# OcNOS®

## Open Compute Network Operating System for Service Providers Version 6.4.2

Release Notes

07 March 2024

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

# Contents

# Introduction

## Overview

OcNOS for Service Providers (SP) 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. With a focus on Aggregation Router and Cell Site Router Solutions for efficient 4G/5G rollout, IP Infusion offers disaggregated solutions that cut costs, expand the vendor landscape, and enable agile service introduction through automation.

The shift to 5G introduces architectural changes in RAN and mobile core, impacting transport capacity and service provisioning. The mobile transport network supports legacy 2G/3G/4G deployments in addition to 5G rollout while adapting to varying traffic flows, catering to diverse use cases from augmented reality to industrial automation. Disaggregation is pivotal, separating networking software from hardware to enhance programmability, automation, and control, resulting in better network management and potential cost savings.

Rising network traffic due to remote work applications has prompted efficient data and performance management. Service Providers must deliver high-performance services reliably, efficiently, and securely. Robust carrier-grade capabilities are needed for effective broadband aggregation and edge routing, accommodating the escalating capacities required for advanced networks. This enables efficient management of high-traffic volumes across applications like mobility, cloud networking, video, and gaming.

## OcNOS Software

Open Compute Network Operating System (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.

# About this Release

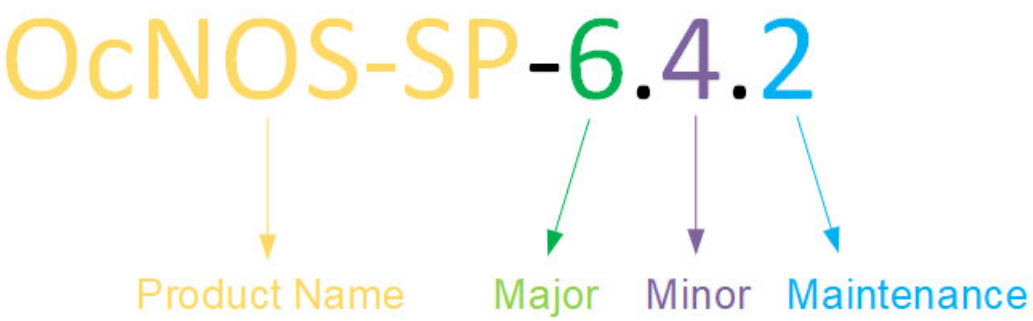
OcNOS-SP Release 6.4.2 introduces new open 400G ZR/ZR+ optics and multiple software enhancements. This document provides a high-level overview of these additions, highlighting their main capabilities and benefits.

## IP Maestro Support

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

## IP Infusion Product Release Version

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




**Product Name:** IP Infusion Product Family

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

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

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

# Release 6.4.2

## Enhanced Security and Performance

### Support for RADIUS Authorization

The current implementation of Remote Authentication Dial-In User Service (RADIUS) authentication assigns ‘Privileged Exec’ mode to any user irrespective of the user’s privilege. This behavior is modified in the current release. The RADIUS server is enhanced with an authorization service to assign the Exec or Privileged Exec mode to the authenticated users based on the privilege level.

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

### Seamless BFD on Qumran2

Seamless-BFD is a simplified mechanism for using BFD with a large proportion of negotiation aspects eliminated. In network traffic, S-BFD detects a link failure, and the traffic immediately switches to a backup path. The traffic returns to primary once the link is up or the corresponding path becomes active. S-BFD provides a quick convergence time of 50 milliseconds.

For more information on Seamless BFD On Qumran2, refer to OcNOS Key Feature document, Release 6.4.2.

## Support of 2.5G Speed on Edgecore AS5912-54X Switch

Enhanced support for OcNOS on the Edgecore AS5912-54X switch now enables to use 2.5G speed on 48 ports. This enhancement broadens the switch's capabilities beyond the initiadlly supported speeds of 10M/100M/1000M and 10G on 48 ports. The ports designed for 10G speed can now be configured for 2.5G.

For more information, see the Support of 2.5G Speed on Edgecore AS5912-54X Switch section in the OcNOS Key Feature document, Release 6.4.2.

# Open 400G ZR/ZR+ Optics Support

This section provides the new ZR/ZR+ transceiver details introduced in the OcNOS 6.4.2 release with some use cases:

- **Long-haul optical communication** allows seamless data transfer between long distances, typically around 400 kilometers. It uses the DWDM technology, allowing for efficient data transport over long distances.

  **Benefits** - The efficient transportation of data over longer distances without signal degradation.

- **Metro connection** is the network infrastructure that provides the connectivity within a metropolitan area. It also uses the DWDM technology.

  **Benefits** - The data transfer is highly reliable with high bandwidth.

- **Data Center Interconnect** uses open 400G ZR/ZR+ optics for a high bandwidth single-span direct link between two data centers.

  **Benefits** - The high bandwidth and low latency support the applications requiring real-time data transfer.

## Ciena 176-3580-900

OcNOS supports WaveLogic 5 Nano (WL5n) 100G–400G Standard QSFP-DD transceivers with advanced coherent optical technology. This transceiver is a critical component of an Open Line System (OLS) and is compatible with Qumran2A and Qumran2C platforms. The dBm value of -10 provides sufficient signal power for the data transmission. The low power consumption and transport costs make it beneficial.

**Figure 1: WaveLogic™ 5 Nano 100G–400G Standard QSFP-DD Transceiver**

| Vendor | Part Number | SKU | Type | Form Factor | Interface | Reach | Temperature |
|---|---|---|---|---|---|---|---|
| Ciena | 176-3580-900 | OcNOS-SP-PLUS | ZR+ | QSFP-DD | 400G | 480km | Commercial |

## Coherent FTCD3323R1PCL

OcNOS supports the FTCD3323R1PCL transceiver, which supports multi-rate coherent transmission. Multi-rate coherent provides flexible data transmission speed based on the network requirements. This transceiver is a critical component of an OLS and is compatible with Qumran2A and Qumran2C platforms. The inbuilt EDFA and the dBm value of 0 provides high signal power for the data transmission with a high reach of 600 kilometers.

**Figure 2: 400G ZR+ QSFP-DD-DCO Transceiver**

| Vendor | Part Number | SKU | Type | Form Factor | Interface | Reach | Temperature |
|---|---|---|---|---|---|---|---|
| Coherent | FTCD3323R1PCL | OcNOS-SP-PLUS | ZR+ | QSFP-DD | 400G | 600km | Commercial |

# Improved Management

## PTP SMPTE Profile Support

The Timing and Synchronizing functionality on OcNOS is enhanced to support SMPTE Precision Time Protocol (PTP) profile.

The SMPTE PTP profile is based on IEEE Standard 1588-2008 and includes a description of parameters, their default values, and permitted ranges. This standard specifies a PTP for synchronizing audio/video equipment in a professional broadcast environment.

The SMPTE ST 2059-2 profile defines a point in time, the SMPTE Epoch, which is used for the alignment of real-time signals; formulae that specify the ongoing alignment of signals to time since the SMPTE Epoch; and formulae that specify the calculation of SMPTE ST 12-1 time address values and SMPTE ST 309 date values.

For more information, see the PTP SMPTE Profile Support section in the OcNOS Key Feature document, Release 6.4.2.

## Enhanced Streaming Telemetry Platform States

Streaming Telemetry in OcNOS introduces new platform states that provide an understanding of the operational status and attributes of various components, including memory, board Field Replaceable Unit (FRU), and temperature. The inclusion of these platform states enhances visibility into the health and performance of the networking hardware,

enabling network administrators to access information and improve their ability for enhanced management and troubleshooting.

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

# Improved Routing

## New Ingress-l2-subif and Ingress-ipv4-subif Group

Introduced two new parameters in the command "hardware-profile filter" to support L2 ACL and IP ACL over sub-interfaces with an optimized group, featuring a 160-bit width size. It enables the simultaneous attachment of L2, L3 V4/V6 ACLs, and QoS policers. Additionally, users can now activate EVPN VXLAN/MPLS features.

For more information, see the System Configure Mode Commands section in the OcNOS System Management guide, Release 6.4.2.

# Improved Network Resilience

## EVPN Active-Standby Single-Active

EVPN Active-Standby in OcNOS provides a solution for availability and resiliency in network environments. By implementing Single-Active redundancy mechanisms within the EVPN Multihoming framework, OcNOS ensures continuous connectivity even in the event of a Provider Edge (PE) device failure. With Single-Active, one PE device remains active while the other stands by, ready to take over if needed. This feature enhances network fault tolerance, minimizes downtime, and optimizes data exchange, improving network reliability.

For more information, refer to the EVPN Active-Standby section in the OcNOS MPLS Guide, Release 6.4.2.

## Entropy Labels for OSPF Segment Routing

Entropy Labels (ELs) are designed to improve load balancing in MPLS networks. This approach simplifies the load-balancing procedure, leading to increased efficiency and flexibility.

For more information, see the Entropy Labels for ISIS or OSPF Segment Routing section in the *OcNOS Key Feature document*, Release 6.4.2.

# Release 6.4.1

OcNOS-SP Release 6.4.1 introduced a new Broadcom J2C+ based Aggregation Router, along with several software features, and product enhancements.

## Hardware Platform

This section provides the new hardware details introduced in the OcNOS 6.4.1 release.

### UfiSpace S9610-36D

With OcNOS support for the UfiSpace S9610-36D, the combination of hardware and software ensures seamless integration, introducing advanced networking features, management capabilities, and streamlined operations. This hardware is equipped with Broadcom's cutting-edge Jericho 2C+ chipset, delivering speed and performance for networking needs. With 14.4Tbps of throughput, this device meets connectivity standards and ensures the ability to keep up with network demands. This 36 x 400G disaggregated open router empowers high capacity networks and drives the evolution of 5G services and future applications.

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

**Figure 3: UfiSpace S9610-36D**

The table below provides hardware details for the device, including the switching ASIC, port configuration, hardware revision, and SKU.

| SWITCHING ASIC | PORT CONFIGURATION | HARDWARE REVISION | SKU |
|---|---|---|---|
| Broadcom J2C+ BCM | 36x400G QSFP-DD | Label Revision: N/A<br>Diag Version: 0.1.2 CPLD 1 Version: 0.1 CPLD 2 Version: 0.1 CPLD 3 Version: 0.1 | OcNOS-SP-IPADV-CE-AGGR-14400<br>OcNOS-SP-PLUS-14400<br>OcNOS-SP-IPBASE-14400<br>OcNOS-SP-MPLS-14400 |

For more information, refer to the **S9610-36D Port Mapping** chapter in the *OcNOS UfiSpace Install Guide*, Release 6.4.1.

### Edgecore AS5916-54XKS-OT

OcNOS introduces support for the Edgecore AS5916-54XKS-OT variant, equipped with a Trusted Platform Module (TPM) chip. The TPM chip enhances the security features of this platform, providing data encryption, secure boot, and authentication for network management and operation.

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

**Figure 4: Edgecore AS5916-54XKS-OT**

The table below provides hardware details for the device, including the switching ASIC, port configuration, hardware revision, and SKU.

| SWITCHING ASIC | PORT CONFIGURATION | HARDWARE REVISION | SKU |
|---|---|---|---|
| Qumran-MX BCM88375_B0 | 48 x 10G SFP+ ports<br>6 x 100G QSFP28 ports | Label Revision: R03E<br>CPLD 1 Version: 15<br>CPLD 2 Version: 7<br>Fan CPLD Version: 3 | OcNOS-SP-CSR-800<br>OcNOS-SP-IPBASE-800<br>OcNOS-SP-MPLS-800<br>OcNOS-SP-IPADV- CE-AGGR-800 |

For more information, refer to the **Edgecore AS5916-54XKS-OT Port Mapping** chapter in the *OcNOS Edgecore Install Guide*, Release 6.4.1.

# Enhanced Security and Performance

## NetConf Port Access Control and TCP Port Closure

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

This feature supports the following:

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

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

## Role-Based Access Control

Role-Based Access Control (RBAC) in OcNOS allows the creation of custom user roles locally, providing administrators with the flexibility to define specific groups of commands that they can allow or deny for each role. Users can be assigned to these user roles on a per-switch basis or by utilizing a TACACS+ server.

For more information, refer to the Role-Based Access Control section in the *OcNOS Key Feature document*, Release 6.4.1.

## Hide the Remote AS using the neighbor local-as CLI

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

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

## Port Breakout (100G) for AS7316-26XB (Qumran-AX) Platform

The AS7316-26XB Qumran1 device accommodates a combination of port breakout options with hybrid port speeds. On this device, The AS7316-26XB supports 16 (xe0 to xe15) 10GbE SFP+ ports, 8 (xe16 to xe23) 25GbE SFP28 ports and 2 (ce0 and ce1) 100 GbE QSFP28 ports. Using port breakout, divide the 100Gr QSFP28 ports (ce0 and ce1) into 4X25G configurations if desired.

For more information, refer to Port Breakout (100G) for 26XAS7316-26XB (Qumran-AX) Platform *OcNOS Key Feature* document, Release 6.4.2.

## Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform

The S9500-30XS Qumran1 device accommodates a combination of port breakout options with hybrid port speeds. On this device, supports 20 (xe0 to xe19) 10GbE SFP+ ports, 8 (xe20 to xe27) 25GbE SFP28 ports and 2 (ce0 and ce1) 100 GbE QSFP28 ports. Using port breakout, divide the 100Gr QSFP28 ports (ce0 and ce1) into 4X25G configurations if desired.

For more information, refer to Port Breakout (100G) for S9500-30XS (Qumran-AX) Platform *OcNOS Key Feature* document, Release 6.4.2.

## Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform

The AS7315-27X Qumran1 device accommodates a combination of port breakout options with hybrid port speeds. On this device, configure 4 ports (port 1-4) with 25G Ethernet SFP28 interfaces, 20 ports (port 5-24) with 10GbE SFP+ interfaces, and 3 ports (port 25-27) with 100G Ethernet QSFP28 interfaces. Using port breakout, divide the 100G QSFP28 ports (ce0, ce1, and ce2) into 4X25G configurations if desired.

For more information, refer to Port Breakout (100G) for AS7315-27X (Qumran-AX) Platform *OcNOS Key Feature* document, Release 6.4.1.

## Port Breakout (400G) for Qumran2 Series Platforms

The port breakout capability offers a robust and secure solution to divide 400GbE ports into multiple ports, ensuring a reliable network infrastructure. In today's networks, there is a demand for a diverse range of Ethernet interface speeds, including 10GbE, 25GbE, 40GbE, and 100GbE. It is essential to have a variety of cost-effective cabling options. This flexibility is crucial to address connectivity requirements and facilitate seamless migrations as network and density needs continue to evolve.

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

## Support IGMP Snooping for Provider Bridge

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

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

Note: The IGMP snooping has been enabled for SVLAN only

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

## TCP MSS for BGP neighbors

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

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

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

## TCP MSS Configuration for LDP sessions

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

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

## TWAMP-One Way Measurement

The TWAMP-One Way Measurement feature has been designed for meticulous measurement of forward and reverse delays within TWAMP. This cutting-edge capability requires the synchronization of high-precision timing, offering a new level of network performance analysis.

For more information, see the delay-profile interfaces subcommands section in the *System Configure Mode Commands*, Release 6.4.1.

## Two-Way Active Measurement Protocol Client

The Two-Way Active Measurement Protocol (TWAMP) Client stands as a robust network performance measurement feature implemented on routers. It takes charge of initiating and managing network performance tests, and serves as a crucial part of the control session. Paired with a TWAMP server, it enables bi-directional measurements, allowing for comprehensive assessment, troubleshooting, and quality of service assurance within the network infrastructure. This feature is instrumental in maintaining optimal network performance and reliability.

For more information, see the Two-Way Active Measurement Protocol Client section in the *OcNOS Key Feature document*, Release 6.4.1.

## Increase the Limit of BGP peers in a Peer-Group

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

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

## EVPN-IRB for OSPF or ISIS for Single-Homing

Ethernet VPN with Integrated Routing and Bridging (EVPN-IRB) with OSPF or ISIS for single-homing is a feature designed to enhance the efficiency and simplicity of network connectivity in single-homing scenarios. This solution brings together the power of EVPN-IRB and the routing capabilities of OSPF or ISIS, making it an ideal choice for various network environments. This feature streamlines the network infrastructure, making it easier to manage the network's Layer 3 routing while seamlessly integrating with EVPN-MPLS.

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

## Password Strength Enhancements

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

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

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

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

## RADIUS Server Authentication Failure and Fallback

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

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

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

By default, the fallback to local authentication is applied when the RADIUS server is unreachable.

For more information, see Fall Back Option for RADIUS Authentication section in the *OcNOS Key feature* document, Release 6.4.1.

## Modified Extended ACL Deny Rule Behavior in VTY

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

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

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

## Timing and Synchronization Support

The OcNOS Precision Time Protocol (PTP) clock and synchronization feature is supported on three Edgecore platforms (AS7946-30XB, AS7946-74XKSB and AS7535-28XB (Hardware Revision 2)).

The GrandMaster clock synchronization feature is not supported on these platforms in Release 6.4.1.

For more information, refer to the *Precision Time Protocol Configuration* section in the *OcNOS Timing and Synchronization Guide*, Release 6.4.1.

## PTP G.8275.2 Profile Source IP as Loopback

This feature enables the loopback IP address on a Precision Time Protocol (PTP) clock port. The master device manages and monitors the slave device by configuring a single source IP loopback address in the PTP port of the master device. The single source IP means that the slave device has only one IP address for the PTP port. This feature helps continuously keep the PTP active by using a loopback IP address even when a device interface is down.

For more information, refer to the PTP G.8275.2 Profile Source IP as Loopback Configuration chapter of the *Precision Time Protocol Configuration* section in the *OcNOS Timing and Synchronization Guide*, Release 6.4.1.

## 400G PM Alarm

The 400G Performance Monitoring (PM) alarm monitors and detects performance issues like the bit error rate and signal power in the network. This feature extends OcNOS performance-related monitoring capabilities and provides additional performance monitors and alarms.

Access the additional set of 400G performance monitoring parameters, such as Transmitter FEC Detected Degrade (Tx FDD), Transmitter FEC Excessive Degrade(Tx FED), Receiver FEC Detected Degrade (Rx FDD), and Receiver FEC Excessive Degrade (Rx FED), to receive an automatic alarm notification on the CLI interface, via an SNMP trap, or through the Netconf interface. The automatic alarm is triggered when the monitored parameter crosses the configured value.

For more information, refer to the 400G PM Alarm section in the *OcNOS Key Feature document*, Release 6.4.1.

# Improved Network Resilience

## Entropy Labels for ISIS Segment Routing

Entropy Labels (ELs) are designed to improve load balancing in MPLS networks. This approach simplifies the load-balancing procedure, leading to increased efficiency and flexibility.

For more information, see the Entropy Labels for ISIS or OSPF Segment Routing section in the *OcNOS Key Feature document*, Release 6.4.1.

## ERPS with CFM Down-MEP over Bridge-Domain

In OcNOS, ERPS with CFM Down-MEP over Bridge-Domain combines the benefits of Ethernet Ring Protection Switching (ERPS) with Continuity Fault Management (CFM), ensuring faster traffic switchover and enhancing network resilience. This feature enables the configuration of ERPS over Layer 2 sub-interfaces mapped under bridge-domains, optimizing network resource utilization. It offers the flexibility to configure Layer 2 sub-interfaces as ring ports and supports the creation of multiple ERPS instances for various logical ERPS rings.

For more information, refer to the ERPS with CFM Down-MEP over Bridge-Domain section in the *OcNOS Key Feature document*, Release 6.4.1.

## SR-Policy Mapping to Seamless BFD

Seamless Bidirectional Forwarding Detection (SBFD) monitors the policy best path, when seamless BFD detects any link failure, a backup candidate path is activated for end-to-end protection. If the best path link is up, traffic switches again from the backup path to the primary path.

EVPN and SBFD features doesn't work when configured simultaneously in Qumran-UX and Qumran-AX series platforms.

## RSVP Detour Over Ring Topology

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

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

## IS-IS Protocol: Robust TLV Handling

The IS-IS protocol relies on Type-Length-Value (TLV) encoding within Protocol Data Units (PDUs) to convey critical information. To support ongoing protocol evolution while preserving backward compatibility, IS-IS implementations gracefully manage unrecognized TLVs.

This adaptive approach extends to sub-TLVs nested within TLVs and IS-IS ensures protocol integrity by independently validating PDUs regardless of TLV validation. This guarantees that valid PDUs are accepted, even when specific TLVs exhibit anomalies such as incorrect syntax or data values exceeding expected bounds.

## Commit Rollback

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

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

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

# Improved Management

## Streaming Telemetry

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

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

## CFM over EVPN-MPLS for ELINE Multi-Homing

Enhance network reliability with the Connectivity Fault Management (CFM) feature in OcNOS, now extended to support MultiHoming scenarios. CFM (802.1g, connectivity Fault Management) operations like Continuity-Check Messsage (CCM), Loopback ping (LB), Link-trace (LT) are supported between PE-PE Multi-Homing scenario.

Monitor network connections, efficiently identify faults, and streamline troubleshooting while maintaining robust support for Multi-Homing environments.

For more information, refer to the CFM over EVPN-MPLS for ELINE MultiHoming section in the *OcNOS Key Feature document*, Release 6.4.1.

## Route Monitor

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

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

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

## Enhancements for OpenConfig Translation

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

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

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

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

## NetConf “remove” Operation

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

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

## DHCP Server Group

Dynamic Host Control Protocol (DHCP) Group provides the capability to specify multiple DHCP servers as a group on the DHCP relay agent and to correlate a relay agent interface with the server group.

This feature helps one configure the DHCP IPv4 and IPv6 groups and attach server IP addresses to the group. Creating a maximum of 32 IPv4 and 32 IPv6 groups per VRF is allowed, and configuring eight DHCP servers is permitted for each DHCP server group.

The DHCP relay agent forwards the request message from the DHCP client to multiple DHCP servers in the group. Forwarding the request message to multiple DHCP servers increases the reliability of obtaining network configuration information.

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

## Custom Syslog

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

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

## Enhanced VE-ID Range

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

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

## VRRP over MLAG with Custom VRF

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

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

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

## Enhanced Graceful Restart

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

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

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

6.4.1.

## SFTP and SCP Enhancements

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

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

## Remove "tech-support" file

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

Currently, there is no way to delete this file. Now the operator has access to a new CLI to remove the log file from the `/var/log` directory.

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

remove file (techsupport)

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

# EVPN Services

## EVPN Active-Standby

EVPN Active-Standby in OcNOS provides a solution for availability and resiliency in network environments. By implementing Port-Active redundancy mechanisms within the EVPN Multihoming framework, OcNOS ensures continuous connectivity even in the event of a Provider Edge (PE) device failure. Port-Active allows multiple PE devices to be active simultaneously, each with specific ports, ensuring efficient traffic routing. This feature enhances network fault tolerance, minimizes downtime, and optimizes data exchange, improving network reliability.

For more information, refer to the EVPN Active-Standby section in the *OcNOS Key Feature document*, Release 6.4.1.

## TWAMP over L3VPN with SRv6

TWAMP over L3VPN with SRv6 feature enhances network performance monitoring with TWAMP over L3VPN, leveraging SRv6 technology for precise measurements. This feature empowers routers to function as Label Edge Router(LERs) and intermediate routers while ensuring configurable accuracy and supporting various L3VPN scenarios. It evaluates link delay metrics to troubleshoot latency and meet SLAs effectively.

For more information, see the TWAMP over L3VPN with SRv6 section in the *OcNOS Segment Routing Configuration Guide*, Release 6.4.1.

## TWAMP over EVPN-L3VPN over SR Configuration

TWAMP over EVPN-L3VPN over SR Configuration feature elevates the network's performance monitoring capabilities with TWAMP over EVPN-L3VPN over SR Configuration. This feature enables precise measurement of network latency and performance. It facilitates the detection of packet loss and empowers efficient network troubleshooting within a seamless EVPN-L3VPN environment with the added advantages of Segment Routing (SR).

For more information, see the TWAMP over EVPN-L3VPN with SR section in the *OcNOS Segment Routing Configuration Guide*, Release 6.4.1.

## TWAMP over L3VPN with SR

Experience enhanced network monitoring and troubleshooting with TWAMP over L3VPN with SR. This feature measures network latency, detects packet loss, and gains access to comprehensive performance metrics, ensuring a more robust and efficient network operation.

For more information, see the TWAMP over L3VPN with SR section in the *OcNOS Segment Routing Configuration Guide*, Release 6.4.1.

### Enhanced EVPN Route Show Command

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

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

## Improved Routing

### Static Route Tracking using Object Tracking (IP SLA)

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

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

### BGP VPNv4 Route Display Command

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

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

### Inbound Route Filter for EVPN

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

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

### Anycast Gateway Routing for Multiple Subnets in EVPN-IRB

The existing feature provides multiple subnet support for EVPN-IRB. Anycast gateway routing for multiple subnets has been enhanced to allow configuration of both Router MAC and Anycast MAC addresses for primary and secondary subnets. It allows the use of either one of these gateways for access to multiple subnets under the Layer 2 VNID.

For more information, see the Anycast Gateway Routing for Multiple Subnets in EVPN-IRB section in the *OcNOS Key Feature document*, Release 6.4.1.

## Sub-Interface Support for PIM (Qumran1 and Qumran2)

Layer 3 Protocol-Independent Multicast (PIM) traffic over the L3 sub-interface is now supported on Qumran-2A/Jericho 2C+ platforms.

For more information, refer to the *OcNOS MPLS Guide*, Release 6.4.1.

## Enable PIM-DM Sub-Interface

Protocol Independent Multicast (PIM)- Dense Mode (PIM-DM) is a data-driven multicast routing protocol. It enables all interfaces to run within each router inside the PIM domain.

For more information, PIM Dense Mode Configuration refer to the OcNOS MPLS document, Release 6.4.1.

## Enable PIM-SM Sub-Interface

Interfaces eth1.1 and eth2.1 are enabled for PIM-SM to participate within each of routers inside the PIM domain. For more information, Enable PIM-SM Sub-Interface refer to the *OcNOS MPLS Guide*, Release 6.4.1

## UDLD Support on Layer 3 Interface

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

The UDLD protocol enables to monitor the physical links and detect when a unidirectional link exists. Upon detection user can either block the port or notify the link status based on the network administration configuration.

UDLD works in two different modes:

- Normal mode
- Aggressive mode

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

# Ethernet Services

## EVPN-ELINE CFM Multihoming

When a multihomed CE is configured as an attachment circuit, the Ethernet Segment Route is sent. The main purpose of this route is to discover other PEs that share the ES and to perform DF elections, fast convergence, and Split Horizon.

Another route sent by PE, when a CE is multi-homed, is the Ethernet A-D Route per EVI. This is used to announce a *l*abel (unicast/alias label) that can be used for load sharing by the remote PEs.

For more information, refer to the section EVPN-ELINE CFM Sub-Interface on Multi-Homing in the *OcNOS Carrier Ethernet*, Release 6.4.1.

## VPWS-CFM and Y.1731 over Sub-Interface

Y1731 extensions of CFM (Connectivity Fault Management) like LM (Loss Measurement), DM (Delay Measurement), and SLM (Synthetic Loss Measurement) are supported on Single Homing scenario of EVPN-MPLS ELINE service.

The network administrator is generally informed about the failure in the connection based on the reception of CCM or by the user. The administrator then initiates Loop Back or Link Trace accordingly to quickly determine and then isolate the fault condition.

The CFM information is conveyed in Protocol frames called CFM PDUs. The CFM PDUs contain the appropriate control and status information used to detect, verify, and isolate faults. It also contains information for path discovery in CFM-enabled links.

Currently, this feature is supported only for EVPN-ELINE Single home and UP MEP services on both Qumran1 and Qumran2 series platforms.

For more information, refer to the section CFM Over VPWS in the *OcNOS Carrier Ethernet*, Release 6.4.1.

## Y.1731 CFM Single Homing

CFM provides capabilities useful for detecting, verifying and isolating connectivity failures in Virtual Bridged Local Area Networks through Continuity Check, Loop Back and Link Trace protocols. These capabilities are used in networks operated by multiple independent organizations, each with restricted access to each other's equipment.

The network administrator is generally informed about the failure in the connection based on the reception of Continuity Check Messages or by the user. The administrator then initiates Loop Back or Link Trace accordingly to quickly determine and then isolate the fault condition.

The CFM information is conveyed in Protocol frames called CFM Protocol Data Units (CFM PDUs). The CFM PDUs contain the appropriate control and status information used to detect, verify and isolate faults. It also contains information for path discovery in CFM-enabled links.

Currently, supported only for EVPN-ELINE Single home and up MEP service on both Qumran1 and Qumran2 series platforms.

For more information, refer to the section EVPN-ELINE Interface on Single Homing in the *OcNOS Carrier Ethernet* , Release 6.4.1.

### Technical Support

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

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

### Technical Documentation

For core commands and configuration procedures, visit: https://docs.ipinfusion.com/service-provider/.

### Technical Sales

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