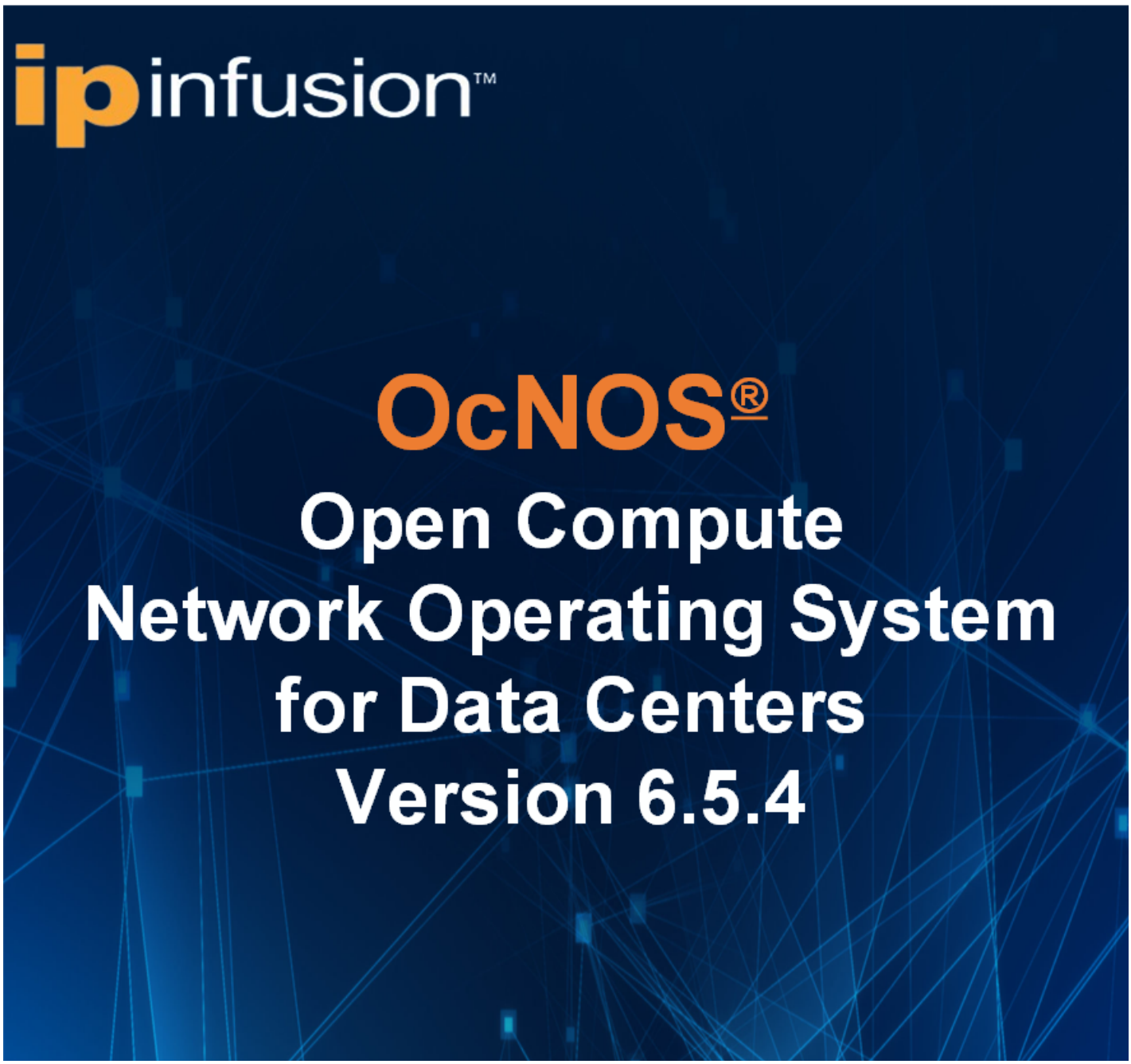



# Release Notes

April 2025

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

# Contents

# 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

Open Compute Network Operating System (OcNOS) 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

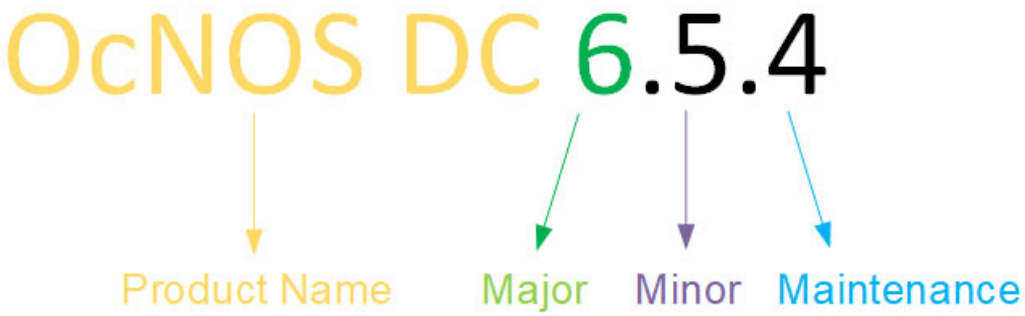
OcNOS works with applications in diverse network environments, including data centers, service provider networks, enterprise networks, and cloud deployments. It provides an open, flexible environment and extensive protocol support for software-defined networking (SDN) and disaggregated networks.

## About this Release

Release 6.5.4 offers new software enhancement features.

## 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 6.5.4

OcNOS DC Release 6.5.4 introduces several software features, and product enhancements along with support for a few new hardware devices.

## Improved Routing

### disable-l3-termination

A new CLI command disable-l3-termination has been introduced to provide finer control over Layer 3 termination behavior in VXLAN deployments. This command allows administrators to disable L3 termination for a specific MAC address within a given VPN context.

With the introduction of this CLI, users can explicitly disable L3 termination for packets ingressing on network ports with destination MAC addresses matching Anycast MACs within a specific VPN. This ensures that such packets are handled as intended, without being unnecessarily uplifted to the CPU.

For more information, refer to the disable-l3-termination section in the *OcNOS VxLAN Guide*, Release 6.5.4.

# Release 6.5.3

OcNOS DC Release 6.5.3 introduces several software features, and product enhancements along with support for a few new hardware devices.

## Enhanced Security and Performance

### BGP Bogon Prefix Filtering IPv4

The BGP Bogon Prefix Filtering feature in OcNOS allows administrators to block invalid or reserved IP addresses from being propagated through BGP. Bogon prefixes, such as unallocated IP ranges or special-use addresses, should not appear in the global routing table to avoid security risks if routed. The new `bgp enable-bogon-filtering` command provides flexibility to manage which prefixes are filtered, ensuring only valid routes are accepted. To implement, administrators can enable filtering for specific IPv4 prefixes. These changes will apply to new BGP updates, with a recommended BGP hard reset to ensure full effect.

For more information, refer to the BGP Bogon Prefix Filtering IPv4 section in the *OcNOS Layer 3 Guide*, Release 6.5.3.

### Max Password Age

The maximum age for a user password for OcNOS is 60 days.The password policy setting describes how long users can
use their password before it expires. This helps the users periodically change their passwords.When a user's password is updated, the expiry is set according to the user's role. This can be modified or updated per user. Once the expiry is set at the user level, the system will check for user-level expiry.

When a user logs in and `cmlsh` is invoked, for the admin the admin user, it is prompted to change the password. A non-admin receives a message to contact the admin to update the password. If the user password has expired and it is not updated witin the next 30 days, the user account is removed from the database.

For more information, refer to the Configurable Password Policy section in *OcNOS System Management Guide,* Release 6.5.3.

### Removing Users with Expired Passwords

When a user's password is updated, the expiration date is set depending on the user's role. This is modified per user. Once the expiry is set, the system will automatically check for expired passwords. When a user login and `cmlsh` is invoked, the user will be prompted to change the password. A non-admin user will receive a message to contact the admin to update the password.

For more information, refer to the Configurable Password Policy section in *OcNOS System Management Guide*, Release 6.5.3.

### Enhanced SSH Encryption Algorithm

The security encryption algorithms used in Secure Shell (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 ciphers 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
- ssh server algorithm kex
- ssh server algorithm mac
- ssh server default algorithm
- show ssh server algorithm

For more details refer to the SSH Encryption section in *OcNOS System Management Configuration Guide,* Release 6.5.3.

# Improved Management

## Enhanced System Management Protocols Support for User-Defined VRFs

OcNOS previously limited support for System Management protocols to the Default and Management VRFs. To address more flexible deployment needs, this support has been extended to allow these protocols to operate within user-defined VRFs. This enhancement improves management plane connectivity and enables better customization for a wider range of network environments.

For more information, refer to the In-band Management over Custom VRF section in *System Management Configuration Guide*, Release 6.5.3.

## Support for HTTPS and SFTP in NetConf

NetConf allows the complete OcNOS configuration to be replaced with a full Command Management Layer (CML) configuration. It also enables the backup of configurations in XML or JSON formats from all databases to a server. Previously, this was limited to insecure methods like HTTP and FTP, but the new feature introduces support for secure methods like HTTPS and SFTP.

For more details, refer to the URL Capabilities section in the *NetConf Configuration User Guide*, Release 6.5.3.

## Modifying Temperature Sensor Threshold Value

The OcNOS platform has been upgraded to modify the default hardware temperature threshold value. Users who wish to adjust the present temperature sensor threshold values for their convenience can change to the desired value.

However, IPI strongly recommends not to modify the default policy as it may lead to hardware component failure.

For more information, refer to the Modifying Temperature Sensor Threshold Value section in the *OcNOS System Management Configuration Guide, Release 6.5.3*.

## Improved SNMP Trap Forwarding Mechanism for Network Element Reboots

Introduced enhancements to the SNMP trap forwarding mechanism for improved reliability during Network Element (NE) reboots. The changes ensure that SNMP traps, including Cold Start traps, are cached and forwarded correctly even when the routing path to the SNMP server is not yet established.

For more information, refer to the snmp-server trap-cache command in the *OcNOS System Management Configuration Guide*, Release 6.5.3.

## User Confirmation Prompt Added for License Release Command

Introduced a confirmation command that prompts users with the message:

"Installed license will be released. Please confirm to proceed? (y/n):"

This ensures that users explicitly confirm their intention before executing the "license release" command, enhancing operational safety and preventing accidental license releases.

For more details, refer to the Installing a Floating License on a Switch section in the *OcNOS License Server Guide*, Release 6.5.3.

## New MIBs for Enhanced SNMP Functionality

OcNOS software ships with additional Management Information Bases (MIBs) to enhance SNMP functionality by separating the physical and logical interfaces in SNMP requests. This feature is disabled by default. To enable it, use the command "snmp ent-ipi-iftable" command.

For more information, refer to the snmp ent-ipi-iftable command in the *OcNOS System Management Configuration Guide*, Release 6.5.3.

# Hardware Platforms

This section provides the new hardware details introduced in the OcNOS 6.5.3 release.

## Edgecore AS9736-64D (Tomahawk 4)

OcNOS supports the AS9736-64D high-performance switch designed for data center and cloud computing environments. It is ideal for large-scale data center deployments that needs super-spine, spine and leaf topologies. It is powered by the 400G Tomahawk 4 (Broadcom BCM56990) chipset with 4x100G port breakout which facilitates the deployment of a super-spine, spine switch supporting 100/400 GbE super-spine to spine or spine to leaf interconnects.

This hardware is equipped with:

- 64 x QSFP-DD switch ports, each supporting 1 x 400G QSFP56-DD, 1 x 100G QSFP28, 1 x 40G QSFP+, or via breakout cables 2 x 200G (2 x 4 lanes 50G PAM4), 4 x 100G (4 x 2 lanes 50G PAM4), 2 x 50G (2 x 2 lanes 25G NRZ), 4 x 25G NRZ, or 4 x 10G NRZ.
- 2 x SFP+ switch ports, each support 1x10 GbE
- Incorporates Broadcom Tomahawk 4 switch series silicon.
- 2 RU form factor.
- Supports hot/cold aisles with front-to-back airflow SKU.
- All ports on front; PSUs and fans accessible from rear.
- Hot-swappable, load-sharing, redundant 2400 W AC/HVDC PSUs.
- 3+1 redundant, hot-swappable fan modules.
- Hardware switch pre-loaded with Open Network Install Environment (ONIE) for automated loading of compatible open source and commercial NOS offerings.

Note: No support for 4x10 and 4x25 in 6.5.2 release.

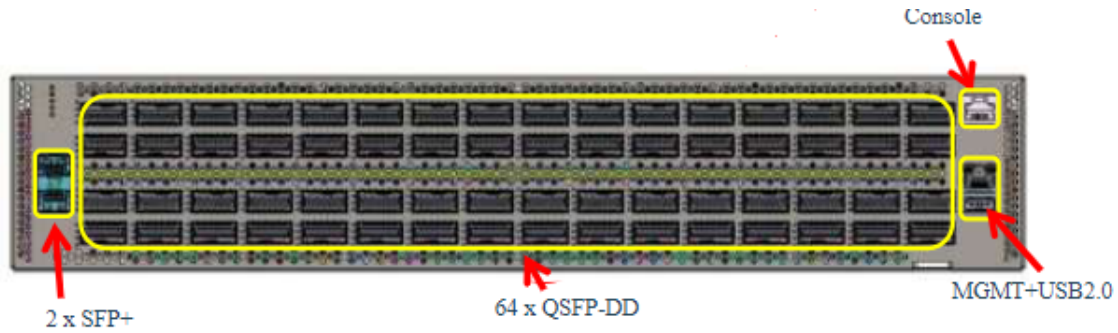



**Figure P-1: Front and Back Panel View**

For more details on the ASIC Model, Ports, SKU, and Hardware Revision, refer to the OcNOS Hardware Compatibility List.

## Edgecore AS9726-32DB (Trident 4)

The OcNOS AS9726-32DB (trident 4 ) Edgecore DCS510 is a spine switch designed for high-performance data centers, providing line-rate L2 and L3 switching across 32 QSFP-DD ports. Each port supports 1x400 GbE or 1x100 GbE, and can be configured with breakout cables to support 4x100 GbE or 4x25 GbE. The DCS510 is ideal for deployment as a spine switch with 100/400 GbE interconnects. This open network switch comes with the Open Network Install Environment (ONIE), allowing the installation of compatible Network Operating System (NOS) software, including both open source and commercial options.

This hardware is equipped with:

- QSFP56-DD switch ports, each supporting 1 x 400 GbE, or via breakout cables 2 x 200G GbE or 4 x 100 and XE ports 10g.
- Upper 16 ports support up to 24 W per transceiver.
- Lower 16 ports support up to 14 W per transceiver.
- Incorporates Broadcom Trident 4 switch series silicon for non-blocking line-rate performance.
- 1 RU form factor.
- Supports hot/cold aisles with front-to-back and back-to-front airflow SKUs.
- All ports on front; PSUs and fans accessible from rear.
- Hot-swappable, load-sharing, redundant 1500 W PSUs.
- 5+1 redundant, hot-swappable fan modules.
- Hardware switch pre-loaded with Open Network Install Environment (ONIE) for automated loading of compatible open source and commercial NOS offerings..

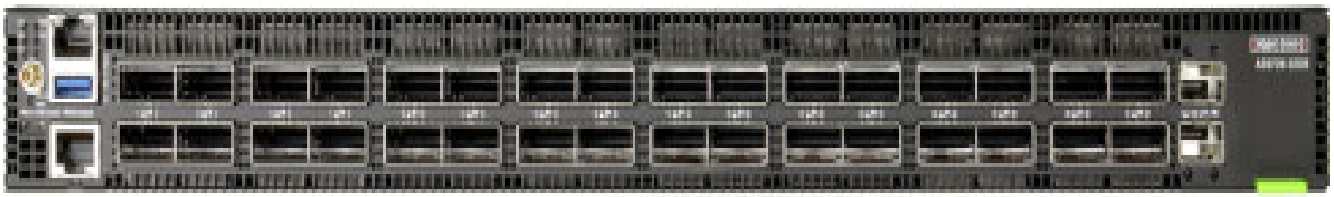


**Figure P-2: Front Panel View**

For more details on the ASIC Model, Ports, SKU, and Hardware Revision, refer to the OcNOS Hardware Compatibility List.

## NEC 400G OpenZR+ Transceiver

The 400G QSFP-DD DCO optical transceiver adheres to OIF 400ZR/Open ZR+ and is intended for use in the DCI/metro network. Digital coherent optical communication technology enables high-capacity and long-distance transmission. The use of NEC‘s compact, high-density mounting technology and the DSP based on a 7nm CMOS process has resulted in a compact size and low power consumption.

Features:

- For DCI/Metro WDM application
- Adhere to the OIF 400ZR/Open ZR+
- Full C-band tunable

# Release 6.5.2

OcNOS DC Release 6.5.2 introduces several software features, and product enhancements along with support for a few new hardware devices.

## Enhanced Security and Performance

### sFlow with Multiple Collector

The sFlow monitoring system is enhanced to add more collectors to receive sample data for analysis. For more information, refer to Configure sFlow for Multiple Collectors in the OcNOS *System Management Guide*, Release 6.5.2.

### Zero Touch Provision on Data Ports

Zero touch provisioning (ZTP), or zero-touch enrollment, is enhanced to perform remote provisioning on two distinct cases: during the new device boot-up before OcNOS is up or after a reboot of the pre-installed OcNOS device. The ZTP is supported on the management interface, all out-of-band, and in-band interfaces that are UP.

The following is not supported in ZTP:

- Downloading licenses via the license server
- Terminating the ZTP process through NetConf

For more information on ZTP, refer to the *Automatic Install using Zero Touch Provisioning* section in the *OcNOS Installation* Guide, Release 6.5.2.

### No IP Unreachable

The no ip unreachable feature is used to prevent the device from sending Internet Control Message Protocol (ICMP) unreachable messages. These messages are typically generated when a router cannot forward a packet because the destination is unreachable.

For more information, refer to No IP Unreachable section in the *System Management guide*.

### Multicast IPv6

The TR3 boards offer a range of IPv6 multicast features that enhance network efficiency, scalability, and control:

**PIM - Sparse Mode (PIM-SM)-IPv6**: Routes multicast packets efficiently across large networks using a central Rendezvous Point (RP) to manage data distribution, ensuring delivery only to requested areas.

**Bootstrap Router (BSR) Mechanism for PIMv6**: Automates RP information distribution, reducing manual configuration and enhancing scalability.

**Static Rendezvous Point Configuration-IPv6**: Allows manual configuration of RPs for greater control and predictability in multicast routing, supporting redundancy with multiple RPs.

**PIM - Source Specific Multicast-IPv6 (SSM)**: Optimizes multicast routing for specific source-receiver pairs, eliminating the need for an RP and reducing resource overhead.

**PIM MIB for IPv6**: Provides tools for monitoring and managing multicast operations, offering insights into routing tables and performance metrics.

**MLD**: Multicast Listener Discovery manages group memberships and controls traffic flow on IPv6 links, directing multicast traffic only to interested receivers.

**Considerations for MLD Snooping Switches**: MLD snooping optimizes multicast traffic by ensuring only interested hosts receive packets, requiring adequate resources for processing and maintaining network scalability.

For more information, refer to *the OcNOS Multicast Configuration Guide*, Release 6.5.2.

## No Support for MPLS

Starting with the OcNOS DC Release 6.5.2x release, MPLS support has been discontinued. Customers are encouraged to review all impacted network configurations and accommodate this change.

## Discard Unknown Multicast Traffic

The Layer 2 switch treats the received multicast packet as unknown when there is no explicit group join request from any of the hosts for the destination group. The unknown multicast traffic is either forwarded to all ports (except the ingress port) within the VLAN or discarded.

A new command `l2 unknown mcast (flood|discard)` is introduced to implement this capability.

This feature enables the option to drop the unknown multicast traffic in any snooping configurations. For example, execute the commands discussed in the IGMP Snooping Configuration section.

This feature is supported on Qumran platforms. It reduces the traffic at the egress node and efficiently uses the hardware resources.

For more information, refer to l2 unknown mcast CLI command reference section in *OcNOS Multicast Configuration Guide*, Release 6.5.2.

## Restricted Access to Privilege Mode based on User Role

The Remote Authentication server behavior is enhanced to support auto enabled privilege level mode based on the user role specified in the authentication server. A new CLI `disable default auto-enable` is introduced to implement it. Executing this CLI removes the default access to the privilege execute mode to any user.

For more information, refer to Restricted Access to Privilege Mode based on User Role CLI command reference in OcNOS *System Management Configuration* Guide Release 6.5.2.

## AAA Support for Serial Console Connection in VRF Management

The remote authentication servers RADIUS or TACACS are enhanced to support the full-fledged AAA solution for serial console connection using the default and management VRF. For more information, refer to AAA Configuration for Console Connection in OcNOS *System Management Guide*, Release 6.5.2.

## BGP MD5 Authentication for BGP Dynamic Peer Groups

The BGP dynamic remote neighbor peer authentication mechanism has been enhanced to accept requests tagged with MD5 signatures.

## EVPN E-Tree

OcNOS enhances Ethernet VPN Ethernet-Tree (EVPN E-Tree) to manage communication within broadcast domains, incorporating redundancy through multi-homing. It optimizes traffic routing and control by categorizing network nodes

based on predefined definitions of EVPN instances as Leaf or Root nodes. OcNOS VXLAN EVPN E-Tree supports efficient traffic control, enhances security by isolating Leaf hosts, provides scalability across network sizes, and improves network performance.

For more information, refer to EVPN VXLAN E-Tree in the *OcNOS Key Feature document*, Release 6.5.2.

# Improved Network Resilience

## LACP Aggregator Force-up

Link Aggregation Control Protocol (LACP) Aggregator Force-Up, an extension to LACP, allows a link to be forced into an active state without successful LACP negotiation. It ensures continuous operation even when connected devices, such as servers during boot stages, might not support LACP or face temporary configuration limitations. Aggregator Force-Up enhances network reliability and flexibility by maintaining active links under various conditions.

For more information, refer to LACP Aggregator Force-up section in the *Layer2 Guide*, Release 6.5.2.

## Enhanced Ping CLI with More Options

The existing `ping` CLI is enhanced with the following additional capabilities:

- Provides additional parameters for count, datasize, interval, broadcast and timeout for both non-enable and enable mode.
- Allows setting of the interval option to zero for both command line and interactive ping options.
- Supports the CLI on VRF, non VRF and VRF management interfaces.

For more information, refer to ping CLI section in the *OcNOS System Management Guide*, Release 6.5.2.

## 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.

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`.

For more information, refer to the Configurable Password Policy section in *OcNOS System Management Guide*, Release 6.5.2.

# Improved Management

## Interface Error Disable for Storm Control

This feature adds storm control as a possible cause to the interface errdisable. If the BUM traffic hits the storm control's bandwidth thresholds, the interface is moved into error disable state. For more information, refer to ErrDisable for Storm-Control Configuration, Fundamental Layer 2 Commands section in the *OcNOS DC Layer 2 Configuration Guide*, Release 6.5.2.

## DHCPv6 Prefix Relay Delegation

OcNOS supports the multiple prefix delegation to a single client. The maximum configurable number of prefixes is between 1 and 64, and the default number is 8.

For more information, refer to DHCPv6 Prefix Delegation Configuration in the *OcNOS System Management Guide*, Release 6.5.2.

## Event Manager

The event manager feature facilitates the automatic execution of an action based on the event (operator log messages) that occurred in a device. When an event has occurred, and if it matches with one of the configured events in the database, then the corresponding action is executed automatically.

For more information, refer to Event Manager in the *OcNOS System Management Guide*, Release 6.5.2.

## Enhanced Streaming Telemetry

OcNOS enhances streaming telemetry capabilities, including dial-out subscription method, poll mode subscriptions, once mode subscriptions, support for the OpenConfig data model, PROTO/JSON encodings, and in-band telemetry in the global and user-defined VRFs. These enhancements benefit network operators by enabling continuous data streaming, on-demand data retrieval, and the availability of additional data models for streaming telemetry.

### Dial Out Mode

Dial-out telemetry or persistent subscriptions ensure continuous data streaming even if the gRPC session terminates unexpectedly. This mode simplifies telemetry subscription configuration and management using standard OpenConfig and IPI data models, enhancing network monitoring and troubleshooting capabilities. Additionally, it facilitates reliable communication between the OcNOS device and collector servers, ensuring uninterrupted data flow for improved network visibility and operational efficiency.

For more information, refer to Streaming Telemetry Dial-Out Mode in the *OcNOS Streaming Telemetry Guide*, Release 6.5.2.

### Poll Mode Subscription

Poll mode subscriptions allow for on-demand data retrieval through a long-lived RPC. Subscribers initiate this mode by sending a Subscribe request message, followed by sending an empty Poll message to receive the desired data.

### Once Mode Subscription

In Once mode subscription, the OcNOS device responds to a subscribe request with a one-time data retrieval, similar to a get request. Upon receiving the “Once mode” subscribe request, the device sends back the subscribe response for all subscriptions in the list and terminates the RPC.

### OpenConfig and IPI Data Model Support

OcNOS supports the OpenConfig data model for both Dial-In and Dial-Out operations. Users can specify the type of XPath (openconfig or ipi) in the origin field of the provided path, allowing for efficient and flexible telemetry configurations. Also, introduces new states that provide insights into the operational status and attributes of various components,

For more information, refer to Streaming Telemetry Data Models in the *OcNOS Streaming Telemetry Guide*, Release 6.5.2.

### PROTO or JSON Encoding

Enhances streaming encoding support by adding PROTO and JSON formats for Dial-in and Dial-out subscriptions. PROTO encoding enables efficient data serialization between clients and the OcNOS device using protobuf messages. This enhancement streamlines data transmission, allowing for fast communication.

JSON encoding extends encoding support to include quoted string values and unquoted number values. JSON encoding is the default setting when the encoding type is unspecified, improving interoperability and simplifying configuration for network operators.

### gNMI In-Band Support

OcNOS enhances gNMI In-Band support to enable streaming telemetry data transmission across any one of the default, management, or user-defined VRFs using the new VRF parameter `feature streaming-telemetry (vrf (NAME|management)|)`. If no specific VRF is configured, streaming telemetry is automatically enabled within the default VRF. This facility increases flexibility in network management by allowing telemetry data transmission across different VRFs.

### Port Number Change for gNMI Server

The gNMI server now listens for incoming gRPC connections on the IANA-defined standard gNMI port number 9339, replacing the previous non-standard port 11162.

Note: This update changes the default dial-in streaming telemetry method to use port 9339, enhancing compatibility and simplifying network configurations.

### Update to gNMI Source Field

The source field in the dial-out gNMI response now uses the MAC address associated with the management port of the host machine or target (e.g., e8:c5:7a:fe:fd:32) instead of the constant string `gnmi_target`. This change ensures that each gNMI device has a unique target ID, allowing the collector to distinguish responses between different targets.

For more information, refer to the *OcNOS Streaming Telemetry Guide*, Release 6.5.2.

## OpenConfig

OcNOS extends support for OpenConfig Translation for ISIS, BGP, VLAN, LACP, LLDP, OSPFv2, QoS, and Tunnel Interface to name a few. This enables network administrators to manage the additional components using standardized YANG models and 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.

For more information, refer to the ISIS OpenConfig Translation, BGP OpenConfig Translation, OSPFv2 Openconfig Translation, LACP OpenConfig Translation, Tunnel Interfaces OpenConfig Translation, VLAN OpenConfig Translation LLDP OpenConfig Translation, QoS OpenConfig Translation sections in the *OcNOS OpenConfig Command Reference* document, Release 6.5.2.

## BFD on LAG Interface

To interop with older routers, where micro-bfd support is not available, a new CLI, "`bfd session`" command, is introduced and operated by a control plane. The BFD packet TX/RX and state machine runs in the control plane.

For more information, refer to BFD Support on LAG Interface section in the *OcNOS Layer 3 Guide*, Release 6.5.2.

## Dynamic Port Breakout

The port breakout functionality supports the division of 100GbE ports into distinct configurations, such as 4x10GbE, 4x25GbE, and 2x50GbE, using a secure and highly reliable breakout cabling solution. Networks today demand a combination of interface speeds, including 10Gb, 25Gb, 40Gb, and 100Gb Ethernet, to accommodate a diverse range of flexible connectivity options. Additionally, cost-effective cabling solutions are crucial to address connectivity needs and facilitate smooth migrations as network speeds and density requirements evolve.

The port breakout feature offers the flexibility to split a 100G port into 4X10G, or 4X25G, 2X50G. When performing a port breakout on the 100G port (ce1), the original port (ce1) is replaced by four 10G ports, namely ce1/1, ce1/2, ce1/3, and ce1/4. All Layer 2 (L2) and Layer 3 (L3) features applicable to normal ports can be executed on these breakout ports.

For more information, refer to Dynamic Port Breakout (100G) on Qumran AX and MX in the *OcNOS System Management Guide*, Release 6.5.2.

## Signal Integrity in QFPP-DD

Signal Integrity in the context of Quad Small Form Factor Pluggable Double Density (QSFP-DD) refers to the maintenance of the quality of electrical signals transmitted and received by the QSFP-DD module. QSFP-DD is a high-speed, high-density interface used primarily in data center applications to interconnect switches, servers, and other networking equipment.

Maintaining signal integrity is crucial in high-speed data transmission because any degradation or distortion of the signals can lead to errors, reduced performance, or even complete failure of communication between devices. In the case of QSFP-DD, which supports data rates of up to 400 Gbps per port, ensuring signal integrity is particularly challenging due to the high data rates and the compact form factor of the module.

This feature provides a way to override the default transceiver signal integrity settings in case they are not enough to achieve a stable electrical connection with the host side peer.

For more information, refer to Signal Integrity in QSFP-DD in the *OcNOS System Management Guide*, Release 6.5.2.

## VLAN to VNID mapping

OcNOS introduces a new method of Virtual Extensible Local Area Network (VXLAN) configuration by mapping a Virtual Local Area Network (VLAN) to a VXLAN network Identifier (VNID). This method allows the configuration of more access ports. Release 6.5.2 introduces the following CLIs to configure and validate the VLAN to VNID mapping:

- `access-if-vxlan`

- `nvo vxlan id <VNID> ingress-replication  bridge-vlan <VLAN ID>`
- `show nvo vxlan vlan-vnid (<VLAN ID> <VNID>) | (<VNID> <VLAN ID>) <VLAN-VNID MAP Summary>`

For more information, refer to VLAN to VNID Mapping in *OcNOS Virtual Extensible Local Area Network Guide*, Release 6.5.2.

# Improved Routing

## Multi Topology Routing in ISIS

Multi Topology (MT) in ISIS allows separate IPv4 and IPv6 address family topologies to be used for routing and to coexist without interference. It enables computation of separate Shortest Path First (SPF) tree, per level and per address family within a single domain.

This release supports MT in address families IPv4 (Topology 0) and IPv6 (Topology 1).

For more information on ISIS Multi Topology, refer to the following RFC: https://datatracker.ietf.org/doc/html/rfc5120.

For configuration information, refer to ISIS Multi Topology in the *OcNOS Layer3 Guide*, Release 6.5.2.

## OSPFv2 Multi-Area Adjacency with Multiple Interfaces

OSPFv2 Multi-Area Adjacency allows configuration of one or more interfaces of the ‘Backbone Area’ (aka 'Area 0') for the same 'Regular Area'.

For more information on ISIS Multi Topology, refer to the following RFC: https://datatracker.ietf.org/doc/html/rfc5120

For configuration information, refer to Multi-Area Redundant Adjacency Configuration in *OcNOS Layer 3 Configuration Guide*, Release 6.5.2.

## Commit Configuration Management

To display the running configuration in JSON or XML format and to view configuration differences between commits respectively, two new CLI commands, '`show json/xml commit config`', '`show json/xml commit diff`”, and “`save cml commit-history WORD`” have been added.

For more information, refer to show json/xml commit config WORD, show json/xml commit diff WORD WORD, and save cml commit-history WORD commands in the *OcNOS System Management Guide*, Release 6.5.2.

## Multi-Line Banner Support

OcNOS provides support for displaying multi-line banner messages, enabling users to configure banner messages spanning multiple lines.

For more information, refer to Multi-Line Banner Support in the *OcNOS System Management Guide*, Release 6.5.2.

few new hardware devices.

# Hardware Platforms

This section provides the new hardware details introduced in the OcNOS 6.5.2 release.

## Edgecore AS4625-54T (Trident 3-X2)

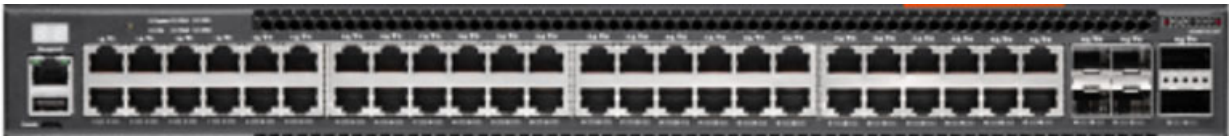
OcNOS supports the versatile AS4625-54T1G switch for 1G/Full advertise in Auto-Negotiation with the RJ-45 copper ports. It is ideal as a management switch in data center networking, enterprise access networking, and campus access networking.

This hardware is equipped with:

- Intel® Atom® COMe module with C3508 4-Core 1.6GHz x86 processor
- Full line-rate L2/L3 forwarding and switching
- Hot-swappable, load-sharing, redundant AC PSUs
- Fixed 2+1 redundant fans
- 1GbE connections to server node and storage node management ports in rack, with uplinks to management network aggregation switches

It includes 54 total ports as follows:

- 48 x 10/100/1000BASE-T RJ-45 ports
- 6 x 1G/10G SFP+ uplink ports



**Port Panel View**

For more details on the ASIC Model, Ports, SKU, and Hardware Revision, refer to the OcNOS Hardware Compatibility List.

## UfiSpace S9110-32X [TR3-X7]

OcNOS provides support for the UfiSpace S91101-32X, a white box data center switch with open network capabilities. This device enables load balancing and provides congestion management.

This hardware is equipped with

- High density 32 x 100G service interfaces
- 3.2Tbps switching capacity,
- Intel® Denverton 4-Cores
- Broadcom Trident3-X7 Silicon
- individual BMC for monitoring and managing equipment health status
- Hot swappable power supplies with 1+1 redundancy support
- Hot swappable fan modules with 2+1 redundancy support

The front panel image below provides a view of all the ports on the device.


**Front and Back Views**

For more details on the ASIC Model, Ports, SKU, and Hardware Revision, refer to the OcNOS Hardware Compatibility List.

## NEC 400G OpenZR+ Transceiver

The 400G QSFP-DD DCO optical transceiver adheres to OIF 400ZR/Open ZR+ and is intended for use in the DCI/metro network. Digital coherent optical communication technology enables high-capacity and long-distance transmission. The use of NEC‘s compact, high-density mounting technology and the DSP based on a 7nm CMOS process has resulted in a compact size and low power consumption.

Features:

- For DCI/Metro WDM application
- Adhere to the OIF 400ZR/Open ZR+

Full C-band tunable

# Security Update

To ensure product security, OcNOS undergoes rigorous vulnerability scanning and promptly addresses any issues that are found. Request a detailed OcNOS Security Report from the IPI sales team.

# Technical Supports

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at https://www.ipinfusion.com/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://www.ipinfusion.com/documentation/ocnos-product-documentation/data-centers/release-6-5/.

For training videos, visit: https://www.ipinfusion.com/ocnos-zero-to-hero-training-videos/.

For a list of supported platforms and SKUs of OcNOS features, refer to the feature matrix https://www.ipinfusion.com/documentation/ocnos-feature-matrix/.

## Technical Sales

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