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 4
Overview 4
Key Benefits of OcNOS 4
Technical Supports 4
Technical Documentation 5
Technical Sales 5
Documentation Disclaimer 5
About this Release 5
IP Infusion Product Release Version 5

Release 6.6.0 6
Enhanced Security and Performance 6
Security with AES Encryption 6
Enhancing IPv6 Multicast with TR3 Boards for Scalable Network Operations 6
Improved Management 6
Global Terminal Monitor Behavior Enhancement 6
CMM Chassis MIB Enhancement 6
CMLSH Commit-Confirmed and Rollback CLI Enhancements 7
Enhanced Streaming Telemetry 7
Improved Traffic Monitoring with ERSPAN 9
Syslog Messages Support over SNMP Traps 9
Improved Routing 9
Support for BGP Multiple Large Communities 9
Static Route Behavior in VRF 9
ACL on IRB Interface Over VXLAN EVPN 10
Bidirectional Forwarding Detection Commands 10
Updates to the CFM and Y.1731 for ETH-TST and ETH-LM 10
Revised Revertive Time Range 10
BGP Peer Group Activation and Binding Guidelines 10
Improved Network Resilience 11
Low Latency FEC Support for RS-108 11
Enhanced Global Configuration Mode 11
Enhances Monitoring with 'show' Command 11
Management over User-Defined VRF 11
Hardware Platforms 11
UfiSpace S9300-32D 12
Security Update 12

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 enhancements in traffic monitoring and filtering support for 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.

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 Supports

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 Data Centers solution.

Documentation Disclaimer

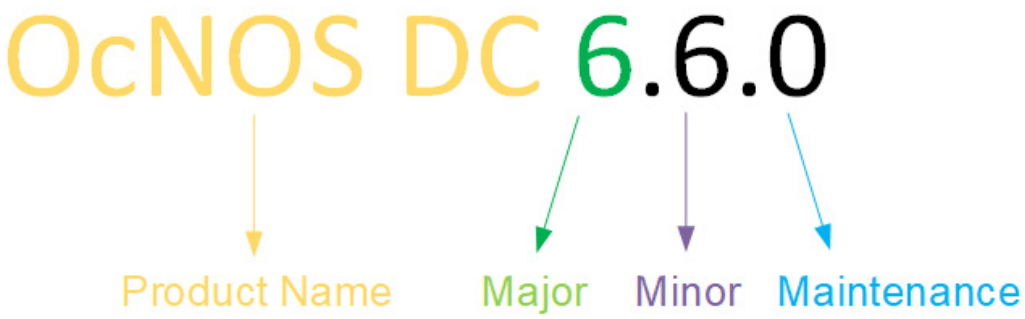
OcNOS version 6.6.0 provides an enhanced website experience for select topics included in this release. As a result, some navigational elements on the website may display a few discrepancies.

About this Release

Release 6.6.0 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 6.6.0

OcNOS DC Release 6.6.0 introduces several software features, and product enhancements along with support for a few new hardware device.

Enhanced Security and Performance

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.

Enhancing IPv6 Multicast with TR3 Boards for Scalable Network Operations

The TR3 boards significantly enhance IPv6 multicast capabilities by integrating PIM-Sparse Mode (PIM-SM) with a centralized Rendezvous Point (RP) for optimized routing, the Bootstrap Router (BSR) mechanism for automated RP distribution, and static RP configuration for improved control and redundancy. PIM Source-Specific Multicast (PIM-SSM) eliminates the need for RPs, streamlining source-specific routing. Multicast Listener Discovery (MLD) enables efficient MCASTv6 group membership management, while MLD snooping ensures multicast streams reach only interested hosts, reducing network load. These advanced features, combined with IPv6 multicast support across XGS devices including TD3-X3, TD3-X5, TD3-X7, TH3, TH2, TH, and TH+ models enable scalable, efficient, and controlled MCASTv6 network operations.

For more information, refer to the MLD Configuration section in the *OcNOS Multicast Configuration Guide*, Release 6.6.0.

Improved Management

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.

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.

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:

- Added a prerequisite for show commit list, requiring cml commit-history to be enabled.
- Updated the commit-rollback command syntax to commit-rollback to WORD (description LINE|).
- Updated the clear cml commit-history command syntax to clear cml commit-history (WORD|).
- Changed the cml commit-history (enable | disable) command from EXEC mode to CONFIG mode.
- Updated the cml commit-id rollover command syntax to cml commit-id rollover (enable | disable).

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 Config, State, and 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.

Improved Traffic Monitoring with ERSPAN

Encapsulated Remote Switched Port Analyzer (ERSPAN) is a function used for monitoring network traffic. It utilizes Generic Routing Encapsulation (GRE) based tunneling mechanism to transport mirrored traffic from the source to the destination over Layer 3 IP network.

Using ERSPAN, you can monitor both ingress and egress traffic, and the mirrored traffic can be sent to a remote monitoring device for analysis without being restricted by Layer 2 boundaries.

For more information, refer to the Traffic Mirroring using ERSPAN section in the *OcNOS Key Features document,* 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 Syslog Commands in the *OcNOS System Management Guide*, Release 6.6.0.

Improved Routing

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.

ACL on IRB Interface Over VXLAN EVPN

OcNOS supports IP ACL configuration on the IRB interface attached to the VxLAN EVPN topology. It enables traffic filtering for the routed packets using the IRB interface.

For more details, refer to the ACL on IRB Interface Over VXLAN EVPN section in the System Management 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.

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 Commands section in *OcNOS Carrier Ethernet 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 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.

Enhances Monitoring with 'show' Command

OcNOS introduces the show hsl evpn multihoming esi command, allowing customers to efficiently monitor the HSL state for ES-LAG connections. This enhancement provides improved visibility and simplifies troubleshooting, ensuring better network management and operational efficiency.

For more information, refer to the VXLAN Commands section in the *OcNOS Layer 3 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.

Hardware Platforms

This section provides the new hardware details introduced in the OcNOS 6.6.0 release.

UfiSpace S9300-32D

OcNOS supports the UfiSpace S9300-32D hardware, a high-performance white box switch designed for modern data center networks with rich features, multiple protocols support, and run-time programmability, enabling high performance in the most demanding environments. It supports centralized management of computing resources with efficient Ethernet connectivity.

It supports the following:

- High density 400GE interfaces in 1RU chassis
- 12.8Tbps switching bandwidth capacity
- Broadcom Trident4 Silicon
- 32 x 40/100/200/400G QSFPDD ports
- 2x 10GbE SFP+ ports
- 1 x GbE OOB management port (CPU)
- 1 x RS232 console port in RJ45 form factor
- 1 x USB 3.0 Type-A general purpose port
- BMC for monitoring and managing equipment health status
- 1 + 1 hot swappable power supply field replaceable units
- 5 + 1 hot swappable fan field replaceable units

S9300-32D Front View

S9300-32D Rear View

Figure P-1: Front and Rear View of S9300-32D

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

For port mapping information, refer to *UfiSpace Installation Guide,* Release 6.6.0

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.