination prefix and a mask length.
`anycast`	Make an anycast address which is assigned to a set of interfaces that belong to different devices. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 address 3ffe:506::1/64

#configure terminal
(config)#interface eth4
(config-if)#ipv6 address fe80::ab8/64
```

ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the `no` parameter with this command to turn off IPv6 forwarding.

Command Syntax

```
ipv6 forwarding
ipv6 forwarding vrf NAME
no ipv6 forwarding
no ipv6 forwarding vrf NAME
```

Parameters

`NAME`	Virtual Routing or Forwarding name

Default

No default value is specified

Command Mode

Command mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#ipv6 forwarding
```

ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `ge` and `le` specify the range of the prefix length to be matched.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax

```
ipv6 prefix-list WORD
 (deny|permit) (X:X::X:X/M|any)
 (deny|permit) X:X::X:X/M ge <0-128>
 (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
 (deny|permit) X:X::X:X/M le <0-128>
 (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
 seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
 seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128>
 seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-128>
 description LINE
 no seq <1-4294967295> (deny|permit) (X:X::X:X/M|any)
 no description
no ipv6 prefix-list WORD
ipv6 prefix-list sequence-number
no ipv6 prefix-list sequence-number
```

Parameters

`WORD`	Name of the prefix list.
`deny`	Reject packets.
`permit`	Accept packets.
`X:X::X:X/M`	IP address mask and length of the prefix list mask.
`any`	Take all packets of any length. This is the same as specifying ::/0 for X:X::X:X/M.
`le`	Maximum prefix length match
`ge`	Minimum prefix length match
`<0-128>`	Prefix length to match
`<1-4294967295>`	Sequence number of the prefix list.
`sequence-number`	

	To suppress sequence number generation, give the `no ipv6 prefix-list sequence-number` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ipv6 prefix-list` command. To enable sequence number generation, give the `ipv6 prefix-list sequence-number` command.
`LINE`	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist
(config-ipv6-prefix-list)#seq 12345 deny 3ffe:345::/16 le 22 ge 14
```

ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a point-to-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax

```
ipv6 unnumbered IFNAME
no ipv6 unnumbered
```

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following example creates a tunnel on eth1:

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode vxlan
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

link-debounce-time

Use this command to set the debounce time for linkup and linkdown transitions for the interface.

User can set only one of the timers (either linkup or linkdown) by setting the other one to 0.

Use the `no` form of this command to turn off the link debounce timer on the interface.

Command Syntax

```
link-debounce-time <0-5000> <0-5000>
no link-debounce-time
```

Parameter

`<0-5000>`	timer value in milliseconds for the linkup transition
`<0-5000>`	timer value in milliseconds for the linkdown transition

Default

By default, it is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 5.0.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#link-debounce-time 4000 5000
(config-if)#link-debounce-time 0 5000
(config-if)#link-debounce-time 3000 0
```

© 2025 IP Infusion Inc. Proprietary

loopback

Use this command to loopback TX or RX packets at MAC or PHY level.

Use the `no` form of the command to remove loopback configuration.

Command Syntax

```
loopback (tx | rx) (mac | phy)
no loopback
```

Parameter

`tx`	Loopback TX packets
`rx`	Loopback RX packets
`mac`	Loopback TX or RX packets at MAC level
`phy`	Loopback TX or RX packets ar PHY level

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 5.0.

Example

```
#configure terminal
(config)#int ce1/2
(config-if)#loopback rx phy

#configure terminal
(config)#int ce1/2
(config-if)#no loopback
```

loss-measurement dynamic

This command enables the loss measurement. This command is tied to the delay measurement session already created to measure the delay. In case this command is issued without the delay-measurement command previously issued, an error is returned.

Use the `no` form of this command should be used to disable the loss measurement.

Command Syntax

```
loss-measurement dynamic
no loss-measurement dynamic
```

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 5.1.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#loss-measurement dynamic
(config-if)#no loss-measurement dynamic
```

loss-measurement uni-link-loss

Use this command to advertise the loss (as a packet percentage) between two directly connected IS-IS/OSPF neighbors.

The A bit is set when the measured value of this parameter exceeds its configured maximum threshold. The A bit is cleared when the measured value falls below its configured reuse threshold.

Use the `no` parameter with this command to unset uni-link-loss on the current interface.

Command Syntax

```
loss-measurement uni-link-loss ((static VALUE) | (a-bit-threshold min VALUE max
  VALUE))
no loss-measurement uni-link-loss (static | a-bit-threshold)
```

Parameter

`static`	Static value
`VALUE`	Loss percentage in six precision float format. eg: 3.123456
`a-bit-threshold`	Threshold values to set/clear A-bit
`min`	Reuse threshold
`VALUE`	Reuse threshold percentage in six precision float format. eg:3.123456
`max`	Maximum threshold
`VALUE`	Maximum threshold percentage in six precision float format. eg:3.123456

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#loss-measurement uni-link-loss static 12.3
(config-if)#no loss-measurement uni-link-loss static
(config-if)#loss-measurement uni-link-loss a-bit-threshold min 1.12 max 2.2
(config-if)#no loss-measurement uni-link-loss a-bit-threshold
```

mac-address

Use this command to configure a MAC address for Layer 3 interfaces. Interface can be Layer 3 physical interface or routed VLAN interface or port-channel.

Use the `no` form of this command to remove the MAC address from an interface.

Command Syntax

```
mac-address  HHHH.HHHH.HHHH
no mac-address
```

Parameters

`mac-address`	mac-address in HHHH.HHHH.HHHH format (only supported on L3 Interfaces)

Default

None

Configuration mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.4.2.

Examples

```
OcNOS(config)#int xe46
OcNOS(config-if)#mac-address 00e0.aaaa.bbbb
```

mac-address secondary peer-mlag

Use this command to enable L3 termination of data-packets on both the MLAG peers applicable on SVI interfaces.

Use the `no` form of this command to disable.

Command Syntax

```
mac-address secondary peer-mlag
no mac-address secondary peer-mlag
```

Parameters

NA

Default

Disabled

Configuration mode

Interface mode

Applicability

This command was introduced before OcNOS version 6.1.0.

Examples

```
OcNOS(config)#interface vlan1.10
OcNOS(config-if)#mac-address secondary peer-mlag
OcNOS(config-if)#exit
```

monitor speed

Use this command to enable speed monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

Command Syntax

```
monitor speed
no monitor speed
```

Default

By default, speed monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor speed
(config-if)#no monitor speed
```

monitor queue-drops

Use this command to enable queue-drops monitoring on interface.

Use the `no` parameter with this command to disable monitoring.

Command Syntax

```
monitor queue-drops
no monitor queue-drops
```

Default

By default, queue-drops monitoring will be disabled

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#monitor queue-drops
(config-if)#no monitor queue-drops
```

monitor speed threshold

Use this command to modify default speed monitor threshold on interface.

Use the `no` parameter with this command to set the monitor speed threshold to its default.

Note: Warning threshold must be greater than recovery threshold and it is recommended to keep a difference of 10 percent to avoid frequent notifications caused by variations in average speed.

Command Syntax

```
monitor speed threshold warning <1-100> recovery <1-100>
no monitor speed threshold
```

Parameter

`<1-100>`	Warning level threshold value in percentage
`<1-100>`	Recovery level threshold value in percentage

Default

By default, warning threshold is 90 percentage and recovery is 80 percentage.

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)# monitor speed threshold warning 80 recovery 70
(config-if)#no monitor speed threshold
```

mtu

Use this command to set the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) for an interface

Use the `no` parameter with this command to set the MTU to its default.

Note: To allow jumbo frames over SVI interfaces, it is mandatory to configure the applicable MTU for the specific SVI interfaces.

Limitation for MTU configuration on Label-Switching:

Creating a sub-interface automatically increases the physical interface MTU size by 8 bytes to accommodate double VLAN tag encapsulation.

Configuring label switching for physical layer-3 interfaces adds 20 bytes internally to the MTU to accommodate up-to five labels. However, configuring label-switching on sub-interface does not change the MTU of physical interface. Hence, the physical interface requires a manual increase in MTU size.

During the BGP update, in case the control packet contains 1500 bytes when it reaches the hardware, the hardware adds the Encapsulation for the sub-interface and MPLS header (Additional bytes). Now, the hardware drops it as physical port MTU is limited to 1500 bytes.

While configuring MTU on label-switching enabled with Subinterface/SVI/LAG and the Parent Physical port follow guide lines mentioned below:

It is recommended to configure higher MTU on network ports in comparison with access ports. Hence, increase the MTU on both physical and sub-interfaces to accommodate the PDU.
When using sub-interface for MPLS network interfaces, considering the default MTU of 1500, minimum MTU configuration recommendation is as follows

- ***Sub-interface***: MTU 1520 (to accommodate 5 MPLS labels)
- ***Physical interface:*** MTU 1528: (Default MTU 1500 + double encap 8 + MPLS up-to 5 labels 20) = 1528).

  Note: MTU configuration is considered from IP header onwards. Hence, OcNOS adds 14 bytes to MTU internally to accommodate L2 header. The effective MTU in hardware will be 1528+14 = 1542.
- ***LAG interface:*** MTU is applied on all members internally
- ***SVI:*** When label-switching enabled on VLAN interface, MTU value must be manually increased by at least 20 bytes on Parent interfaces of VLAN.
  Example, default MTU must be set as 1520 instead of 1500 on label-switching parent interface label switched VLAN interface. (Parent Interface MTU >= label switched VLAN interface MTU + 20).

Command Syntax

```
mtu <64-65536>
no mtu
```

Parameter

`<64-65536>`	Specify the size of MTU in bytes: `<64-16338>` for L2 packet `<576-9216>` for L3 IPv4 packet `<1280-9216>` for L3 IPv6 packet

<576-65536> for IPv4 packet

<1280-65536> for IPv6 packet on loopback interface

Default

By default, MTU is 1500 bytes

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#mtu 120
```

multicast

Use this command to set the multicast flag for the interface.

Use the `no` form of this command to disable this function.

Command Syntax

```
multicast
no multicast
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#multicast
```

show flowcontrol

Use this command to display flow control information.

Command Syntax

```
show flowcontrol
show flowcontrol interface IFNAME
```

Parameters

`interface IFNAME`	Specify the name of the interface to be displayed.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show flowcontrol interface` command displaying flow control information:

```
#show flowcontrol interface ge1
Port    Send FlowControl    Receive FlowControl RxPause TxPause

        admin    oper         admin    oper

-----   ------- --------     ------- --------      ------- -------
ge1      on       on            on       on             0       0
#
```

Table 5-10 explains the show command output fields.

Table 5-10: show flow control output

Entry	Description
Port	Interface being checked for flowcontrol.
Send admin	Displays whether the flowcontrol send process is administratively on or off.
FlowControl oper	Displays whether send flowcontrol is on or off on this interface.
Received admin	Displays whether the flowcontrol receive process is administratively on or off.
FlowControl oper	Displays whether receive flowcontrol is on or off on this interface.
RxPause	Number of received pause frames.
TxPause	Number of transmitted pause frames.

show hardware-discard-counters

Use this command to check device level discard counters.

Command Syntax

```
show hardware-discard-counters
```

Parameters

None

Command Mode

Exec mode

Applicability

The command is introduced before OcNOS version 1.3.

Qumran devices do not support discard counters per interface. Only global level counters are available for advanced debugging using the show hardware-discard-counters command.

Examples

```
#show hardware-discard-counters
+-------------------------------------------------+--------------------+
| Registers                                       | Core 0             |
+-------------------------------------------------+--------------------+
 CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR                     437
   Reason : QNUM_NOT_VALID                         Y
 EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER            8894
   Reason : SRC_EQUAL_DEST_INT                     Y
```

See Table 5-11 and Table 5-12 for details:

Table 5-11: Table detailing about counters supported

Register	Description
CGM_VOQ_SRAM_ENQ_RJCT_PKT_CTR for QAX	Drop is due to PPdecision to drop, or invalid destination received from PPblocks.
IQM_QUEUE_ENQ_DISCARDED_PACKET_COUNTER for QMX	The packet DP (Drop Precedence) is higher than the configured Drop DP.
EGQ_PQP_DISCARD_UNICAST_PACKET_COUNTER	Seen with unknown unicast frames, source and destination learnt from same interface.

Table 5-12: Table detailing about reasons supported

Register	Description
QNUM_NOT_VALID for QAX QUEUE_NOT_VALID_STATUS for QMX	Seen with Vlan Discards, ACL Drops, Storm Control, STP Blocked Port.
DP_LEVEL_RJCT for QAX DP_LEVEL_STATUS for QMX	Seen with Policer Discards.
SRC_EQUAL_DEST_INTF	Seen when traffic is not learned, but is still forwarded/flooded.

show interface

Use this command to display interface configuration and status information.

Command Syntax

```
show interface (IFNAME|)
show interface brief (IFNAME|)
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1
Interface xe1/1
  Scope: both
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: ecf4.bb6e.934b
  Physical:ecf4.bb6e.934b  Logical:(not set)
  Port Mode is access
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full(auto) link-speed 1g(auto)
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
DHCP client is disabled.
  Last Flapped: 2016 Nov 05 22:40:23 (00:19:25 ago)
  Statistics last cleared: 2016 Nov 05 04:49:55 (18:09:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec
  RX
    unicast packets 39215813 multicast packets 0 broadcast packets 0
    input packets 39215813 bytes 2666662432
    jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0
    input error 0
    input with dribble 0 input discard 0
    Rx pause 0
  TX
    unicast packets 38902 multicast packets 437 broadcast packets 0
    output packets 437 bytes 28018
    jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0
    output discard 0
    Tx pause 0
```

Table 5-13 explains the output fields.

Table 5-13: show interface output details

Field	Description
Scope	Interface can be used for communication within the device and outside the device (Both).
Flexport	Specifies whether the ports has Breakout capabilities or is a Non-Control Port.
Breakout Control Port (Active)	Specifies whether Breakout is active or disabled.
Hardware is ETH Current HW addr	The MAC address of the interface.
Physical	Displays the physical MAC address of the interface.
Logical	Displays the logical MAC address (if any) of the interface.
Port Mode	Displays the port mode: Router, VLAN access, switch, or trunk.
Interface index	Index number, Metric, MTU size, duplex-full (auto) or half-duplex, minimum link speed in gigabits, and if the interface is up, broadcasting, and multicasting.
VRF Binding	Show whether the interface is VRF bound and (if bound) with what VRF, if Label Switching is enabled or disabled, and if a virtual circuit is configured.
DHCP client	The state of the DHCP client – whether this interface is connected to a DHCP server.
Last Flapped	Date and time when the interface last flapped.
Statistics last cleared	Date and time when the interface's statistics were cleared.
5 minute input rate	Input rate in bits/second and packets/second
5 minute output rate	Output rate in bits/second and packets/second
RX	Counters for unicast packets, multicast packets, broadcast packets, input packets, bytes, jumbo packets, runts, giants, CRC errors, fragments, jabbers, input errors, input with dribble input discards, and receive pause.
TX	Counters for unicast packets, multicast packets, broadcast packets, output packets, bytes, jumbo packets, output errors, collisions, differed packets, input late collisions, output discards, and transmit pause.

```
#show interface brief xe51

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate
       FR - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual Port
       CVP - Channelised Virtual Port, METH - Management Ethernet, UNK- Unknown
       ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA - InActive
       PD(Min L/B) - Protocol Down Min-Links/Bandwidth
       OTD  - Object Tracking Down
       DV - DDM Violation, NA - Not Applicable
       NOM - No operational members, PVID - Port Vlan-id
       Ctl - Control Port (Br-Breakout/Bu-Bundle)


--------------------------------------------------------------------------------
Ethernet   Type     PVID  Mode      Status  Reason  Speed Port Ch #  Ctl Br/Bu  Loopbk
Interface
--------------------------------------------------------------------------------
xe51        ETH     --    routed     down    OTD     10g   --         No         No
```

show interface capabilities

Use this command to display interface capabilities

Command Syntax

```
show interface (IFNAME|) capabilities
```

Parameters

IFNAME	Displays the name of a specific interface for which status and configuration data is desired.

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 capabilities
xe1/1
Speed(FD) : 10MB,100MB,1000MB,10GB,20GB,40GB
Interface : xgmii
Medium : copper
Loopback : none,MAC,PHY
Pause : pause_tx,pause_rx,pause_asymm
Flags : autoneg
Encap : IEEE,HIGIG,HIGIG2

OcNOS#show interface cd49 capabilities
cd49
Speed(FD)            : 400GB
Speed(HD)            : 400GB
Medium               : copper,fiber
Pause                : pause_tx/pause_rx/pause_asymm
Encap                : IEEE
FEC                  : RS-272-2xN,RS-544-2xN,BASE-R(CL74),RS(CL91)

OcNOS#show interface cd49/1 capabilities
cd49/1
Speed(FD)            : 100GB
Speed(HD)            : 100GB
Medium               : copper,fiber
Pause                : pause_tx/pause_rx/pause_asymm
Encap                : IEEE
FEC                  : RS(CL91),RS-544,RS-272,BASE-R(CL74)

OcNOS#show interface cd49/1 capabilities
cd49/1
Speed(FD)            : 40GB,100GB
Speed(HD)            : 40GB,100GB
Medium               : copper,fiber
Pause                : pause_tx/pause_rx/pause_asymm
```

```
Encap                   : IEEE
FEC                     : BASE-R(CL74),RS(CL91),RS-544,RS-272-2xN,RS-544-2xN
```

Table 5-14 explains the show command output fields.

Table 5-14: show interface capabilities output details

Field	Description
Interface number	The identifying ID number of the interface – eht0, xe1, etc.
Speed (FD)	The Flexible Data-Rates (FD) of the interface
interface	XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of Gigabit Ethernet.
Medium	Members have to have the same medium type configured. This only applies to Ethernet port-channel. Copper, fiber optics, etc.
Loop back	The loop back between the MAC and PHY layers.
Pause	Pause transmit, pause receive, pause asymmetrically.
Flags	Interface flags set for Auto-negotiation.
Encap	Encapsulation – IEEE, HIGIG, and HIGIG2 specifications – HIGIG is a proprietary protocol that is implemented by Broadcom. The HIGIG protocol supports various switching functions. The physical signaling across the interface is XAUI, four differential pairs for receive and transmit (SerDes), each operating at 3.125 Gbit/s.

show interface counters

Use this command to display the ingress and egress traffic counters on the interface.

Note: Counters are meant for debugging purpose and the accuracy of the transmit discard counter is not guaranteed in all scenarios.

Command Syntax

```
show interface (IFNAME|) counters (active|)
show interface cpu counters
```

Parameter

IFNAME	Interface name.
active	Statistics for link-up interfaces.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters
Interface xe1/1
  Scope: both
  Rx Packets: 1000
  Rx Bytes: 1000000
  Rx Unicast Packets: 1000
  Rx Packets from 512 to 1023 bytes: 1000
  Tx Packets: 3897
  Tx Bytes: 249408
  Tx Multicast Packets: 3897
  Tx Packets with 64 bytes: 3897
  Tx Packet rate: 1 pps
  Tx Bit rate: 255 bps

#show interface cpu counters
CPU Interface
  Tx Packets: 104508
  Tx Bytes: 7106272
  Tx Discard Packets: 89613672
  Tx Discard Bytes: 5735237844
  Rx Discard Packets: 11938
```

Table 5-15 explains the output fields.

Table 5-15: show interface counters output details

Field	Description
Receive Counters	Rx Packets Rx Bytes Rx Unicast Packets Rx Multicast Packets Rx Broadcast Packets Rx Packets with 64 bytes Rx Packets from 65 to 127 bytes Rx Packets from 128 to 255 bytes Rx Packets from 256 to 511 bytes Rx Packets from 512 to 1023 bytes Rx Packets from 1024 to 1518 bytes Rx Packets from 1519 to 2047 bytes Rx Packets from 2048 to 4095 bytes Rx Packets from 4096 to 9216 bytes Rx Jumbo Packets Rx Discard Packets (not applicable for Qumran platform) Rx Packets with error Rx CRC Error Packets Rx Undersized Packets Rx Oversized Packets Rx Fragment Packets Rx Jabber Packets Rx MAC error Packets Rx Pause Packets Rx Unrecognized MAC Control Packets Rx Drop Events Rx Packet rate Rx Bit rate

Table 5-15: show interface counters output details

Field	Description
Transmit Counters	Tx Packets Tx Bytes Tx Unicast Packets Tx Multicast Packets Tx Broadcast Packets Tx Packets with 64 bytes Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes Tx Packets from 256 to 511 bytes Tx Packets from 512 to 1023 bytes Tx Packets from 1024 to 1518 bytes Tx Packets from 1519 to 2047 bytes Tx Packets from 2048 to 4095 bytes Tx Packets from 4096 to 9216 bytes Tx Jumbo Packets Tx Discard Packets (not applicable for Qumran platform) Tx Packets with error Tx Collisions Tx Late Collisions Tx Excessive Collisions Tx Pause Packets Tx Packet rate Tx Bit rate
CPU Interface Counters	Tx Packets Tx Bytes Tx Discard Packets Tx Discard Bytes Rx Discard Packets

show interface counters drop-stats

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for physical ports and cpu ports, but not for the out-of-band management (OOB) management port or logical interfaces.

Note: Drops in the CPU queue are listed under `Tx Multicast Queue Drops`, whether the packet is unicast or multicast

Command Syntax

```
show interface (IFNAME|) counters drop-stats
show interface cpu counters drop-stats
```

Parameter

`IFNAME`	Physical interface name
`cpu`	CPU interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.1.

For Qumran devices, only error statistics are applicable and discard counters are not applicable. Only global level counters are available for advanced debugging using the command show hardware-discard-counters.

Example

```
#show interface xe32/2 counters drop-stats
+---------------------+----------------+----------------+--------------------+
| Counter Description | Count          | Last Increment | Last Increment Time
|
+---------------------+----------------+----------------+--------------------+
 Rx Bad CRC errors     0                0
 Rx Undersize errors   0                0
 Rx Oversize errors    0                0
 Rx Fragments errors   0                0
 Rx Jabbers errors     0                0
 Rx Port Block Drops   6                1                2016 Nov 09 08:59:33
 Rx Vlan Discards      0                0
 Rx ACL/QOS Drops      0                0
 Rx Policy Discards    0                0
 Rx EGR Port Unavail   38784            5                2016 Nov 09 18:19:31
 Rx IBP Discards       0                0
 Tx Port Block Drops   359              1                2016 Nov 09 08:59:33
 Tx Vlan Discards      0                0
 Tx TTL Discards       0                0
 Tx Unknown Discards   359              1                2016 Nov 09 08:59:33
 Tx Ucast Queue Drops  0                0
 Tx Mcast Queue Drops  0                0
+---------------------+----------------+----------------+--------------------+
```

Table 5-16 explains the output fields.

Table 5-16: show interface counters drop-stats output details

Field	Description
Counter Description	Shows the type of packet and/or the reason why the packet was dropped.
Count	The number of packets dropped for each reason.
Last Increment	Number of packets dropped since this command was last entered.
Last Increment Time	Date and time when the last packet was dropped.
Rx Bad CRC errors	Received packets dropped because they didn't pass the cyclic Redundancy Check (CRC).
Rx Undersize errors	Number of received runt packets dropped.
Rx Oversize errors	Number of received giant packets dropped
Rx Fragments errors	Number of received packet fragments dropped
Rx Jabbers errors	Received packets dropped because of jabber – long packet error.
Rx Port Block Drops	Received packets dropped because port blocking is enabled (not applicable for Qumran platform).
Rx Vlan Discards	VLAN received packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).
Rx ACL/QOS Drops	Received packets match a field processing entry with a drop or color drop action, such as: User-configured ACL that denies traffic Service policy with a police action that drops the traffic received at a rate higher than the configured limit. (not applicable for Qumran platform)
Rx Policy Discards	Received packets dropped because of device policies violated, such as a storm control rate violation (not applicable for Qumran platform).
Rx EGR Port Unavail	No output port can be determined for these received packets. This counter increments along with other counter types in this table because it is a "catchall" for multiple types of discards as shown below (not applicable for Qumran platform): VLAN check failed MTU check failed ACL/QoS drops Policy discards Source MAC is null Destination IP/source IP address is null Source MAC address and destination MAC address are the same Forwarding lookup failure
Rx IBP Discards	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface. (not applicable for Qumran platform)
Tx Port Block Drops	Transmitted packets dropped because port blocking is enabled (not applicable for Qumran platform).
Tx Vlan Discards	Transmitted VLAN packets dropped because there is no VLAN configured on the port (not applicable for Qumran platform).

Table 5-16: show interface counters drop-stats output details (Continued)

Field	Description
Tx TTL Discards	Transmitted packets discarded because their Time To Live (TTL) has ended. (not applicable for Qumran platform)
Tx Unknown Discards	Transmitted packets dropped for unknown reason. May have something to do with the condition/configuration of the port at the other end of the connection (not applicable for Qumran platform).
Tx Ucast Queue Drops	Transmitted packets dropped as a result of Unicast buffer overflow.
Tx Mcast Queue Drops	Transmitted packets dropped as a result of Multicast buffer overflow.

show interface counters error-stats

Use this command to display the ingress error traffic counters on the interface.

Command Syntax

```
show interface (IFNAME|) counters error-stats
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters error-stats
+----------+-------------+--------+----------+---------+-----------+---------+
|Interface |Total errors |Bad CRC |Undersize |Oversize | Fragments | Jabbers |
+----------+-------------+--------+----------+---------+-----------+---------+
 xe1/1      120           8        100        10        2           0
```

Table 5-17 explains the columns in the output.

Table 5-17: error traffic counters

Column	Description	Causes
Interface	Name of the interface	Point of interconnection in network.
Total errors	Total number of all types of errors	Number of errors in network.
Bad CRC	Number of packets received by the port from the network, where the packets have no CRC or a bad CRC.	Packet data modified making the CRC invalid.
Undersize	Total number of packets received that are less than 64 octets long (which exclude framing bits, but include the FCS) and have a good FCS value.	Bad frame generated by the connected device.
Oversize	Number of packets received by the port from the network, where the packets were more than maximum transmission unit size.	Faulty hardware, dot1q, or ISL trunking configuration issues.
Fragments	Total number of frames whose length is less than 64 octets (which exclude framing bits, but which include the FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.
Jabbers	Total number of frames whose length is more than the maximum MTU size. (which exclude framing bits, but which include FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.

show interface counters (indiscard-stats|outdiscard-stats)

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for data ports and CPU ports, not for the out-of-band management (OOB) management port or logical interfaces.

Command Syntax

```
show interface (IFNAME|) counters (indiscard-stats|outdiscard-stats)
show interface cpu counters (indiscard-stats|outdiscard-stats)
```

Parameter

`IFNAME`	Physical Interface name.
`indiscard-stats`	Discard reasons for ingress dropped packets.
`outdiscard-stats`	Discard reasons for egress dropped packets.
`cpu`	CPU Interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Examples

```
#show interface xe1/3 counters indiscard-stats
+---------------------+----------------+----------------+---------------------+
| Counter Description | Count          | Last Increment | Last Increment Time |
+---------------------+----------------+----------------+---------------------+
 STP Discards          0                0
 Vlan Discards         0                0
 ACL Drops             0                0
 Policy Discards       0                0
 EGR Port Unavail      1092867          1092867          2016 Oct 25 19:54:58
 IBP Discards          0                0
+---------------------+----------------+----------------+---------------------+

#show interface counters indiscard-stats
+-------------+------------------+---------------+---------------+-----------------+------------------+-------------+------
--------------+
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy Discards | EGR Port Unavail | IBP Discards |   Total
Discards   |
+-------------+------------------+---------------+---------------+-----------------+------------------+-------------+------
--------------+
xe1           0                  0               35703           0                 11                 0             35714
xe2           0                  0               295744          0                 13604              0             309348
xe3           0                  0               9501            0                 20405              0             29906
xe5           0                  0               0               0                 13602              0             13602
xe49/1        0                  0               0               0                 0                  20658         20658
xe52/1        0                  3               856029          10                13613              0             869642
xe54/1        0                  5371            0               0                 5371               0             5371
cpu           0                  0               0               0                 6                  0             N/A

#show interface counters outdiscard-stats
```

```
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
--------------+
|  Interface  | Port Block Drops | Vlan Discards | TTL Discards | Unknown Discards |  UcastQ Drops  |  McastQ Drops  |   Total
Discards    |
+-------------+-----------------+--------------+-------------+-----------------+---------------+---------------+------
--------------+
xe1           0                 0              0             204338            0               0               204338
xe2           0                 0              0             1094368           0               0               1094368
xe3           0                 0              0             818672            0               0               818672
xe52/1        0                 0              0             1275156           0               0               1275156
xe54/1        0                 0              0             13575             0               0               13575
cpu           0                 0              0             0                 N/A             1014224         N/A
```

Table 5-18 explain the fields in the command output.

Table 5-18: indiscard statistic output details

Statistic	Description
STP Discards	Packets received when the ingress interface is not in STP forwarding state.
Port Block Drops	Packets discarded on an ingress interface where port blocking is configured.
VLAN Discards	VLAN tagged packets received on a port which is not a member of the VLAN or untagged packets received on a trunk port.
ACL/QoS Drops	Incoming packets match a field processing entry with a drop or color drop action, such as: 1. User-configured ACL that denies traffic 2. Service policy with a police action that drops the traffic received at a rate higher than the configured limit
Policy Discards	Device policies violated, such as a storm control rate violation, source or destination discards when L2 tagged traffic received on router interface.
EGR (Egress) Port Unavail	No output port can be determined for this packet. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below: 1. VLAN check failed 2. MTU check failed 3. ACL/QoS drops 4. Policy discards 5. Source MAC is null 6. Destination IP/source IP address is null 7. Source MAC address and destination MAC address are the same 8. Source MAC is configured as static on other interface 9. Forwarding lookup failure
IBP Drops	Ingress Back Pressure (ingress congestion) when the ingress packet buffer is full for an interface.
Total Discards	Total number of ingress dropped packets.

Table 5-19 explain the fields in the command output.

Table 5-19: outdiscard statistics

Statistics	Description
Port Block Drops	Packets discarded on an egress interface where port blocking is configured.
VLAN Discards	Packets discarded because an invalid VLAN tag is encountered at an egress interface.
TTL Discards	Packets discarded because the Time-To Live (TTL) of the outgoing packet has passed.

Table 5-19: outdiscard statistics

Statistics	Description
Unknown Discards	Packets discarded for other possible reasons like ACL drop in egress or a policer drop in egress. Discards caused by congestion at queues and drops at queues are not counted under unknown discards.
Unicast Queue Drops	Packets dropped in the unicast queues because of congestion.
Multicast Queue Drops	Packets dropped in the multicast queues because of congestion.
Total Discards	Total number of egress dropped packets.

show interface counters protocol

Use this command to display protocol packets received at the CPU by the control plane.

Command Syntax

```
show interface (IFNAME|) counters protocol
```

Parameters

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
#show interface counters protocol
Interface ce1/1
  lacp                  : 4
  icmp6                 : 5
```

Table 5-20 explain the fields in the command output.

Table 5-20: show interface counters protocol output details

Field	Description
Interface	Name of the configured interface.
lacp	Total number of lacp protocol in the interface.
icmp6	Total number of icmp6 protocol in the interface.

show interface counters queue-drop-stats

Use this command to display dropped packets in the CPU queue and the last increment time.

Command Syntax

```
show interface cpu counters queue-drop-stats
```

Parameters

cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
show interface cpu counters queue-drop-stats
+------------------+----------------+----------------+---------------------+
|    Queue Name    |     Count      | Last Increment | Last Increment Time |
+------------------+----------------+----------------+---------------------+
arp                  169735545        9145653          2017 Oct 23 14:33:54
```

Table 5-21 explain the fields in the command output.

Table 5-21: show interface counters queue-drop-stats output details

Field	Description
Queue Name	Name of the protocol.
Count	Number of arp protocols in the interface.
Last Increment	Final increment number in the protocol.
Last Increment time	Time of the last increment in the protocol.

show interface counters queue-stats

Use this command to display transmitted and dropped packet and byte counts of individual queues.

Note: In Qumran devices, all packets dropped in a queue are counted (even policer drops).

Command Syntax

```
show interface (IFNAME|) counters queue-stats
show interface cpu counters queue-stats
```

Parameters

IFNAME	Interface name.
cpu	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Note: Default traffic counters are not supported on Qumran AX.

Example

```
#show interface counters queue-stats
D - Default Queue, U - User-defined Queue
+--------+----------------+------+-----------+------------+------------+---------------+
|Interface|Queue/Class-map|Q-Size|Output pkts|Output bytes|Dropped pkts|Dropped bytes  |
+--------+----------------+------+-----------+------------+------------+---------------+
xe1/1     q1           (D) 0      12          1368         0            0
xe1/1     mc-q7        (D) 0      1           82           0            0
xe25      q1           (D) 0      6           684          0            0

#show interface xe1/1 counters queue-stats
D - Default Queue, U - User-defined Queue
+---------------+------+-------+-  -------+------------+--------------+
|Queue/Class-map|Q-Size|Tx pkts| Tx bytes |Dropped pkts|Dropped bytes |
+---------------+------+-------+----------+------------+--------------+
q0             (D) 0     0       0          0            0
q1             (D) 0     12      1368       0            0
q2             (D) 0     0       0          0            0
q3             (D) 0     0       0          0            0
q4             (D) 0     0       0          0            0
q5             (D) 0     0       0          0            0
q6             (D) 0     0       0          0            0
q7             (D) 0     0       0          0            0
mc-q0          (D) 0     0       0          0            0
mc-q1          (D) 0     0       0          0            0
mc-q2          (D) 0     0       0          0            0
mc-q3          (D) 0     0       0          0            0
mc-q4          (D) 0     0       0          0            0
mc-q5          (D) 0     0       0          0            0
mc-q6          (D) 0     0       0          0            0
mc-q7          (D) 0     1       82         0            0

#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
|   Queue/Class-map  | Q-Size |     Tx pkts     |     Tx bytes      |  Dropped pkts   |   Dropped bytes   |
+--------------------+--------+-----------------+-------------------+-----------------+-------------------+
igmp              (E) 800592   14519             987292              1304163           88683084
```

```
arp             (E) 1250496  1008785          68597380          0               0
```

Table 5-22 explain the fields in the command output.

Table 5-22: queue flags detail

Flag	Meaning
D	Default queue of the port.
U	User defined queue of the port.
E	Outgoing hello packet's queue in the port.
I	Incoming hello packet's queue in the port.
Q	Hello packet's queue size in bytes.

Table 5-23 explain the fields in the command output.

Table 5-23: show interface counters queue-stats output details

Field	Description
Interface	A defined physical interface to which the queue is associated.
Queue/Class-map	Queues associated with a QoS class-map.
Q-Size	The size of a specified queue in bytes.
Output pkts	The number of out bound packets residing in the queues.
Output Bytes	The number of bytes in the outbound queue.
Dropped pkts	The number of packets dropped because of queue overflow.
Dropped bytes	The number of bytes dropped because of queue overflow.
Tx pkts	The number of transmit packets contained in the out bound queue.
Tx bytes	The number of transmit bytes contained in the out bound queue.

show interface counters speed

Use this command to display the current average speed on the interface.

Command Syntax

```
show interface (IFNAME|) counters speed (kbps|mbps|gbps|)
```

Parameter

IFNAME	Interface name.
kbps	Kilobits per second.
mbps	Megabits per second.
gbps	Gigabits per second.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#show interface counters speed
* indicates monitor is active
+------------+--------------+--------------------+---------------------------
---------------+
|            |              |     Threshold(%)   |          Current average
speed           |
|  interface | configured   +--------------------+-------------+-------+------
-------+-------+
|            | speed ( bps) | Warning | Recovery |  Rx ( bps)  |   %   |  Tx (
bps)  |   %   |
+------------+--------------+---------+----------+-------------+-------+------
-------+-------+
  ce45       100000000000   90        80         0           0.00    0
0.00
  xe7        10000000000    90        80         0           0.00    0
0.00
  xe31       10000000000    90        80         0           0.00    0
0.00
  xe33       10000000000    90        80         0           0.00    0
0.00
  xe39       10000000000    90        80         0           0.00    0
0.00
  xe40       10000000000    90        80         0           0.00    0
0.00
#
```

show interface counters summary

Use this command to display the summary of traffic counters on a specific interface or all interfaces.

Note: This command is supported for the out-of-band management (OOB) management interface.

Command Syntax

```
show interface (IFNAME|) counters summary
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show interface xe1/1 counters summary
+-----------+-------------------------------+-------------------------------+
|           |              Rx               |              Tx               |
| Interface |-------------------------------+-------------------------------|
|           |    packets    |     bytes     |    packets    |     bytes     |
+-----------+---------------+---------------+---------------+---------------+
 xe1/1       11032977        11032960000     61              3904


#show interface counters summary
+-------------+--------------------+--------------------+--------------------+--------------------+
|  Interface  |     Rx packets     |      Rx bytes      |     Tx packets     |      Tx bytes      |
+-------------+--------------------+--------------------+--------------------+--------------------+
 eth0          206222               13756391             235123               337010937
 po1           809121               72989094             825221               90605534
 xe1/1         0                    0                    1                    114
 xe3/1         43                   4730                 21                   2298
 xe5/1         29                   3178                 21                   2298
 xe8           10                   1076                 14                   1532
 xe9/1         16                   1760                 21                   2298
 xe11/1        0                    0                    7                    766
 xe19/1        12426292             1298526692           6                    620
 xe21/1        13                   1386                 14                   1532
 xe28/1        3144                 202370               21                   2298
 xe30/1        3161                 202304               7                    766
 xe32/1        694067               61687838             710274               79315093
 xe32/2        115054               11301256             114947               11290441
 xe32/3        603759               51208946             620502               68865557
 xe32/4        7                    766                  7                    766
```

Table 5-24 explain the fields in the command output.

Table 5-24: show interface counters summary output details

Field	Description
Interface	The particular interface.
RX	Number of hello packets received from the neighbor.
TX	Number hello packets transmitted to the neighbor.
bps	Bytes per second.
pps	Packets per second.
RX bps	Number of hello packets received from the neighbor in bytes per second.
RX pps	Number of hello packets received from the neighbor in packets per second.
TX bps	Number hello packets transmitted to the neighbor in bytes per second.
Tx pps	Number hello packets transmitted to the neighbor in packets per second.

show interface fec

Use this command to display the FEC (forward error correction) statistics for an interface.

Note: You can only display FEC statistics for physical interfaces and not for management or logical interfaces.

Command Syntax

```
show interface (IFNAME|) fec
```

Parameters

IFNAME	Physical Interface name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#sh int ce54 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce54           on        cl91        cl91        0                     12


#sh int ce53 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce53           auto      cl91        cl91        0                      0


#sh int ce52 fec
+-------------+--------+-----------+-------------+----------------------+------------------------+
| Interface   | Config | HW Status | Oper Status | Corrected Block Count| Uncorrected Block Count|
+-------------+--------+-----------+-------------+----------------------|------------------------+
 ce52           off       off         off         0                      0
```

Table 5-20 explain the fields in the command output.

Table 5-25: show interface fec

Field	Description
Interface	Name of the configured interface.
config	Configured value.
HW Status	FEC currently programmed in HW.
Oper Status	FEC currently operating over the link.

Table 5-25: show interface fec (Continued)

Corrected Block Count	Number of the corrected block count.
Uncorrected Block Count	Number of the uncorrected block count.

show ip forwarding

Use this command to display the IP forwarding status.

Command Syntax

```
show ip forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on
#
```

Table 5-26 explain the fields in the command output.

Table 5-26: show ip forwarding

Field	Description
vrf (management)	Management VRF is for management purposes. IP forwarding packet is on.
vrf (default)	The default VRF uses the default routing context for ip forwarding. IP forwarding packet is on.

show ip interface

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax

```
show ip interface brief
show ip interface IFNAME brief
```

Parameters

`IFNAME`	Interface name.
`brief`	Brief summary of IP status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface             IP-Address      Admin-Status          Link-Status
eth0                 *10.10.26.101    up                    up
lo                    127.0.0.1       up                    up
lo.management         127.0.0.1       up                    up
xe1/1                 10.1.1.1        up                    up
xe1/2                 unassigned      down                  down
xe1/3                 unassigned      down                  down
xe1/4                 unassigned      down                  down
xe2                   unassigned      up                    down
xe3/1                 unassigned      up                    up
xe3/2                 unassigned      down                  down
xe3/3                 unassigned      down                  down
```

Table 5-27 explain the fields in the command output.

Table 5-27: show ip interface output details

Field	Description
Interface	Interface name, also specifies interface type (eth0, lo, xe1/1, and xe1/2).
IP-Address	The IP address assigned to the interface. An asterisks indicates that the IP address was provided by DHCP.

Table 5-27: show ip interface output details (Continued)

Field	Description
Admin-Status	Interface is up and functioning or down.
Link-Status	Interface is connected and passing traffic.

show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

Syntax Description

```
show ip prefix-list
show ip prefix-list WORD
show ip prefix-list WORD seq <1-4294967295>
show ip prefix-list WORD A.B.C.D/M
show ip prefix-list WORD A.B.C.D/M longer
show ip prefix-list WORD A.B.C.D/M first-match
show ip prefix-list summary
show ip prefix-list summary WORD
show ip prefix-list detail
show ip prefix-list detail WORD
```

Parameters

`WORD`	Name of a prefix list.
`A.B.C.D/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Lookup longer prefix.
`<1-4294967295>`	Sequence number.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display all routes (selected and not selected), use the `show ip route database` command.

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

Command Syntax

```
show ip route A.B.C.D
show ip route (database|)
show ip route (database|) (bgp|connected|database|isis|fast-
  reroute|interface|isis|kernel|mbgp|mstatic|next-hop|ospf|rip|static)
show ip route summary
show ip route vrf WORD (database|)
show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
```

Parameters

`A.B.C.D`	Network in the IP routing table.
`A.B.C.D/M`	IP prefix <network>/<length>, for example, 35.0.0.0/8.
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	Routing table database.
`fast-reroute`	Fast reroute repair paths.
`interface`	Interface.
`isis`	IS-IS.
`kernel`	Kernel.
`mbgp`	Multiprotocol BGP routes.
`mstatic`	Multicast static routes.
`next-hop`	Next hop address.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes.
`WORD`	Routes for a Virtual Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example: Display FIB Routes

The following shows output for the best routes.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       E - EVPN,
v - vrf leaked
       * - candidate default
```

show ip route A.B.C.D/M longer-prefixes

Use this command to see all subnets of a specified network if they are present in the routing table. Please use this command with mask information.

Command Syntax

```
show ip route A.B.C.D/M longer-prefixes
```

Parameters

```
A.B.C.D/M
```

Command Mode

Exec-mode and Privileged exec-mode

Applicability

This command was introduced in OcNOS version 1.3.6.

Example

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked

    - candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, eth1, 00:00:23
C     10.12.41.0/24 is directly connected, eth0, 00:00:23
S     55.0.0.0/8 [1/0] is directly connected, eth1, 00:00:23
S     55.0.0.0/12 [1/0] is directly connected, eth1, 00:00:23
S     55.0.0.0/24 [1/0] is directly connected, eth1, 00:00:23
S     55.1.0.0/16 [1/0] is directly connected, eth1, 00:00:23
S     55.1.1.0/24 [1/0] is directly connected, eth1, 00:00:23
C     127.0.0.0/8 is directly connected, lo, 00:00:23

Gateway of last resort is 10.30.0.11 to network 0.0.0.0

K*      0.0.0.0/0 via 10.30.0.11, eth0
O       9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:18:56
K       10.10.0.0/24 via 10.30.0.11, eth0
C       10.10.31.0/24 is directly connected, eth2
S       10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
C       10.30.0.0/24 is directly connected, eth0
```

```
S       11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
S       16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O       17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:20:54
C       45.45.45.45/32 is directly connected, lo
O       55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:20:54
C       127.0.0.0/8 is directly connected, lo

#sh ip route 55.0.0.0/7 longer-prefixes
Routing entry for 55.0.0.0/8
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.0.0.0/8 longer-prefixes
Routing entry for 55.0.0.0/8
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1
```

```
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.0.0.0/11 longer-prefixes
Routing entry for 55.0.0.0/12
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.0.0.0/16 longer-prefixes
Routing entry for 55.0.0.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.1.0.0/16 longer-prefixes
Routing entry for 55.1.0.0/16
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.1.0.0/20 longer-prefixes
Routing entry for 55.1.1.0/24
```

```
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#sh ip route 55.1.0.0/24 longer-prefixes
% Network not in table
#
#sh ip route 55.1.1.0/24 longer-prefixes
Routing entry for 55.1.1.0/24
Known via "static", distance 1, metric 0,  External Route Tag: 0, best

    directly connected, eth1

#
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route and K indicates that the route has been learned from the kernel. Table 5-28 shows these codes and modifiers.

Table 5-28 explain the fields in the command output.

Table 5-28: route codes and modifiers

Code	Meaning	Description
K	kernel	Routes added through means other than by using the CLI; for example by using the operating system route command. Static routes added using kernel commands and static routes added using OcNOS commands are different. The kernel static routes are not redistributed when you give the `redistribute static` command in a protocol. However, the kernel static routes can be redistributed using the `redistribute kernel` command.
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols. Routes for connected networks always exist in the kernel routing table but as an exception are not marked as kernel routes because OcNOS always calculates entries for these routes upon learning interface information from the kernel.
S	static	Routes manually configured via CLI which are not updated dynamically by IGPs.
The codes below are for routes received and dynamically learned via IGP neighbors. These networks are not directly connected to this device and were announced by some other device on the network. IGPs update these routes as the network topology changes.		
R	RIP	RIP routing process and enter Router mode.
B	BGP	Route is from an Border Gateway Protocol.
O	OSPF	Modifiers for OSPF: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2

Table 5-28: route codes and modifiers

Code	Meaning	Description
i	IS-IS	Modifiers for IS-IS: L1 - IS-IS level-1 L2 - IS-IS level-2 ia - IS-IS inter area
Other modifiers:		
v	vrf leaked	The device has two or more VRFs configured and each has at least one interface bound to it. While each VRF will have its own routing table, the VRFs can learn each other's routes.
*	candidate default	Route has been added to the FIB. With equal cost paths to a destination, the router does per-packet or per-destination load sharing. An asterisk ("*") means that the route is being used at that instant for forwarding packets. If you run the same `show ip route x.x.x.x` command over and over, you might see the * moving between the route entries.
>	selected route	When multiple routes are available for the same prefix, the best route. When multiple entries are available for the same prefix, OcNOS uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. OcNOS populates the FIB with the *best* route to each destination
p	stale info	A route information that is marked stale due to graceful restart.

After the codes, the header has default gateway information:

```
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```

The "gateway of last resort", also called the default gateway, is a static route that routes IP address 0.0.0.0 (all destinations) through a single host (the gateway). The effect of setting a gateway is that if no routing table entry exists for a destination address, packets to that address will be forwarded to the gateway router.

Route Entry Fields

Table 5-29 explains the each route entry fields.

Table 5-29: route entry output details

Field	Description
Codes and modifiers	As explained in Table 5-28.
IP address	IP address of the remote network.
Administrative distance and metric	The administrative distance determines how trustworthy this route is. If there is a similar route but with a smaller administrative distance, it is used instead, because it is more "trustworthy". The smaller the administrative distance, the more trustworthy the route. Directly connected routes have an administrative distance of 0, which makes them the most trustworthy type of route.The metric varies from protocol to protocol, and for OSPF the metric is cost, which indicates the best quality path to use to forward packets. Other protocols, like RIP, use hop count as a metric. For neighboring routers, the metric value is 1.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.

Table 5-29: route entry output details

Field	Description
Outgoing interface name	Interface used to get to the next-hop address for this route.
Duration	Length of time that this route has been present in the routing table. This is also the length of time this route has existed without an update. If the route were removed and then re-added (if the cable was disconnected, for instance), this timer would begin again at 00:00:00.

Route Entry Examples

```
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
```

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via nexthop 10.10.31.16.
- The outgoing local interface for this route is eth2.
- This route was added 20 minutes and 54 seconds ago.

```
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
```

- This route is the same as the other OSPF route above; the only difference is that it is a Type 2 External OSPF route.

```
C       10.10.31.0/24 is directly connected, eth2
```

- This route is directly connected.
- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth2.

```
K       10.10.0.0/24 via 10.30.0.11, eth0
```

- This route in the network 10.10.0.0/24 was learned from the kernel routing table (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The outgoing local interface for this route is eth0.

```
K*      0.0.0.0/0 via 10.30.0.11, eth0
```

- This is a default route that was learned from the kernel (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The local interface for this route is eth0.

Example: Display OSPF Routes

The following is the output with the `ospf` parameter:

```
#show ip route ospf
O       1.1.1.0/24 [110/20] via 2.2.2.1, eth2, 00:00:44
O IA    4.4.4.0/24 [110/21] via 2.2.2.1, eth2, 00:00:44
#
```

Example: Display Route Summary

The following is the output with the `summary` parameter.

```
#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source    Networks
kernel          1
```

```
    connected       5
    ospf            2
    Total           8
    FIB             2
```

Example: Display RIB Routes

The following shows displaying database routes.

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

K    *> 0.0.0.0/0 via 10.30.0.11, eth0
O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:19:21
K    *> 10.10.0.0/24 via 10.30.0.11, eth0
O       10.10.31.0/24 [110/1] is directly connected, eth2, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:21:19
K    *  10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:19:21
O       16.16.16.16/32 [110/11] via 10.10.31.16, eth2, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:21:19
K    *  127.0.0.0/8 is directly connected, lo
C    *> 127.0.0.0/8 is directly connected, lo
```

The codes and modifier at the start of each route entry are explained in Table 5-28.

Routes in the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. Unselected routes have neither the * nor the > symbol.

Route Database Entry Examples

This example shows 2 entries in the route database; one learned from the kernel and the other derived from interface information.

```
K    * 10.30.0.0/24 is directly connected, eth0
C    *> 10.30.0.0/24 is directly connected, eth0
```

- Both these routes are in the same network 10.30.0.0/24.
- The first route has originated from the kernel. The * indicates that it has been added to the FIB.
- The second route is derived from the IP address of local interface eth0. It is marked as a connected route. Since a connected route has the lowest administrative distance, it is the selected route.

```
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
```

```
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
```

- The same prefix was learned from OSPF and from static route configuration.
- Static routes are preferred over OSPF routes, so the static route is selected and installed in the FIB.

  Note: If the static route becomes unavailable, OcNOS automatically selects the OSPF route and installs it in the FIB.

Example: Display VRF Routes

The following is the output with the `vrf` parameter:

```
#show ip route vrf vrf31
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
* - candidate default

IP Route Table for VRF "vrf31"
O            2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
O            20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:29
C            21.1.1.0/24 is directly connected, vlan1.4, 00:02:54
C            31.31.1.1/32 is directly connected, lo.vrf31, 00:03:02
O            40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:43
C            127.0.0.0/8 is directly connected, lo.vrf31, 00:03:05

Gateway of last resort is not set
```

The following is the output with the `vrf database` parameter:

```
#show ip route vrf vrf31 database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,
ia - IS-IS inter area, E - EVPN,
v - vrf leaked
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "vrf31"
O    *>  2.2.2.2/32 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  10.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
O    *>  20.1.1.0/24 [110/2] via 21.1.1.2, vlan1.4, 00:01:32
C    *>  21.1.1.0/24 is directly connected, vlan1.4, 00:02:57
O        21.1.1.0/24 [110/1] is directly connected, vlan1.4, 00:02:57
C    *>  31.31.1.1/32 is directly connected, lo.vrf31, 00:03:05
O        31.31.1.1/32 [110/1] is directly connected, lo.vrf31, 00:03:00
O    *>  40.40.1.1/32 [110/3] via 21.1.1.2, vlan1.4, 00:00:46
B     >  50.1.1.0/24 [200/0] via 41.41.41.41, 00:00:18
C    *>  127.0.0.0/8 is directly connected, lo.vrf31, 00:03:08

Gateway of last resort is not set
```

© 2025 IP Infusion Inc. Proprietary

show ip vrf

This command displays routing information about VRFs.

Command Syntax

```
show ip vrf
show ip vrf WORD
```

Parameter

WORD	Virtual Routing and Forwarding name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ip forwarding
 vrf (management) :IP forwarding is on
 vrf (default) :IP forwarding is on
```

show ipv6 forwarding

Use this command to display the IPv6 forwarding status.

Command Syntax

```
show ipv6 forwarding
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
 vrf (management) :IPv6 forwarding is on
 vrf (default) :IPv6 forwarding is on#
```

show ipv6 interface brief

Use this command to display information about interfaces. To display information about a specific interface, include the interface name.

Command Syntax

```
show ipv6 interface brief
show ipv6 interface IFNAME brief
```

Parameters

IFNAME	Name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show ipv6 interface brief
Interface           IPv6-Address                Admin-Status
lo                  ::1                         [up/up]

gre0                unassigned                  [admin down/down]

eth3                3ffe:abcd:104::1            [up/up]
                    3ffe:abcd:103::1
                    fe80::2e0:29ff:fe6f:cf0

eth1                fe80::260:97ff:fe20:f257    [up/up]

eth2                unassigned                  [admin down/down]

eth3                unassigned                  [admin down/down]

sit0                unassigned                  [admin down/down]

tun24               unassigned                  [admin down/down]

tunl0               unassigned                  [admin down/down]
```

Table 5-30 explains the each interface brief entry.

Table 5-30: show interface brief output details

Field	Description
Interface	Name of the interface.
IPv6-Address	IPv6 address. An asterisk (“*”) means the address was assigned by the DHCPv6 client.
Admin-Status	Status of the interface: The first part of the field indicates if the interface is up. The second part indicates if the interface is running.

show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes in the FIB can be viewed using `show ipv6 route`.

Command Syntax

```
show ipv6 route vrf WORD (database|)
show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route (database)
show ipv6 route (database) (bgp|connected|isis|kernel|ospf|rip|static)
show ipv6 route X:X::X:X
show ipv6 route X:X::X:X/M
show ipv6 route summary
```

Parameters

`X:X::X:X`	Network in the IP routing table.
`X:X::X:X/M`	Prefix <network>/<length>, e.g., 35.0.0.0/8
`all`	All IPv6 routes
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	IPv6 routing table database.
`isis`	IS-IS.
`IFNAME`	Interface name
`kernel`	Kernel.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes
`WORD`	Routes from a Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

See Table 5-28 and Table 5-29 for an explanation of the codes and fields in the output.

```
#show ipv6 route
Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
```

```
       I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.
C> * ::1/128 is directly connected, lo
C> * 3ffe:1::/48 is directly connected, eth1
C> * 3ffe:2:2::/48 is directly connected, eth2
#
```

show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

Syntax Description

```
show ipv6 prefix-list
show ipv6 prefix-list WORD
show ipv6 prefix-list WORD seq <1-4294967295>
show ipv6 prefix-list WORD X:X::X:X/M
show ipv6 prefix-list WORD X:X::X:X/M longer
show ipv6 prefix-list WORD X:X::X:X/M first-match
show ipv6 prefix-list summary
show ipv6 prefix-list summary WORD
show ipv6 prefix-list detail
show ipv6 prefix-list detail WORD
```

Parameters

`WORD`	Name of prefix list.
`X:X::X:X/M`	IP prefix <network>/<length> (for example, 35.0.0.0/8).
`first-match`	First matched prefix.
`longer`	Look up longer prefix.
`<1-4294967295>`	Sequence number of an entry.
`detail`	Detail of prefix lists.
`summary`	Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries
   seq      5 permit 172.1.1.0/16
   seq     10 permit 173.1.1.0/16
   seq     15 permit 174.1.1.0/16
```

show hosts

Use this command to display the IP domain-name, lookup style and any name server.

Command Syntax

```
show hosts
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show hosts

       VRF: management

DNS lookup is enabled
 Default domain      : .com
 Additional Domain   : .in .ac
 Name Servers        : 10.12.3.23
Host                                                                    Address
----                                                                    -------
test                                                                    10.12.12.67
test                                                                    10::23

 * - Values assigned by DHCP Client.
```

Table 5-31 explains the output fields.

Table 5-31: show hosts fields

Entry	Description
VRF: management	DNS configuration of specified VRF
DNS lookup is enabled	DNS feature enabled or disabled
Default domain	Default domain name used to complete unqualified host names (names without a dotted decimal domain name).
Additional Domain	A list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.
Name Servers	DNS server addresses that are used to translate hostnames to IP addresses.

Table 5-31: show hosts fields

Entry	Description
Host Address test 10.12.12.67 test 10::23	Static hostname-to-address mappings in DNS.
* - Values assigned by DHCP Client.	* in name-server indicates it has been learned dynamically.

show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

Command Syntax

```
show running-config interface IFNAME
show running-config interface IFNAME bridge
show running-config interface IFNAME ip igmp
show running-config interface IFNAME ip multicast
show running-config interface IFNAME ip pim
show running-config interface IFNAME ipv6 ospf
show running-config interface IFNAME ipv6 rip
show running-config interface IFNAME ipv6 pim
show running-config interface IFNAME isis
show running-config interface IFNAME lacp
show running-config interface IFNAME ldp
show running-config interface IFNAME mpls
show running-config interface IFNAME mstp
show running-config interface IFNAME ospf
show running-config interface IFNAME ptp
show running-config interface IFNAME rip
show running-config interface IFNAME rstp
show running-config interface IFNAME rsvp
show running-config interface IFNAME stp
show running-config interface IFNAME synce
```

Parameters

`bridge`	Bridge.
`ip`	IPv4 (see also show running-config interface ip).
`ipv6`	IPv6 (see also show running-config interface ipv6).
`isis`	Intermediate System to Intermediate System.
`lacp`	Link Aggregation Control Protocol.
`ldp`	Label Distribution Protocol.
`mpls`	Multi-Protocol Label Switching.
`mstp`	Multiple Spanning Tree Protocol.
`ospf`	Open Shortest Path First.
`ptp`	Precision Time Protocol.
`rip`	Routing Information Protocol.

`rstp`	Rapid Spanning Tree Protocol.
`rsvp`	Resource Reservation Protocol.
`stp`	Spanning Tree Protocol.
`synce`	Synchronous Ethernet.

Command Mode

Privileged Exec mode and Config Mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 bridge
!
interface eth1
 switchport
 bridge-group 1
 switchport mode access
 user-priority 3
 traffic-class-table user-priority 2 num-traffic-classes 3 value 3 traffic-
class-table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table
user-priority 7 num-traffic-classes 2 value 0 traffic-class-table user-
priority 7 num-traffic-classes 3 value 0 traffic-class-table user-priority 7
num-traffic-classes 4 value 0 traffic-class-table user-priority 7 num-traffic-
classes 5 value 0 traffic-class-table user-priority 7 num-traffic-classes 6
```

show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

Command Syntax

```
show running-config interface IFNAME ip (igmp|multicast|pim|)
```

Parameters

`IFNAME`	Interface name.
`igmp`	Internet Group Management Protocol.
`multicast`	Multicast.
`pim`	Protocol Independent Multicast.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1
 switchport
```

show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

Command Syntax

```
show running-config interface IFNAME ipv6 (mld|multicast|ospf|pim|rip|)
```

Parameters

`IFNAME`	Interface name.
`mld`	Multicast Listener Discovery
`multicast`	Multicast
`ospf`	Open Shortest Path First
`pim`	Protocol Independent Multicast
`rip`	Routing Information Protocol

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
#show running-config interface eth1 ipv6 rip
!
interface eth1
 switchport
```

show running-config ip

Use this command to show the running system of IP configurations.

Command Syntax

```
show running-config ip (dhcp|mroute|route)
```

Parameters

`dhcp`	Dynamic Host Configuration Protocol.
`mroute`	Static IP multicast route.
`route`	Static IP route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ip route
!
ip route 3.3.3.3/32 eth3
ip route 3.3.3.3/32 eth2
ip route 200.0.0.0/16 lo
!
```

show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

Command Syntax

```
show running-config ipv6 (access-list|mroute|neighbor|prefix-list|route|)
```

Parameters

`access-list`	Access list.
`mroute`	Static IPv6 Multicast route.
`neighbor`	Static IPv6 neighbor entry.
`prefix-list`	IPv6 prefix-list.
`route`	Static IPv6 route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde
 seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 eth2
ipv6 route fe80::/64 eth2
!
```

show running-config prefix-list

Use this command to display the running system status and configuration details for prefix lists.

Command Syntax

```
show running-config prefix-list
```

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
(config)#show running-config prefix-list
!
ip prefix-list abc
 seq 5 permit any
!
ip prefix-list as
 description annai
!
ip prefix-list wer
 seq 45 permit any
!
(config)#
```

shutdown

Use this command to shut down an interface.

Use the `no` form of this command to bring up an interface.

Command Syntax

```
shutdown
no shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth3`.

```
#configure terminal
(config)#interface eth3
(config-if)#shutdown
```

speed

Use this command to set the link speed of the interface.

Use the `no` parameter to reset the speed to its default value.

- On copper ports, auto-negotiation is enabled by default. Limited auto-negotiation is also supported, allowing users to advertise a specific speed for an interface. For example, user can configure an interface to auto-negotiate only with a 100m peer.
- On fiber optic ports, auto-negotiation is disabled by default. Auto-negotiation is not supported on fiber optic medium or AOC for speeds 10g and beyond. IP Infusion Inc.does not recommend using auto speed on such transceivers. For DAC cables, both force and auto-negotiation are supported.
- IP Infusion Inc. recommends configuring the same speed mode on both peers.
- When user configure an interface with the speed auto option, the negotiated parameters are speed, duplex, flowcontrol, and fec, each configured separately. Refer to the respective command for details.

Note:

- For 10g DAC or AOC, setting speed auto negotiates with a maximum of 1G.
- Interface speed setting is only supported on physical front-panel ports and not supported on Management interface `eth0`.
- Configuring or unconfiguring speed will reset FEC to auto mode.

Table 5-32 shows the IP Infusion Inc. recommendations for front-panel port speed and transceivers.

Table 5-32: Recommendations

Supported/ Recommended	Explanation
Not Supported	When the front panel port capability is less than the transceiver's capability, the behavior is undefined.
Not Recommended	When the transceiver's capability matches the front panel port capability, reducing the speed is not recommended.
Recommended	When the transceiver's capability is less than the front panel port capability, the behavior is undefined, and the link might still come up. Set the speed to match the transceiver's capability.

Table 5-33 shows examples of front-panel configurations:

Table 5-33: Front-panel configurations

Front Panel Port	Explanation
Front Panel Port 100g	Use the `speed 40g` command with 40g transceivers. IP Infusion Inc. does not recommend to use 40g on 100g speed transceivers.
Front Panel Port 40g	Do not use 100g transceivers.

Table 5-33: Front-panel configurations (Continued)

Front Panel Port	Explanation
Front Panel Port 25g	Use the `port-group` command to reduce the speed to 10g when using 10g transceivers. IP Infusion Inc. does not recommend to use 10g on 25g speed transceivers. Set the speed to 1g when using 1g transceivers. Below 25g, port speed can vary (10g or 1g) for ports within the same port group, e.g., one port can have 1g while the remaining have 10g. However, one port at 25g and the rest at 10g is not allowed. Using the `no speed` command at the interface level tries to set the speed to 25g for one port in the `port-group` while others may be at 10g or 1g, which is not allowed. Use the `no port-group` command in such cases.
Front Panel Port 10g	Do not use 25g transceivers. Set the speed to 1g when using 1g transceivers.
Front Panel Port 1g	Do not use 10g or 25g transceivers..

Command Syntax

```
speed (10m | 100m | 1g | 2.5g | 10g | 20g | 25g | 40g | 50g | 100g | auto (10m | 100m
  | 1g) )
no speed
```

Parameter

`10m`	Set the speed to 10 megabits per second.
`100m`	Set the speed to 100 megabits per second.
`1g`	Set the speed to 1 gigabit per second.
`2.5g`	Set the speed to 2.5 gigabits per second.
`10g`	Set the speed to 10 gigabits per second.
`20g`	Set the speed to 20 gigabits per second.
`25g`	Set the speed to 25 gigabits per second.
`40g`	Set the speed to 40 gigabits per second.
`50g`	Set the speed to 50 gigabits per second.
`100g`	Set the speed to 100 gigabits per second.
`auto`	Auto negotiate the speed
`auto 10m`	Auto negotiate only with a 10Mb peer
`auto 100m`	Auto negotiate only with a 100Mb peer
`auto 1g`	Auto negotiate only with a 1g peer

Default

None

Command Mode

Interface mode

Applicability

Introduced before OcNOS version 1.3 and added parameters `auto 10m, auto 100m, and auto 1g` in the OcNOS version 6.4.2.

Example

Enable auto-negotiation:

```
OcNOS#configure terminal
OcNOS(config)#interface xe0
OcNOS(config-if)#speed auto 10m
```

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured `routed` by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

User should be prompted for confirmation, while executing `switchport/no switchport` command. To support this requirement, please refer the command `enable/disable confirmation-dialog`.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no switchport
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport

(config)#interface eth0
(config-if)#no switchport

#configure terminal
(config)#enable confirmation-dialog
(config)#interface xe5
(config-if)#switchport
Are you sure? (y/n): y
(config-if)#
(config-if)#exit

(config)#disable confirmation-dialog
(config)#
(config)#interface xe5
(config-if)#switchport
(config-if)#
```

switchport allowed ethertype

Use this command to indicate which types of traffic will be allowed on the switchport.

Note: A maximum of 5 Ethertype values can be assigned on an interface.

Command Syntax

```
switchport allowed ethertype {arp|ipv4|ipv6|mpls|ETHTYPE|log}
```

Parameters

`arp`	ARP traffic
`ipv4`	IPv4 traffic
`ipv6`	IPv6 traffic
`mpls`	MPLS traffic
`ETHTYPE`	Traffic of any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is not available on Qumran platforms.

Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```

switchport protected

Use this command to enable or disable the protected port feature on an interface.

Command Syntax

```
switchport protected (community | isolated | promiscuous)
no switchport protected
```

Parameter

`community`	Community mode
`isolated`	Isolated mode type
`promiscuous`	Protected mode type

Default

Promiscuous

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0. The `community` mode is not supported in Qumran2 series platforms (J2C PLUS, Q2A, Q2C, Q2U).

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport protected isolated
(config-if)#no switchport protected

(config)#interface po1
(config-if)#switchport protected promiscuous
(config-if)#no switchport protected
```

transceiver

Use this command to set the type of Small Form-factor Pluggable (SFP) transceiver inserted in the physical port.

Use the `no` form of this command to remove the setting.

Command Syntax

```
transceiver (1000base-sx|1000base-lx|1000base-ex|1000base-cx|10gbase-sr|10gbase-
  lr|10gbase-er|10gbase-cr|25gbase-sr|25gbase-lr|25gbase-er|25gbase-cr|40gbase-
  sr4|40gbase-lr4|40gbase-er4|40gbase-cr4|100gbase-sr4|100gbase-lr4|100gbase-
  er4|100gbase-cr4)
no transceiver
```

Parameters

`1000base-cx`	SFP 1000base-cx
`1000base-ex`	SFP 1000base-ex
`1000base-lx`	SFP 1000base-lx
`1000base-sx`	SFP 1000base-sx
`100gbase-cr4`	QSFP28 100gbase-cr4
`100gbase-er4`	QSFP28 100gbase-er4
`100gbase-lr4`	QSFP28 100gbase-lr4
`100gbase-sr4`	QSFP28 100gbase-sr4
`10gbase-cr`	SFP+ 10gbase-cr
`10gbase-er`	SFP+ 10gbase-er
`10gbase-lr`	SFP+ 10gbase-lr
`10gbase-sr`	SFP+ 10gbase-sr
`25gbase-cr`	SFP+ 25gbase-cr
`25gbase-ers`	SFP+ 25gbase-er
`25gbase-lr`	SFP+ 25gbase-lr
`25gbase-sr`	SFP+ 25gbase-sr
`40gbase-cr4`	QSFP 40gbase-cr4
`40gbase-er4`	QSFP 40gbase-er4
`40gbase-lr4`	QSFP 40gbase-lr4
`40gbase-sr4`	QSFP 40gbase-sr4

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 5.0.

Examples

```
(config)#interface ce1/1
(config-if)#transceiver 40gbase-lr4
```

tx cdr-bypass

Use this command to by-pass the transmitter Clock Data Recovery (CDR) on transceivers which supports CDR control and operating at lower speeds than maximum operating speed.

Use the `no` form of this command to disable CDR by-pass.

Command Syntax

```
tx cdr-bypass
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.5.2.

Examples

```
#configure terminal
(config)#interface ce1
(config-if)#tx cdr-bypass
 Bypass the TX CDR control

(config)#interface ce1
(config-if)#no tx cdr-bypass
```

rx cdr-bypass

Use this command to by-pass the receiver Clock Data Recovery (CDR) on transceivers which supports CDR control and operating at lower speeds than maximum operating speed.

Use the no form of this command to disable CDR by-pass

Command Syntax

```
rx cdr-bypass
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.5.2.

Examples

```
#configure terminal
(config)#interface ce1
(config-if)#rx cdr-bypass
 Bypass the RX CDR control

(config)#interface ce1
(config-if)#no rx cdr-bypass
```

CHAPTER 6 Time Range Commands

This chapter describes the commands used to create and manage time range objects which are used to add a timing boundary for specified activities. The activity starts, ends, and repeats at the specific times that you set.

- end-time (absolute)
- end-time after (relative)
- frequency
- frequency days (specific days)
- start-time (absolute)
- start-time after (relative)
- start-time now (current)
- time-range

end-time (absolute)

Use this command to set the end time for the time range to an absolute time.

Command Syntax

```
end-time HH:MM <1-31> (january | february | march | april | may | june | july |
  august | september | october | november | december) <1995-2035>
```

Parameters

`HH:MM`	End time hour and minutes
`<1-31>`	Day of the month
`april`	Month of April
`august`	Month of August
`december`	Month of December
`february`	Month of February
`january`	Month of January
`july`	Month of July
`june`	Month of June
`march`	Month of March
`may`	Month of May
`november`	Month of November
`october`	Month of October
`september`	Month of September
`<1995-2035>`	Year

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#end-time 10:10 20 february 2021
```

end-time after (relative)

Use this command to set the end time for the time range to a relative time in minutes, from the configured start time.

Command Syntax

```
end-time after <1-129600>
```

Parameters

<1-129600>	Number of minutes from the start time

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#end-time after 100
```

frequency

Use this command to set the frequency for the time range.

Command Syntax

```
frequency (daily|hourly|weekly)
```

Parameters

`daily`	Daily frequency
`hourly`	Hourly frequency
`weekly`	Weekly frequency

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#frequency hourly
```

frequency days (specific days)

Use this command to set the frequency for the time range to specific days of the week.

Command Syntax

```
frequency days WORD
```

Parameters

`WORD`	Colon-separated list of 3-letter days of the week for the days on which the range is repeated. For example: `mon:tue:wed:thu:fri:sat:sun`

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#frequency days mon:wed:fri
(config)#exit
(config)#time-range TIMER2
(config-tr)#frequency days mon:tue:wed:thu:fri:sat:sun
```

start-time (absolute)

Use this command to set the start time for the time range to an absolute time.

Command Syntax

```
start-time HH:MM <1-31> (january | february | march | april | may | june | july |
  august | september | october | november | december) <1995-2035>
```

Parameters

HH:MM	End time hour and minutes
<1-31>	Day of the month
april	Month of April
august	Month of August
december	Month of December
february	Month of February
january	Month of January
july	Month of July
june	Month of June
march	Month of March
may	Month of May
november	Month of November
october	Month of October
september	Month of September
<1995-2035>	Year

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time 09:09 20 february 2021
```

start-time after (relative)

Use this command to set the start time for the time range to a relative time in minutes, from the current time.

Command Syntax

```
start-time after <1-129600>
```

Parameters

<1-129600>	Number of minutes from the current time

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time after 100
```

start-time now (current)

Use this command to set the start time for the time range to the current system time.

Command Syntax

```
start-time now
```

Parameters

None

Default

N/A

Command Mode

Time range mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
(config)#time-range TIMER1
(config-tr)#start-time now
```

time-range

Use this command to create a time range and go into the time range mode to configure the time range. If the time range already exists, then it will be edited.

Use the `no` form of this command to remove a time range object.

Command Syntax

```
time-range NAME
no time-range NAME
```

Parameters

`NAME`	Name of the time range.

Default

N/A

Command Mode

Configuration mode

Applicability

This command was introduced in OcNOS version 5.0.

Example

```
#configure terminal
(config)# time-range TIMER1
(config-tr)#?
Time Range configuration commands:
  WORD        String
  abort       Abort Transaction
  commit      commit
  end         End current mode and change to EXEC mode
  end-time    The end time for the Time Range
  exit        End current mode and down to previous mode
  frequency   The frequency of the Time Range
  help        Description of the interactive help system
  no          Delete
  quit        Exit current mode and down to previous mode
  show        Show running system information
  start-time  The start time for the Time Range
```

CHAPTER 7 VLOG Commands

This chapter describes virtual router log (VLOG) commands.

- show vlog all
- show vlog clients
- show vlog terminals
- show vlog virtual-routers

show vlog all

Use this command to display the output of all virtual router log `show` commands. For column descriptions, refer to descriptions of the individual commands.

Command Syntax

```
show vlog all
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog all

Type     Name      FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8  12  vr222    ---        1
tty   /dev/pts/4  13  <PVR>    ---        1

VR-Name  VR-Id  PVR-Terms  VR-Terms                  LogFile
CurSize
<PVR>        0          1         0         /var/local/zebos/log/pvr/my-log
1624320
vr111        1          0         0         n/a
n/a
vr222         2           0         1          /var/local/zebos/log/vr222/log-
vr222         0
vr333         3           0         0          /var/local/zebos/log/vr333/log-
vr333         0

Name  Id  MsgCnt        ConTime              ReadTime
NSM    1       1  Fri May-15 21:05:04  Fri May-15 21:05:04
IMI   19       1  Fri May-15 21:05:02  Fri May-15 21:05:02
```

Table 7-34 explains the output:

Table 7-34: show vlog all details

Name	Name of protocol module
Id	Protocol module identifier

Table 7-34: show vlog all details

MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

Table 7-35 explains the output:

Table 7-35: show vlog all details

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

Table 7-36 explains the output:

Table 7-36: show vlog all details

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

show vlog clients

Use this command to display all attached virtual router log clients (protocol modules).

Command Syntax

```
show vlog clients
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog clients

Name   Id  MsgCnt          ConTime                ReadTime
NSM     1       1     Fri May-15 21:05:04  Fri May-15 21:05:04
IMI    19       1     Fri May-15 21:05:02  Fri May-15 21:05:02
```

Table 7-37 explains the output:

Table 7-37: show vlog clients details

Name	Name of protocol module
Id	Protocol module identifier
MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

show vlog terminals

Use this command to display all active connections where VLOGD is forwarding log output.

Command Syntax

```
show vlog terminals
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog terminals

Type      Name      FD  UserVR  AllVrs  VRCnt
tty   /dev/pts/8   12  vr222     ---      1
tty   /dev/pts/4   13  <PVR>     ---      1
```

Table 7-38 explains the output:

Table 7-38: show virtual router log terminals details

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

show vlog virtual-routers

Use this command to display virtual router statistics such as the number of terminals attached.

Command Syntax

```
show vlog virtual-routers
```

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before OcNOS version 1.3.

Example

```
>enable
#show vlog virtual-routers

VR-Name  VR-Id  PVR-Terms  VR-Terms LogFile
CurSize
<PVR>         0  1          0        /var/local/zebos/log/pvr/my-log
1624320
vr111         1  0          0        n/a                                    n/a
vr222         2  0          1        /var/local/zebos/log/vr222/log-vr222   0
vr333         3  0          0        /var/local/zebos/log/vr333/log-vr333   0
```

Table 7-39 explains the output:

Table 7-39: show vlog virtual-routers details

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals
LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

CHAPTER 8 Linux Shell Commands

This chapter is a reference for Linux shell commands that you can run at the OcNOS prompt.

Table 8-40 describes the commands. Note the following:

- You must be in privileged exec mode to run these commands.
- You cannot use the pipe (“|”) or redirect (">") operators.

Table 8-40: Linux shell commands

Command	Description
`cat` *file*	Display contents of *file*
`cd`	Change to home directory
`cd` *dir*	Change directory to *dir*
`cp` *file1 file2*	Copy *file1* to *file2*
`cp -r` *dir1 dir2*	Copy *dir1* to *dir2*; create *dir2* if it does not exist
`dir`	Display contents of current directory
`less` *file*	Display the contents of file
`ls` *options*	Display contents of current directory
`mkdir` *dir*	Create a directory *dir*
`more` *file*	Display the contents of *file*
`mv` *file1 file2*	Rename *file1* to *file2*
`mv` *file dir*	Move *file* to directory *dir*
`pwd`	Display current directory
`rmdir` *dir*	Remove a directory *dir* (only if empty)

CHAPTER 9 System Configure Mode Commands

This chapter provides a reference for the system configure mode commands.

- delay-profile interfaces
- delay-profile interfaces subcommands
- forwarding profile
- load-balance enable
- show forwarding profile limit
- show hardware-profile filters
- evpn mpls irb
- hardware-profile filter (Qumran1)
- hardware-profile filter (Qumran2)
- hardware-profile flowcontrol
- hardware-profile service-queue
- hardware-profile statistics
- hardware-profile bgp-flowspec-mode
- ip redirects
- show nsm forwarding-timer
- show queue remapping

© 2025 IP Infusion Inc. Proprietary

delay-profile interfaces

Use this command to go into the delay-profile mode to edit the parameters of the "interfaces" profile. In this mode, the user is able to edit the delay measurement profile parameters.

Command Syntax

```
delay-profile interfaces
```

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#delay-profile interfaces
(config-dp-intf)#
```

delay-profile interfaces subcommands

The following commands are to edit the delay-profile parameters.

Note: According to IGP-TE RFC8570 and RFC7471, the advertised delay should be unidirectional. So when the mode is set to two-way, the advertised delay is “Average_RTT_delay / 2” and when the mode is set to one-way, the advertised delay is “Average_FWD_delay”. The default value is “two-way”.

Command Syntax

```
mode <two-way>|<one-way>
burst-interval <1000-15000>
burst-count <1-5>
interval < 30-3600>
sender-port <1025-65535>
advertisement periodic
advertisement periodic threshold <1-100>
advertisement periodic minimum-change <0-10000>
no advertisement periodic
advertisement accelerated
advertisement accelerated threshold <1-100>
advertisement accelerated minimum-change <0-10000>
no advertisement accelerated
```

Parameters

`one-way`	The one-way value sets the mode to one-way measurement.
`two-way`	The two-way value sets the mode to two-way measurement.
`<1000-15000>`	Set the burst interval in milliseconds. The default value is 3000 milliseconds and the range is 1000-15000 milliseconds
`<1-5>`	Set the number of packets to be sent at each burst interval. The default value is 1 and the range is 1-5
`<30-3600>`	Set the computation interval in seconds. The default computation interval is 30 seconds. The range is 30-3600 seconds. This will be used also as the periodic advertisement interval.
`<1-100>`	Set the advertisement threshold percentage in the range of 1-100 (for periodic, default=10% and for accelerated, default=20%
`<1025-65535>`	Set the TWAMP sender port value in the range 1025-65535. If not specified, the default value is 862)
`<0-10000>`	Set the advertisement minimum change in microseconds in the range 0-10000 (for periodic, default=1000 and for accelerated, default=2000)

Command Mode

delay-profile interfaces mode

Default

The default mode value is “two-way”.

Applicability

This command was introduced in OcNOS version 5.1.

Examples

```
#configure terminal
(config)#delay-profile interfaces
(config-dp-intf)#mode two-way
(config-dp-intf)#burst-count 5
(config-dp-intf)#burst-interval 3000
(config-dp-intf)#interval 30
(config-dp-int)#sender-port 862
(config-dp-intf)#advertisement periodic threshold 10
(config-dp-intf)#advertisement periodic minimum-change 1000
(config-dp-intf)#advertisement accelerated
(config-dp-intf)#advertisement accelerated threshold 20
(config-dp-intf)#advertisement accelerated minimum-change 2000
(config-dp-intf)#no advertisement periodic
(config-dp-intf)#commit
(config-dp-intf)#exit
(config)#
```

evpn mpls irb

Use this command to enable EVPN MPLS IRB (Integrated Routing & Bridging) feature.

Command Syntax

```
evpn mpls irb
```

Parameters

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 6.0.0

Examples

```
(config)#evpn mpls irb
```

The following table list the qualifiers for TCAM group.

Table 9-41: TCAM Group

Group	Qualifiers
evpn-irb	L4 Ports Destination Port Source IP Destination IP Source/Destination MAC1/MAC2 Ethertype

forwarding profile

Use this command to configure different forwarding profiles in hardware.

Note: To apply profile configuration changes in the hardware, you must save the configuration and reboot, except when modifying the default profile.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use this `no` command to set the forwarding table size to the default.

Command Syntax

```
forwarding profile (kaps (profile-one | profile-two)) | (elk-tcam (profile-one |
  profile-two | profile-three | custom-profile))
no forwarding profile (kaps) | (elk-tcam (custom-profile))
```

Parameters

For details about these profiles, see show forwarding profile limit.

`kaps`	Internal KBP routing table
`profile-one`	KAPS profile one
`profile-two`	KAPS profile two
`elk-tcam`	External TCAM routing table
`profile-one`	external TCAM profile one
`profile-two`	external TCAM profile two
`profile-three`	external TCAM profile three
`custom-profile`	external TCAM custom profile
`< 10-90>`	percent of ipv4 routes
`< 10-90>`	percent of ipv6 routes

Default

The default forwarding profile are as below

Table 9-42:

Is ELK-TCAM present	KAPS	ELK-TCAM
Yes	profile-two	profile-one
No	profile-one	N/A

Note:

1. elk-tcam profiles are supported only on hardware models which have external TCAM for routing.
2. forwarding profile-three is applicable on hardware model Agema AGC7648A.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version SP 1.0. The `no` version of the command was introduced in OcNOS version 5.0.

Examples

```
#configure terminal
(config)# forwarding profile elk-tcam profile-one
(config)# no forwarding profile elk-tcam
```

hardware-profile filter (Qumran1)

Use this command to enable or disable ingress IPv4 or IPv6, egress IPv6 filter groups, EVPN-MPLS,VxLAN filter and TWAMP IPv4 or IPv6 groups. Disabling filter groups increases the configurable filter entries.

Disabling a TCAM filter group is not allowed if the group has any entries configured in hardware. Group dependent entries must be explicitly removed before disabling the TCAM group.

Note:

- This feature is supported for IPv4 unicast and IPv4 BGP/MPLS VPN service based on RFC 8955.
- The `qos`, `qos-ext`, and `qos-policer` filter groups can only be used for Layer 2 and IPv4 traffic. For IPv6 traffic QoS classification and actions, users must enable the `ingress-ipv6-qos` group and create an IPv6 ACL which can be matched in a class-map for applying QoS actions. For more details, refer to the *Quality of Service Guide*.
- Usually the number of extended ingress filter groups that can be created at the same time is 3. If the PIM bidirectional feature is enabled, only 2 ingress extended filter groups can be created.
- The `ipv4-ext` and `qos-policer grp` parameters are not supported together.
- For better utilization of TCAM resources, it is recommended to enable the large groups first and then smaller groups. For example, Using `admin` credentials, configure `evpn-mpls-mh` as last filter as it is the smallest group.

Example 1

```
(config)#hardware-profile filter ingress-ipv4-ext enable
(config)#hardware-profile filter ingress-ipv6 enable
(config)#hardware-profile filter qos-ext enable
(config)#hardware-profile filter ingress-l2 enable
(config)#hardware-profile filter evpn-mpls-mh enable
```

Example 2

```
(config)#hardware-profile filter ingress-ipv4-qos enable
(config)#hardware-profile filter ipv4-bgp-flowspec enable
(config)#hardware-profile filter ingress-l2 enable
(config)#hardware-profile filter vxlan enable
(config)#hardware-profile filter vxlan-mh enable
```

Example 3

```
(config)#hardware-profile filter qos-ext enable
(config)#hardware-profile filter egress-ipv4 enable
(config)#hardware-profile filter ipv4-bgp-flowspec enable
(config)#hardware-profile filter ingress-ipv4 enable
(config)#hardware-profile filter ingress-ipv4 enable
```

The `twamp-ipv4` hardware profile sets up a PMF group to manage TWAMP IPv4 traffic, enabling precise hardware time stamping of TWAMP packets. These packets are identified by their source IP, destination IP, source UDP port, and destination UDP port. When a packet is recognized as a TWAMP packet, the `bcmFieldActionOam` action is applied, directing the packet to the OAMP module for time stamping. Additionally, the `bcmFieldActionForward` action is used to ensure the packet is encapsulated with the correct FEC. If the packet includes MPLS labels, the predefined qualifiers will not match. In this scenario, user-defined qualifiers are added to the same PMF group to identify the TWAMP packet.

The `twamp-ipv6` hardware profile establishes two PMF groups to manage TWAMP IPv6 traffic, differentiating between MPLS and non-MPLS traffic due to the inability to fit user-defined qualifiers in a single PMF group. These groups ensure accurate hardware time stamping of TWAMP packets, identified by their source IPv6, destination IPv6,

source UDP port, and destination UDP port. When a packet is recognized as a TWAMP packet, the `bcmFieldActionOam` action is applied, sending the packet to the OAMP module for time stamping. Additionally, the `bcmFieldActionForward` action ensures the packet is encapsulated with the correct FEC. If the packet includes MPLS labels, the predefined qualifiers will not match. In this case, user-defined qualifiers are added to identify the TWAMP packet, and since the IPv6 qualifiers cannot be included in the same group, they are created in a separate group.

Note: Enabling TWAMP hardware profiles requires a system reboot.

Command Syntax

```
hardware-profile filter (ingress-l2|ingress-l2-ext|ingress-ipv4|ingress-ipv4-
  ext|ingress-ipv4-qos|ingress-ipv6|ingress-ipv6-ext|ingress-ipv6-ext-
  vlan|ingress-ipv6-qos|qos-ipv6|ingress-arp|qos|qos-ext|qos-policer|egress-
  l2|egress-ipv4|evpn-mpls-cw|evpn-mpls-mh|vxlan|vxlabn-mh|cfm-domain-name-
  str|twamp-ipv4|twamp-ipv6|twamp-ipv6-mpls|ipv4-bgp-flowspec|) (enable|disable)
```

Parameter

`ingress-l2`	Ingress L2 ACL filter group.
`ingress-l2-ext`	Ingress L2 ACL, QoS, mirror filter group.
`ingress-ipv4`	Ingress IP ACL filter group.
`ingress-ipv4-ext`	Ingress IP ACL, mirror, PBR filter group.
`ingress-ipv4-qos`	Ingress IPv4 group for ACL match QoS.
`ingress-ipv6`	Ingress IPv6 ACL, mirror, PBR filter group
`ingress-ipv6-ext`	Ingress IPv6 group to support 128-bit address qualification support on physical interface.
`ingress-ipv6-ext-vlan`	Ingress IPv6 group to support 128-bit address qualification support on vlan interface and subinterface.
`ingress-ipv6-qos`	Ingress IPv6 group for ACL match QoS.
`qos-ipv6`	Ingress QOS IPv6 group for IPv6 QoS support with statistics.
`ingress-arp`	Ingress ARP group.
`qos`	Ingress QoS filter group
`qos-ext`	Ingress QoS extended filter group.
`qos-policer`	Ingress extended QoS group for hierarchical policer support.
`egress-l2`	Egress L2 ACL filter group
`egress-ipv4`	Egress IP ACL filter group.
`evpn-mpls-mh`	Ingress EVPN MPLS Multi-Homing Forwarding Group
`vxlan`	Ingress VxLAN Forwarding group
`vxlan-mh`	Ingress VxLAN Multi-Homing Forwarding Group.
`cfm-domain-name-str`	Egress CFM domain group.
`twamp-ipv4`	TWAMP IPv4 filter group.
`twamp-ipv6`	TWAMP IPv6 filter group.
`twamp-ipv6-mpls`	TWAMP IPv6 MPLS filter group.
`ipv4-bgp-flowspec`	BGP FlowSpec filter group.

`ingress-l2`	Ingress L2 ACL filter group.
`enable`	Enable filter group.
`disable`	Disable filter group

Default

By default, all filter groups are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#hardware-profile filter ingress-ipv4 enable
OcNOS(config)#hardware-profile filter ingress-ipv4 disable
OcNOS(config)#hardware-profile filter egress-ipv4 enable
OcNOS(config)#hardware-profile filter egress-ipv4 disable
```

Table 9-43: Supported groups and the feature dependency on the groups

Group	Key Size	Security	QoS	PBR	Mirror	Statistics		
						QMX	QAX	QUX
ingress-l2	160	Yes	No	N/A	No	Yes	Yes	Yes
ingress-l2-ext	320	Yes	No	N/A	Yes	Yes	Yes	Yes
ingress-ipv4	160	Yes	No	No	No	Yes	Yes	Yes
ingress-ipv4-ext	320	Yes	No	Yes	Yes	Yes	Yes	Yes
ingress-ipv4-qos	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
ingress-ipv6	320	Yes	No	Yes	Yes	Yes	Yes	Yes
Ingress-ipv6-ext	320	N/A	Yes	No	Yes	Yes	Yes	Yes
Ingress-ipv6-ext-vlan	320	N/A	Yes	No	Yes	Yes	Yes	Yes
ingress-ipv6-qos	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos-ipv6	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos	160	N/A	Yes	N/A	N/A	No	No	No
qos-ext	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos-policer	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
egress-l2	320	Yes	N/A	N/A	N/A	Yes	Yes	Yes

Table 9-43: Supported groups and the feature dependency on the groups (Continued)

Group	Key Size	Security	QoS	PBR	Mirror	Statistics		
						QMX	QAX	QUX
egress-ipv4	320	Yes	N/A	N/A	N/A	Yes	Yes	Yes
cfm-domain-name-str	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv4	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv6	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv6-mpls	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes
Ipv4-bgp-flowspec	320	N/A	N/A	N/A	N/A	No	No	No

Table 9-44: Comparison between basic and extended group qualifiers

Basic Group	Supported Qualifiers	Supported Action	Extended Group	Supported Qualifiers	Supported Action
ingress-l2	Source MAC Destination MAC Ether Type (ip, ipv6, mpls, arp, cfm, fcoe) VLAN ID Inner VLAN ID	Permit, Deny	ingress-l2-ext	Source MAC Destination MAC Ether Type VLAN ID Inner VLAN ID COS	Permit, Deny, Policer, Mirror, Assign Queue, COS Remark
ingress-ipv4	Source IP Destination IP IP Protocols L4 Ports	Permit, Deny	ingress-ipv4-ext	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID TCP flags	Permit, Deny, Mirror

Table 9-44: Comparison between basic and extended group qualifiers (Continued)

Basic Group	Supported Qualifiers	Supported Action	Extended Group	Supported Qualifiers	Supported Action
ingress-ipv6	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 Protocols L4 Ports VLAN ID DSCP	Permit, Deny, Mirror, Assign Queue,	ingress-ipv6-ext	Source IPv6 address full 128 bits Destination IPv6 address full 128 bits L4 Ports IPv6 Protocols Physical interface	Permit, Deny, Assign Queue, DSCP Remark, Policer, Mirror
qos	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP	Assign Queue, COS Remark, DSCP Remark, Policer	qos-ext	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP IP RTP L4 Ports Destination MAC Traffic type	Assign Queue, COS Remark, DSCP Remark, Policer

Table 9-45: Qualifiers for other groups

Group	Qualifiers	Actions
ingress-ipv6-ext-vlan	Source IPv6 address full 128 bits Destination IPv6 address full 128 bits L4 Ports IPv6 Protocols vlan interface subinterface	Permit, Deny, Assign Queue, DSCP Remark, Policer, Mirror
egress-l2	Source MAC Destination MAC VLAN ID Inner VLAN ID COS	Permit, Deny
egress-ipv4	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID	Permit, Deny

Table 9-45: Qualifiers for other groups (Continued)

Group	Qualifiers	Actions
qos-policer	VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP Topmost EXP IP RTP L4 Ports	Assign Queue, COS Remark, DSCP Remark, Policer, Hierarchical Policer and Storm Control
ingress-ipv4-qos	Source IP Destination IP IP Protocols L4 Ports DSCP VLAN ID Inner VLAN ID TCP flags	Policer, Assign Queue, DSCP Remark
ingress-ipv6-qos	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 Protocols L4 Ports VLAN ID DSCP	Assign Queue, DSCP Remark, Policer
qos-ipv6	IPv6 Protocols L4 Ports VLAN ID COS Inner VLAN ID Inner COS Ether Type DSCP	Assign Queue, COS Remark, DSCP Remark, Policer
ingress-arp	ARP Request/Response ARP IP address ARP MAC address VLAN ID Inner VLAN ID	Permit, Deny
cfm-domain-name-str	MA ID	
twamp-ipv4	- predefined qualifer IPV4_SIP - predefined qualifer IPV4_DIP - predefined qualifer L4_SRC_PORT - predefined qualifer L4_DST_PORT - user-defined qualifer MplsSrcIpv4_qual - user-defined qualifer MplsDstIpv4_qual - user-defined qualifer MplsUdpPorts_qual	

Table 9-45: Qualifiers for other groups (Continued)

Group	Qualifiers	Actions
twamp-ipv6	For non-MPLS group: - predefined qualifer IPV6_SIP - predefined qualifer IPV6_DIP - predefined qualifer L4_SRC_PORT - predefined qualifer L4_DST_PORT For MPLS group: - user-defined qualifer MplsSrcIpv6_qual - user-defined qualifer MplsDstIpv6_qual - user-defined qualifer MplsUdpPorts_qual	
Ipv4-bgp-flowspec	VRF ID Source IP Destination IP IP Protocols L4 Ports ICMP Type/Code TCP Flags PacketSize DSCP IP Fragmentation Note: The following traffic filter types of the components range value can be specified only with non-range value. • Type 3: IP Protocol • Type 7: ICMP type • Type 8: ICMP code • Type 10: Packet length • Type 11: DSCP (Diffserv Code Point)	

hardware-profile filter (Qumran2)

Use this command to enable or disable ingress IPv4 or IPv6, egress IPv6 filter groups, EVPN-MPLS,VxLAN filter and TWAMP IPv4 or IPv6 groups. Disabling filter groups increases the configurable filter entries.

Disabling a TCAM filter group is not allowed if the group has any entries configured in hardware. Group dependent entries must be explicitly removed before disabling the TCAM group.

Note:

- This feature is supported for IPv4 unicast and IPv4 BGP/MPLS VPN service based on RFC 8955.
- Updating the access list may take a long time in a scaled configuration because the hardware must reshuffle the filter entries when configuring a high-priority filter.
- Use the `ingress-IPv4-subif` and `ingress-IPv6-subif-ext` groups when ACL is required on the sub-interfaces only. Use `ingress-IPv4-ext` and `ingress-IPv6` groups when ACL is required on physical, sub-interface, LAG, and IRB interfaces.
- Enabling TWAMP hardware profiles requires a system reboot.
- In the ingress direction, Qumran-2C (Q2C) series platforms supports stats for 16k filter entries, and Qumran-2A (Q2A) series platforms supports 8k filter entries. For the egress direction, Qumran-2C (Q2C) series platforms supports 8k, and Qumran-2A (Q2A) series platforms supports 4k.

For better utilization of TCAM resources it is recommended to enable large groups first and then smaller groups.

Example

```
hardware-profile filter qos-policer enable          # QoS policer/storm control
hardware-profile filter ingress-ipv6 enable         # IPV6 ACL
hardware-profile filter ingress-l2-subif enable     # MAC ACL
hardware-profile filter ingress-ipv4-subif enable   # IPv4 ACL
hardware-profile filter ingress-ipv6-ext-subif enable  # IPv6 ACL
```

Command Syntax

```
hardware-profile filter (dhcp-snoop|dhcp-snoop-ipv6|egress-dst-ipv6|egress-
  ipv4|egress-ipv4-ext|egress-ipv6|egress-l2|egress-l2-ext|egress-l2-mlag|egress-
  qos-policer|egress-qos-policer-ext|egress-src-ipv6|ingress-arp|ingress-
  ipv4|ingress-ipv4-ext|ingress-ipv4-qos|ingress-ipv4-subif|  ingress-ipv6-ext-
  subif|ingress-ipv6|ingress-ipv6-ext|ingress-ipv6-ext-vlan|ingress-ipv6-
  qos|ingress-l2|ingress-l2-ext|ingress-l2-subif|ipsg|ipsg-ipv6|qos|qos-ext|qos-
  ipv6|qos-policer|evpn-mpls-cw|evpn-mpls-mh|vxlan|vxlan-mh|twamp-ipv4|twamp-
  ipv6|twamp-ipv6-mpls|vxlan|ipv4-bgp-flowspec|) (enable|disable)
```

Parameter

`dhcp-snoop`	Ingress DHCP Snooping group
`dhcp-snoop-ipv6`	Ingress IPv6 DHCP Snooping group
`ingress-arp`	Ingress ARP group for ARP ACL support
`ingress-l2`	Ingress L2 ACL filter group.
`ingress-l2-ext`	Ingress L2 ACL, QoS, mirror filter group.
`ingress-l2-subif`	Ingress L2 group for ACL on L2/L3 Subinterfaces.

ipsg	Ingress IP Source Guard group
ipsg-ipv6	Ingress IPv6 Source Guard group
ingress-ipv4	Ingress IP ACL filter group.
ingress-ipv4-ext	Ingress IP ACL, mirror, PBR filter group.
ingress-ipv4-qos	Ingress IPv4 group for ACL match QoS.
ingress-ipv4-subif	Ingress IPv4 group for ACL on L2/L3 Subinterfaces.
ingress-ipv6-ext-subif enable	IPv6 processing on ingress sub-interfaces.
ingress-ipv6	Ingress IPv6 ACL, mirror, PBR filter group
ingress-ipv6-ext	Ingress IPv6 extended group with 128-bit address support for ACL , ACL match QOS on physical interfaces.
ingress-ipv6-ext-vlan	Ingress IPv6 extended group with 128-bit address support for ACL, ACL match QOS on SVI interfaces.
ingress-ipv6-ext-subif	Ingress IPv6 extended group with 128-bit address support for ACL, ACL match QOS on Sub interfaces.
ingress-ipv6-qos	Ingress IPv6 group for ACL match QoS.
qos-ipv6	Ingress QOS IPv6 group for IPv6 QoS support with statistics.
qos	Ingress QoS filter group
qos-ext	Ingress QoS extended filter group.
qos-ipv6	Ingress QOS IPv6 group for IPv6 QoS support with statistics
qos-policer	Ingress extended QoS group for hierarchical policer support with statistics.
egress-l2	Egress L2 ACL filter group
egress-l2-mlag	Egress L2 group for ACL only on MLAG interface.
egress-l2-ext	Egress L2 extended (mac) group for ACL on subinterface.
egress-dst-ipv6	Egress Destination IPv6 group for ACL
egress-ipv4	Egress IP ACL filter group.
egress-ipv4-ext	Egress IPv4 extended group for ACL on subinterface
egress-ipv6	Egress IPv6 group for ACL
egress-qos-policer	Egress QoS policer group only for physical and LAG interface
egress-qos-policer-ext	Egress extended QOS policer group
egress-src-ipv6	Egress Source IPv6 group for ACL
twamp-ipv4	Ingress TWAMP IPv4 Forwarding group.
twamp-ipv6	Ingress TWAMP IPv6 Forwarding group.
twamp-ipv6-mpls	Ingress TWAMP IPv6 MPLS Forwarding group.
ipv4-bgp-flowspec	BGP FlowSpec filter group.
evpn-mpls-mh	Ingress EVPN MPLS Multi-Homing Forwarding Group
vxlan	Ingress VxLAN Forwarding group
vxlan-mh	Ingress VxLAN Multi-Homing Forwarding Group.
vxlan	Ingress Vxlan Forwarding group

`enable`	Enable filter group.
`disable`	Disable filter group

Default

By default, all filter groups are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and changed in OcNOS version 3.0.

Examples

```
OcNOS#configure terminal
OcNOS(config)#hardware-profile filter ingress-ipv4 enable
OcNOS(config)#hardware-profile filter ingress-ipv4 disable

OcNOS(config)#hardware-profile filter egress-ipv4 enable
OcNOS(config)#hardware-profile filter egress-ipv4 disable
```

Table 9-46: Supported groups and the feature dependency on the groups

Group	Key Size	Security	QoS	PBR	Mirror	Statistics		
						Q2U	Q2A	Q2C, J2C+
dhcp-snoop	160	Yes	No	N/A	No	Yes	Yes	Yes
Dhcp-snoop-ipv6	160	Yes	No	N/A	No	Yes	Yes	Yes
Ingress-arp	320	Yes	No	N/A	No	Yes	Yes	Yes
ingress-l2	160	Yes	No	N/A	No	Yes	Yes	Yes
ingress-l2-ext	320	Yes	No	N/A	Yes	Yes	Yes	Yes
ingress-l2-subif	160	Yes	No	N/A	No	Yes	Yes	Yes
ingress-ipv4	160	Yes	No	No	No	Yes	Yes	Yes
ingress-ipv4-ext	320	Yes	No	Yes	Yes	Yes	Yes	Yes
ingress-ipv4-qos	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
ingress-ipv4-subif	160	Yes	No	Yes	No	Yes	Yes	Yes
ingress-ipv6	320	Yes	No	Yes	Yes	Yes	Yes	Yes
Ingress-ipv6-ext	320	N/A	Yes	No	Yes	Yes	Yes	Yes
Ingress-ipv6-ext-vlan	320	N/A	Yes	No	Yes	Yes	Yes	Yes
Ingress-ipv6-ext-subif	320	N/A	Yes	No	Yes	Yes	Yes	Yes

Table 9-46: Supported groups and the feature dependency on the groups (Continued)

Group	Key Size	Security	QoS	PBR	Mirror	Statistics		
						Q2U	Q2A	Q2C, J2C+
ingress-ipv6-qos	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
Ipsg	160	Yes	No	N/A	N/A	Yes	Yes	Yes
Ipsg-ipv6	160	Yes	No	N/A	N/A	Yes	Yes	Yes
qos-ipv6	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos	160	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos-ext	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
qos-policer	320	N/A	Yes	N/A	N/A	Yes	Yes	Yes
egress-l2	320	Yes	N/A	N/A	N/A	Yes	Yes	Yes
egress-l2-ext	160	Yes	N/A	N/A	N/A	Yes	Yes	Yes
egress-l2-mlag	80	Yes	N/A	N/A	N/A	Yes	Yes	Yes
egress-dst-ipv6	160	Yes	N/A	N/A	N/A	Yes	Yes	Yes
egress-ipv4	160	Yes	N/A	N/A	N/A	Yes	Yes	Yes
egress-ipv4-ext	160	Yes	N/A	N/A	N/A	Yes	Yes	Yes
Egress-ipv6	320	Yes	N/A	N/A	N/A	Yes	Yes	Yes
Egress-qos-policer	160	No	Yes	N/A	N/A	Yes	Yes	Yes
Egress-qos-policer-ext	160	No	Yes	N/A	N/A	Yes	Yes	Yes
Egress-src-ipv6	160	Yes	No	N/A	N/A	Yes	Yes	Yes
evpn-mpls-mh	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
vxlan	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
vxlan-mh	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv4 (Having MPLS enabled SKUs)	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes
Twamp-ipv4 (MPLS disabled SKUs)	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv6	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes
twamp-ipv6-mpls	320	N/A	N/A	N/A	N/A	Yes	Yes	Yes

Table 9-46: Supported groups and the feature dependency on the groups (Continued)

Group	Key Size	Security	QoS	PBR	Mirror	Statistics		
						Q2U	Q2A	Q2C, J2C+
Vxlan	160	N/A	N/A	N/A	N/A	Yes	Yes	Yes
Ipv4-bgp-flowspec	320	N/A	N/A	N/A	N/A	No	No	No

Table 9-47: Comparison between basic and extended group qualifiers

Basic Group	Extended Qualifiers	Supported Actions	Extended Group	Supported Qualifiers	Supported Actions
dhcp-snoop	SourcePort L4 DestinationPort IPv4 Protocol Destination Mac InterfaceClass Ethertype Vlan				
dhcp-snoop-ipv6	L4 Destination port IP6NextHeader DstIp6High Ethertype				
ingress-l2	Source MAC Destination MAC Ether Type VLAN ID Inner VLAN ID	Permit, Deny	ingress-l2-ext	Source MAC Destination MAC Ether Type VLAN ID Inner VLAN ID COS Inner CoS IPv4 Protocols	Permit, Deny, Policer, Mirror, Assign Queue, COS Remark
ingress-l2-subif	Source Mac Destination Mac Ethertype	Permit, Deny			
ingress-ipv4	Source IP Destination IP IP Protocols L4 Dest Ports L4 Src Ports	Permit, Deny	ingress-ipv4-ext	Source IP Destination IP IP Protocols DSCP/ToS L4 Dest Ports L4 Src Ports VLAN ID Inner VLAN ID TCP flags Packet Length range check L4 Source/ Destination Port Range Check	Permit, Deny, Mirror

Table 9-47: Comparison between basic and extended group qualifiers

Ingress-ipv4-subif	Source IP Destination IP IPv4 Protocol Type L4 Destination Port L4 Source Port Packet Length Range Check L4 Source/Destination Port Range Check	Permit, Deny			
ingress-ipv4-qos	Source IP Destination IP IPv4 Protocols L4 Destination Port L4 Source Port L4 Source/Destination Port Range Check DSCP VLAN ID Inner VLAN ID TCP flags	Policer, Assign Queue, DSCP Remark			
ingress-ipv6	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 NextHeader L4 Destination Port L4 Source Port VLAN ID IPv6 Traffic Class IPv6 Hop Limit L4 Source/Destination Port Range Packet Length Range Check	Permit, Deny, Assign Queue, Mirror	ingress-ipv6-ext	Source ipv6 address full 128 bits Destination ipv6 address full 128 bits L4 Destination Port L4 Source Port IPv6 NextHeader	Permit, Deny, Assign Queue, DSCP Remark,
ingress-ipv6-ext-vlan	Source ipv6 address full 128 bits Destination ipv6 address full 128 bits L4 Destination Port L4 Source Port IPv6 NextHeader	Permit, Deny, Assign Queue, DSCP Remark, s			
ingress-ipv6-ext-subif	Source ipv6 address full 128 bits Destination ipv6 address full 128 bits L4 Destination Port L4 Source Port IPv6 NextHeader	Permit, Deny, Assign Queue, DSCP Remark			

Table 9-47: Comparison between basic and extended group qualifiers

ingress-ipv6-qos	Source IPv6 (n/w part) Destination IPv6 (n/w part) IPv6 NextHeader L4 Destination Port L4 Source Port L4 Source/Destination Port Range VLAN ID IPv6 Traffic Class	Assign Queue, DSCP Remark, Policer			
ipsg	Source MAC Source IP VLAN ID				
Ipsg-ipv6	Source MAC Source IP6 High VLAN ID				

Table 9-48: Qualifiers for other groups

Group	Supported Qualifiers	Supported Actions	Extended Group	Supported Qualifiers	Supported Actions
egress-l2	Source MAC Destination MAC VLAN ID Inner VLAN ID CoS Inner CoS	Permit, Deny	egress-l2-ext	Source Mac Destination Mac VLAN ID Inner VLAN ID CoS Inner CoS	Permit, Deny
egress-l2-mlag	Source Port Destination Port Layer Record Type	Deny			
egress-ipv4	Source IP Destination IP IPv4 Protocol L4 Destination Port L4 Source Port DSCP VLAN ID Inner VLAN ID	Permit, Deny	egress-ipv4-ext	Source IP Destination IP IPv4 Protocol L4 Destination Port L4 Source Port DSCP VLAN ID Inner VLAN ID	Permit, Deny

Table 9-48: Qualifiers for other groups

egress-dst-ipv6	Destination IPv6 High (N/W part) IPv6 Next Header IPv6 Traffic Class L4 Destination Port L4 Source Port	Permit, Deny			
egress-ipv6	Destination IPv6 High (N/W part) Source IPv6 High (N/W part) IPv6 Next Header IPv6 Traffic Class L4 Destination Port L4 Source Port VLAN ID	Permit, Deny			
egress-qos-policer	Destination Mac VLAN ID CoS DSCP L4 Destination Port L4 Source Port IPv4 Protocols	Policer	egress-qos-policer-ext	Destination Mac VLAN ID CoS DSCP L4 Destination Port L4 Source Port IPv4 Protocols SVI interface Subinterface	Policer
egress-src-ipv6	Source IPv6 High (N/W part) IPv6 Next Header IPv6 Traffic Class L4 Destination Port L4 Source Port	Permit, Deny			
qos	Ether Type VLAN ID CoS Inner VLAN ID Inner CoS DSCP Topmost EXP IP Flags	Assign Queue, COS Remark, DSCP Remark, Policers	qos-ext	Ether Type VLAN ID COS Inner VLAN ID Inner COS DSCP Topmost EXP IP Flags IP Protocols L4 Destination Port L4 Source Port L4 Source/ Destination Port Range	Assign Queue, COS Remark, DSCP Remark, Policer
evpn-mpls-mh	USER_DEFINED_IP MPLS LABEL				
vxlan					

Table 9-48: Qualifiers for other groups

vxlan-mh	Source IP Destination IP				
qos-policer	Destination MAC Ether Type VLAN ID COS Inner VLAN ID Inner CoS DSCP IP Protocols IP Flags Topmost EXP L4 Destination Port L4 Source Port L4 Source/ Destination Port Range Traffic type	Assign Queue, COS Remark, DSCP Remark, Policer, Hierarchical Policer and Storm Control			
qos-ipv6	Ether Type VLAN ID COS Inner VLAN ID Inner CoS IPv6 Next Header IPv6 Traffic Class L4 Destination Port L4 Source Port L4 Source/ Destination Port Range	Assign Queue, COS Remark, DSCP Remark, Policer			
ingress-arp	ARP Request/ Response ARP IP address ARP MAC address VLAN ID Inner VLAN ID	Permit, Deny			
twamp-ipv4	IPv4 Source IP IPv4 Destination IP UDP Source port UDP Destination port IPv4 Type of Service				
twamp-ipv6	UDP Source port UDP Destination port IPv6 Source IP IPv6 Destination IP				
twamp-ipv6-mpls	UDP Source port UDP Destination port IPv6 Source IP IPv6 Destination IP				

Table 9-48: Qualifiers for other groups

vxlan	Forwarding Types Ethernet Type IPv4 Y1731				
Ipv4-bgp-flowspec	VRF ID Source IP Destination IP IP Protocols L4 Ports ICMP Type/Code TCP Flags PacketSize DSCP IP Fragmentation The following traffic filter types of the components range value can be specified only with non-range value. Type 3: IP Protocol Type 7: ICMP type Type 8: ICMP code Type 10: Packet length Type 11: DSCP (Diffserv Code Point)				

Table 9-49: Total available entries for each group

Group Name	Q2U	Q2A	Q2C	Q2C+
dhcp-snoop	10240	10240	19456	19456
dhcp-snoop-ipv6	10240	10240	19456	19456
Ingress-arp	4608	4608	8704	8704
Ingress-l2	10240	10240	19456	19456
Ingress-l2-ext	4608	4608	8704	8704
Ingress-l2-subif	10240	10240	19456	19456
Ipsg	10240	10240	19456	19456
Ipsg-ipv6				
Ingress-ipv4	10240	10240	19456	19456
Ingress-ipv4-ext	4608	4608	8704	8704
Ingress-ipv4-qos	4608	4608	8704	8704
Ingress-ipv4-subif	10240	10240	19456	19456

Table 9-49: Total available entries for each group

Ingress-ipv6	4608	4608	8704	8704
Ingress-ipv6-ext	4608	4608	8704	8704
ingress-ipv6-ext-vlan	4608	4608	8704	8704
ingress-ipv6-ext-subif	4608	4608	8704	8704
Ingress-ipv6-qos	4608	4608	8704	8704
Qos-ipv6	4608	4608	8704	8704
Qos	4605/4608	4608	8704	8704
Qos-ext	4605/4608	4608	8704	8704
Qos-policer	4605/4608	4608	8704	8704
Egress-l2	4608	4608	8704	8704
Egress-l2-ext	10240	10240	19456	19456
Egress-l2-mlag	20480	20480	38912	38912
Egress-dst-ipv6	10240	10240	19456	19456
Egress-ipv4	10240	10240	19456	19456
Egress-ipv4-ext	10240	10240	19456	19456
Egress-ipv6	4608	4608	8704	8704
Egress-qos-policer	10240	10240	19456	19456
Egress-qos-policer-ext	10240	10240	19456	19456
Egress-src-ipv6	10240	10240	19456	19456
Twamp-ipv4	4608	4608	8704	8704
Twamp-ipv6	4608	4608	8704	8704
Twamp-ipv6-mpls	4608	4608	8704	8704
Vxlan	10240	10240	19456	Not supported

© 2025 IP Infusion Inc. Proprietary

hardware-profile flowcontrol

Use this command to globally enable or disable hardware-based flow control.

Syntax

```
hardware-profile flowcontrol (disable|enable)
```

Parameters

`disable`	Disable flow control globally
`enable`	Enable flow control globally

Default

By default flow control is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 3.0.

Examples

```
#configure terminal
(config)#hardware-profile flowcontrol enable
```

hardware-profile service-queue

Use this command to set the number of service-queue counts to create in hardware.

Use the no form of this command to set the service queue profile to default

Note: Reboot the switch after giving this command for the changes to take effect.

Command Syntax

```
hardware-profile service-queue (profile1| profile2)
no hardware-profile service-queue
```

Parameter

`profile1`	Supports new 4 queue-bundle per service (default)
`profile2`	Supports new 8 queue-bundle per service

Default

By default, `profile1` is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile service-queue profile2
(config)#no hardware-profile service-queue
```

hardware-profile statistics

Use this command to enable or disable filter statistics in hardware.

Note: In Q1, you must reboot the switch after giving this command for the changes to take effect. For Q2, Statistic profiles are updated dynamically.

Note: If both ACL and QOS statistics are required on the same interface, then both ingress-acl and ingress-qos profiles must be enabled and this will limit other profiles from being enabled. More details on restrictions explained below.

Note: When any two or all of MAC ACL or IP ACL or QoS service-policy are configured on the same interface or in its dependent interface, their entries will use statistics entries from ingress-acl statistics profile, and as a result the statistics is updated on only one entry based on the hardware-profile filter created later.

Note: Cfm-slm statistics is supported only on Q2 devices.

Command Syntax

```
hardware-profile statistics (ac-lif|cfm-ccm|cfm-lm |cfm-slm|ingress-acl|ingress-
  qos|egress-acl|mpls-pwe|tunnel-lif|voq-full-color|voq-fwd-drop) (enable|disable)
```

Parameter

`ac-lif`	VXLAN access ports statistics
`cfm-ccm`	Cfm ccm counter statistics
`cfm-lm`	Cfm Loss Measurements statistics
`cfm-slm`	Cfm Synthetic Loss Measurements statistics
`tunnel-lif`	VXLAN tunnels statistics
`ingress-acl`	Ingress ACL, QoS, and PBR statistics
`ingress-qos`	Ingress QoS statistics (explicit)
`egress-acl`	Egress ACL statistics
`mpls-pwe`	Pseudowire logical interfaces statistics
`voq-full-color`	Statistics for all VOQ counters
`voq-fwd-drop`	Statistics for forward drop VOQ counters
`enable`	Enable statistics
`disable`	Disable statistics

Default

In Q1, By default, only ingress-acl statistics profile is enabled. Other statistics profiles are disabled.

In Q2, By default, `voq-full-color, cfm-ccm` statistics profile is enabled. Other statistics profiles are disabled. The `voq-full-color` cannot be disabled.

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 1.3 and this command is applicable for Qumran. The `voq-full-color` and `voq-fwd-drop,cfm-slm,cfm-lm and cfm-ccm` options are applicable for Qumran2.

Examples

```
#configure terminal
(config)#hardware-profile statistics tunnel-lif enable
```

Table 9-50 provides details of scalable numbers of each statistics profiles and the applications that use the statistics profiles. For example, the `ingress-acl` profile is used by ACL, QoS, and PBR applications and all of them share the statistics entries from this profile. So, consuming 8k statistics entries for ACL application means that QOS and PBR applications do not get any statistics.

There are limitations on the number of statistics profiles that can be enabled at a time. This limitation is based on the stages that each profile uses. Table 9-50 shows the four stages: ingress, ingress queuing, egress1, and egress2; and only two statistics profiles per stage can be configured.

For example, if both the `ingress-acl` and `mpls-acl` profiles are configured, then no more profiles that use the “ingress stage” can be enabled because only two profiles are allowed per stage. To use another “ingress-based” profile, you must first disable at least one of the profiles that are currently using the ingress stage.

Table 9-50: Qumran 1 Statistics profile capacity (maximum numbers in best case scenario)

Statistics profile	Stage	QMX	QAX	QUX	Application
ingress-acl	Ingress	~8k	~6k	~1.5K	Ingress ACL, QoS, PBR
egress-acl	Egress1	~8k	~2k	~2k	Egress ACL
ingress-qos	Ingress	~8k	~6k	~1.5K	QoS
voq-full-color	Ingress queuing	~13k	~6k	~6K	QoS (queue statictics)
voq-fwd-drop	Ingress queuing	~32k	~16k	~16K	QoS (queue statictics)
tunnel-lif	Ingress Egress2	~16k	N/A	N/A	VXLAN and MPLS (LSP/tunnels)
mpls-pwe	Ingress Egress2	~16k	~8k	~1K	MPLS (pseudowire)
cfm-ccm	Ingress	~3k	~800	~800	CFM (ccm)
cfm-lm	Ingress Egress2	~6k	~1.5k	NA	CFM (loss measurement)
ac-lif	Ingress Egress2	~32k	N/A	N/A	VXLAN and MPLS (access-port)

Table 9-51: Qumran2 Statistics profile capacity (maximum numbers in best case scenario)

Statistics profile	Stage	Q2A/Q2U	Q2C/J2C	Application
ingress-acl	Ingress	~8k	~16k	Ingress ACL, QoS, PBR
egress-acl	Egress1	~4k	~8k	Egress ACL
ingress-qos	Ingress	~4k	~8k	Ingress QoS policer

Table 9-51: Qumran2 Statistics profile capacity (maximum numbers in best case scenario) (Continued)

Statistics profile	Stage	Q2A/Q2U	Q2C/J2C	Application
Egress-qos	Egress	~4k	~8k	Egress qos policer
voq-full-color	Ingress queuing	~6552	~19k	QoS (queue statictics)
voq-fwd-drop	Ingress queuing	~16k	~48k	QoS (queue statictics)
slm	Ingress	~2k	~2k	OAM SLM
cfm-ccm	Ingress	~2k	~2k	CFM_CCM_RX_TX & CCM-BANK-0 RX/TX
cfm-lm	Ingress Egress	~2k ~2k	~2k ~2k	CFM (loss measurement)
ac-lif	Ingress Egress	~8k ~8k	~32k ~32k	VXLAN and MPLS (access-port)

hardware-profile bgp-flowspec-mode

Use this command to set BGP flowspec mode that specifies the installation rules to the hardware.

Note: No support for Install-partial option in Q2.

Setting hardware profile to bgp-flowspec-mode requires, disabling and enabling the ipv4-bgp-flowspec to take effect.

Chose a appropriate option based on usage. Use `install-all` option for normal case.

Syntax

```
hardware-profile bgp-flowspec-mode (install-all|install-partial|no-prioritizing)
```

Parameters

`install-all` FLOWSPEC rules are prioritized. The already installed all rules are reinstalled when a new rule is added. (default)

`install-partial`

FLOWSPEC rules are prioritized. Do not reinstall all previously installed rules when a new rule is added to avoid unnecessary reinstallation.

`no-prioritizing`

FLOWSPEC rules are not prioritized. Install only rules requested to add but not reinstall any other rules when a new rule is added.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 6.3.5.

Example

```
(config)#hardware-profile filter ipv4-bgp-flowspec disable
(config)#commit
(config)#hardware-profile bgp-flowspec-mode no-prioritizing
(config)#commit
(config)#hardware-profile filter ipv4-bgp-flowspec enable
(config)#commit
```

ip redirects

Use this global command to trap ICMP redirect packets to the CPU and on interface to enable ICMP redirects in kernel.

Use the no form of this command to disable the ICMP redirect message on an interface.

Note: This command is applicable for both ipv4 and ipv6 interfaces.

Syntax

```
ip redirects
no ip redirects
```

Parameters

None

Default

None

Command Mode

Configure and Interface mode

Applicability

This command was introduced in OcNOS version 3.0.

Example

```
#configure terminal
(config)#ip redirects


(config)#no ip redirects


#configure terminal
(config)#interface xe1/1
(config-if)#ip redirects


#configure terminal
(config)#interface xe1/1
(config-if)#no ip redirects
```

load-balance enable

Use this command to enable load-balancing configurations in hardware.

Use the no option to reset the load balancing to default settings.

Note: When the command `load-balance enable` is issued, the default load-balance settings are unset. User then has to configure the new load-balancing parameters.

Command Syntax

This form unsets load balancing globally:

```
load-balance enable
```

This form resets load balancing globally to default settings:

```
no load-balance enable
```

By default, load balancing is enabled for ECMP and LAG.

This form sets hashing based on IPv4 fields:

```
load-balance (ipv4 {src-ipv4 | dest-ipv4 | srcl4-port | destl4-port | protocol-id})
no load-balance (ipv4 {src-ipv4 | dest-ipv4 | srcl4-port | destl4-port | protocol-
  id})
```

This form sets hashing based on IPv6 fields:

```
load-balance (ipv6 {src-ipv6 | dest-ipv6 | srcl4-port | destl4-port | protocol-id |
  next-hdr})
no load-balance (ipv6 {src-ipv6 | dest-ipv6 | srcl4-port | destl4-port | protocol-
  id | next-hdr})
```

This form sets hashing based on L2 fields:

```
load-balance (l2 {dest-mac|src-mac|ether-type|vlan})
no load-balance (l2 {dest-mac|src-mac|ether-type|vlan})
```

This form sets hashing on an MPLS fields:

```
load-balance (mpls {labels})
no load-balance (mpls {labels})
```

Following additional parameters are supported on Dune DNX boards:

```
load-balance inner-ipv4 ({non-symmetric| protocol-id| src-dest-ipv4})
no load-balance inner-ipv4 ({non-symmetric| protocol-id| src-dest-ipv4})

load-balance inner-l2 ({ether-type| non-symmetric| src-dest-mac| vlan})
no load-balance inner-l2 ({ether-type| non-symmetric| src-dest-mac| vlan})
```

```
load-balance src-dest-l4port (non-symmetric)
no load-balance src-dest-l4port
```

Note: The configured load balancing parameters are global and will be applicable to all LAG & ECMP created in the hardware.

Parameters

`ipv4`	Load balance IPv4 packets
`src-ipv4`	Source IPv4 based load balancing
`dest-ipv4`	Destination IPv4 based load balancing
`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`protocol-id`	Protocol ID based load balancing
`ipv6`	Load balance IPv6 packets
`src-ipv6`	Source IPV6 based load balancing
`dest-ipv6`	Destination IPv6 based load balancing
`srcl4-port`	Source L4 port based load balancing
`destl4-port`	Destination L4 port based load balancing
`l2`	Load balance L2 packets
`src-dest-mac`	Source Destination based load balancing
`non-symmetric`	Non symmetrical based load balancing
`ether-type`	Ether-type based load balancing
`Vlan`	VLAN-based load balancing
`mpls`	Load balance MPLS packets
`labels`	label stack based load balancing
`inner-ipv4`	Load balancing on IPv4 packet
`inner-l2`	Load balancing on L2 packet
`src-dest-l4port`	Source Destination l4port based load balancing
`non-symmetric`	Non symmetric based load balancing
`protocol-id`	Protocol Id based load balancing
`src-dest-ipv4`	Source Destination IPV4 based load balancing
`ether-type`	Ether-type based load balancing
`src-dest-mac`	Source Destination based load balancing
`next-hdr`	Next Header Field for IPV6

`src-dest-ipv6` Source Destination IPV6 based load balancing

Command Mode

Configure mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
(config)#load-balance enable
(config)#load-balance ipv4 src-ipv4
```

show forwarding profile limit

Use this command to display the forwarding profile table sizes.

Note: 1k is 1024 entries.

Command Syntax

```
show forwarding profile limit
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version SP 1.0.

Examples

```
#show forwarding profile limit

-------------------------------------------------------------------------------
          L3 (Ipv4/Ipv6) KAPS Forwarding Profile
-------------------------------------------------------------------------------
Active (*)   Configured (*)  Profile-type     IPv4-db-size     IPv6-db-size
                             profile-one      NA               NA
   *           *             profile-two      -                200k

-------------------------------------------------------------------------------
          L3 (Ipv4/Ipv6) ELK TCAM Forwarding Profile
-------------------------------------------------------------------------------
Active (*)   Configured (*)  Profile-type     IPv4-db-size     IPv6-db-size
   *           *             profile-one      ~1024k           -
                             profile-two      -                ~1024k
                             profile-three    ~2048k           -

NOTE: for external-tcam profile-three, URPF should be disabled &
       number of vrf's limited to 255
-------------------------------------------------------------------------------
          L2 forwarding table
-------------------------------------------------------------------------------
            Max Entries: 768k

 NOTE: 1k is 1024 entries

#
```

show hardware-profile filters

Use this command to show details of TCAM filter groups which are enabled. By default, all filter groups are disabled.

Command Syntax

```
show hardware-profile filters
```

Parameter

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 3.0.

Examples

```
#show hardware-profile filters

Note: Shared count is the calculated number from available resources.
      Dedicated count provides allocated resource to the group.
      If group shares the dedicated resource with other groups, then dedicated
      count of group will reduce with every resource usage by other groups.

+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10495     0     1         10486   2048        8448
```

Table 9-52 explains the output fields.

Table 9-52: show hardware-profile filters

Field	Description
Ingress	Ingress filtering is a method used to prevent suspicious traffic from entering a network.
TCAMS	Number of ternary content addressable memory (TCAM) entries a particular firewall filter.
Free Entries	Number of TCAM filter entries available for use by the filter group.
Used Entries	Number of TCAM filter entries used by the filter group.
Total Entries	Number of TCAM total filter entries to the filter group.

Table 9-52: show hardware-profile filters (Continued)

Field	Description
Dedicated Entries	Number of TCAM filter entries dedicated to the filter group.
Shared Entries	Number of TCAM filter entries shared to the filter groups.

Operational details of TCAM profiles

TCAM group statistics comprises of three parts:

- **Total Entries** – Total configurable entries on the TCAM group. Total has two parts. One is dedicated and other is shared. Dedicated count is the guaranteed entry count for the group. Shared count a logical count calculated for the group from shared pool available at the time of show command execution
- **Used Entries** – Count of entries that have been configured on the TCAM group. Used entries are shown are shown in percentage format as well as an indication of how much TCAM space is used up. However, percentage calculation includes shared pool and subject to change drastically when shared pool is taken up by different group.
- **Free Entries** – Count of possible remaining entries on the TCAM group. Free entries count is not the guaranteed count as the count includes the shared pool count into account.

When a TCAM group is enabled in the device, no hardware resource (bank) is associated with the group. Thus, dedicated count will be initially zero. Total count will be same as shared count which is calculated based on the group width. Group width is determined by width consumed by the qualifiers or width consumed by the actions.

Example of show output when qos-ext group is enabled on QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10496     0     0         10496   0           10496
```

When an entry is created on the group for the first time, either a single bank or a bank pair is allocated to the group. A group consuming single bank or a bank pair is decided by group width. Groups like qos, ingress-l2, and ingress-ipv4 consume single bank and groups like qos-ext, qos-policer, ingress-l2-ext, ingress-ipv4-ext, ingress-ipv4-qos, ingress-ipv6, ingress-ipv6-qos, egress-l2, and egress-ipv4 consume a bank pair.

An example of output when a single entry is created in hardware for qos-ext group on QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      10495     0     1         10496   2048        8448
```

In the above example, dedicated entry count has increased to 2048 as a bank pair is allocated for the group. Unallocated banks capacity is calculated for qos-ext group and counted under shared entries as 8448.

An example of output when 2048 entries are created in hardware for qos-ext group and ingress-l2 and ingress-ipv4-ext groups is enabled with no entries created on those groups for QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      8448     20     2048      10496   2048        8448
 INGRESS L2           16896     0     0         16896   0           16896
 INGRESS IPV4-EXT     8448      0     0         8448    0           8448
```

In the above example, note that the number of entries between ingress-l2 and ingress-ipv4-ext groups vary as ingress-l2 group is a 160-bit wide group consuming only one bank at a time. On the other hand, ingress-ipv4-ext group is 320 bit wide group consuming a group pair at a time. With a bank pair already being consumed by qos-ext group, ingress-ipv4-ext group gets possible total entries of 8448 in comparison to 10496 by qos-ext group.

When all the created entry count goes beyond the entries of dedicated bank pair (or a bank), group will be allocated with another bank pair (or a bank) and subsequently shared pool count will reduce across all other groups.

An example of output when 2049 entries are created in hardware for qos-ext group with ingress-l2 and ingress-ipv4-ext groups enabled with no entries created on those groups for QMX device is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      8447      20    2049      10496   4096        6400
 INGRESS L2           12800     0     0         12800   0           12800
 INGRESS IPV4-EXT     6400      0     0         6400    0           6400
```

When a bank is consumed by ingress-l2 group, effect on qos-ext group will still be the count of a bank pair with one bank not usable for qos-ext group even if it is available. The bank can be used by groups which consume single bank.

An example of output when an entry is created in hardware for ingress-l2 group with qos-ext and ingress-ipv4-ext groups in the state as mentioned in above example is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      6399      24    2049      8448    4096        4352
 INGRESS L2           12799     0     1         12800   2048        10752
 INGRESS IPV4-EXT     4352      0     0         4352    0           4352
```

In the above example scenario, it can be noted that the used entry percentage for qos-ext group jumped from 20 to 24 as a result of drastic reduction in total entry count due to bank movement from shared pool to dedicated bank.

Hardware doesn’t optimize the utilization of banks when entries are removed from one of the banks resulting in entries used shown up less than capacity of one bank but still multiple banks would be dedicated to a group.

An extended example of above scenario with 10 entries removed from qos-ext group is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 INGRESS-QOS-EXT      6409      24    2039      8448    4096        4352
 INGRESS L2           12799     0     1         12800   2048        10752
 INGRESS IPV4-EXT     4352      0     0         4352    0           4352
```

It can be noted that the used entry count has come down to 2039 which is less than the capacity of bank pair i.e. 2048. However, since entries are used up across two set of bank pairs, both bank pairs will still be dedicated. If there is a need to recover bank pair from dedicated pool, all the entries should be deleted and re-created in hardware.

TCAM groups are further divided into sub-categories which can share the dedicated banks between the groups. TCAM groups such as ingress-l2, ingress-l2-ext, ingress-ipv4, ingress-ipv4-ext, ingress-ipv4-qos, qos, qos-ext, qos-policer are considered under default sub-category and don't serve IPv6 traffic. TCAM groups such as ingress-ipv6, ingress-ipv6-qos, and qos-ipv6 are meant for IPv6 traffic and are considered under IPv6 sub-category.

Only four 320-bit wide groups that belong to same sub-category can be created. For default sub-category, number is limited to three as system group will be created by default.

When three default sub-category groups are created along with one group from IPv6 sub-category, one of the default sub-category group will share the bank pair with IPv6 group. This will result in dedicated count to be shown lesser by the number that the other shared group is consuming. With every single resource consumed by one group will reduce the same number from other shared group.

An example of above scenario is shown below:

```
#show hardware-profile filters
...
+--------------------+---------+---------------+----------------------------+
|                    | Free    |     Used      |       Total Entries        |
| TCAMS              | Entries |---------------|----------------------------|
|                    |         |  %  | Entries | Total | Dedicated | shared |
+--------------------+---------+-----+---------+-------+-----------+--------+
 QOS-EXT              6399      0     1         6400    2048        4352
 INGRESS IPV4-ACL-EXT 6398      0     2         6400    2048        4352
 INGRESS IPV4-QOS     6382      0     1         6383    2031        4352
 INGRESS IPV6-ACL     6382      0     17        6399    2047        4352
```

Note that ingress-ipv4-qos group has shared the resource with ingress-ipv6 group. TCAM group ingress-ipv4-qos has consumed 1 entry and ingress-ipv6 group has consumed 17 entries. Hence, dedicated count for ingress-ipv4-qos group is shown as 2031 (2048 - 17) and dedicated count for ingress-ipv6 group is shown as 2047 (2048 - 1).

Capacity of TCAM profiles

Entries created on other TCAM groups affect the capacity of a particular TCAM group. This dependency is explained in the section Operational details of TCAM profiles.

In this section maximum configurable entries per group when no entries created on other groups are listed below.

Table 9-53: Maximum configurable entries

TCAM Groups	QMX	QAX	QUX
ingress-l2	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)	3584
ingress-l2-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 +256 x 1)	1792
ingress-ipv4	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)	3584
ingress-ipv4-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
ingress-ipv4-qos	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
ingress-ipv6	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
ingress-ipv6-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
ingress-ipv6-ext-vlan	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
ingress-ipv6-qos	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
qos-ipv6	12288 (2048 x 6)	5120 (1024 x 5)	1792
qos	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)	3584
qos-ext	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
qos-policer	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
egress-l2	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
egress-ipv4	10496 (2048 x 5 + 256 x 1)	4352 (1024 x 4 + 256 x 1)	1792
cfm-domain-name-str	20992 (2048 x 10 + 256 x 2)	9728 (1024 x 9 + 256 x 2)	3584

Combination of TCAM profiles

Device supports configuration of only one egress group in the system. Hence out of the egress groups cfm-domain-name-str, egress-l2 and egress-ipv4, only one egress group can be enabled.

In other words, solution with CFM features enabled, cannot have egress security filters.

Configuration of ingress groups are subject to the sub-category to which a group belongs. Sub-category of each group is shown below:

Table 9-54: Sub-category of groups

Category	Groups in the category
default (ingress)	ingress-l2 ingress-l2-ext ingress-ipv4 ingress-ipv4-ext ingress-ipv4-qos qos qos-ext qos-policer
Ipv6 (ingress)	ingress-ipv6, ingress-ipv6-qos, qos-ipv6, ingress-ipv6-ext, ingress-ipv6-ext-vlan
default (egress)	egress-l2, egress-ipv4
cfm (egress)	cfm-domain-name-str

Note: Per sub-category, not more than three groups can be created if the group key size is 320 bits wide.

show nsm forwarding-timer

Use this command to display the information of Graceful Restart capable MPLS clients to NSM that are currently shutdown. Use the option LDP or RSVP to see the particular module information.

Command Syntax

```
show nsm (ldp| rsvp) forwarding-timer
```

Parameters

`ldp`	Use this parameter to display the protocol LDP information.
`rsvp`	Use this parameter to display the protocol RSVP information.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before OcNOS version 5.0.

Example

```
#sh nsm rsvp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
    RSVP        ACTIVE           100           2021/08/18 04:49:23
#sh nsm ldp forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
     LDP        ACTIVE           111           2021/08/18 04:50:37
#sh nsm forwarding-timer
Protocol-Name  GR-State  Time Remaining (sec)   Disconnected-time
     LDP        ACTIVE           110           2021/08/18 04:50:37
    RSVP        ACTIVE            96           2021/08/18 04:49:23
```

show queue remapping

Use this command to display the traffic class-to-hardware-queue mapping in hardware.

Command Syntax

```
show queue remapping
```

Parameters

N/A

Default

N/A

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 1.3.

This command is only available on Qumran platforms.

Examples

When service-queue `profile1` is set:

```
#show queue remapping

Port queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           2           |
|      3     |           3           |
|      4     |           4           |
|      5     |           5           |
|      6     |           6           |
|      7     |           7           |
+------------+-----------------------+

Service queue remapping:
+------------+-----------------------+
|  Queue/tc  |     hardware-queue    |
+------------+-----------------------+
|      0     |           0           |
|      1     |           1           |
|      2     |           1           |
|      3     |           1           |
```

```
|      4      |           2             |
|      5      |           2             |
|      6      |           3             |
|      7      |           3             |
+-------------+-------------------------+
```

When service-queue `profile2` is set:

```
#show queue remapping

Port queue remapping:
+-------------+-------------------------+
|  Queue/tc   |     hardware-queue      |
+-------------+-------------------------+
|      0      |           0             |
|      1      |           1             |
|      2      |           2             |
|      3      |           3             |
|      4      |           4             |
|      5      |           5             |
|      6      |           6             |
|      7      |           7             |
+-------------+-------------------------+

Service queue remapping:
+-------------+-------------------------+
|  Queue/tc   |     hardware-queue      |
+-------------+-------------------------+
|      0      |           0             |
|      1      |           1             |
|      2      |           2             |
|      3      |           3             |
|      4      |           4             |
|      5      |           5             |
|      6      |           6             |
|      7      |           7             |
+-------------+-------------------------+
```

CHAPTER 10 Source Interface Commands

This chapter is a reference for source interface commands. The source Interface feature routes management traffic to a dedicated interface using `iptables` NAT rules.

The source interface feature is supported for the protocols shown in Table 10-55.

Table 10-55: Source interface protocols and port numbers

Protocol	Default port number
Tacacs+	49
Radius	1812 and 1813
Snmp	161 and 162
Ntp	123
Syslog	514

Note: Because management applications are allowed only on the default and management VRF, the commands in this chapter are supported on the "management" and "default" VRFs only.

This chapter contains these commands:

- ip source-interface
- ipv6 source-interface
- show ip source-interface detail
- show ipv6 source-interface detail
- show running-config ip source-interface
- show running-config ipv6 source-interface

ip source-interface

Use this command to configure the IPv4 source interface for a protocol.

Use the `no` form of this command to remove the IPv4 source interface for a protocol.

Note: It is possible that the router may establish an outgoing TCP connection using an interface that does not have a valid or routable IP address. In such case, the user must specify the address of a different interface to use as the source IP address for the outgoing connection. For this scenario, the command ip source-interface or ipv6 source-interfaceis used.

Command Syntax

```
ip source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port (0|<1025-
  65535>)|) (vrf VRF_NAME|)
no ip source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius)
```

Parameters

`IFNAME`	Interface name (lo or physical interface)
`tacacs+`	Terminal Access Controller Access Control System
`ntp`	Network Time Protocol
`snmp`	Simple Network Management Protocol
`syslog`	syslog
`radius`	Remote Authentication Dial-In User Service
`<1025-65535>`	Port number. Default value is as per the protocol.
`VRF_NAME`	Virtual Routing and Forwarding name

Default

The default port 0 is assigned to the protocol.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ip source-interface xe1 ntp
(config)#ip source-interface xe2 radius port 1025
(config)#ip source-interface xe3 syslog port 65535 vrf management
```

ipv6 source-interface

Use this command to configure the IPv6 source interface for a protocol.

Use the `no` form of this command to remove the IPv6 source interface for a protocol.

Command Syntax

```
ipv6 source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius) (port (0|<1025-
  65535>)|) (vrf VRF_NAME|)
no ipv6 source-interface IFNAME (tacacs+|ntp|snmp|syslog|radius)
```

Parameters

`IFNAME`	Interface name (lo or physical interface)
`tacacs+`	Terminal Access Controller Access Control System protocol
`ntp`	Network Time Protocol
`snmp`	Simple Network Management Protocol
`syslog`	syslog
`radius`	Remote Authentication Dial-In User Service
`<1025-65535>`	Port number. Default value is as per the protocol.
`VRF_NAME`	Virtual Routing and Forwarding name

Default

The default port 0 is assigned to the protocol.

Command Mode

Configure mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#configure terminal
(config)#ipv6 source-interface xe1 ntp
(config)#ipv6 source-interface xe2 radius port 1025
(config)#ipv6 source-interface xe3 syslog port 65535 vrf management
```

© 2025 IP Infusion Inc. Proprietary

show ip source-interface detail

Use this command to display the IPv4 source interface status in detail.

Command Syntax

```
show ip source-interface detail
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#show ip source-interface detail
Source-Interface Detailed Information
=====================================
  Protocol : tacacs+
  Interface : lo
  Address : 1.1.1.1
  Status : Active
  VRF Name : Default

  Protocol : radius
  Interface : lo
  Address : 1.1.1.1
  Status : Active
  VRF Name : Default
```

Table 10-56 explains the output fields.

Table 10-56: Output fields

Field	Description
Protocol	tacacs+, ntp, snmp, syslog, or radius
Interface	Interface name (lo or physical interface)
Address	IP address
Status	Whether active or inactive
VRF Name	Virtual Routing and Forwarding name

show ipv6 source-interface detail

Use this command to display the IPv6 source interface status in detail.

Command Syntax

```
show ipv6 source-interface detail
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#show ipv6 source-interface detail
Source-Interface Detailed Information
=====================================
  Protocol : tacacs+
  Interface : lo
  Address : ::1
  Status : Active
  VRF Name : Default

  Protocol : radius
  Interface : lo
  Address : ::1
  Status : Active
  VRF Name : Default
```

Table 10-56 explains the output fields.

show running-config ip source-interface

Use this command to display the IPv4 source interface running configuration.

Command Syntax

```
show running-config ip source-interface
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0

Example

```
#show running-config ip source-interface
ip source-interface lo tacacs+ port 1025
ip source-interface lo radius
ip source-interface lo.management ntp vrf management
ip source-interface lo.management syslog port 1026 vrf management
ip source-interface ge3 snmp
```

show running-config ipv6 source-interface

Use this command to display the IPv6 source interface running configuration.

Command Syntax

```
show running-config ipv6 source-interface
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in OcNOS version 4.0.

Example

```
#show running-config ipv6 source-interface
ipv6 source-interface lo tacacs+ port 1025
ipv6 source-interface lo radius
ipv6 source-interface lo.management ntp vrf management
ipv6 source-interface lo.management syslog port 1026 vrf management
ipv6 source-interface ge3 snmp
```

CHAPTER 11 Smart SFP Commands

This chapter is a reference for the Smart SFP commands:

- ddm raise
- show interface transceiver details
- show interface transceiver detail remote
- show interface transceiver protocol
- show interface transceiver protocol remote
- show interface transceiver protocol stats
- show interface transceiver remote
- show interface transceiver threshold violations remote
- xcvr <IFNAME> tx-disable <1-256> remote
- xcvr <IFNAME> reset remote
- xcvr loopback

ddm raise

Use this command to raise a false alarm on the remote smart SFP.

Use this command to clear the false alarm on the remote smart SFP.

Command Syntax

```
ddm raise false alarm IFNAME
  (((temperature|voltage|voltage2|current|rxpower|txpower|frequency-
  error|wavelength-error|snr|resisi|leveltrans|teccurrent|prefecber|
  uncorrectedber|lasertemp) VALUE)| tec-fault) (remote|)
no ddm raise false alarm IFNAME
  (temperature|voltage|voltage2|current|rxpower|txpower|frequency-
  error|wavelength-error|tec-fault|snr|resisi|leveltrans|teccurrent|prefecber|
uncorrectedber|lasertemp) (remote|)
```

Parameters

None

Default

By default, the debug command is not configured.

Command Mode

Configuration mode

Applicability

This command was introduced before OcNOS version 6.2.0.

Example

The following command displays detailed information ddm raise.

```
OcNOS(config)#conf t
OcNOS(config)#ddm raise false alarm xe1 temperature +95.00 remote
OcNOS(config)#ddm raise false alarm xe1 voltage +3.50 remote
```

show interface controller details

Use this command to display the EEPROM details.

Command Syntax

```
show interface (IFNAME|) controllers (remote)
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
remote	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0

Example

The following command displays detailed information of smart SFP.

```
OcNOS#show interface controllers remote
Codes: SMF - Single Mode Fiber, MMF - Multi Mode Fiber, FC - Fiber Channel
       OM1 - 62.5 Micron MMF [200MHzkm @ 850nm & 500MHzkm @ 1310nm]
       OM2 - 50 Micron MMF [500MHzkm @ 850nm & [500MHzkm @ 1310nm]
       OM3 - 50 Micron MMF [2000MHz*km @ 850nm], OUI - Vendor ID
       OM4 - 50 Micron MMF [4700MHz*km @ 850nm], BR - Bit Rate, CC - Check
Code
       AOC - Active Optical Cable, ACC -  Active Copper Cable, PC - Power
Class
       CDR - Clock Data Recovery, CLEI - Common Language Equipment
Identification
       LR - Long Reach, SR - Short Reach, IR - Intermediate Reach
       CCA - Copper Cable Attenuation

############################################################
Port Number                    : 24
Name                           : WTD
OUI                            : 0x0 0x1c 0xad
Part No                        : RTXM330-8921
Serial_Number                  : ME223702430001
Identifier                     : SFP/SFP+/SFP28
Ext. Identifier                : GBIC/SFP Is Defined By Two-Wire Interface ID
Only
Connector Type                 : LC (Lucent Connector)
Ethernet/Ext-Eth Compliance    : 100GBASE-LR4 or 25GBASE-LR
SONET Compliance               :
```

```
Infiniband Compliance          :
ESCON Compliance               :
FCLink Length                  :
FC Technology                  :
FC Transmission Media          :
FC Speed                       :
SFP+ Cable Technology          :
Length SMF                     : 10 (Kilometers)
Length SMF                     : 100 (X 100 Meters)
Length OM1                     : 0 (X 10 Meters)
Length OM2                     : 0 (X 10 Meters)
Length OM3                     : 0 (X 10 Meters)
Length OM4                     : 0 (X 10 Meters)
Revision Level                 : V01
Wavelength                     : 1269nm
Manufacturing Date             : 220809   (yymmddvv, v=vendor specific)
Encoding Algorithm             : 64B/66B
CC                             : 0x25
CC Ext.                        : 0x68
Nominal BR                     : 255 (X 100 MBd)
Max BR                         : 103
Min BR                         : 0
Options Implemented            : Power Level 3
                                 Paging
                                 Internal Re-Timer Or CDR
                                 Cooled Laser Trasnmitter
                                 Power Level 2
                                 RATE_SELECT
                                 TX_DISABLE
                                 TX_FAULT
                                 Rx Loss Of Signal (LOS)
DDM Support                    : Yes
```

show interface transceiver details

Use this command to display details of transceivers and threshold violations.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|(protocol
  (stats|))|)(remote|)
```

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.
`detail`	Transceiver information such as voltage, temperature, power, and current.
`threshold violation`	Transceiver threshold violations.
`Codes`	* Not Qualified By IP Infusion, ** Not Supported By Module.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver details.

```
OcNOS#sh int transceiver detail
Codes:  * Not Qualified By IP Infusion,  ** Not Supported By Module,  -- No
Power,  - Not Applicable


Intf       DDM        Temp       AlertMax   CritMax    CritMin    AlertMin
                      (Celsius)  (Celsius)  (Celsius)  (Celsius)  (Celsius)
-------------------------------------------------------------------------


ce0        Active*    +22.52     +85.00     +80.00     -5.00      -10.00
ce2        Active     +20.32     +75.00     +70.00     +0.00      -5.00
xe4        Active*    +23.62     +95.00     +85.00     -40.00     -50.00
xe5        Active*    +19.79     +100.00    +95.00     -35.00     -40.00
xe16       Active*    +25.84     +95.00     +85.00     -10.00     -50.00
xe26       Active     +19.01     +95.00     +90.00     -20.00     -25.00



Intf       DDM        Volt       AlertMax   CritMax    CritMin    AlertMin
```

```
                        (Volts)     (Volts)     (Volts)     (Volts)     (Volts)
-------------------------------------------------------------------------------
ce0         Active*     +3.314      +3.600      +3.500      +3.100      +2.900
ce2         Active      +3.260      +3.630      +3.465      +3.135      +2.970
xe4         Active*     +3.260      +3.600      +3.500      +3.100      +3.000
xe5         Active*     +3.253      +3.600      +3.500      +2.900      +2.800
xe16        Active*     +3.284      +3.630      +3.500      +3.030      +2.930
xe26        Active      +3.289      +3.900      +3.700      +2.900      +2.700



Intf        DDM         Lane        Curr        AlertMax    CritMax     CritMin
AlertMin
                                    (mA)        (mA)        (mA)        (mA)
(mA)
-------------------------------------------------------------------------------
-------
ce0         Active*     1           +6.114      +15.000     +12.000     +2.000
+0.000
                        2           +6.120      +15.000     +12.000     +2.000
+0.000
                        3           +6.110      +15.000     +12.000     +2.000
+0.000
                        4           +6.116      +15.000     +12.000     +2.000
+0.000
ce2         Active      1           +7.464      +13.000     +11.000     +5.000
+3.000
                        2           +7.540      +13.000     +11.000     +5.000
+3.000
                        3           +7.444      +13.000     +11.000     +5.000
+3.000
                        4           +7.474      +13.000     +11.000     +5.000
+3.000
xe4         Active*     -           +6.100      +110.000    +100.000    +1.000
+1.000
xe5         Active*     -           +7.552      +15.000     +13.000     +2.000
+1.000
xe16        Active*     -           +5.800      +15.000     +12.000     +3.000
+2.000
xe26        Active      -           +7.050      +17.000     +14.000     +2.000
+1.000



Intf        DDM         Lane        RxPwr       AlertMax    CritMax     CritMin
AlertMin
                                    (dBm)       (dBm)       (dBm)       (dBm)
(dBm)
-------------------------------------------------------------------------------
-------
ce0         Active*     1           -0.185      +4.400      +3.400      -13.298    -
14.306
                        2           +0.342      +4.400      +3.400      -13.298    -
14.306
                        3           +0.396      +4.400      +3.400      -13.298    -
14.306
                        4           -2.927      +4.400      +3.400      -13.298    -
14.306
ce2         Active      1           +1.302      +3.400      +2.400      -11.002    -
14.001
```

```
                        2          +1.486     +3.400     +2.400     -11.002    -
14.001
                        3          +1.581     +3.400     +2.400     -11.002    -
14.001
                        4          +1.594     +3.400     +2.400     -11.002    -
14.001
xe4         Active*     -          -1.890     +2.500     +0.500     -14.401    -
16.402
xe5         Active*     -          -40.000    +3.000     +0.000     -13.002    -
16.003
xe16        Active*     -            --       +2.000     +1.000     -14.401    -
16.402
xe26        Active      -          -5.933     +1.000     -1.002     -18.013    -
20.000


Intf        DDM         Lane       TxPwr      AlertMax   CritMax    CritMin
AlertMin
                                   (dBm)      (dBm)      (dBm)      (dBm)
(dBm)
-------------------------------------------------------------------------------
-------
ce0         Active*     1          -0.085     +4.400     +3.400     -9.201     -
10.205
                        2          -0.161     +4.400     +3.400     -9.201     -
10.205
                        3          +0.217     +4.400     +3.400     -9.201     -
10.205
                        4          +0.204     +4.400     +3.400     -9.201     -
10.205
ce2         Active      1          +0.297     +5.000     +3.000     -8.000     -
10.000
                        2          -0.078     +5.000     +3.000     -8.000     -
10.000
                        3          +0.131     +5.000     +3.000     -8.000     -
10.000
                        4          +0.323     +5.000     +3.000     -8.000     -
10.000
xe4         Active*     -          -1.316     +2.500     +0.500     -8.199     -
10.200
xe5         Active*     -          -2.299     +1.000     +0.000     -7.001     -
8.000
xe16        Active*     -          -1.000     +2.500     +2.000     -8.199     -
10.200
xe26        Active      -          -4.441     -2.000     -2.000     -11.024    -
11.739

Intf        DDM         Lane       Freq-Err   AlertMax   CritMax    CritMin
AlertMin
                                   (GHz)      (GHz)      (GHz)      (GHz)
(GHz)
-------------------------------------------------------------------------------
-------

Intf        DDM         Lane       Wave-Err   AlertMax   CritMax    CritMin
AlertMin
                                   (nm)       (nm)       (nm)       (nm)
(nm)
-------------------------------------------------------------------------------
-------

Intf        DDM         Lane       Tx         Rx-LOS     Tx-LOS
```

```
-------------------------------------------------------------------------------
ce0         Active*     1           On          Off         Off
                        2           On          Off         Off
                        3           On          Off         Off
                        4           On          Off         Off
ce2         Active      1           On          Off         Off
                        2           On          Off         Off
                        3           On          Off         Off
                        4           On          Off         Off
xe4         Active*     -           On          Off         -
xe5         Active*     -           On          On          -
xe9         Inactive*   -           On          On          -
xe11        Inactive*   -           On          On          -
xe13        Inactive*   -           On          On          -
xe14        Inactive*   -           On          On          -
xe16        Active*     -           On          On          -
xe26        Active      -           On          Off
```

Table 11-57 explains the output fields.

Table 11-57: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliamperes used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.
Codes *	Not Qualified By IP Infusion, ** Not Supported By Module

show interface transceiver detail remote

Use this command to display all the threshold values for volt, temperature, and power for the remote transceiver.

Command Syntax

```
show interface (IFNAME|) transceiver detail remote
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
remote	Interface name
detail	Remote transceivers information

Default

None.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver detail remote.

```
OcNOS#show interface transceiver detail remote

      Intf       DDM        Temp       AlertMax   CritMax    CritMin
AlertMin
                              (Celsius)  (Celsius)  (Celsius)  (Celsius)
(Celsius)
      ------------------------------------------------------------------
---

      Intf       DDM        Volt       AlertMax   CritMax    CritMin
AlertMin
                              (Volts)    (Volts)    (Volts)    (Volts)
(Volts)
-------------------------------------------------------------------------
```

show interface transceiver protocol

Use this command to display the OAM protocol status and module status of the local module.

Command Syntax

```
show interface (IFNAME|) transceiver protocol
```

Parameters

IFNAME	Interface name. If not specified, this command displays details for all connected transceivers.
protocol	OAM protocol status, and module status of local module.

Default

None.

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver protocol.

```
OcNOS#show interface transceiver protocol

      ############################################################
      Port Number                    : 2
      OAM status                     : On
      Local status                   : Link failure
```

show interface transceiver protocol remote

Use this command to display the OAM protocol status and module status of the remote module.

Command Syntax

```
show interface (IFNAME|) transceiver protocol remote
```

Parameters

IFNAME	Interface name. If not specified, this command displays details of all connected transceivers.
protocol	OAM protocol status, and module status of the remote module.
remote	Remote transceiver information

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver protocol remote.

```
OcNOS#show interface transceiver protocol remote

      ############################################################
      Port Number                    : 2
      Remote status                  : Remote TCVR Ready
```

show interface transceiver protocol stats

Use this command to display the protocol frame statistics.

Command Syntax

```
show interface (IFNAME|) transceiver protocol stats
```

Parameters

IFNAME	Interface name. If not specified, this command displays details for all connected transceivers.
protocol	OAM protocol status, and module status of local module.
stats	Protocol frame statistics

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver protocol stats

```
OcNOS#show interface transceiver protocol stats

      ############################################################
      Port Number                    : 2
      OAM frames Sent                : 1583
      OAM frames received corretly   : 1
      OAM frames received with error: 2
```

show interface transceiver remote

Use this command to display the remote transceiver information.

Command Syntax

```
show interface (IFNAME|) transceiver remote
```

Parameters

IFNAME	Interface name. If not specified, this command displays details for all connected transceivers.
remote	Remote transceiver information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver remote

```
OcNOS#show interface transceiver remote

      Intf       DDM        Temp       Voltage    Lane       Tx         Rx-Los
Tx-
       Los     Current    TxPower    RxPower    Freq-Err   Wave-Err
                            (Celsius)  (volt)
                (mA)       (dBm)      (dBm)      (GHZ)      (nm)
       ------------------------------------------------------------------------
--------
       ----------------------------------------------------------------
```

show interface transceiver threshold violations remote

Use this command to display the details of remote transceivers and threshold violations.

Command Syntax

```
show interface (IFNAME|) transceiver (detail|threshold violation|) remote
```

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.
`detail`	Transceiver information, such as voltage, temperature, power, and current.
`threshold violation`	Transceiver threshold violations.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of interface transceiver threshold violations remote.

```
OOcNOS#show interface transceiver threshold violations remote
       Intf       Lane       Timestamp            Type of alarm
       ----       ----       ---------            -------------
```

xcvr <IFNAME> tx-disable <1-256> remote

Use this command to laser off the remote transceiver for <1-256> seconds and to turn the laser ON.

Command Syntax

```
xcvr <IFNAME> tx-disable <1-256> remote
```

Parameters

IFNAME	Interface name.
remote	Remote transceiver.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of xcvr <IFNAME> tx-disable <1-256> remote.

```
OcNOS#xcvr xe2 tx-disable 2 remote
```

xcvr <IFNAME> reset remote

Use this command to reset the remote transceiver.

Command Syntax

```
xcvr <IFNAME> reset remote
```

Parameters

IFNAME	Interface name.
remote	Remote transceiver.
reset	Reset remote transceiver

Default

None

Command Mode

Exec mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of xcvr <IFNAME> reset remote.

```
OcNOS#xcvr xe2 reset remote
```

xcvr loopback

Use this command to loopback Tx and Rx Input loop back for remote.

Use this command to loopback Tx and Rx Output loop back for remote.

Command Syntax

```
xcvr loopback (in|out) remote
no xcvr loopback (in|out) remote
```

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in OcNOS version 6.2.0.

Example

The following command displays detailed information of xcvr loopback.

```
OcNOS(config)#int xe2
OcNOS(config-if)#xcvr loopback in remote
OcNOS(config-if)#commit
OcNOS(config-if)#end
OcNOS#conf t
OcNOS(config)#int xe2
OcNOS(config-if)#xcvr loopback out remote
OcNOS(config-if)#commit
OcNOS(config-if)#end
```

CHAPTER 12 Commit Rollback

Overview

The Commit Rollback capability in Common Management Layer Commands (CMLSH) is designed to execute a rollback operation for a set of configurations that were previously committed, with each commit operation identified by a unique commit ID. The Commit ID is numeric value and is generated by the CMLSH Commit, Confirmed Commit and Commit Rollback.

This Commit Rollback application is used for rolling back the commits that are performed after the specified commit ID whether they were executed through either Commit or Confirmed Commit operations.

Here, you find the description for Commit and Confirmed Commit:

- **Commit operation**: Involves committing the candidate configuration to the running configuration.
- **Confirmed Commit operation**: Provides more options to the commit operation with timeout parameter, user could provide timeout for the commit (default is 300 seconds).

During this timeout interval, users can either confirm the commit or cancel it, and if no confirmation or cancellation is provided before the timer expires, commit will be automatically rolled back after timeout.

Commit Rollback Characteristics

The Confirmed-Commit operation temporarily applies the configuration for the duration specified in seconds. If the user does not confirm the configuration within this timeframe, an automatic rollback will be initiated once the timer expires. For committing the configurations with timings, see commit.

Once the configurations are confirmed, users can use the commit rollback operation to revert the configuration, whether it is for a commit operation or a confirmed commit operation.

Benefits

With the integration of CMLSH Commit Rollback with Standard or Confirmed Commit, users can initiate a rollback operation for any specific commit, utilizing the associated commit ID to revert the configurations to their previous state. In this way, reverting to an earlier state, functional configuration is possible in case the new configuration is compromised or if the configuration makes the device unstable.

Prerequisites

Before configuring this operation, enable cml commit-history to ensure the commit records are stored in the commit history list. By default, `cml commit-history` is enabled. For enabling or disabling it, see cml commit-history (enable | disable).

show commit list

Use this command to display a record of commit operations stored in the commit history list.

Note: For commit records to be stored in the commit history list, enable cml commit-history (enable | disable). Otherwise, commit operations will not be stored.

Command Syntax

```
show commit list
```

Parameter

None

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for `show commit list`:

```
#show commit list
S.No.         ID           User    Client         TimeStamp              Commit Status                       Description
~~~~~  ~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542224876712    ocnos    cmlsh    20-05-2023 00:23:44             Confirmed                          NA
```

commit-rollback

Use this command to revert configurations to a previously committed stable state. This action will remove configurations made after the provided commit ID (Word).

Note: To use commit-rollback, cml commit-history must be enabled.

Command Syntax

```
commit-rollback to WORD (description LINE|)
```

Parameter

`Word` Commit ID associated with recorded commit operations stored within the commit-history list.

`description LINE` [Optional] Short description about commit-rollback, maximum 65 characters.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example output for `commit-rollback WORD`:

```
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                       Description
~~~~~  ~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542445002144   ocnos    cmlsh    20-05-2023 00:27:25             Confirmed                          NA
```

Example of a Commit Rollback to the Commit List ID 1684542445002144:

```
#commit-rollback to 1684542445002144 description commit-rollback Test
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684542445002144   ocnos    cmlsh    20-05-2023 00:27:25            Confirmed                           NA
  2    1684542402123428   ocnos    cmlsh    20-05-2023 00:28:45    Rollback to 20-05-2023 00:27:25        commit-rollback Test
```

Example of an automatic Commit Rollback

```
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
#show run router ospf
!
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#router ospf 5
(config-router)#router ospf 6
(config-router)#commit confirmed timeout 20 description This is to test auto rollback of config
(config-router)#end
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
  1    1698242643599569    root    cmlsh    25-10-2023 14:04:03           Remaining Time: 17            This is to test auto
rollback of config

#show run router ospf
!
router ospf 5
!
router ospf 6
!
#
Warning!!! Confirmed-commit timed out for commitid: 1698242643599569
#show commit list

S.No.         ID           User    Client         TimeStamp              Commit Status                      Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~   ~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~
  1    1698242643599569    root    cmlsh    25-10-2023 14:04:03           Timed-out (Reverted)         This is to test auto
rollback of config

#show run router ospf
!
#
```

clear cml commit-history (WORD|)

Use this command to delete any specific entry mentioned by commit ID or to delete entire list entries.

Note: To use the commit-rollback operation, the `cml commit-history` operation must be enabled, and note that commit-rollback cannot be used for deleted entries.

Command Syntax

```
clear cml commit-history (WORD|)
```

Parameter

`Word`	commit ID of the recorded commit operations into commit-history list

Default

When no parameter is provided, the commit history is deleted by default. If you specify the 'Word' parameter, it will delete the specific commit record.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for clear commit using Commit History ID:

```
#show commit list

S.No.          ID           User    Client         TimeStamp               Commit Status                        Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684486018411866   ocnos    cmlsh    19-05-2023 08:46:58             Confirmed                             NA
  2    1684486037040268   ocnos    cmlsh    19-05-2023 08:47:17             Confirmed

#clear cml commit-history 1684486018411866
#show commit list

S.No.          ID           User    Client         TimeStamp               Commit Status                        Description
~~~~~  ~~~~~~~~~~~~~~~~~   ~~~~~   ~~~~~~   ~~~~~~~~~~~~~~~~~~~     ~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~
  1    1684486037040268   ocnos    cmlsh    19-05-2023 08:47:17             Confirmed                             NA
```

cml commit-history (enable | disable)

Use this command to enable or disable confirmed commit operation (commit-history operation). To verify the state of the operation, use the command `show cml commit-history state`.

Note:

- By default, cml commit-history operation is enabled.
- After disabling the cml commit-history operation, confirmed commit CLIs cannot be used, rendering the commit confirmed, confirm-commit, and cancel-commit operations unavailable.

Command Syntax

```
cml commit-history (enable | disable)
```

Parameter

`Enable`	Enables commit confirmed and commit rollback operations
`Disable`	Disables commit confirmed and commit rollback operations

Default

By default, commit confirmed and commit rollback operations are enabled.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for enabling Commit History:

```
#cml commit-history enable
Warning!!! commit-history feature is enabled, confirmed commit and commit-
rollback features are available for use.
```

Example for disabling Commit History:

```
#cml commit-history disable
Warning!!! commit-history feature is disabled, confirmed commit and commit-
rollback features can not be used.
```

cml commit-id rollover (enable | disable)

Use this command to enable or disable commit entry rollover when the maximum count of 50 commit entries is reached. When enabled, older commit entries will be automatically deleted from the commit history list to record new entries.

To verify the state of the operation, use command `show cml commit-id rollover state`.

Note:

- By default, cml commit-id rollover operation is enabled.
- The cml commit-history operation must be enabled to use this operation.
- The commit-rollback operation can not be used for deleted entry.
- When this operation is disabled and the number of commit entries reaches the maximum count, the addition of commit records to the commit history list will be stopped.

Command Syntax

```
cml commit-id rollover (enable | disable)
```

Parameter

`Enable`	Enables commit ID rollover
`Disable`	Disables commit ID rollover

Default

By default, commit ID rollover is enabled.

Command Mode

Exec mode

Applicability

This command is introduced in OcNOS 6.4.1.

Example

Example for verifying commit ID rollover state:

```
#show cml commit-id rollover state
cml commit-id rollover feature is enabled
```

Index

A
aaa accounting default 109
aaa accounting details 110
aaa authentication attempts login 109
aaa authentication login 109
aaa authentication login console 111
aaa authentication login default 111
aaa authentication login default fallback error 113
aaa authorization config-commands default 114
aaa group server 114
aaa local authentication attempts max-fail 115
abort transaction 1359
Access Lists 426
arp A.B.C.D MAC 1292
Authentication 426
authentication 1222
B
banner 1276
begin modifier 37
BGP community value
    command syntax 35
braces
    command syntax 34
C
Chassis Management Module Commands 746
clear crypto sa map 1222
clear ip prefix-list 1437
clear ipv6 neighbors 1438
clear ntp statistics 461
clear ssh hosts 189
clear tfo counter 825
Client 426
clock timezone 1279
cml force-unlock config-datastore 1361
cml lock config-datastore 1362
cml logging 1363
cml netconf translation 1364
cml unlock config-datastore 1365
cmlsh multiple-config-session 1367
cmlsh transaction 1370
cmlsh transaction limit 1371
command abbreviations 33
command completion 33
command line
    errors 33

help 32
keyboard operations 36
command modes 40
configure 40
exec 40
interface 40
privileged exec 40
router 40
command negation 34
command syntax
? 35
. 35
() 34
{} 34
| 34
A.B.C.D/M 35
AA:NN 35
BGP community value 35
braces 34
conventions 34
curly brackets 34
HH:MM:SS 35
IFNAME 35
interface name 35
IPv4 address 35
IPv6 address 35
LINE 35
lowercase 34
MAC address 35
monospaced font 34
numeric range 35
parantheses 34
parentheses 34
period 35
question mark 35
square brackets 35
time 35
uppercase 34
variable placeholders 35
vertical bars 34
WORD 35
X:X::X:X 35
X:X::X:X/M 35
XX:XX:XX:XX:XX:XX 35
commit 1372
common commands
banner 1276

clear ip prefix-list 1437
configure terminal 1280
copy running-config startup-config 1286
disable 1289, 1318
enable 1291
enable password 1292
end 1293
exit 1295
ip prefix-list 1458
ip remote-address 1461
ip unnumbered 1462
ipv6 prefix-list 1466
ipv6 unnumbered 1468
log syslog 594
reload 1313, 1314
service advanced-vty 1314
service password-encryption 1315
service terminal-length 1316
show access-list 1318
show cli 1318
show ip prefix-list 1528
show startup-config 1334
show version 1342
write terminal 1352
Common NSM Layer 2 commands
flowcontrol off 1449
show flowcontrol interface 1481
configuration 815
configure mode 40
configure terminal 1280
configuring sFlow 613
Control Port Group 815, 826, 828
copy 1414
copy ftp running-config (interactive) 1417
copy ftp startup-config 1412, 1413
copy ftp startup-config (interactive) 1418
copy http startup-config 1417
copy http startup-config (interactive) 1422
copy running-config 1406
copy running-config (interactive) 1407
copy running-config start-config 1286
copy scp (startup-config|running-config) 1414
copy scp startup-config 1414
copy scp startup-config (interactive) 1419
copy sftp (startup-config|running-config) 1415
copy sftp startup-config 1415
copy sftp startup-config (interactive) 1420

copy startup-config 1408
copy startup-config (interactive) 1409
copy system file 1410
copy system file (interactive) 1411
copy tftp startup-config 1416
copy tftp startup-config (interactive) 1421
crypto ipsec transform-set 1222
crypto isakmp policy 1224
crypto map (Configure Mode) 1224
curly brackets
    command syntax 34
D
ddm monitor 797
debug cml 1377
debug cmm 749
debug ddm 800, 803
debug dns client 401
debug ntp 463
debug radius 139
debug sflow 689
debug snmp-server 537
debug ssh server 191
debug tacacs+ 127
debug telnet server 178
debug user-mgmt 250
DHCP 266
disable 1289, 1318
do 1290
domain-name, ip 404
E
enable 1291
enable password 1292
end 1293
exec command mode 40
exit 1295
F
Fail Over Group 815
feature dhcp 323
feature ntp 463
feature sflow 690
feature ssh 192
feature tacacs+ 128
feature telnet 179
fec 1448
flowcontrol off 1449
fog tfc 827
fog type 828

H
hardware-profile portmode 1452
hardware-profile portmode bundle 1452
I
if-arbiter 1453
IFNAME 35
interface 1454
interface mode 40
ip address 1455
ip address dhcp 324, 1456
ip dhcp client request 325
ip dhcp relay 338, 340
ip dhcp relay address 341
ip dhcp relay information option 343
ip domain-list 402
ip domain-lookup 403
ip domain-name 404
ip forwarding 1457
ip host 405
ip name-server 406
ip prefix-list 1458
ip proxy-arp 1460
ip remote-address 1461
ip unnumbered 1462
ip vrf 1463
ip vrf forwarding 1463
IPv4 address
    command syntax 35
IPv6 address
    command syntax 35
ipv6 address 1464
ipv6 dhcp relay 346, 348
ipv6 dhcp relay address 349
ipv6 dhcp relay subscriber-id 352
ipv6 forwarding 1465
ipv6 prefix-list 1466
ipv6 unnumbered 1468
L
LINE 35
link-type 829
locator led 752
log syslog 594
Logging Console Configuration 573
logging level 596
logging logfile 598
logging source-interface 603
logging timestamp 603

logout 1303
M
MAC address
command syntax 35
Maxpoll and Minpoll Configuration 428
Monitor Port Group 815, 826, 827, 828
Monitor Port Groups 827
multicast 1480
Multicast Commands
multicast 1480
show ip rpf 1505
N
NSM Commands
arp A.B.C.D MAC 1292
clear ipv6 neighbors 1438
if-arbiter 1453
interface 1454
ip address 1455
ip address dhcp 1456
ip forwarding 1457
ip proxy-arp 1460
ipv6 address 1464
ipv6 forwarding 1465
multicast 1480
show debugging nsm 1326
show ip forwarding 1507
show ip interface brief 1508
show ipv6 forwarding 1523
show ipv6 interface brief 1524
show ipv6 route 1526
show nsm client 1329
show router-id 1600
ntp access-group 466
ntp authenticate 466
NTP Authentication 429
ntp authentication-key 467
NTP Configuration 427
ntp enable 468
ntp logging 470
ntp master 473
ntp peer 473
ntp server 476
ntp trusted-key 479
P
parantheses
command syntax 34
parentheses

command syntax 34
Peer 426
period
command syntax 35
ping 1305
port breakout configuration 1112, 1231, 1239, 1253, 1262
port bundle enable 1480
prefix-list 1458
privileged exec mode 40
Q
question mark
command syntax 35
R
RADIUS Server Accounting 64
RADIUS Server Authentication 56
radius-server deadtime 140
radius-server directed-request 140
radius-server host 140
radius-server host acct-port 142
radius-server host auth-port 143
radius-server host key 146
radius-server key 146
radius-server retransmit 147
radius-server timeout 147
reload 1313, 1314
reset log file 1559
router mode 40
S
Server 426
server 118
service 1314
service advanced-vty 1314
service password-encryption 1315
service terminal-length 1316
set security-association lifetime 1226
set session-key 1226
set transform-set 1227
sFlow 690
sflow collector 691, 692
show aaa accounting 119
show aaa authentication 119
show aaa authentication login 120
show access-list 1318
show cli 1318
show cmlsh multiple-config-session status 1390
show commands 37
exclude modifier 38

include modifier 38
redirect modifier 39
show crypto ipsec transform-set 1229
show debug radius 148
show debug ssh server 193
show debug tacacs+ 129
show debug telnet server 180
show debugging nsm 1326
show errdisable details 1600
show flowcontrol interface 1481
show hosts 407
show ip dhcp relay 353
show ip dhcp relay address interface 354
show ip forwarding 1507
show ip interface brief 1508
show ip prefix-list 1528
show ip vrf 1522
show ipv6 dhcp relay 358
show ipv6 dhcp relay address 359
show ipv6 forwarding 1523
show ipv6 interface brief 1524
show ipv6 route 1526
show logging 604
show logging last 606
show logging logfile 607
show logging logfile last-index 608
show logging logfile start-seqn end-seqn 609
show logging logfile start-time end-time 610
show max-transaction limit 1395
show nsm client 1329
show ntp authentication-keys 480
show ntp authentication-status 481
show ntp client 482
show ntp logging-status 482
show ntp peers 485
show ntp peer-status 483
show ntp statistics 486
show ntp status 488
show ntp trusted-keys 488
show priority-flow-control details 803
show process 1330
show radius-server 149
show role name 252
show router-id 1600
show running-config 1331
show running-config aaa 124
show running-config dhcp 360

show running-config dns 409
show running-config interface 1531
show running-config interface ip 1533
show running-config interface ipv6 1534
show running-config ipv6 access-list 1536
show running-config ntp 489
show running-config prefix-list 1537
show running-config radius 151
show running-config snmp 538
show running-config ssh server 194
show running-config switch 1332
show running-config syslog 611
show running-config tacacs+ 130
show running-config telnet server 181
show sflow 697
show sflow interface 699
show snmp 539
show snmp community 540
show snmp engine-id 542
show snmp group 543
show snmp host 544
show snmp user 545
show snmp view 546
show ssh server 197
show startup-config 1334
show system restore failures 1399
show system-information 774
show tacacs-server 131
show telnet server 182
show tfo 830
show transaction current 1400
show transaction last-aborted 1401
show transceivers details 811
show user-account 252
show username 198
show users 1340
show version 1342
show vlog all 1559
show vlog clients 1561
show vlog terminals 1562
show vlog virtual-routers 1563
Simple Network Management Protocol 526
snmp-server community 549
snmp-server contact 551
snmp-server enable snmp 554
snmp-server enable traps 555
snmp-server group 560

snmp-server host 560
snmp-server location 562
snmp-server tcp-session 565
snmp-server user 567
snmp-server view 569
Software Monitoring and Reporting-406371cb-b162-43e8-b29e-15e4927833e8 662
square brackets
    command syntax 35
SSH Client session 161
ssh key 204
ssh login-attempts 206
ssh server port 215
syslog-504b94b3-047a-47cc-8e89-9cd6ed649951 588
T
tacacs-server deadtime 133
tacacs-server directed-request 133
tacacs-server host 133
tacacs-server key 135
Telnet 177, 1047
telnet server port 185
time
    command syntax 35
traceroute 1349
trigger failover 832
Trigger Failover Commands 824
U
username 253
username keypair 218
username sshkey 217
V
vertical bars
    command syntax 34
VLOG commands 1558
    reset log file 1559
    show vlog all 1559
    show vlog clients 1561
    show vlog terminals 1562
    show vlog virtual-routers 1563
VPN Commands
    ip vrf 1463
    ip vrf forwarding 1463
    show ip vrf 1522
W
WORD 35
write terminal 1352