



OcNOS®

Open Compute Network Operating System Security Guide

Security Guide
February 2026

© 2026 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	5
Audience	5
Conventions	5
IP Infusion Product Release Version	5
Related Documentation	5
Feature Availability	6
Migration Guide	6
IP Maestro Support	6
Technical Support	6
Technical Sales	6
Technical Documentation	6
Introduction	7
Overview	7
OcNOS Software	7
Functional Planes of a Switching or Routing Device	8
Management Plane Protection	9
Authentication, Authorization and Accounting (AAA)	9
Password Hashing	10
TACACS+ Server	10
TACACS+ Server Authentication	10
TACACS+ Server Accounting	10
TACACS+ Server Authorization	11
RADIUS Server	11
RADIUS Server Authentication	11
RADIUS Server Accounting	12
Root File System Checksum Verification	12
Secure Shell (SSH)	12
SSH Keys	12
SSH Encryption	13
Feature Characteristics	13
Benefits	15
Prerequisites	15
Configuration	15
Topology	15
Validation	17
DHCP Snooping	18
IP Source Guard	18
Dynamic ARP Inspection (DAI)	19
Management ACL	19
SNMP	19
Network Time Protocol Client	21
Log Management	21

Control Plane Protection	22
Rate Limiting of Control Plane Traffic	22
Proxy ARP	24
IP Redirects	24
Authentication or Confidentiality for OSPFv3	25
Data Plane Protection	26
SYN Cookies	26
Port Security	26
Access Control List	27
BGP FlowSpec Support for IPv4	28
Storm Control	28
STP Root Guard	29
STP BPDU Guard	29
sFLOW	29
Port Isolation for MLAG	30
Background Port Isolation Security	30
MAC Authentication Bypass (MAB)	31
OS Security	34
Filesystem Capabilities	34
SMACK	34
Stack Protector	34
Pointer Obfuscation	34
Libs/mmap ASLR	34
brk ASLR	34
VDSO ASLR	35
Built as PIE	35
Built with Fortify Source	35
Built with RELRO	35
Symlink Restrictions	35
Hardlink Restrictions	35
Older Protocol Vulnerabilities	36
Memory	36
Malloc Heap Memory Protection	36
Stack ASLR	36
Exec ASLR	36
/proc/\$pid/maps Protection	36
Configurable Password Policy	36
Integrating PAM to OcNOS	37
Kernel	37
0-Address Protection	37
ACL Support Over Management, VTY and Loopback	37
DHCP Relay Option 82	38
OcNOS Scan with Security Database	38
Abbreviations	39

Preface

This guide describes how to configure OcNOS.

Audience

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

Conventions

[Table 1](#) on page 5 shows the conventions used in this guide.

Table 1: Conventions

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

IP Infusion Product Release Version

Each integer in release number indicates Major, Minor, and Maintenance release versions. Build numbers that follow the release 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; including, a significant marketing change or direction in the product.

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

Maintenance Version: A collection of product bugs or hotfixes usually scheduled every 30 or 60 days, based on the number of hotfixes.

Related Documentation

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

Feature Availability

Each OcNOS SKU contains a set of supported features. For a list of available features based on the SKU that you purchased. Refer to the *Feature Matrix*.

Migration Guide

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

IP Maestro Support

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

Technical Support

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at the [Technical Assistance Center](#).

Customers and partners enjoy full access to 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 Sales

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

Technical Documentation

For core commands and configuration procedures, visit: [Product Documentation](#).

For training videos, visit: [OcNOS Free Training Videos](#).

For a list of supported platforms and SKUs of OcNOS features, refer to the [OcNOS Feature Matrix](#).

Disclaimer

The global documentation site is evolving to provide an enhanced website user experience for select topics included in this release. Some guides are now available outside the existing documentation library and can be accessed directly from custom documentation landing pages. These guides offer robust in-built search functionality.

For the latest documentation, visit the product-specific documentation landing page and select the relevant guide.

Comments

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

Introduction

Overview

A Network Operating System (NOS) makes up the core of a switching or routing device. To gain unauthorized access to the device, disrupt services, steal data, or cause other malicious activities, hackers use some loopholes in the implementation of the switching and routing protocol stack to cause a denial of service, or to sniff and re-route the data flowing through the networking device.

A compromised networking device causes huge financial losses to the manufacturers, service providers, and service users. To overcome all these issues, NOS provides different layers of protection against various security threats. This document aims to familiarize the readers with the different layers of protection mechanisms available in OcNOS to prevent and minimize security threats.

OcNOS encompasses the future demands of mobile and wireline networks. It goes beyond delivering greater bandwidth at reduced costs, addressing the requirements of emerging applications like mobile broadband, IoT networks, autonomous vehicles, and smart wireless devices. IP Infusion offers disaggregated solutions that cut costs, expand the vendor landscape, and enable agile service introduction through automation.

OcNOS Software

OcNOS is a network operating system designed to run on Commercial Off-The-Shelf (COTS) platforms, 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.

Functional Planes of a Switching or Routing Device

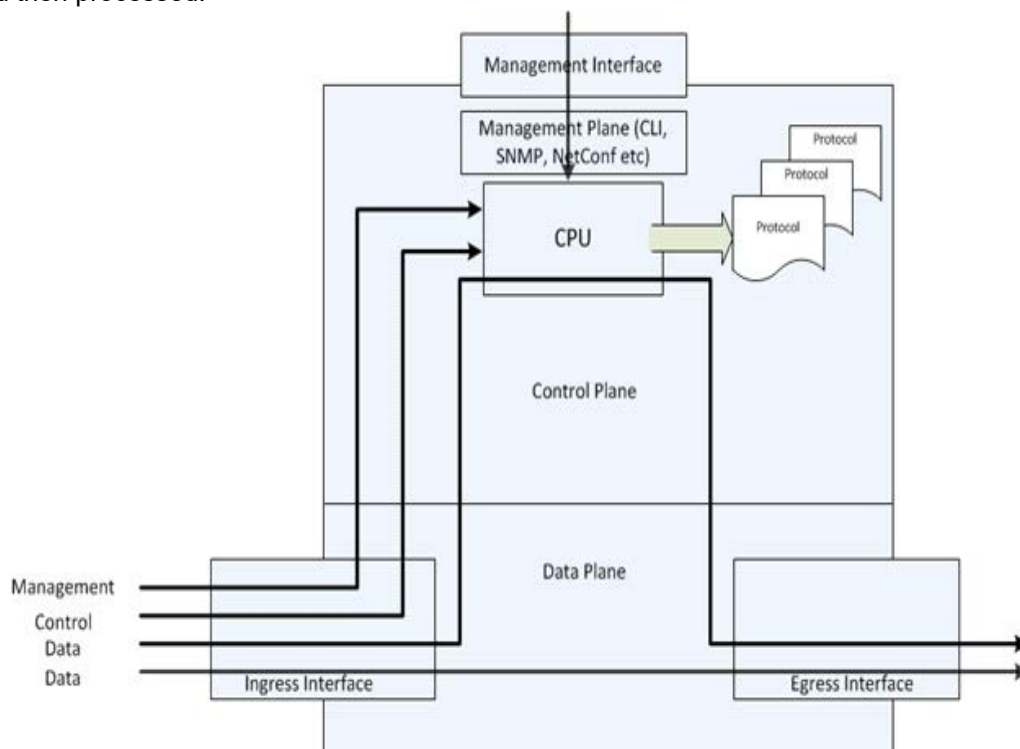
A Switching or Routing usually has three different functional planes:

- **Control Plane:** It is responsible for managing and controlling, how data packets are forwarded. It normally runs the protocols and applications that build various switching and routing tables based on which switching or routing devices forward traffic. In a network, the control plane plays a major role in handling tasks related to routing, signaling, network management, and communication between network devices.
- **Data Plane:** The data plane provides the packet-switching functionality and is responsible for moving user traffic from one point to another based on the information provided by the control plane.

The traffic entering the switching or routing devices are categorized into the following:

- **Management Plane:** The management plane is responsible for monitoring, configuring, maintaining, and troubleshooting network elements.
- **Control Plane Traffic:** Control Plane Traffic mainly includes the routing or switching protocol, the messages that it receives from its neighbors, such as – STP BPDU, or route update.
- **Data Plane Traffic:** Data Plane Traffic is either switched or routed by networking ASIC from the incoming interface to the outgoing interface as programmed by the control plane. For some traffic, such as ARP, DHCP or routing lookup, missed packets are sent to the control plane for decision-making and then forwarded to the outgoing interface.

Management Plane Traffic: Management Plane Traffic is destined to the switch or router itself. The packets typically contain device configuration or management protocol-related messages. Management traffic can enter the switch or router through a dedicated management interface or one of the data ports and is processed by the CPU in the control plane. When management traffic enters the device through one of the switch ports, it is sent to the CPU in the control plane and then processed.



Protecting all three device planes is crucial from an overall security perspective. OcNOS supports features and mechanisms to cover each functional plane of a switching or routing device.

Management Plane Protection

The management plane consists of features with which we can configure the devices.

It must be protected, as any security incident that undermines the management plane can destabilize the network or the entire system.

OcNOS includes the following features to harden the management plane.

Authentication, Authorization and Accounting (AAA)

AAA is a framework for controlling access to device resources, enforcing policies, auditing usages, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the switch.
- Authorization determines what the user can do.
- Accounting tracks the user activities and provides an audit trail for billing or resource tracking.

The OcNOS AAA framework is used to secure the management plane by restricting who can log in to the device and assign a role to a specific user so that they can perform changes only allowed by that role.

- **Network Administrator:** Administrators have access permissions to change the switch configuration permanently. Changes are persistent across the reset or reboot of the switch.
- **Network Engineer:** Engineers are responsible for making permanent changes to switch or router configuration. Changes are persistent across the reset or reboot of the switch.
- **Network Operators:** Operators have access permission to make permanent changes to the switch configuration. Changes are not persistent across the reset or reboot of the switch.
- **Network User:** Users have the permission to display information only. They cannot modify any existing configuration.
- **RBAC User:** RBAC users have access to change only permitted configuration.

OcNOS prevents brute-force attacks using the techniques below.

Following measures allow access to only authenticated users.

Account Management

Managing accounts allows you to configure how many login attempts can fail before a user's account is locked, how much time can expire in seconds after which the account is automatically unlocked, and how to manually clear the lock for a customer who is locked out of their account.

1. Configure the maximum allowable failed attempts and timeout in seconds after which the account will be automatically unlocked using the below commands:

```
aaa local authentication attempts max-fail <1-25>
```

By default, the user account gets locked when a user enters an incorrect password more than four times.

2. Configure the timeout value in seconds to automatically unlock the account. By default, once a user account is locked, the lock is cleared after 1200 seconds (20 minutes).

```
aaa local authentication unlock-timeout <1-3600>
```

The Alert operations log below appears when a user account is locked.

```
OcNOS : HOSTP : ALERT : [USER_MGMT_ACCOUNT_LOCKED_1]:
```

Once the threshold for unsuccessful authentication attempts is exceeded by the user 'test' the user account is locked.

3. Use this command to manually clear the lock for a user.

```
clear aaa local user lockout username USERNAME
```

Password Hashing

The system passwords are encrypted using salted SHA-512 based password hashes, which are more resistant to brute force attacks.

The passwords are encrypted using the following command.

Configure Password Hashing

Use the following commands to configure password hashing.

#configure terminal	Enter configure mode
(config)#enable password mypasswd	Enable the password
(config)#service password-encryption	Encrypt the password

TACACS+ Server

TACACS+ Server Authentication

Terminal Access Controller Access Control System (TACACS+) is a remote authentication protocol utilized to communicate with an authentication server, that is frequently used in UNIX networks. With TACACS, a network device communicates with an authentication server to determine whether a particular user is allowed to access the device.

The TACACS+ protocol is the latest generation of TACACS. TACACS+ uses TCP for its transport.

OcNOS Supports TACACS+ Server Authentication to restrict users logging in to the switch.

TACACS+ authentication is enabled with a configuration similar to this example:

Configure TACACS+ Server Authentication

Use the following commands to configure TACACS+ Server Authentication.

(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.

TACACS+ Server Accounting

To verify the TACACS+ accounting process, connect 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 the corresponding username and password.

Enable accounting for TACACS+ server:

Configure TACACS+ Server Accounting

Use the following commands to enable TACACS+ Server Accounting.

(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

TACACS+ Server Authorization

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

Users with privilege-level lower than or equal to zero and privilege-level higher than fifteen are treated as read-only, and are mapped to 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+. After successful authentication, a user can enter privileged exec mode, irrespective of their privilege level, without being prompted for an enable mode password. However, based on their role, they will not be able to issue certain commands if they are not allowed to perform certain operations.

Example: A network user is limited to read-only access and is exclusively able to execute show commands. They are unable to enter configure mode, and any attempt to execute a disallowed command prompts an error message.

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

The following attribute-value pair in the TACACS+ server fetches user privilege information.

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

RADIUS Server

RADIUS Server Authentication

Remote Authentication Dial-In User Service (RADIUS) is a remote authentication protocol commonly used in UNIX networks to communicate with an authentication server.

A RADIUS client-server model consists of the RADIUS server being responsible for receiving user connection requests, authenticating the user and then returning all configuration information necessary for the client to deliver services to the user.

The key points for RADIUS authentication are as follows:

- The transactions between the client and the server are authenticated using a shared key. This key is never sent over the network.
- The password is encrypted it is before sent over the network.
- OcNOS supports RADIUS server authentication to restrict the users logging in to the switch.

Enable RADIUS server

Enable authentication for RADIUS server.

<code>(config)#aaa authentication login default vrf management group radius</code>	Enable authentication for radius server configured for management VRF. Authorization is also enabled by default.
<code>(config)#aaa authentication login default group radius</code>	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.

RADIUS Server Accounting

RADIUS server accounting helps measure the resources that a user consumes during access.

Enable RADIUS Server Accounting

Enable accounting for the RADIUS server.

<code>(config)#aaa accounting default vrf management group radius</code>	Enable accounting for radius server configured for vrf management
<code>(config)#aaa accounting default group radius</code>	Enable accounting for radius server configured for default vrf

Root File System Checksum Verification

The OcNOS installation package includes a checksum verification mechanism. During the upgrade process, the system performs checksum verification to ensure the integrity of the installation package. If the verification fails, OcNOS automatically reverts to the previously installed version.

Secure Shell (SSH)

SSH is a protocol that allows data to exchange between two network devices using a secure channel. SSH is a replacement for Telnet and other insecure remote shells that sends information, notably passwords, through plain text, rendering them susceptible to packet analysis. The encryption used by SSH is to provide confidentiality and integrity of data in an unsecured network.

SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

OcNOS supports SSH access to the switch. The network administrator allows only SSH access to the switch, making all communication between the switch and the end user secure. SSH Configuration

SSH is performed with IPv4 and IPv6 addresses.

Configure Secure Shell (SSH)

Use the following commands to Configure Secure Shell.

<code>#configure terminal</code>	Enter configure mode
<code>(config)#ssh login-attempts 2 vrf management</code>	Set the number of login attempts to 2
<code>(config)#exit</code>	Exit configure mode

SSH Keys

Use the ssh key command to generate new RSA/DSA keys for the SSH server. By default, the system has an RSA or DSA public or private key pair placed in `/etc/ssh/`. If you want to regenerate RSA keys, you must specify the force

option

Configure SSH Keys

Use the following commands to configure SSH Keys.

#configure terminal	Enter configure mode
(config)#ssh key rsa force vrf management	Enter the force option to regenerate SSH RSA keys
(config)#exit	Exit configure mode

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 algorithm hostkey
- 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. By default, all the ciphers are supported for a new SSH client to connect with the SSH server.
 - KEY
 - MAC
 - Hostkey
 - 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)
 - HOSTKEY algorithms
 - ssh-ed25519,
 - ssh-rsa
- 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)
- Extends 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 hostkey HOSTKEY_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. Set the SSH server HOSTKEY algorithm for the management VRF.

```
(config)#ssh server algorithm hostkey ssh-rsa vrf management
```
5. 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 dif-fie-hellman-group14-sha256 dif-fie-hellman-group16-sha512 dif-fie-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. Set the SSH server HOSTKEY algorithm for the default VRF.

```
(config)#ssh server algorithm hostkey ssh-rsa  
(config)#commit
```
5. 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. Set the SSH server HOSTKEY algorithm for the user defined **vrf1**.

```
(config)#ssh server algorithm hostkey ssh-rsa vrf vrf1
```

6. Commit the configuration and exit.

```
(config)#commit
```

```
(config)#exit
```

Validation

Execute the following show command to view the SSH server information.

```
#show running-config 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
ssh server algorithm hostkey ssh-rsa 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 dif-fie-hellman-group16-sha512
dif-fie-hellman-group18-sha512
ssh server algorithm hostkey ssh-rsa

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 dif-fie-hellman-group14-sha1 dif-
fie-hellman-group14-sha256 vrf vrf1
ssh server algorithm hostkey ssh-rsa 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,
  HostKeyAlgorithms ssh-rsa

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,
  HostKeyAlgorithms ssh-rsa

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
```

```
HostKeyAlgorithms ssh-rsa
```

DHCP Snooping

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers from offering IP addresses to DHCP clients. Rogue DHCP servers are often used in 'man-in-the-middle' or 'Denial of Service' attacks for malicious purposes. 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:

- It validates messages received from untrusted sources and filters out invalid news.
- It rate limits traffic from trusted and untrusted sources.
- It builds and maintains the snooping binding database that contains information about un-trusted hosts with their leased IP addresses.
- It uses the snooping binding database to validate subsequent requests from untrusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. User can enable the feature on a single VLAN or on a range of VLANs.

Enable DHCP Snooping on a VLAN

Use the following commands to activate DHCP Snooping on a VLAN.

#configure terminal	Enter the configure mode
(config)#vlan 2 bridge 1	Configure a VLAN for the bridge
(config)#ip dhcp snooping vlan 2 bridge 1	Enable the DHCP Snooping on the VLAN 2
(config)#commit	Commit the configuration to running-configuration

IP Source Guard

IP Source Guard (IPSG) restricts IP traffic on non-routed, layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. Use IPSG to avoid traffic attacks when a host attempts to use its neighbor's IP address. Enable IPSG when DHCP snooping is enabled on an untrusted interface.

Enable IPSG on OcNOS for a particular interface. Once IPSG is activated on an interface, the switch restricts all IP traffic received on that interface, except for DHCP packets permitted 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 source binding table and denies all other traffic.

Use this command to enable the IPSG feature at the interface level.

Command Syntax

```
ip verify source dhcp-snooping-vlan
```

Use the no form of this command to disable the IPSG on an interface.

Command Syntax

```
no ip verify source dhcp-snooping-vlan
```

Dynamic ARP Inspection (DAI)

DAI provides a security measure to allow users 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 redirected to Control Plane and validated against the MAC to IP binding database before getting forwarded. ARP coming on an untrusted port is inspected, validated and forwarded to the destination or dropped.

Configure Dynamic ARP Inspection

Use the following commands to configure Dynamic ARP Inspection.

#configure terminal	Enter the 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 the bridge
(config)#commit	Commit the configuration to running-configuration

Management ACL

Management Port ACL provides a basic level of security for accessing the management network. Use ACLs to decide which types of management traffic to forward or block at the management port.

When configuring an 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 permit or deny actions. Each entry is associated with a sequence number in the range of <1-268435453>. The lower the sequence number, higher the priority.

Configure the system to allow a certain IP address for a protocol and prevent any other IP address from matching the protocol.

Configure Management ACL

Use the following commands to configure Management ACL.

#configure terminal	Enter the configure mode
(config)#ip access-list mgmt	Create an IP access list named management
(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh	Create an access rule to permit the TCP connection with source address 10.12.45.57 with the destination address 10.12.29.49 on the destination port equal to SSH

SNMP

SNMP offers a standardized framework and a common language to monitor and manage devices in a network.

SNMP v3 security level determines if an SNMP message must be protected from disclosure and if the message is must be authenticated.

The security levels are:

- noAuthNoPriv: Provides neither authentication nor encryption

- `authNoPriv`: Provides authentication but no encryption
- `authPriv`: Provides authentication and encryption

Note: SNMP is defined in RFCs 3411-3418.

Configure SNMP

Use the following commands to configure SNMP.

<code>#configure terminal</code>	Enter the configure mode
<code>(config)#snmp-server view all.1 included vrf management</code>	Creates an SNMP view labeled "all" for the OID-Tree and as ".1" for vrf management
<code>(config)#snmp-server community test group network-operator vrf management</code>	Set the community string as "test" for a group of users with "network-operator" privilege
<code>(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management</code>	Specify host "10.12.6.63" to receive SNMP version 2 notifications at UDP port number 162 with community string as "test"
<code>config)#snmp-server enable snmp vrf management</code>	Start the SNMP agent
<code>(config)#exit</code>	Exit the configure mode

Configure the security levels using the following commands:

noAuthNoPriv

```
ocnos(config)#snmp-server user test1 network-admin vrf management
ocnos(config)#snmp-server community test1 group network-admin vrf management
ocnos(config)#commit
ocnos(config)#exit
```

authNoPriv

```
ocnos(config)#snmp-server user test2 network-admin auth md5 test1234 vrf management
ocnos(config)#snmp-server community test2 group network-admin vrf management
```

authPriv

```
ocnos(config)#snmp-server user test3 network-admin auth sha test1234 priv des test1234 vrf management
ocnos(config)#snmp-server community test3 group network-admin vrf management
```

Validation

```
OcNOS#show snmp user
SNMP USERS
User
Groups
```

	Authentication		Privilege (enforce)
test1	no	no	network-admin
test2	MD5	no	network-admin
test3	SHA	DES	network-admin

```
OcNOS#show snmp group
```

community/user	group	version	Read-View	Write-view	Notify-view
test1	network-admin	3	all	none	all
test2	network-admin	3	all	none	all

test3	network-admin	3	all	none	all
test2	network-operator	2c/1	all	none	all
test2	network-admin	2c/1	all	none	all
test3	network-operator	2c/1	all	none	all
test3	network-admin	2c/1	all	none	all

Network Time Protocol Client

Network Time Protocol (NTP) is used to synchronize the clocks of a computer system with a specific reference time source. It is essential that all the nodes within a network have their clock correctly synchronized with a reference time source. This helps to track the network events accurately such as security violations, interpreting events within Syslog data files as well as validating the digital certificates.

OcNOS supports NTP client that allows users to configure an association with a remote server. In this mode, the client clock can synchronize to the remote server which acts as a reference time source.

After configuring the NTP server, wait for a few minutes for the client device to synchronize its clock with the server.

Configure NTP Client

Use the following commands to configure NTP client.

# configure terminal	Create the access list
(config)# ntp enable vrf management	Enable NTP
(config) # ntp server 10.10.10.15 vrf management	Configure NTP client address in the NTP allow list

Log Management

OcNOS supports logging messages to a Syslog server in addition to logging to a file or the console (local or ssh or telnet console). OcNOS messages are logged to a local Syslog server (the machine on which OcNOS executes) and to one or more remote Syslog servers (a maximum of 8 remote Syslog servers are supported). Remote Syslog servers can either be configured with IPv4 or IPv6 addresses or hostnames.

Support for In-band management over default VRF

OcNOS supports Syslog over the default and management VRFs using the in-band management interface and the out-of-band (OOB) management interface, respectively.

By default, Syslog runs on the management VRF.

Enabling and logging to a file

Use the following commands to enable and log a file.

(config)#feature rsyslog	Enable feature on default or management VRF. By default this feature runs on the management VRF
(config)#logging level ospf 7	This enable debug messages for OSPF module. This is configurable either if default of management VRF
(config)#logging logfile ospf1 7	This creates the log file where the logs are saved. The path of the file will be in the directory /log/ospf1. Log File size 4096-4194304 bytes

Control Plane Protection

Control Plane Policing (CoPP) manages the traffic flow destined for the host router CPU for control plane processing. CoPP limits the traffic forwarded to the host CPU and minimizes impact on system performance.

1. CoPP has organized the handling of control packets by providing per-protocol hardware CPU queues. Control packets are queued in different CPU queues based on protocol.
2. Per-protocol CPU queue rate limits and buffer allocations are programmed. Thus, by default every CPU queue is rate-limited to provide a 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.

Limitation:

1. OcNOS does not support per-queue rate modification and usage monitoring.
2. All CPU queues are pre-programmed with default rate limits and buffer allocations to ensure a default stable and balanced behavior across protocols.
3. Rate limits are in terms of kilobits per second (kbps). Hardware does not support packets per second (PPS).

OcNOS supports a mechanism to protect the switch's control plane from such DOS attack.

A majority of the packets enter a switch through the data plane. Out of these packets, there are some packets that need to be handled by the control plane processor, for example, Layer2 protocol packets, Layer-3 protocol packets, keep-alive packets, and ICMP packets. This type of traffic is often referred to as control plane traffic.

A considerable amount of control plane traffic can overload a switch's control plane and degrade its performance. A rogue network device or a misbehaving routing protocol can generate massive control plane packets, which can overwhelm the switch's processor. This will eventually result in a (DOS attack).

Rate Limiting of Control Plane Traffic

OcNOS has an in-built mechanism to rate limiting control plane traffic. This automatically prevents any DOS attack by rogue control plane traffic. The following table describes the default rate limiting values for various types of control plane traffic.

Queue	Name	Comments
0	Default CoS Queue	Unmapped traffic will take this queue
1	L3 Nexthop Cos Queue	L3 Next Hop hit
2	L3 header error CoS Queue	Cosq for L3 header Error
3	Multicast miss Cos Queue	Cosq for Multicast lookup Failure

4	IP Multicast miss Cos Queue	Cosq for IP multicast lookup failure
5	Unicast L3 miss Cos Queue	Cosq for l3 destination lookup failure
6	My station CoS Queue	Cosq for my station copy to cpu packets
7	IP Multicast Reserved CoS Queue	cosq for reserved IPMC packets
8	L3 slow path CoS Queue	Cosq for L3 slow path processed packets
9	Unused	Unused
10	BGP CoS Queue	Cosq for BGP packets
11	VRRP CoS Queue	Cosq for VRRP Packets
12	LDP CoS Queue	Cosq for LDP Packets
13	RIP CoS Queue	Cosq for RIP Packets
14	OSPF CoS Queue	Cosq for OSPF Packets
15	DHCP CoS Queue	Cosq for DHCP Packets
16	ICMPv6 CoS Queue	Cosq for ICMPv6 packets (Pingv6, Neighbor and router discovery, MLD)
17	MPLS OAM CoS Queue	Cosq for MPLS OAM Packets
18	PIM Cos Queue	Cosq for PIM packets
19	ARP CoS Queue	Cosq for ARP Packets
20	IGMP CoS Queue	Cosq for IGMP Packets
21	L2CP cos Queue	Cosq for L2 control packets
22	CCM CoS Queue	Cosq for Continuity check message Packets

23	BFD CoS Queue	Cosq for BFD Packets
24	PTP CoS Queue	Cosq for PTP Packets
25	ISIS CoS Queue	Cosq for IS-IS packets
26	NAT Cos Queue	Cosq for Network Address translation Packets
27	Trill CoS Queue	Cosq for Trill control Packets
28	L2 Move CoS Queue	Cosq for station movement Packets
29	MC Switch CoS Queue	Cosq for Multicast Switch to CPU Packets
30-47	Unused	Unused

Note: The queue numbers might vary slightly across boards.

Proxy ARP

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 the destination. The Proxy typically routes the captured traffic to the intended destination through another interface. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.

An attacker can exhaust all available memory if they send many ARP requests. Man-in-the-middle attacks enable a network host to spoof the router's MAC address, which results in unsuspecting hosts sending traffic to the attacker.

Use `no ip proxy-arp` to disable Proxy ARP.

Note: Proxy ARP is disabled by default.

IP Redirects

Use this global command to trap ICMP redirect packets to the CPU and on the interface to enable ICMP redirects in the kernel. Use the `no` form of this command to disable the ICMP redirect message on an interface.

To improve the security aspect, on observation of some un-intended reception of ICMP redirects on a particular interface, this can be disabled optionally.

Note: This command is applicable for both IPv4 and IPv6 interfaces.

Syntax

```
ip redirects
```



```
no ip redirects
```

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
```

Authentication or Confidentiality for OSPFv3

Open Shortest Path First (OSPF) v2 defines fields in its protocol header to provide security.

In OSPFv3, security protocol header fields were removed. OSPFv3 relies on the IPv6 Authentication Header (AH) and IPv6 Encapsulating Security Payload (ESP) to provide integrity, authentication, and confidentiality. This command is valid on both IPv4 and IPv6 interfaces.

Reference: <https://datatracker.ietf.org/doc/html/rfc4552>

Data Plane Protection

The switch or router architecture forwarding function directs incoming frames and packets on an interface. Routers and switches leverage the control plane to handle incoming data, and based on the control plane logic, the data plane then forwards the traffic to the subsequent hop en route to its destination. The frames or packets in the data plane traverse through the device, and this aspect is also referred to as the forwarding plane.

SYN Cookies

SYN Flooding is one form of DOS attack. A TCP session requires a three-way handshake between two endpoints. The SYN cookies technique is used to protect against SYN flooding attacks. SYN cookies distinguish an authentic SYN packet from a faked one. When the server sees a possibility of SYN flooding on a port, it generates a SYN cookie instead of an initial sequence number that is transparent to the client.

SYN cookies have the following properties:

- SYN cookies are generated when the SYN queue hits the upper limit. The server behaves like the SYN queue is enlarged. SYN cookies have the following properties.
- The generated SYN cookie is used in place of the initial sequence number. The server returns the SYN+ACK response to the client and discards the SYN queue entry.

If the server receives a subsequent ACK response from the client, the server reconstructs the SYN queue entry using the information encoded in the TCP sequence number.

OcNOS terminal displays the below message when a SYN Flood command is issued.

```
TCP: TCP: Possible SYN flooding on port 23. Sending cookies. Check SNMP counters.
```

Port Security

Users can limit each port's ingress traffic by limiting MAC addresses (source MACs) that send traffic to the ports. Port Security enables users to configure the maximum number of secured MACs for each port. Switches learn secured MAC addresses dynamically (learned by the switch during traffic inflow) or statically (user-configured MACs). At most, dynamically learned or statically programmed MAC addresses can be the maximum number (up to 1000) of secured MACs configured for a particular port. Traffic from all other MAC addresses is dropped once the switch reaches the maximum limit for secured MACs.

The violated MACs are logged in Syslog messages.

Configure Port Security

Use the following commands to configure Port Security.

(config)#interface gel	Enter the interface mode
(config-if)#switchport	Make the interface Layer 2
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport mode hybrid	Configure the mode as trunk
(config-if)#switchport hybrid allowed vlan all	Configure 'allowed VLAN all' on the interface
(config-if)#switchport port-security	Enable dynamic mode port security

(config-if)#switchport port-security maximum 3	Limit secure MAC configuration to three MAC addresses
(config-if)#exit	Exit the interface mode

Note: Port Security is supported on XGS and Qumran1 devices only.

Access Control List

Access Control List (ACL) is a set of rules used to filter traffic. Each rule specifies a set of conditions, such as source address, a destination address, type of packet, or combination of these items. When a device determines that an ACL applies to a packet, it tests the packet under the conditions of all rules. The first match decides whether the packet is allowed or blocked.

Packet filtering helps to restrict network traffic and control network usage by specific users or devices. ACLs filter traffic that passes through the switch and permit or deny packets that cross specified interfaces. An ACL is a collection of “permit” and “deny” conditions that apply to packets. To verify the packet has the specific permissions to be forwarded, the switch compares the fields in the packet against any applied ACLs as soon as a packet is received on an interface. Depending upon the criteria specified in the access lists. It tests packets one by one against the conditions in the access list. The initial match decides whether the switch accepts or rejects the packets.

ACLs provide basic security for the network. It controls which host can access different network parts or which types of traffic are forwarded or blocked. For example, using ACL, it is possible to allow email traffic to be delivered but not telnet traffic.

Based on the following match criteria, OcNOS supports filtering traffic using ACL.

- Source IP address
- Destination IP address
- IP Protocol type
- TCP or UDP source port
- TCP or UDP destination port
- Source MAC address
- Destination MAC address
- Ether Type

Configuring ACLs

Use the following commands to configure an ACL to protect the data plane.

(config)# mac access-list ACL1mac	Create the 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 the ACL mode
(config)# hardware-profile filter ingress-l2 enable	Enable the hardware profile for the ACL
(config)#int xe13	Enter 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 changes
(config-if)#exit	Exit the transaction

BGP FlowSpec Support for IPv4

BGP flow specification (flowspec) allows users to rapidly deploy and propagate filtering and policing functionality among a large number of BGP peer routers to mitigate the effects of a distributed denial-of-service (DDoS) attack over your network.

The BGP flow specification (flowspec) feature allows users to deploy and propagate filtering and policing functionality rapidly between a large number of BGP peer routers and to mitigate the effects of a distributed denial-of-service (DDoS) attack over your network.

It addresses the following needs:

- Drops the traffic.
- Injects it in a different VRF for analysis.

Configure BGP Flowspec

Use the following commands to configure BGP flowspec:

<code>(config)#policy-map type pbr CE1</code>	Configure the policy map type PBR with the policy name
<code>(config-pmap-pbr)# class type traffic ocnos2</code>	Enter the class map traffic class name
<code>(config-pmap-pbr-c)# police rate 21000 bps</code>	Enable the policy rate
<code>(config-pmap-pbr-c)#exit</code>	Exit from the policy map traffic
<code>(config-pmap-pbr)#exit</code>	Exit the from policy map
<code>(config)#policy-map type pbr PE1</code>	Configure the policy map type PBR with policy name
<code>(config-pmap-pbr)# class type traffic ocnos</code>	Enter the class map traffic class name
<code>(config-pmap-pbr-c)# police rate 4444444 bps</code>	Enable the policy rate
<code>(config-cmap-tr)#exit</code>	Exit from the class map
<code>(config)#commit</code>	Commit the configuration
<code>(config)#flowspec</code>	Configure the flowspec
<code>(config-flowspec)#address-family ipv4</code>	Enter the address-family mode with IPv4
<code>(config-flowspec-af)#service-policy type pbr PE1</code>	Enable the service policy type PBR with the policy name
<code>(config-flowspec-af)#service-policy type pbr CE1</code>	Enable service policy type PBR with a different policy name
<code>(config-flowspec-af)#exit</code>	Exit the address family mode
<code>(config-flowspec)#commit</code>	Commit the configuration

Storm Control

Storm Control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of BUM packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

OcNOS provides CLIs to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when the traffic utilization reaches the specified level.

For example

```
# configure terminal
```

```
(config)# interface xe10
(config-if)# storm-control broadcast level 30
```

After the above configuration on interface “xe10”, the broadcast traffic is not forwarded once the incoming packets reach 30% of the interface speed.

STP Root Guard

The standard spanning tree protocol does not provide any means for the network administrator to enforce the topology of the switched Layer2 network securely. Implementing topology is essential in the network with shared administrative control where different administrative entities control one switched network.

Any switch can be the root bridge in a network. The forwarding topology of the switched network is calculated based on the root bridge position, among other parameters. However, the optimal forwarding topology places the root bridge at a predetermined location. In a standard STP, any bridge in the network with a lower bridge ID, takes the role of the root bridge. To secure the root bridge position the administrator sets the root bridge priority to 0. But there is no guarantee against a bridge with a priority of 0 and a lower MAC address.

The root guard ensures the port enabled on the root guard is the designated port. Normally, root bridge ports are all assigned ports. If the bridge receives superior STP BPDU on a root guard-enabled port, the root guard enforces the position of the root bridge by moving the root guard to the root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port.

STP BPDU Guard

The Bridge Protocol Data Unit (BPDU) Guard feature is used along with the PortFast feature. The PortFast feature allows an access port of a switch to transition to the STP forwarding state directly. These access ports should never receive a BPDU.

This feature from OcNOS prevents an attacker from plugging into an access port and acts as a superior switch.

Command Syntax

```
bridge <1-32> spanning-tree portfast bpdu-guard
bridge <1-32> spanning-tree portfast bpdu-filter
no bridge <1-32> spanning-tree portfast bpdu-guard
no bridge <1-32> spanning-tree portfast bpdu-filter
```

Parameters

<1-32>	Specify the bridge group ID
bpdu-filter	Specify to filter the BPDUs on portfast enabled ports
bpdu-guard	Specify to guard the portfast ports against BPDU receive

sFLOW

Sampled Flow (sFlow) is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent embedded in a switch or router and a sFlow Collector.

The sFlow agent samples packets and polls traffic statistics for the device it monitors. The switching or routing device performs the packet sampling at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs and sampled packets to a sFlow collector for analysis.

The sFlow agent samples either packets or counter:

- **Sampling packets:** Packet sampling is done by the hardware at wire speed. At a defined sampling rate, the agent selects one packet as a sample.
- **Sampling counters:** Interface statistics such as generic and Ethernet counters are polled at a defined interval. Enable sFlow and a collector before enabling sFlow sampling on an interface.

sFlow feature is supported on physical interface and LAG interface. Configuring sampling on a LAG interface enables sampling on all member ports that are part of that LAG interface

Configure sFlow

Use the following commands to configure sFlow.

#configure terminal	Enter the 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
(config)#interface xe1	Enter the 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 the ingress directions
(config-if)#sflow sampling-rate 1024 direction egress max-header-size 120	Set the sFlow sampling interval on the interface in the egress directions
(config-if)#sflow enable	Start packet sampling on the interface
(config-if)#end	Exit the interface and configure mode

Port Isolation for MLAG

The feature prohibits communication between Isolated ports across MLAG switches. The protected port communicates with an unprotected port and vice-versa. Protected ports prevent the exchange of unicast, broadcast, or multicast traffic between ports on the same switch to prevent one neighbor from seeing the traffic generated by another.

Background Port Isolation Security

Port Isolation (PI) allows the traffic of multiple downstream clients to access the upstream infrastructure (such as servers, services, of the Internet) while restricting the communication between downstream clients or entities.

PI works with the following types of ports:

- Promiscuous ports
- Isolated ports
- Community ports

Promiscuous ports guarantee connectivity to upstream servers and devices. Any traffic arriving on Isolated, Community, or other Promiscuous ports is directed towards Promiscuous ports. Traffic received on Promiscuous ports is then transmitted to any different port.

Isolated Ports ensure that the attached clients send and receive traffic only to or from Promiscuous ports.

Community Ports ensure that traffic from attached devices is sent to only Promiscuous ports and ports that are part of the same community. The Community ports do not forward traffic to and from Isolated ports.

The traffic patterns and the associated rules provide a configurable security settings according to user needs.

Typical examples of deployments that use this feature are fiber-to-the home or enterprise.

The enhancements to Port Isolation just extend the rules to MLAG ports in a pair of switches that are configured to provide MLAG redundancy.

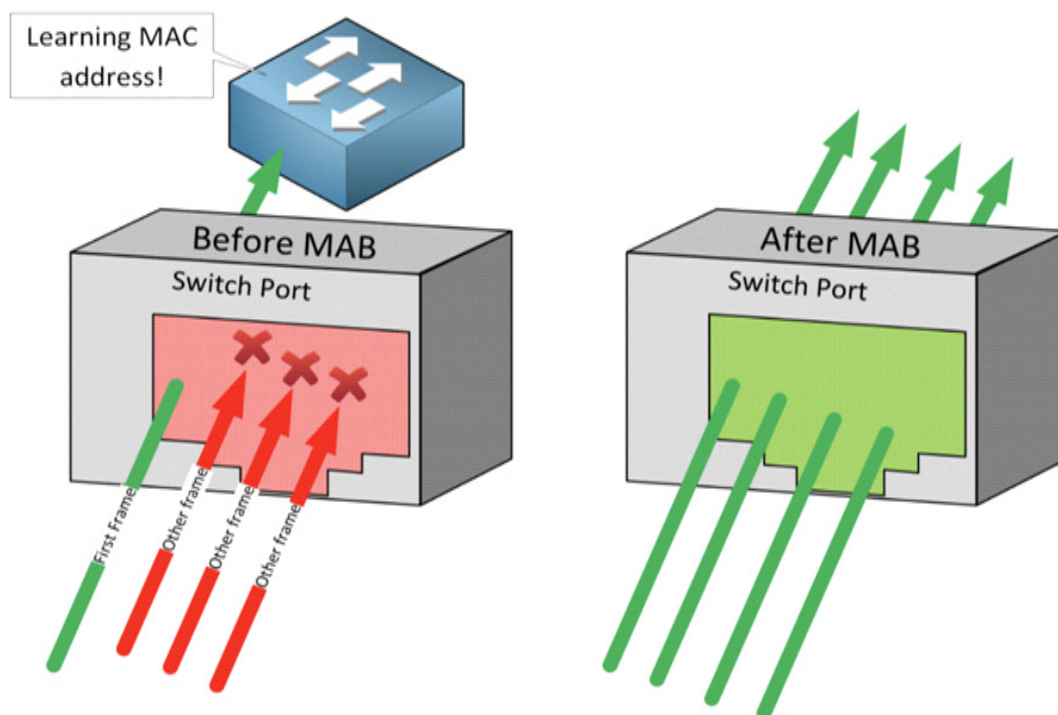
Configuration

For simplicity only the port configuration is illustrated here.

```
interface mlag1
switchport
switchport protected promiscuous
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
load-interval 30
shutdown
!
interface mlag2
switchport
switchport protected isolated
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
load-interval 30
!
interface mlag3
switchport
switchport protected community
bridge-group 1
switchport mode trunk
switchport trunk allowed vlan all
load-interval 30
!
```

MAC Authentication Bypass (MAB)

MAC Authentication Bypass (MAB) is used for a non-authenticating device (a device without an 802.1X supplicant running on it) connecting to a network with 802.1X enabled. With 802.1X authentication, the switch sends an identity request (EAP-Identity-Request) periodically after the link state is changed to “up.” Additionally, the endpoint supplicant sends a periodic EAP over LAN Start (EAPoL-Start) message into the switch port to speed up authentication. If a device cannot authenticate, it must wait until the dot1x timeout occurs, and MAC Authentication Bypass (MAB) will occur. It can access the network if the device's MAC address is in the correct database.



When we enable MAB on a switch port, the switch drops all frames except for the first frame to learn the MAC address. Any frame can be used to understand the MAC address except for CDP, LLDP, STP, and DTP traffic. Once the switch has learned the MAC address, it contacts the RADIUS authentication server to check if it permits the MAC address.

Configure MAC Authentication Bypass

Use the following commands to configure MAC Authentication Bypass.

Switch#configure terminal	Enter the configure mode
Switch(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1
OcNOS (config)#commit	Commit the configuration to be running configuration
Switch(config)#dot1x system-auth-ctrl	Enable dot1x authentication globally
Switch(config)#auth-mac system-auth-ctrl	Enable the MAC authentication bypass globally
Switch(config)#radius-server dot1x host 10.1.1.1 key 0 testing123	Specify the host IP and key with string name between the RADIUS server and client
Switch(config)#commit	Commit the transaction
Switch(config)#interface xe0	Configure the interface xe0
Switch(config-if)#switchport	Enable the switch port on the interface
Switch(config-if)#bridge-group 1	Associate the bridge to an interface
Switch(config-if)#switchport mode access	Configure the port as access
Switch(config-if)#dot1x port-control auto	Enable authentication (through RADIUS) on port (xe0)
Switch(config-if)#dot1x mac-auth-bypass enable	Enable MAC authentication bypass on the interface
OcNOS (config)#commit	Commit the configuration to the running configuration
Switch(config)#interface xe9	Configure interface xe9

Switch(config-if)#ip address 10.1.1.2/24	Set the IP address on interface xe9
Switch(config-if)#commit	Commit the transaction
Switch(config-if)#end	Exit the configure mode

OS Security

OS security involves the implementation of control techniques that protect your assets from unauthorized modification, deletion or theft. The common techniques used to protect operating systems include the use of antivirus software and other endpoint protection measures, regular OS patch updates, a firewall for monitoring network traffic, and the enforcement of secure access through least privileges and user controls.

Filesystem Capabilities

The need for setuid applications can be omitted through the application of filesystem capabilities using Xattrs available in Debian OS. This helps in preventing the misuse of vulnerable setuid applications.

Programs are vulnerable to set-UID; root privileges are not required every time for a process to run. It is logical to provide a minimal set of privileges to programs that can enable the programs to run effectively. With the normal set-UID approach, programs would run more than the required privileges, increasing the risk of privilege escalation. Using the filesystem capabilities, a program can be provided only with sufficient privileges to run effectively, thereby reducing any security risk that could potentially be caused by this program if it runs with root privileges.

SMACK

Simplified Mandatory Access Control Kernel (SMACK) allows you to use special-purpose, custom ACLs or mandatory ACLs to protect data and interactions from attackers. It secures Linux kernel from being compromised.

Stack Protector

Gcc's `-fstack-protector` provides a randomized stack canary that protects against stack overflows and reduces the chances of arbitrary code execution via controlling return address destinations.

Pointer Obfuscation

Some pointers stored in glibc are obfuscated through `PTR_MANGLE/PTR_UNMANGLE` macros internally in glibc, preventing libc function pointers from being overwritten during runtime.

Libs/mmap ASLR

In OcNOS each execution of a program results in a different mmap memory space layout using address space layout randomization (ASLR). This causes dynamically loaded libraries to get loaded into different locations each time. This prevents an attacker from successfully initiating "return- to- libc" attacks.

brk ASLR

Using an offset, brk ASLR provides the capability to randomize memory locations. This is done relative to exec memory.

VDSO ASLR

Virtual Dynamic Shared Object (VDSO) is a Linux kernel mechanism for exporting a carefully selected set of kernel space routines to user space applications so that the application can call these kernel space routines in-process. This reduces performance impact when a context is switched. Typically, latency occurs when the same kernel space routines are accessed using the system call interface. Use VDSO ASLR to protect against “jump-into-syscall” attacks.

Built as PIE

To protect against memory corruption attacks, a program is built as Position Independent Executables (PIE) with “-fPIE -pie”. This protects against “return-to-text” vulnerabilities.

Built with Fortify Source

To secure glibc and to enable protection while compiling or at run-time, build programs using `D_FORTIFY_SOURCE=2` (and `-O1` or higher). Here are some advantages of this approach:

- Prevent memory from overflowing by specifying a maximum length for “sprintf”, “strcpy” unbounded cells.
- Prevent “%n” attacks when the format string is in a writable memory segment.
- Enable validation of operations such as “system,” “open,” or “write” and their function return codes and arguments.
- Ensure when new files are created that explicit file masks are adhered.

Built with RELRO

RELocation Read-Only (RELRO), is a mitigation technique to harden data sections of an Executable and Linkable Format (ELF) process. Use this technique to relocate vulnerable ELF binaries to a read-only location. This protects against memory corruption attacks such as “GOT-overwrite-style.”

Symlink Restrictions

The Time-of-check to Time-of-Use (ToCToU) security issue stems from an issue caused when an attacker takes advantage of the time in between a check and the use of a resource. This occurs when accessing symbolic links. Based on Debian Linux follow only “world-writable sticky directory” symlinks when you own the symlink and the directory that you are accessing.

Hardlink Restrictions

Like symlinks, a hardlink that refers to world-writable, `/etc/`, and `/home/` directories are also subject to attack, especially if the latter two directories reside in the same partition. On their local home directory, a hacker can create a parallel hardlink to the `/etc/` directory, access unauthorized files using the hardlink, or hijack disk resources for world-writable directories. Debian Linux does not permit the use of hardlinks for files that the user cannot read and write, or otherwise sensitive in nature.

Older Protocol Vulnerabilities

Many old protocols are subject to vulnerabilities. Some such protocols include, Remote Desktop Services, NET/ROM, Amateur X.25, X.25, and Digital Equipment Corporation network (DECnet) protocols. Preferably, upload these protocols to the Linux kernel using modprobe, a loadable a loadable kernel module or remove these vulnerable protocols from the kernel.

Memory

Malloc Heap Memory Protection

Use Heap Protector to protect glibc heap memory manager from corrupted-list/unlink/double-free/overflow issues, thereby providing control structures to protect malloc heap memory areas.

Stack ASLR

To prevent locating the exact area from where each program is executed or to prevent a hacker attacking with an executable payload, assign a different space layout in the memory stack.

Exec ASLR

To protect against memory corruption attacks, a program is executed as Position Independent Executables (PIE) with “-fPIE -pie” to load it into different memory locations. This approach helps ward off memory corruption-based attacks since a hacker cannot locate what memory space to attack.

/proc/\$pid/maps Protection

Prevent ASLR attacks from happening by assigning read-only permissions to the "maps" file for This will ensure protection for a particular process or its owner.

Configurable Password Policy

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.

Setting up strong passwords safeguards sensitive data associated with user accounts, including those of employees and customers, against unauthorized access. Once a strong password is set, a five-step process is used to authenticate the user's access.

- Authentication: Authentication is the process of proving the identity of a specific user who can access a system or resource.
- Identification: The process of identifying a specific user, typically using a username within the system or an application.

- Authorization: Authorization grants users rights and privileges following identification, authentication, and authorization.
- Access Control: Access control refers to a security policy defining specific permissions for accessing data, applications, and utilizing resources.
- Encryption: Encryption refers to converting data into an unintelligible form to prevent unauthorized data usage.

Note: For security reasons and to avoid attacks or breaches, change passwords every quarter.

OcNOS manages the user account and password in its OcNOS configuration. The password is reflected in the Linux standard user management database under `/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.

Integrating PAM to OcNOS

Pluggable Authentication Module (PAM) is a third-party authentication tool that allows system administrators to incorporate multiple authentication mechanisms into an existing system by using pluggable modules. In OcNOS, an actual password change doesn't occur while retaining the plain text password. It's set upon execution of `'commit'` and saved only upon execution of `'write'`.

During OcNOS boot, default configuration like `/usr/local/etc/ZebOS.conf` is read and configured by the system. `'username <user name> password <password>'` configuration is also read, and password for the `<username>` in Linux is updated, at this time.

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`.

Kernel

0-Address Protection

Prevent "NULL dereference" kernel attacks by protecting the "NULL" memory space the kernel user space and shared virtual memory addresses, need to be protected so that user space mapped memory cannot start at address 0.

ACL Support Over Management, VTY and Loopback

To protect in-band and management interfaces and management applications enabled on the default VRF, use ACLs. Using an ACL, you can either deny or allow access to specific management applications via the management interface. Additionally, secure the in-band interfaces with loopback interface ACLs, thereby safeguarding management applications, such as Teletype Network (telnet), Secure Shell (SSH), Network Configuration Protocol (NetConf), Network Time Protocol (NTP), Simple Network Management Protocol (SNMP) and SNMP Traps.

DHCP Relay Option 82

DHCP Relay Agent Information Option 82 (Option 82) uses a DHCP relay agent to allocate network addresses. In this way, it injects a layer of troubleshooting, accounting, and authorization protection, and prevents untrusted sources from making a DHCP client request. Remote IDs that belong to end users are recognized using Option 82 remote ID format. When forwarded packets contain Option 82, it ensures that any DHCP request is accompanied with the remote ID and the agent circuit ID information.

OcNOS Scan with Security Database

With IP Infusion's commitment to security, routine security audits ensure that current and potential vulnerabilities are identified and mitigated. These audits include the latest CVE database, a comprehensive list of publicly disclosed cybersecurity vulnerabilities. By staying abreast of the latest CVEs, OcNOS is protected from potential threats.

Security Database	Origin	Version
NVT	Greenbone Community Feed	20230406T1010
SCAP /CVE/CPE	Greenbone Community Feed	20230406T0511
CERT	Greenbone Community Feed	20230406T0406

Here are some of the specific steps that IP Infusion takes as a part of the OcNOS security suite to ensure product safety:

- Use vulnerability scanners and scripts: A variety of vulnerability scanners and scripts are used to identify potential vulnerabilities in IP Infusion products. These scanners and scripts are regularly updated to tackle the latest vulnerabilities.
- Review the latest CVE database: Staying current with the latest CVE database helps identify any vulnerabilities that may affect OcNOS products. If a vulnerability is identified, steps are taken to mitigate the risk, patches are applied or the affected feature is deactivated.
- Track the remediation of vulnerabilities: Periodic validation of remediation strategies ensure vulnerabilities are properly patched or mitigated. This helps protect OcNOS's products from the latest threats.
- Regular Scanning: Scanning for vulnerabilities on a weekly or monthly basis, ensures that any new threats are promptly identified and addressed.
- NESSUS vulnerability scanning: OcNOS devices are scanned regularly using NESSUS scanning capabilities. Issues are immediately recognized and addressed.

The OcNOS software ensures security and guarantees protection for all customer's data. Upon request, IP Infusion can provide OcNOS security audit reports.

Abbreviations

Acronym	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
CBC	Cipher Block Chaining
COPP	Control Plane Protection
DAI	Dynamic ARP Inspection
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
eCryptfs	Enterprise Cryptographic Filesystem
ELF	Executable and Linkable Format
GOT	Global Offsets Table
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPSG	IP Source Guard
MAC	Media Access Control
NOS	Network Operating System
NTP	Network Time Protocol
OOB	Out-Of-Band Management
PIE	Position Independent Executables
RADIUS	Remote Authentication Dial-In User Service
RELRO	Relocation Read-Only
sFLOW	Sample Flow
SSH	Secure Shell
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UID	User ID
VDSO	Virtual Dynamic Shared Object
VLAN	Virtual LAN
VRF	Virtual routing and forwarding