



OcNOS[®]
Open Compute
Network Operating System
for Data Center
Version 6.4.2

Release Notes

07 March 2024

© 2024 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.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
<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

Introduction	5
Overview	5
OcNOS Software	5
About this Release	5
IP Maestro Support	6
IP Infusion Product Release Version	6
Release 6.4.2	7
Enhanced Security and Performance	7
Multi Home VxLAN IRB with OSPF and ISIS	7
Support for RADIUS Authorization	7
Improved Management	7
Enhanced Streaming Telemetry Platform States	7
Release 6.4.1	8
Hardware Platforms	8
Edgecore AS9716-32D	8
UfiSpace S6301-56ST	9
UfiSpace S8901-54XC	9
Enhanced Security and Performance	10
NetConf Port Access Control and TCP Port Cosure	10
Hide the Remote AS using neighbor local-as CLI	11
Support IGMP Snooping for Provider Bridge	11
TCP MSS for BGP neighbors	11
TCP MSS Configuration for LDP sessions	11
Increase the Limit of BGP peers in a Peer-Group	12
Port Breakout (400G) for Qumran2 Series Platforms	12
Single Home VxLAN IRB with OSPF and ISIS	12
Password Strength Enhancements	12
RADIUS Server Authentication Failure and Fallback	12
Modified Extended ACL Deny Rule Behavior in VTY	13
Improved Network Resilience	13
RSVP Detour Over Ring Topology	13
Commit Rollback	13
Improved Management	14
Streaming Telemetry	14
Support VLAN Range in SPAN	14
Route Monitor	14
Enhancements for OpenConfig Translation	14
NetConf “remove” Operation	15
DHCP Server Group	15
Custom Syslog	15
Enhanced VE-ID Range	15
VRRP over MLAG with Custom VRF	15
Enhanced Graceful Restart	16

Enhanced MAC Mobility	16
SFTP and SCP Enhancements	16
Remove "tech-support" file	16
Port Breakout (100G) for AS5835-54T/AS5835-54X/S8901-54XC (Maverick2) Platform .	17
Improved Routing	17
Static Route Tracking using Object Tracking (IP SLA)	17
BGP VPNv4 Route Display Command	17
BGP Additional Path	17
RSVP-TE Commands	18
Inbound Route Filter for EVPN	18
Enhanced EVPN Route Show Command	18
UDLD Support on Layer 3 Interface	19

Introduction

Overview

IP Infusion's Open Compute Network Operation System Data Center (OcNOS-DC) is used to build both Layer-3 and Layer-2 Data Center fabric as it provides a rich set of control plane features, providing robust quality, ensuring lower costs and, at the same time, providing vendors with a best-of-breed selection for hardware platforms. This release provides support for advanced capabilities such as enhancements to EVPN-VXLAN.

A key concept that will enable next-generation Data Center networks is the separation of the networking software from the switching or routing hardware. One of the biggest advantages of disaggregation is CAPEX reduction, followed by OPEX savings and deployment flexibility.

OcNOS provides a unique value proposition in building modern Data Centers. It provides robust quality with over 600 Original Equipment Manufacturers (OEMs) and end users, with custom solutions for deployments spanning across access, core, transport and data center networking. It is a feature rich solution with extensive legacy and new protocol coverage.

OcNOS also drastically reduces operational costs as it can be used to address multiple solutions such as Data Center, Optical Transport, Cell Site Router, Provider Aggregation, and Passive Optical Networks.

OcNOS Software

OcNOS (Open Compute Network Operating System) is a network operating system designed to run on white-box network hardware, following the principles of disaggregated networking. OcNOS provides a software-based solution for network switches and routers, offering a flexible and open approach to networking.

Key Features of OcNOS:

- Disaggregated Networking
- Robust Protocol Support
- Network Virtualization
- Programmability and Automation
- High Availability and Resilience
- Scalability and Performance

OcNOS works with applications in diverse network environments, including data centers, service provider networks, enterprise networks, and cloud deployments. It provides an open, flexible environment and extensive protocol support for software-defined networking (SDN) and disaggregated networks.

About this Release

Release 6.4.2 offers new software enhancement features. This section provides a high-level introduction to these compelling additions:

The following software enhancements further enhance the data center product deployments:

- Use streaming telemetry with support for real-time data and performance metrics gathered from a OcNOS data center switch using the gNMI protocol.
- Multi Home VxLAN IRB with OSPF and ISIS enhances the flexibility, active-active redundancy mode, and compatibility of network configurations by expanding the functionality of IRB interfaces.

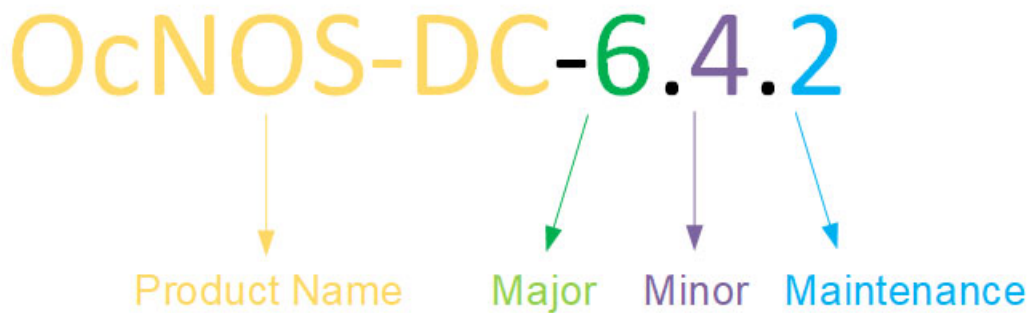
- The RADIUS server assign the role to the authenticated users based on the privilege level specified in the RADIUS server.

IP Maestro Support

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

IP Infusion Product Release Version

IP Infusion moved to a three-digit release version number from a two-digit release version number. An integer indicates major, Minor, and Maintenance release versions. Build numbers are for internal tracking and verification of the software build process and are visible to customers as part of the software version number.



Product Name: IP Infusion Product Family

Major Version: New customer-facing functionality that represents a significant change to the code base; in other words, a significant marketing change or direction in the product.

Minor Version: Enhancements/extensions to existing features, external needs, or internal requirements might be motivated by improvements to satisfy new sales regions or marketing initiatives.

Maintenance Version: It is a collection of product bugs/hotfixes and is usually scheduled every 30 or 60 days, based on the number of hotfixes.

Release 6.4.2

Enhanced Security and Performance

Multi Home VxLAN IRB with OSPF and ISIS

Multi Home VxLAN IRB with OSPF and ISIS enhances the flexibility, active-active redundancy mode, and compatibility of network configurations by expanding the functionality of IRB interfaces to include OSPF and ISIS support. Consequently, it leads to an overall improvement in network performance and connectivity within the network infrastructure.

For more information, refer to the Multi Home VxLAN-EVPN IRB with OSPF or ISIS section in the *VxLAN Configuration Guide*, Release 6.4.2.

Support for RADIUS Authorization

The current implementation of Remote Authentication Dial-In User Service (RADIUS) authentication assigns network-admin role to any user irrespective of the privilege-level. This behavior is modified in the current release. The RADIUS server is enhanced with an authorization service to assign the role to the authenticated users based on the privilege level specified in the RADIUS server.

For more information, refer to RADIUS Authorization Configuration section in the *System Management Guide*, Release 6.4.2.

Improved Management

Enhanced Streaming Telemetry Platform States

Streaming Telemetry in OcnOS introduces new platform states that provide an understanding of the operational status and attributes of various components, including memory, board Field Replaceable Unit (FRU), and temperature. The inclusion of these platform states enhances visibility into the health and performance of the networking hardware, enabling network administrators to access information and improve their ability for enhanced management and troubleshooting.

For more information, refer to the Streaming Telemetry section in the OcnOS Key Feature document, Release 6.4.2.

Release 6.4.1

Hardware Platforms

Release 6.4.1 introduces three new platforms: Edgecore AS9716-32D, UfiSpace S6301-56ST, and UfiSpace S8901-54XC. This section provides more details about each platform.

Edgecore AS9716-32D

The Edgecore AS9716-32D provides support for the following capabilities and comes equipped with configurable ports

Following are the ports supported on the AS9716-32D:

- Contains 32 x QSFP-DD switch ports, each supporting 1 x 400 GbE or 1 x 100 GbE, Or, using port breakout cables, it can support 4 x 100 GbE or 4 x 25 GbE.
- Incorporates Broadcom Tomahawk 3 switch series silicon.
- Provides a 1 RU form factor.
- Supports hot or cold aisles with front-to-back and back-to-front airflow SKUs.
- Provides front access to all ports and rear access to PSUs and fans.
- Ships with hot-swappable, load-sharing, and redundant 1300W PSUs.
- Contains 5+1 redundant, and hot-swappable fan modules.
- Comes pre-loaded with Open Network Install Environment (ONIE) for automated loading of compatible Open Source and Commercial NOS offerings.



AS9716-32D Back and Front Panel

The following table lists the chipset and port layout supported by this platform:

AS9716-32D Compatibility

CHIPSET	HARDWARE REVISION	PORT LAYOUT	SKU
Tomahawk 3 BCM56980_B0	Label Revision : R01C CPLD 1 Version : 2 CPLD 2 Version : 3 CPLD 3 Version : 2 Fan CPLD Version : 242	32 x QSFP-DD switch ports, each supporting 1 x 400 GbE or 1 x 100 GbE, or using breakout cables 4 x 100 GbE or 4 x 25 GbE	OCNOS-DC-IPBASE-12800 OCNOS-DC-PLUS-12800

For more information, refer to **AS9716-32D Port Mapping** chapter in the *OcNOS Edgecore Installation Guide*, Release 6.4.1.

UfiSpace S6301-56ST

The following ports are supported on the UfiSpace S6301-56ST:

- 8 x 1G or 10G SFP+ ports
- 48 x 100M/1G RJ45 port
- 1 x 100/1000M RJ45 management port
- 1 x RJ45 serial console port
- 1 x USB 2.0 Type-A port



S6301-56ST Front and Back Views

The following table lists the chipset and port layout supported by this platform.

S6301-56ST Compatibility

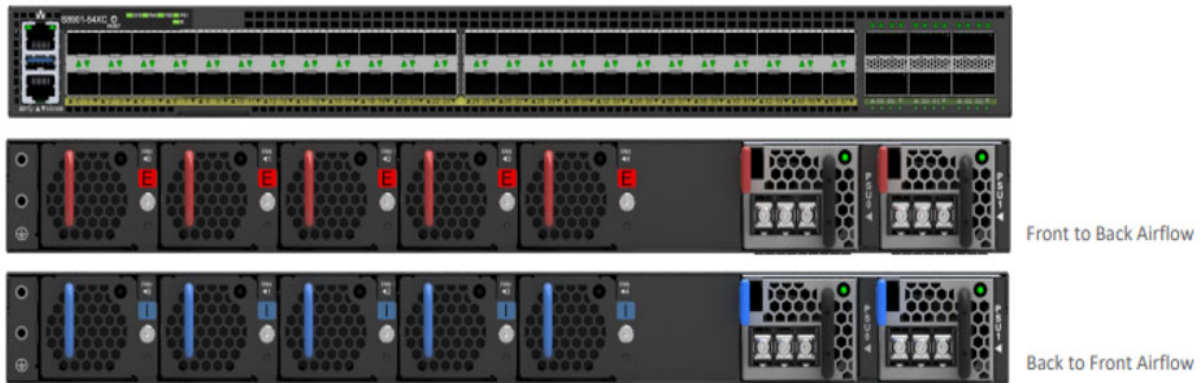
CHIPSET	HARDWARE REVISION	PORT LAYOUT	SKU
Trident3 - X2 BCM56277_A1	Label Revision : N/A Board CPLD Version : 0.3	8 x 1G/10G SFP+ ports 48 x 100M/1G RJ45 port	OCNOS-DC-MGMT-120 OCNOS-DC-IPBASE-120

For more information, refer to **S6301-56ST Port Mapping** chapter in the *OcNOS UfiSpace Installation Guide*, Release 6.4.1.

UfiSpace S8901-54XC

Following are the ports supported on the UfiSpace S8901-54XC:

- 6 x 40/100G QSFP28 ports
- 48 x 1/10/25G SFP28 ports
- 1 x 100/1000M RJ45 management port
- 1 x RJ45 serial console port
- 1 x USB 3.0 Type-A port
- AC and -48V DC PSU options



UfiSpace S8901-54XC Front and Back Views

The following table lists the chipset and port layout supported by this platform:

S8901-54XC Compatibility

CHIPSET	HARDWARE REVISION	PORT LAYOUT	SKU
Trident3 - X5 BCM56770_A0	Label Revision : N/A	6 x 40/100G QSFP28 ports	OCNOS-DC-IPBASE-2000 OCNOS-DC-MPLS-2000
	Diag Version : 0.1.6		
	CPLD 1 Version : 0.2	48 x 1/10/25G SFP28 ports	
	CPLD 2 Version : 0.1		

For more information, refer to **S8901-54XC Port Mapping** chapter in the *OcNOS UfiSpace Installation Guide*, Release 6.4.1.

Enhanced Security and Performance

NetConf Port Access Control and TCP Port Closure

The NetConf subsystem runs on the default access port 830 over SSH and port 6513 over TLS. Typically, these default access ports are not configurable and are always open. Hence, the NetConf port access control feature enhancement ensures that the Netconf-SSH and NetConf-TLS port access can be controlled and configurable through the new CLIs introduced in the 6.4.1 release.

This feature supports the following:

- Allows access control capabilities for the NetConf-SSH and NetConf-TLS ports.
- Enables/disables the port.
- Allows changing the default port.
- Provides access and control for NetConf services through Inband and Outband.
- Applies ACL rules to the NetConf port to control its access
- Provides the ability to disable the TCP ports not in use

For more information, see the NetConf Port Access Control section in the *OcNOS Key Feature document*, Release 6.4.1.

Hide the Remote AS using neighbor local-as CLI

The `neighbor local-as` command has been enhanced to hide the Autonomous System (AS) number of remote router from the external connected BGP peer. The `local-as` CLI command has been modified to add new options `'no-prepend'` and `'replace-as'`. These options replace the remote AS number with the configured alternate AS in the AS_PATH and BGP OPEN message sent from the remote router. Hence, the remote AS is unknown to the external neighbor peer. This makes the neighbor believe that the received routes are from the alternate AS number included in the AS_PATH and BGP OPEN messages. Thus, the AS number of the remote BGP router is unknown to the external peer.

For more information, see the Hide the Remote AS using the neighbor local-as Command section in the *OcNOS Key Feature document*, Release 6.4.1.

Support IGMP Snooping for Provider Bridge

The existing IGMP Snooping capability has been extended to include the Provider Bridged (PB) network. The following capabilities are supported:

- Snooping entries are captured in the PB network
- Egress traffic from the router is tagged with a single SVLAN ID

Note: The IGMP snooping has been enabled for SVLAN only.

For more information, see the Support IGMP Snooping for Provider Bridge section in the *OcNOS Key Feature document*, Release 6.4.1.

TCP MSS for BGP neighbors

The manual configuration between the routing devices establishes the BGP peer that creates a Transmission Control Protocol (TCP) session. This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session. A TCP segment is a unit of data transmitted in a TCP connection.

TCP MSS configuration per BGP neighbor adjusts the BGP Update Packet Size according to the configured value, which prevents the BGP update packet from getting dropped in transit. The configurable MSS range is from 40-1440. Configure TCP MSS per BGP neighbor using the CLI or NetConf interface.

For more information, refer to the TCP MSS configuration for BGP neighbors section in the *OcNOS Key Feature document*, Release 6.4.1.

TCP MSS Configuration for LDP sessions

Label Distribution Protocol (LDP) uses TCP to establish sessions between the devices. This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session. The configuration of the TCP MSS for LDP neighbors helps the neighbors adjust the MSS value of the TCP SYN packet. The configurable MSS range is from 560 to 1440. Configure the TCP MSS through the CLI and NetConf interface.

For more information, refer to the TCP MSS configuration for LDP sessions section in the *OcNOS Key Feature document*, Release 6.4.1.

Increase the Limit of BGP peers in a Peer-Group

The number of BGP peers in a Peer-Group is limited to 32. This means that every time the number of peer members exceeded 32, a new Peer-Group has to be created.

To circumvent this need, the feature has been enhanced to increase the members in a peer group from 32 to 255.

Port Breakout (400G) for Qumran2 Series Platforms

The port breakout capability offers a robust and secure solution to divide 400GbE ports into multiple ports, ensuring a reliable network infrastructure. In today's networks, there is 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 and density needs continue to evolve.

For more information, refer to Port Breakout (400G) for Qumran2 Series Platforms *OcNOS Key Feature* document, Release 6.4.1.

Single Home VxLAN IRB with OSPF and ISIS

Single Home VxLAN IRB with OSPF and ISIS enhances the flexibility and compatibility of network configurations by expanding the functionality of IRB interfaces to include OSPF and ISIS support. Consequently, it leads to an overall improvement in network performance and connectivity within the network infrastructure.

For more information, see the Single Home VxLAN IRB with OSPF and ISIS section in the *OcNOS Key Feature document*, Release 6.4.1.

Password Strength Enhancements

OcNOS has now included enhancements to password strength requirements, and the password must adhere to the following criteria:

- Length: Passwords must be 8-32 characters.
- Character Types: Passwords must contain at least one of each of the following:
 - One uppercase letter
 - One lowercase letter
 - One digit
 - One special character (acceptable special characters: ~`!@#\$%^&*(){}'[]",.</+_-:;)

Note: The following characters are not acceptable in passwords: '=?!>.

For more information, refer to the username command in the *OcNOS System Management Guide*, Release 6.4.1.

RADIUS Server Authentication Failure and Fallback

In the event of a RADIUS server authentication failure, this feature provides the ability to fallback to the local authentication server. This occurs in the following two scenarios:

- When the user is not present in the RADIUS server
- When authentication fails in the RADIUS server

To implement the above requirements, the existing `aaa authentication login default fallback error local non-existent-user vrf management` command 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 more information, see the Fall Back Option for RADIUS Authentication section in the *OcNOS Key Feature document*, Release 6.4.1.

Modified Extended ACL Deny Rule Behavior in VTY

The existing Extended Access Control List (ACL) translation has been enhanced in this release. In general, the Virtual Teletype (VTY) ACLs are more specific to management protocols. Hence, the Extended ACL "Any" rule translation is modified to allow or deny management protocols under the following conditions:

- If the **deny** ACL rule includes any value in protocol, then only Telnet, SSH, NetConf-SSH protocols are denied.
- The **permit** ACL rule remains unchanged.

For more information, see the Modified Extended ACL Deny Rule Behavior in VTY section in the *OcNOS Key Feature document*, Release 6.4.1.

Improved Network Resilience

RSVP Detour Over Ring Topology

In OcNOS, this feature enhances the routing experience by forming a detour in a ring topology. When a failure or congestion occurs in the primary Label Switched Path (LSP), the detour protects data traffic. The detour formation is a local protection mechanism to minimize data traffic loss.

For more information, see the RSVP Detour Over Ring Topology section in the *OcNOS Key Feature document*, Release 6.4.1.

Commit Rollback

Execution of the Commit Rollback functionality within Common Management Layer Commands (CMLSH) allows for the rollback of configurations previously committed. To support this functionality, introduced the following CLIs:

```
show commit list
commit-rollback to WORD (description LINE|)
clear cml commit-history (WORD|)
cml commit-history (enable | disable)
cml commit-id rollover (enable | disable)
show cml commit-history state
```

For more information, refer to Commit Rollback section in the *OcNOS Key Feature document*, Release 6.4.1.

Improved Management

Streaming Telemetry

Streaming Telemetry in OcNOS introduces a dynamic monitoring approach, enabling real-time transmission of structured operational data from routers to external systems. Enable streaming telemetry for monitoring interface counters and the health of the OcNOS target device, including memory, CPU usage, fan speed, and temperature. OcNOS version 6.4.1 introduces the gNMI Server Subscribe model, which enables Dial-in mode Telemetry for the management plane.

For more information, refer to the Streaming Telemetry section in the *OcNOS Key Feature document*, Release 6.4.1.

Support VLAN Range in SPAN

The existing OcNOS-DC Switch Port Analyzer (SPAN) monitor session feature has been enhanced in current release to support VLAN ranges for VLAN monitor sessions. The VLAN range is supported only for ingress traffic.

The following two commands have been updated to support the VLAN ranges:

- hardware-profile filter (XGS)
- filter

For more information, see the Support VLAN Range in SPAN section in the *OcNOS Key Feature document*, Release 6.4.1.

Route Monitor

The Route Monitor feature in OcNOS introduces a standalone tracking mechanism designed to be used by various processes. It monitors the reachability state of an object through IP SLA.

With Route Monitor, multiple tracked objects can be configured on one or more interfaces, collectively influencing the interface's operational state.

For more information, refer to the Route Monitor section in the *OcNOS Key Feature document*, Release 6.4.1.

Enhancements for OpenConfig Translation

OcNOS extended support for ISIS, LDP, and Bridge-Domain OpenConfig Translation. This enhancement enables network administrators to manage these additional components using standardized YANG models. This promotes consistency and simplifies network management. This extension also offers network operators flexibility and comprehensive error reporting through OpenConfig paths, which can be valuable for troubleshooting and diagnostics.

The OpenConfig Translation feature provides the ability to manage multi-vendor networks through a unified interface, reducing operational costs and complexity for network operators.

In previous OcNOS versions, the network-instance type determination on OcNOS was based on the `type` leaf and some configurations that relied on the presence of the number of interfaces or endpoints. However, starting from the OcNOS 6.4.1 release version, the network-instance type determination is based on the `/oc-netinst:network-instances/network-instance/config/type` and `/oc-netinst:network-instances/network-instance/encapsulation/config/encapsulation-type` leaves.

For more information, refer to the ISIS OpenConfig Translation, LDP Openconfig Translation, VLAN OpenConfig Translation, and Network-instance Object Values for “type” Attribute sections in the *OcNOS OpenConfig Command Reference Guide*, Release 6.4.1.

NetConf “remove” Operation

The `remove` operation in Netconf is supported under the `edit-config` category. Users can execute this operation using either the `merge` or `replace` operation types. The `remove` operation functions similarly to the `delete` operation, with one crucial difference. In cases where the requested data is not present in the running configuration, instead of displaying a `data-missing` error, it will ignore this error and continue further processing.

For more information, refer to the Supported Operations chapter in the *OcNOS NetConf User Guide*, Release 6.4.1.

DHCP Server Group

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.

This feature helps one configure the 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 eight DHCP servers is permitted for each DHCP server group.

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 network configuration information.

For more information, refer to DHCP group section in the *OcNOS Key Feature document*, Release 6.4.1.

Custom Syslog

Release 6.4.1 enhances the current ability to configure Syslog only on the default port and permits configuration on a custom port. The existing logging server CLI command is enhanced to provide this additional capability. Typically, using the default port in a production network is not recommended. This feature enhancement allows for secure communications using a custom port as opposed to the default port, port 514, that is not considered secure.

For more information, refer to the Custom Syslog Port Configuration and Syslog chapters in the *OcNOS System Management Guide*, Release 6.4.1.

Enhanced VE-ID Range

In OcNOS, the Virtual Ethernet Identifier (VE-ID) range is increased from 1-64 to 1-65535. This allows network operators to configure and manage Virtual Private LAN Service (VPLS) instances. The VE-ID must be unique for the VPLS peers in a VPLS instance.

For more information, refer to the command reference page for `ve-id` in the Virtual Private LAN Service Commands chapter in the *OcNOS Multi-Protocol Label Switching Guide*, Release 6.4.1.

VRRP over MLAG with Custom VRF

OcNOS provides the capability to configure the Virtual Router Redundancy Protocol (VRRP) over Multi-Chassis Link Aggregation (MLAG) feature for custom Virtual Routing and Forwarding (VRF).

Custom Virtual routing and forwarding (VRF) isolates and virtualizes the network at Layer 3 of the OSI model, as Virtual Local Area Network (VLAN) serves similarly at Layer 2. The VRFs are used to separate the network traffic and efficiently use the routers. VRF can also create Virtual Private Network (VPN) tunnels dedicated to a single network or a client.

For more information, refer to the Custom VRF Configuration section of the VRRP Configuration chapter in the *OcNOS Layer 3 Guide*, Release 6.4.1.

Enhanced Graceful Restart

Executing the graceful restart CLI commands for BGP, ISIS, RSVP and OSPF modules, deletes in progress configurations if not saved and requires manual restart of the devices running these protocols. To address this issue, the following existing graceful restart CLI commands are enhanced to notify the user to save the configurations before executing them.

- restart bgp graceful
- restart ospf graceful
- restart isis graceful
- restart ipv6 ospf graceful
- IS-IS Graceful Restart Configuration
- OSPFv3 Graceful Restart Configuration
- RSVP Graceful Restart Configuration

For more information, refer to the *Layer 3 Configuration Guide*, Release 6.4.1.

Enhanced MAC Mobility

OcNOS introduces improved MAC mobility support for Layer 2 traffic in VXLAN-EVPN networks. Prior to this enhancement, virtual machines faced communication disruptions when moving between Virtual Tunnel End Points (VTEPs) within the network. With this improvement, dynamically learned MAC addresses remain persistent with aging disabled, ensuring uninterrupted communication for dynamic hosts across VTEPs. This enhances network flexibility and reliability. The static host behavior remains unchanged.

SFTP and SCP Enhancements

OcNOS now includes enhancements to the sys-update install and sys-update get functionalities by introducing support for Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP). These additions allow users to benefit from improved flexibility and security in managing software updates. These enhancements support IPv4 and IPv6 addresses and hostnames, helping network administrators and engineers.

For more information, refer to the Licensing and Upgrade Commands chapter in the *OcNOS Licensing Guide*, Release 6.4.1.

Remove "tech-support" file

When the "show techsupport" command is executed, a file is generated in the "/var/log" directory.

Currently, the file deletion command is not implemented, so the problem exists that files cannot be deleted.

Introduced the following new CLI command that enables operators to remove files:

- remove file (techsupport)

For more information, refer to Software Monitoring and Reporting in the *OcNOS System Management* Release 6.4.1.

Port Breakout (100G) for AS5835-54T/AS5835-54X/S8901-54XC (Maverick2) Platform

The AS5835-54T/AS5835-54X/S8901-54XC Maverick2 devices accommodates a combination of port breakout options with hybrid port speeds. These devices support 6 ports (port 49-54) with 100G Ethernet QSFP28 interfaces. By using port breakout, divide the 100G QSFP28 ports (ce49, ce50, ce51, ce52, ce53, and ce54) into 4X10G/4X25G/2X50G as needed. When executing a port breakout on the 100G port ce50, the original ce50 port will be replaced with ce50/1, ce50/2, ce50/3, and ce50/4.

vThese breakout ports permit the configuration of all Layer 2 and Layer 3 features similar to standard ports. In scenarios where no port breakout is applied, ce50/1, ce50/2, ce50/3, and ce50/4 will be removed, and the original ce50 port will be added.

Improved Routing

Static Route Tracking using Object Tracking (IP SLA)

OcNOS has extended support for IPv6 in Static Route Object Tracking using the Internet Protocol Service Level Agreement (IP SLA), enhancing the management and monitoring of IPv6 traffic. Using the capabilities of IP SLA, the feature continuously assesses IP service quality by employing ICMP pings to detect link failures and promptly notify registered clients of any events. The outcome is a resilient network infrastructure, empowering administrators to quickly respond to changes in tracked object values, ensuring network stability and network reliability across IPv4 and IPv6 networks.

For more information, refer to the Static Route Object Tracking using IP SLA chapter in the *OcNOS Layer 3 Guide*, Release 6.4.1.

BGP VPNv4 Route Display Command

OcNOS introduces a new CLI command, `show ip bgp vpnv4 all neighbors A.B.C.D routes`, which enables users to view BGP VPNv4 routes for a specific neighbor. This addition provides users with improved visibility and control over their BGP VPNv4 routes, enhancing network monitoring and management capabilities.

For more information, refer to the `show ip bgp vpnv4` command section in the *OcNOS Layer 3 Guide*, Release 6.4.1.

BGP Additional Path

The Border Gateway Protocol (BGP) ADDPATH allows the advertisement of multiple paths through the same peer session for a given prefix without the new paths implicitly replacing any previous paths. This behavior promotes path diversity and reduces the severity of a network failure, thereby improving the control plane convergence in case of network failures.

This release adds several commands to the IPv4 VRF address-family. The additional commands are listed in this section. Global mode commands in `ipv4 vrf address-family`

Global mode commands in `ipv4 vrf address-family`

- `bgp additional-paths send-receive`
- `bgp additional-paths select best 3`
- `bgp additional-paths select all`

Neighbor level commands added in `ipv4 vrf address-family`

- neighbor A.B.C.D additional-paths send | receive | send-receive
- neighbor A.B.C.D additional-paths all
- neighbor A.B.C.D additional-paths best <2-3>

For more information, refer to the BGP Additional Path *OcNOS Layer 3 Guide*, Release 6.4.1.

RSVP-TE Commands

RSVP-TE is a signaling protocol that supports explicit routing capabilities. As part of this process, an Explicit Route (ER) object is incorporated into the RSVP PATH messages. This object encapsulates a sequence of hops that constitute the explicitly-routed path. Using the ER object, the paths taken by label-switched RSVP-MPLS flows are pre-determined without conventional IP routing.

The following are the new CLI commands added to OcNOS DC.

- primary no-affinity
- no primary affinity
- primary no-record
- no primary record
- primary no-cspf
- no primary cspf
- primary no-record
- no primary record

The following CLI commands are removed from OcNOS DC.

- primary filter
- secondary filter
- elsp-signal-map

For more information, refer to the RSVP-TE Commands section in the *OcNOS DC MPLS*, Release 6.4.1.

Inbound Route Filter for EVPN

The inbound route filtering is available for Ethernet Virtual Private Network (EVPN) address families. By default, Layer 2 Virtual Private Network (L2VPN) EVPN routes are not installed into the VRF BGP table without the matching import route target. This matching mechanism prevents saving the unmatched routes in the remote Route Distinguisher (RD) BGP table and reduces memory consumption.

For more information, see the command reference page for `bgp inbound-route-filter` in the BGP Virtual Private Network Commands chapter in *OcNOS Layer 3 Configuration guide*, Release 6.4.1.

Enhanced EVPN Route Show Command

The enhanced EVPN Route Show Command now includes prefix-route for precision and detail for in-depth insights. It tailors the output to specific requirements, streamlining network management and decision-making with precise, customized data for efficient troubleshooting and enhanced control.

For more information, refer to the `show bgp l2vpn evpn` section in the *VXLAN Commands* document, Release 6.4.1.

UDLD Support on Layer 3 Interface

Layer 3 Unidirectional Link Detection protocol (UDLD) support has been enabled.

The UDLD protocol monitors the physical links and detects when a unidirectional link exists. Upon detection, a user can either block the port or be notified of the link status based on the network administration configuration.

UDLD works in two different modes:

- Normal mode
- Aggressive mode

For more information, see the Unidirectional Link Detection Configuration section in the *OcNOS Layer 3 Configuration guide*, Release 6.4.1.

Technical Supports

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at <http://www.ipinfusion.com/customer-support>.

IP Infusion's maintenance customers and partners can access the support website. The site allows customers and partners to open technical support calls, update open calls with new information, and review the status of open or closed calls. The password-protected site includes technical documentation, Release Notes, and descriptions of service offerings.

Technical Documentation

For core commands and configuration procedures, visit: <https://docs.ipinfusion.com/datacenter/>

Technical Sales

Contact the IP Infusion sales representative for more information about the OcNOS Service Providers solution.

