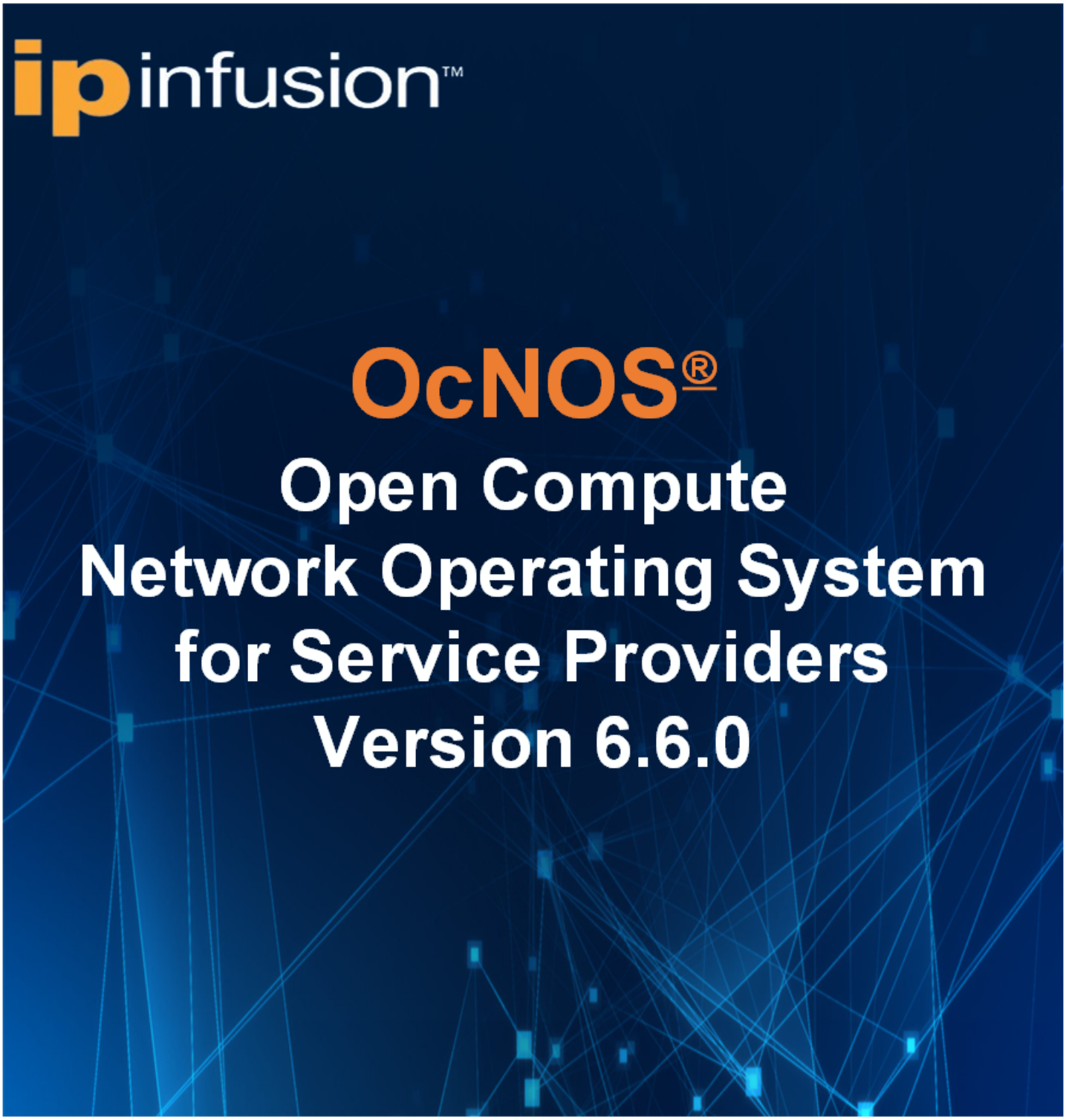


Release Notes

February 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

OcNOS Service Providers (SP) provides a complete solution for access, cell site router and aggregation networks. Support for advanced capabilities such as SR-MPLS, Timing and Synchronization, EVPN Fabric, IP over DWDM with 400G ZR/ZR+ optics, and more is available in OcNOS SP. IP Infusion offers disaggregated solutions that reduces overall Total Cost of Ownership (TCO), expands the vendor landscape, and enables agile service introduction through 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.

Key Benefits of OcNOS

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 benefits of OcNOS:

- Robust Protocol Support
- Network Virtualization
- Programmability and Automation
- 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, extensive protocol support for software-defined networking (SDN) and disaggregated networks.

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 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.

Technical Sales

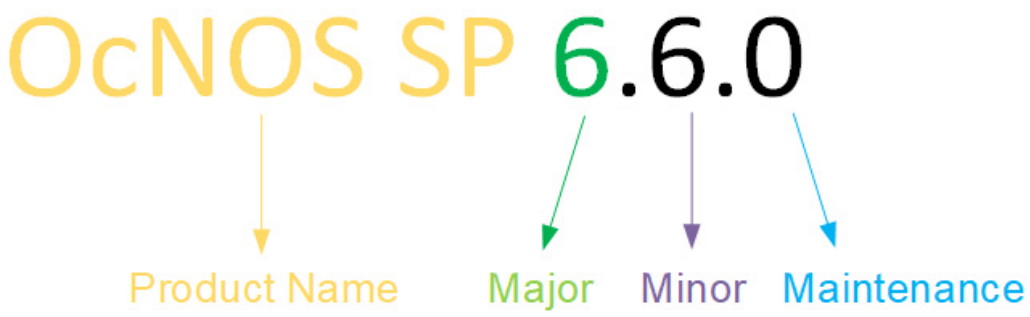
Contact the IP Infusion sales representative for more information about the OcNOS Service Providers solution.

Documentation Disclaimer

OcNOS version 6.6.0 provides an enhanced website experience for select topics included in this release. As a result, some navigational elements on the website may display a few discrepancies.

IP Infusion Product Release Version

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 6.6.0

OcNOS SP Release 6.6.0 introduces several software features, and product enhancements.

Improved Routing

Updating BGP Automated Dynamic Route Policies

The Border Gateway Protocol (BGP) plays a critical role in routing data using route maps, enables precise filtering, and helps modify routing information for optimal advertisement. In OcNOS 6.5.x and earlier, updates to route maps required manual commands to reflect changes in the BGP Routing Information Base (RIB), posing challenges for efficiency.

The introduction of the new bgp auto-policy-soft-reset enable command automates updates to the BGP RIB whenever changes are made to route maps or associated lists. This eliminates the need for manual intervention, simplifying network operations and ensuring seamless updates. With this enhancement, users can avoid executing the `clear ip bgp <> soft in/out` command, as the CLI now handles resets per neighbor or group automatically.

For more information refer to the BGP Automated Dynamic Route Policies Update section in OcNOS *Key Features document*, Release 6.6.0.

SR-Flex Algo for ISIS

OcNOS now supports Flexible Algorithms (Flex-Algo) with IS-IS as the IGP, enabling advanced traffic engineering through customized path computation. In SR environments, Flex-Algo defines routing rules to optimize path selection based on specific network requirements. This capability allows the creation of segregated routing planes, isolating and directing different traffic types through preferred paths to meet distinct service-level agreements (SLAs), especially in 5G networks.

Flex-Algo enables operators to define constraints such as link attributes, latency, and administrative policies, ensuring traffic follows the most efficient route without external controllers. This enhances network efficiency, improves resiliency, and provides deterministic routing for critical applications.

For more information refer to the Flex Algorithm for ISIS section in the *Segment Routing Guide*, Release 6.6.0.

Traffic Steering for Flex-Algo

OcNOS now supports traffic steering using Flexible Algorithms (Flex-Algo) and BGP On-Demand Next Hop (ODN) policies, enabling dynamic and optimized path selection. Flex-Algo directs traffic based on latency, bandwidth, and other network metrics to ensure efficient distribution.

This capability allows OcNOS to compute and adjust optimal paths in real time, adapting to changing network conditions and service demands. BGP UPDATE messages carry color information, with egress PE nodes assigning colors to MPLS service FTNs and advertising them to ingress PE nodes. The ingress node maps the color to an ODN policy, enabling precise and adaptive traffic steering—ideal for 5G and high-performance networks.

For more information refer to the Traffic Steering for Flexible Algorithms section in the *Segment Routing Guide*, Release 6.6.0.

Support for BGP Multiple Large Communities

OcNOS enhances BGP functionality by allowing users to configure multiple large communities in a route map. The character limit has increased from 32 to 255 characters. Additionally, a new `additive` parameter allows users to append large community values to the routes.

For more details, refer to the `set large-community` command in the BGP Commands section of the *OcNOS Layer 3 Guide*, Release 6.6.0.

Static Route Behavior in VRF

OcNOS introduces a new `recursive` parameter in the `ip route` and `ipv6 route` commands. This parameter allows users to enable recursive lookup behavior for the next-hop in each static route, which is disabled by default. It provides control over route resolution. By default, all static routes will be treated as non-recursive unless the user specifies the `recursive` keyword in the static route configuration. For customers upgrading from previous releases, any existing static route configuration will be appended with the `recursive` keyword after the upgrade to version 6.6.0.

Additionally, the egress interface for static routes in a VRF instance is now optional, enhancing configuration flexibility.

For more information, refer to the Fundamental Layer 3 Commands section in the *OcNOS Layer 3 Guide*, Release 6.6.0.

MLAG Active-Standby for VPLS

The Multi-Chassis Link Aggregation (MLAG) Active-Standby for Virtual Private LAN Service (VPLS) feature facilitates the implementation of the MLAG Active-Standby between the VPLS PE devices, enhancing the reliability of VPLS by providing redundancy. During the failure of the Active MLAG link, the Stabdy link becomes Active, changing the topology. The change in the topology requires MAC flush in the peer devices. This feature supports the automatic forwarding of MAC flush messages to the peer devices by configuring `mac flush send on mlag switchover` command.

For more information, refer to the MLAG Active-Standby for VPLS section in *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

Updates to the CFM and Y.1731 for ETH-TST and ETH-LM

The `test-signal frame-size` command has changed to `frame-size`, without change in the functionality. Two new commands `cir` and `eir` are added to help configure the committed information rate (CIR) and excess information rate (EIR) respectively.

For more information refer to the CFM and Y.1731 Commands section in *OcNOS Carrier Ethernet Guide*, Release 6.6.0.

Bidirectional Forwarding Detection Commands

New Command

OcNOS introduces a new `bfd multihop-peer interval` command to facilitate the global configuration of timers for all multi-hop BFD sessions.

For more information, refer to the Bidirectional Forwarding Commands section in *OcNOS Layer 3 Guide*, Release 6.6.0.

Revised Command

The maximum range for `bfd slow-timer <1000-30000>` command has changed to `bfd slow-timer <1000-1703>`, and the default slow timer interval has changed from 2000 to 1703 milliseconds.

For more information, refer to the Bidirectional Forwarding Commands section in *OcNOS Layer 3 Guide*, Release 6.6.0.

Revised Revertive Time Range

The time range for the `switchover type revertive` command has changed from <1-255> to <1-3600>, allowing configuration of a broader range of revertive time.

For more information, refer to the Multi-chassis Link Aggregation Commands section in the *OcNOS Layer 2 Guide*.

BGP Peer Group Activation and Binding Guidelines

OcNOS introduces new restrictions for BGP peer groups, affecting peer binding and activation. These restrictions apply to IPv4, IPv6, and unnumbered peer groups, ensuring configuration controls.

For more details refer to the `neighbor peer-group` command in the BGP Commands section of the *OcNOS Layer 3 Guide*, Release 6.6.0.

Improved Management

Ethernet Service Activation Testing (SAT) Based on ITU-T Y.1564

This release introduces the Ethernet Service Activation Testing (SAT) feature, compliant with the ITU-T Y.1564 standard, on OcNOS devices equipped with Qumran2 and J2C+ chipsets. SAT provides a comprehensive framework for validating Service Level Agreements (SLAs) by measuring key performance indicators (KPIs) such as Frame Delay (FD), Frame Loss Ratio (FLR), and Frame Delay Variation (FDV).

This feature empowers service providers to verify network readiness and SLA compliance before activating services for customers. It enables testing for multiple services on each User Network Interface (UNI) while ensuring compliance with Bandwidth Rate Profiles and Performance Criteria.

For more information, refer to Y.1564 - Ethernet Service Activation Test Methodology in *OcNOS Carrier Ethernet Configuration Guide*, Release 6.6.0.

Global Terminal Monitor Behavior Enhancement

Prior to version 6.6.0, all sessions displayed logging messages by default, and there was no option to disable this feature globally. The new command `[no] terminal monitor default` enables users to either enable or disable logging messages globally, ensuring that new sessions reflect the desired behavior without the need for manual configuration every time.

For more details, refer to the Basic Commands section in the OcNOS System Management Guide, Release 6.6.0.

IPFIX

The number of flow samples per export message setting value in IPFIX is changed from <1-7> to 1 and 8 due to a limit imposed by Broadcom through their latest SDK.

In accordance with the limit imposed by Broadcom's latest SDK, the setting value for the number of flow samples per IPFIX export message is changed from `<1-7>` to `1` and `8`.

For more details, refer to the samples-per-message command in the IPFIX section of the OcNOS System Management Guide, Release 6.6.0.

CMM Chassis MIB Enhancement

The existing OcNOS `IPI-CMM-CHASSIS-MIB.txt` file is deprecated. Renamed `IPI-CMM-CHASSIS-V2-MIB.txt` file to `IPI-CMM-CHASSIS-MIB.txt`.

To get the latest MIB files, visit the IPInfusion GitHub repository.

MAC Move Protection Enhancement for VPLS and H-VPLS

The MAC Move Protection is a Layer 2 mechanism that enables the system to detect MAC address movements across different network ports.

This enhancement specifically applies to VPLS, allowing detection of MAC moves across various attachment circuits (AC), attachment circuits (PW), and Mesh P in any combination. This improvement enhances network stability and security by mitigating unintended MAC movements.

For more details, refer to the MAC Move Protection section in the *OcNOS Multi-Protocol Label Switching Guide,* Release 6.6.0.

MAC Limit Support for VPLS

The MAC-limit provides a mechanism to restrict the number of MAC entries learned by the system at the Layer 2 level.

Enhancements include:

- MAC entry limitation at the AC/Spoke PW level, in addition to the existing VPLS instance level.
- Improved control over MAC learning to enhance network stability and prevent excessive resource consumption.

For more details, refer to the MAC Limit Support for VPLS section in the *OcNOS Multi-Protocol Label Switching Guide,* Release 6.6.0.

MAC Withdrawal Support for VPLS/H-VPLS Redundancy

VPLS/H-VPLS now supports MAC withdrawal messaging triggered by specific switchover scenarios across network elements, improving convergence efficiency.

Enhancements include:

- VPLS multihoming detection to identify redundant paths.
- Recognition of switchover scenarios and their impact on MAC learning.
- Defining the MAC withdrawal trigger origin—whether from MTU-s or PE-rs.
- Optimized forwarding of MAC withdrawal messages to enhance network stability and convergence.

For more details, refer to the MAC Withdrawal Support for VPLS/H-VPLS section in the *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

BVI Integration with L3VPN for Traffic Forwarding

Bridge Virtual Interface (BVI), a virtual interface on a router that acts as a routed interface associated with a single bridge domain has been introduced. BVI serves as an L3 routed interface gateway between the bridge domain (L2 network) and L3VPN, enabling seamless traffic exchange. Incoming tagged packets from L2 subinterfaces are consolidated into the bridge domain, which uses the BVI to forward IP traffic to the L3VPN tunnel.

For more details, refer to the BVI Integration with L3VPN for VPLS/H-VPLS section in the *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

BGP Auto-Discovery (AD) for Simplified VPLS Peer Discovery

BGP Auto-Discovery feature enables the automatic discovery of VPLS peers, eliminating the need for manual peer configuration. Once peers are discovered, pseudo-wires (PWs) are established between them using LDP signaling, there by simplifying and streamlining the VPLS setup process.

For more details, refer to the BGP Auto-Discovery (AD) for LDP VPLS section in the *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

CMLSH Commit-Confirmed and Rollback CLI Enhancements

For Commit-Confirmed:

- Added the optional commit-id parameter for <cancel-commit> and <confirm-commit>, enabling commit management across different sessions.
- Increased the confirmed commit timeout range from 1–500 seconds to 1–86400 seconds (24 hours).
- Restricted normal commit operations from both the same and different sessions while a commit confirmed operation is in progress, ensuring that only one commit confirmed operation is active at any time.

For Commit Rollback:

Enhanced the following CLI commands by providing additional information for clarity:

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

For more details, refer to the Commit-Confirmed and Commit Rollback sections in the *OcNOS System Management Guide*, Release 6.6.0.

Enhanced Streaming Telemetry

Wildcard Support in Sensor Paths

OcNOS supports wildcard capability in streaming telemetry sensor paths to subscribe automatically to multiple components with minimal configuration. Users can dynamically include all appropriate components automatically using wildcard-based sensor paths, reducing operational complexity and increasing scalability. The system automatically streams and monitors telemetry for newly included components with the wildcard pattern. This feature increases Dial-In and Dial-Out telemetry mode flexibility, enhancing network monitoring efficiency.

For more details, refer to the Wildcard Support in Sensor Paths section of the OcNOS Streaming Telemetry Guide, Release 6.6.0.

Enhanced gNMI In-Band Support

OcNOS now enables streaming telemetry across multiple Virtual Routing and Forwarding (VRF) instances, allowing users to manage data for up to four VRFs simultaneously. This enhancement improves efficiency and monitoring capabilities within the network.

For more details, refer to the feature streaming-telemetry section of the OcNOS Streaming Telemetry Guide, Release 6.6.0.

Enhanced Scale Values

OcNOS enhances user control over telemetry maximum subscriptions and minimum sampling intervals. Users can manage the sensor path subscriptions using the command `telemetry maximum-subscribe-paths`, which allows customized monitoring based on specific operational needs. Users set the minimum sampling interval across all VRF instances within a range from `10` to `36000 seconds` using the `telemetry minimum-sample-interval` command. These enhancements help users optimize resource usage while ensuring timely data collection.

For more details, refer to the telemetry maximum-subscribe-paths and telemetry minimum-sample-interval commands in the OcNOS Streaming Telemetry Guide, Release 6.6.0.

VRF Parameter Enhancements

OcNOS now supports VRF-specific telemetry display in the `show streaming-telemetry` command by adding the optional parameters `(vrf (NAME|management)|)`. This update allows users to view telemetry details for specific or all configured VRFs, improving data accessibility and readability.

OcNOS has removed the `(vrf (NAME|management)|)` parameters from the `debug telemetry gnmi` command, enabling users to debug gNMI telemetry and configure tunnel-server retry intervals across all VRFs without specifying a VRF name.

The `grpc-tunnel-server retry-interval` command is moved under the streaming-telemetry feature sub-mode; hence, retry-interval can be set per VRF.

For more details, refer to the individual commands in the streaming telemetry commands section of the OcNOS Streaming Telemetry Guide, Release 6.6.0.

gNMI Stream Data with Source Timestamps

Before OcNOS version 6.6.0, the gNMI Subscribe RPC response timestamp indicated when the gNMI server sent the response packet. In OcNOS version 6.6.0, the timestamp shows when the protocol modules collect the streamed data, providing accurate telemetry, improving synchronization and event correlation, and ensuring precise real-time network analysis.

Streaming Telemetry Over TLS

OcNOS supports streaming telemetry over Transport Layer Security (TLS), ensuring secure, encrypted telemetry data transmission between the gNMI server (OcNOS Target) and gNMI client (Collector). This feature protects telemetry streams from unauthorized access, interception, and tampering while maintaining real-time network monitoring. Users can configure TLS with server, client, and CA certificates, define sensor groups, and establish secure subscriptions with a customizable sample interval. The system also supports an optional insecure TLS mode, allowing certificate validation only when provided. This enhancement improves security, compliance, and reliability in network telemetry streaming.

For more details, refer to the Streaming Telemetry Over Transport Layer Security section in the OcNOS Streaming Telemetry Guide, Release 6.6.0.

gNMI Get RPC Support

OcNOS supports the `gNMI Get RPC` operation with JSON-IETF encoding, expanding its management capabilities alongside the existing `Subscribe` operation. This enhancement allows users to retrieve Configuration, State, or Operational data via the gNMI interface. Since State and Operational data are the same in OcNOS, the system fetches state data for both types when requested. This update improves flexibility and interoperability, enabling more efficient retrieval of network configuration and status information.

For more details, refer to the **Get RPC** section in the OcNOS Streaming Telemetry Guide, Release 6.6.0.

XPath Formatting Rules for gNMIc Subscription

OcNOS now enforces XPath formatting rules for gNMIc subscription commands in Dial-In mode. String keys must be enclosed in double quotes (""), while integer keys must be provided without quotes to ensure correct parsing. Implicit wildcard keys can be specified with or without single quotes. These rules improve command consistency, prevent syntax errors, and enhance compatibility with gNMI-based telemetry subscriptions.

For more details, refer to the XPath Formatting Rules section in the OcNOS Streaming Telemetry Guide, Release 6.6.0.

Data Model Support

OcNOS adds support for additional IPI and OpenConfig data model modules and new transceiver states in the ipi-platform data modules. The new modules `ipi-lldpv2, ipi-bfd, ipi-vrf, ipi-qos, ipi-bgp, ipi-isis, ipi-rib, and oc-cmis` enhance visibility into the operational status and attributes of various components.

For more details, refer to the IPI Data Models and OpenConfig Data Models sections in the OcNOS Streaming Telemetry Guide, Release 6.6.0.

Removal of Layer-2 MPLS Virtual Circuit FIB Entry

The command to remove the Layer-2 MPLS Virtual Circuit FIB entry is changed from `no mpls l2-circuit-fib-entry <1-4294967295>` to `no mpls l2-circuit-fib-entry <1-4294967295> (A.B.C.D|X:X::X:X)`.

For more information, refer to the MPLS Commands section in *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

Suppressing the Operator Logs for the MPLS L2VPN Service

OcNOS introduces `suppress-oper-log mpls l2vpn` command to provide an option to suppress the operator logs for the MPLS L2VPN service.

In case of a transport down event, all the L2VPN services generate operator logs. If users do not want to receive notifications for all the L2VPN services, they can suppress the operator logs. Use the `no` parameter of this command to get back the notifications.

For more information, refer to the MPLS Commands section in *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

Allocating MPLS Labels for Improved Scalability

BGP Route Reflector (RR) or ASBR for VPN IPv4/IPv6 address families allocates per-prefix MPLS labels during a BGP next-hop-self operation. To avoid scalability issues caused by this operation, an enhancement has been made such that RR or ASBR allocates MPLS labels per initial BGP nexthop + per initial MPLS label value.

This enhancement is displayed in the `show mpls ilm-table` command.

For more information, refer to the MPLS Commands section in *OcNOS Multi-Protocol Label Switching Guide*, Release 6.6.0.

Filtering IPv4 and IPv6 Headers for ACL Groups

The `hardware-profile filter-match ingress-ip-outer` command is introduced to make the following ingress ACL groups match only the outer IPv4 and IPv6 headers:

- ingress-ipv4

- ingress-ipv4-ext
- ingress-ipv4-subif
- ingress-ipv6
- ingress-ipv6-ext
- ingress-ipv6-ext-vlan
- ingress-ipv6-ext-subif

For more information refer to the System Configure Mode Commands section in *OcNOS System Management Guide*, Release 6.6.0.

Ensuring Service Continuity with Link Loss Forwarding (LLF) for EVPN EPL Services

Link Loss Forwarding (LLF) for EVPN EPL services provides a critical fault propagation mechanism in point-to-point connections, preventing traffic blackholing by administratively bringing down the local physical link when a remote peer service failure is detected. Enabled per service on a physical interface using the CLI command llf enable, this capability triggers the withdrawal of Ethernet AD per EVI (RT-1) routes and activates traffic failover mechanisms. LLF plays a vital role in maintaining seamless service continuity and is enabled by default for EVPN EPL services.

For more information, refer to the EVPN EPL Link-Loss Forwarding section in the *OcNOS MPLS Configuration Guide*, Release 6.6.0.

Syslog and Trap Notification Support for Storm Control

OcNOS introduces the storm control feature, allowing rate limiting of Broadcast, Unknown Unicast, and Multicast (BUM) traffic at the ingress interface. This configuration is independent of the QoS feature. To verify the BUM rate limit configuration, use the `show storm-control (INTERFACE-NAME|)` command.

On Qumran1 hardware, discard counters for BUM rate limiting are not supported. However, BUM traffic discards can be displayed on Qumran2 using the `show storm-control (INTERFACE-NAME|)` discards command.

For more information refer to the Displaying BUM rate limit information and Displaying BUM discards on Qumran2 section in the *OcNOS Quality of Service Configuration Guide*, Release 6.6.0.

Syslog Messages Support over SNMP Traps

OcNOS provides support for sending `SYSLOG` messages over SNMP traps.

For more information, refer to Logging Server Command Reference in the *OcNOS System Management Guide*, Release 6.6.0.

Management over User-Defined VRF

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

- SNMP Traps
- Ansible
- sFlow

- Source Port Configuration
- TACAS
- Netconf Call home

For more information, refer to the OcNOS System Management Guide, Release 6.6.0.

Improved Network Resilience

Low Latency FEC Support for RS-108

OcNOS introduces a new parameter, `cl108`, for the FEC command to support the configuration of 64/66b 5T low-latency Reed-Solomon (RS) Forward Error Correction (FEC) on designated physical ports. This enhancement improves data transmission reliability and efficiency in fabric environments.

For more details, refer to the fec command in the Interface Commands section of the OcNOS System Management Guide, Release 6.6.0.

Enhanced Global Configuration Mode

OcNOS introduces a Global Configuration mode to streamline network configuration by allowing centralized management of key parameters such as PCH load-balance, load-interval, L2 protocol tunnel, sFlow sampling rate and poll interval, Interface MTU, and LLDP settings for all LLDP-enabled interfaces. This configuration mode ensures consistent configurations across the network.

For more information, refer to Link Layer Discovery Protocol v2 Commands section in the *OcNOS Layer 2 Guide*, Release 6.6.0.

For more information, refer to Interface commands and Monitoring and Reporting Server Commands sections in the *OcNOS System Management Guide*, Release 6.6.0.

IPv6 Address Support for LLDP

OcNOS introduces a new `ipv6-address` parameter in the `set lldp management-address-tlv`, `set lldp port-id-tlv`, and `set lldp port-id-tlv` commands. This enhancement allows users to configure IPv6 addresses for LLDP TLV (Type-Length-Value) attributes, improving network management and addressing capabilities in IPv6-based environments.

For more information, refer to the Link Layer Discovery Protocol v2 Commands section in the *OcNOS Layer 2 Guide, Release 6.6.0*

Managing ErrDisable State Due to BUM Traffic Storms

When an interface port continuously receives Broadcast, Unknown Unicast, and Multicast (BUM) traffic exceeding the configured storm control thresholds, it transitions to the ErrDisable state. In this state, the port becomes inactive and cannot send or receive traffic. Recovery from ErrDisable can be achieved either manually using the shut/no shut command or automatically if a timeout value is configured.

For detailed configuration and recovery procedures, refer to the Spanning Tree Protocol Configuration section in the *OcNOS Layer 2 Guide*, Release 6.6.0.

Ethernet Linear Protection Switching (ELPS) for VLAN-Based Networks

Ethernet Linear Protection Switching (ELPS), based on ITU-T G.8031, provides a fast and reliable protection mechanism for VLAN-based Ethernet networks by reserving a dedicated protection path for a selected working entity. It offers a simpler and more predictable alternative to other survivability mechanisms like Rapid Spanning Tree Protocol (RSTP), making network management more efficient. This implementation is tailored to specific customer requirements, focusing on a modular and flexible CLI restructure, cross-connect support to extend ELPS over bridge-domains, and control plane enhancements to make ELPS bridge-independent. These improvements enhance network reliability, simplify operations, and provide a scalable solution for protection switching in VLAN-based Ethernet environments.

For more information, refer to the Ethernet Linear Protection Switching Configuration section in the *OcNOS Layer 3 Guide,* Release 6.6.0.

Enhanced Security and Performance

Port-Based BGP FlowSpec Disable

The feature allows administrators to selectively disable FlowSpec on Layer 3 interfaces, including VLAN, LAG, sub-interfaces, and physical interfaces. By configuring the `ipv4 flowspec-disable` command, the system installs high-priority disabling rules to prevent regular FlowSpec policies from being applied. This ensures that traffic on disabled interfaces is unaffected by FlowSpec, while other interfaces continue to enforce FlowSpec rules. This feature provides flexibility by excluding specific ports from FlowSpec processing without affecting overall network functionality.

For more details, refer to the `ipv4 flowspec-disable` command in the BGP Flowspec Commands section of the *OcNOS Layer 3 Guide*, Release 6.6.0.

Security with AES Encryption

A new option to encrypt sensitive information, such as authentication keys, using the Advanced Encryption Standard (AES) algorithm is now available in OcNOS. Previously, sensitive data was encrypted using the 3DES algorithm by default. With this update, users can configure AES encryption for enhanced data security.

The AES encryption option provides improved confidentiality and integrity for sensitive data stored in the OcNOS database, particularly for routing protocols such as BGP, OSPF, RIP, IS-IS, LDP, BFD, MSDP, and RADIUS authentication.

For more information, refer to the User Config AES Encryption section in the *OcNOS System Management Guide*, Release 6.6.0.

Control Plane Policing Using ACL

OcNOS now supports ACL-based packet classification and configurable actions for CPU-bound traffic, enhancing Control Plane Policing (CoPP) to improve control and protect against excessive or malicious traffic.

For more information, refer to the Control Plane Policing Using ACL section in the *OcNOS System Management Guide*, Release 6.6.0

Hardware Platform

This section discusses the new hardware introduced in the Release OcNOS 6.6.0.

Transceivers

OcNOS supports the following transceivers and amplifiers:

Ciena IPI-CI-176-3590-900

The Ciena IPI-CI-176-3590-900 is an is an advanced power-efficient, low heat-dissipating, multi-carrier transceiver with multi-span of 100, 200, and 400 GbE speeds for metro regional and single-span Data Center Interconnect (DCI) applications.

For more details, refer to the Cables and Transceivers List.

Fujitsu IPI-FU-FIM38950/130

The 400G ZR/Open ZR+ full C-band tunable coherent optical transceiver supports 100, 200, 300, and 400 GbE speeds.

For more details, refer to the Cables and Transceivers List.

NEC-IPI-NE-OD-QD337SCLS00N

The C-band tunable coherent optical transceiver with 100, 200, and 400 GbE speeds supports DCI and Metro Wavelength Division Multiplexing (WDM). DDM.

For more details, refer to the Cables and Transceivers List.

OFA-WCF-14AG-F15 and OFA-WCF-10AG-F20

The EDFA module supports a 100G or higher-speed channel optical amplification for long-haul fiber optic communication.

For more details, refer to the Cables and Transceivers List.

EdgeCore AS5915-16X

OcNOS supports EdgeCore AS5915-16X, an open cell site gateway platform. This platform has 4x1/10G SFP+, 8x1G SFP, and 4x1G RJ45 fixed ports. This platform also supports network timing and synchronization in the hardware, making it ideal for current LTE and emerging 5G mobile backhaul network solutions.

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

Security Update

To ensure product security, OcNOS undergoes rigorous vulnerability scanning and promptly addresses any issues that are found. OcNOS version 6.6.0 provides a detailed list of CVEs that are included in the OcNOS Security Updates document. In addition, request a detailed OcNOS Security Guide from the IPI sales team.