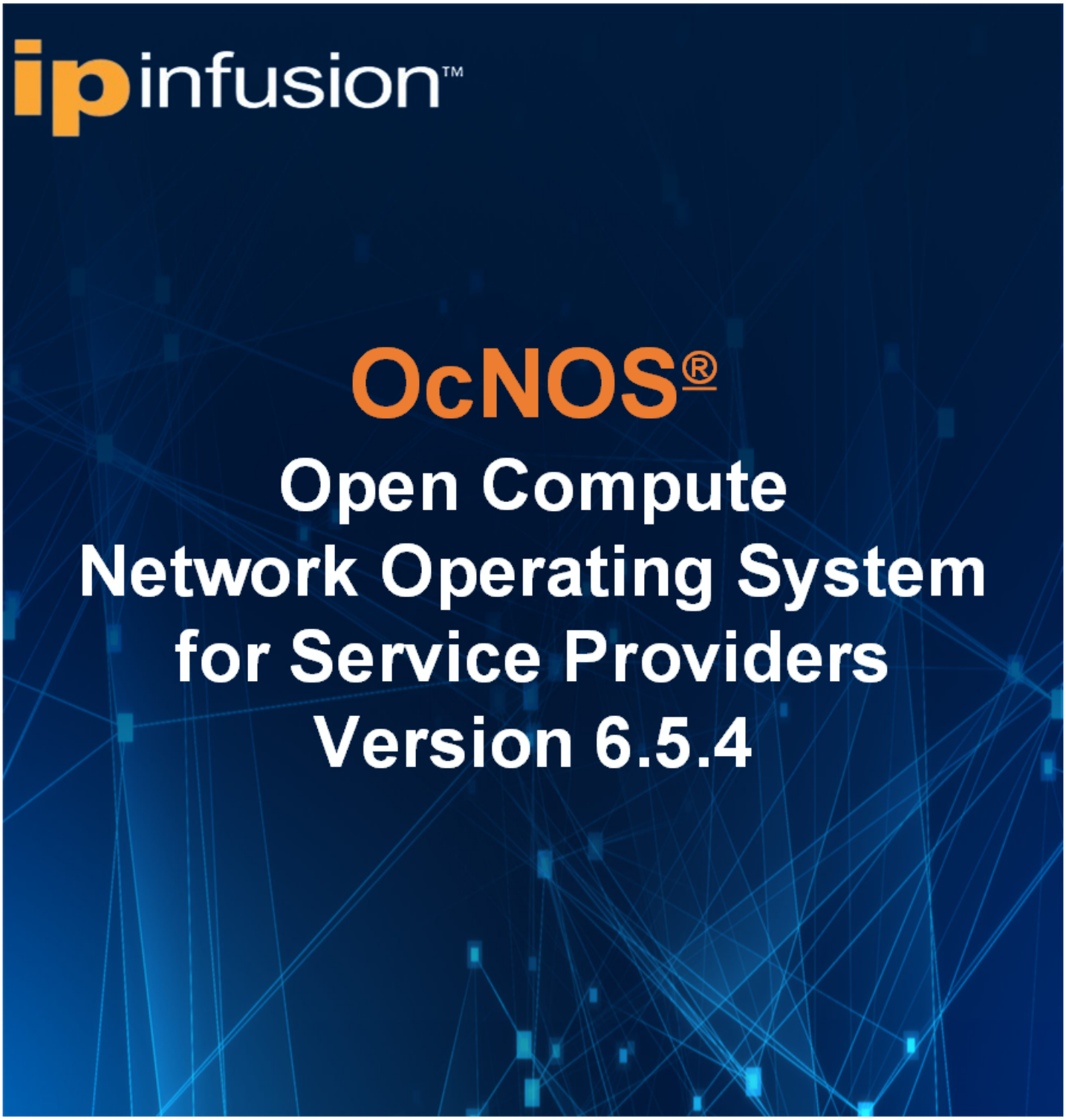


Release Notes

April 2025

IP Infusion Inc.
3979 Freedom Circle
Suite 900
Santa Clara, California 95054
http://www.ipinfusion.com/

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

Contents

Introduction

Overview

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

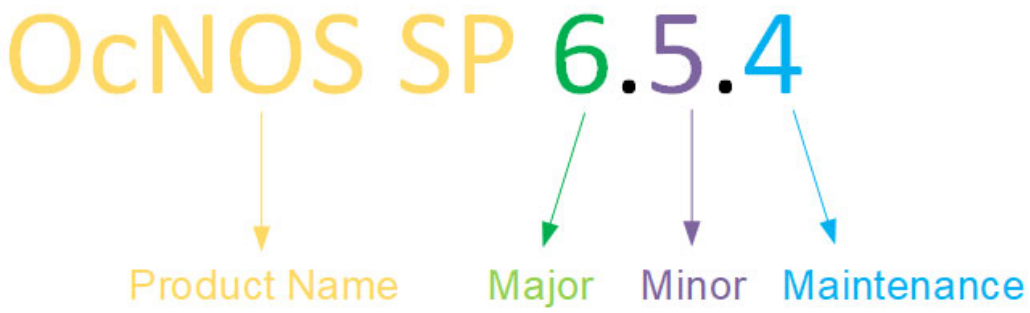
OcNOS works with applications in diverse network environments, including data centers, service provider networks, enterprise networks, and cloud deployments. It provides an open, flexible environment and extensive protocol support for software-defined networking (SDN) and disaggregated networks.

About this Release

OcNOS SP Release 6.5.3 introduces several software features, and product enhancements.

IP Infusion Product Release Version

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



Product Name: IP Infusion Product Family

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

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

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

Release 6.5.4

Improved Routing

The targeted-peer IPv4 configuration in LDP now includes a new tunneling CLI option. This CLI enables targeted peer tunneling for LDP FECs, providing greater flexibility in managing targeted LDP sessions. It allows users to define tunneling parameters directly within the targeted-peer IPv4 configuration.

For more information, refer to the targeted-peer tunneling section in the LDP Commands, Release 6.5.4.

Release 6.5.3

Enhanced Security and Performance

BGP Bogon Prefix Filtering IPv4

The BGP Bogon Prefix Filtering feature in OcNOS allows administrators to block invalid or reserved IP addresses from being propagated through BGP. Bogon prefixes, such as unallocated IP ranges or special-use addresses, should not appear in the global routing table to avoid security risks if routed. The new `bgp enable-bogon-filtering`

command provides flexibility to manage which prefixes are filtered, ensuring only valid routes are accepted. To implement, administrators can enable filtering for specific IPv4 prefixes. These changes will apply to new BGP updates, with a recommended BGP hard reset to ensure full effect.

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

IP ACL Support on the IRB Interfaces

This release introduces IP ACL support for ingress and egress on Integrated Routing and Bridging (IRB) interfaces for both IPv4 and IPv6, including advanced filtering options. Key features include:

- **IRB Interfaces:** ACLs are now configurable with options for IP and Layer 4 headers.
- **Interface-Less Model:** Supports egress ACLs for tunnel and non-tunnel traffic.
- **EVPN Multi-Homing:** Supports egress ACLs for routing interfaces in both MPLS and VXLAN modes.
- **L3VPN MPLS:** Enables ACL application across all interface types in the egress direction.
- **VXLAN**: Offers enhanced ACL management capabilities for VXLAN configurations.

These updates enhance traffic management and filtering capabilities.

For more information, refer to the ACL on IRB Interface over MPLS EVPN, and ACL on IRB Interface over VXLAN EVPN section in the *OcNOS System Management Guide*, Release 6.5.3.

Enhanced ACL Control for MLAG Interfaces

The `hardware-profile filter` command includes a new parameter, `egress-l2-mlag`, specifically for MLAG interfaces operating in `active-active` mode. This enhancement allows users to utilize more than one egress profile. With an active-active MLAG configuration, the `egress-l2-mlag` profile filter must be applied, along with one of the following profiles: `egress-ipv4, egress-dst-ipv6, egress-src-ipv6, egress-qos-policer, or egress-qos-policer-ext`.

For more information, refer to the System Configure Mode Commands section in the *OcNOS System Management Guide*, Release 6.5.3.

Enhanced SSH Encryption Algorithm

The security encryption algorithms used in Secure Shell (SSH) are enhanced to enable the users to use preferable (including weaker algorithms) security mechanisms (for legacy SSH clients) if they want to use them in their network apart from the default cipher algorithms. The default SSH configurations do not use these weaker encryption ciphers algorithms due to security priority.

However, OcNOS allows the users to enable or disable the desired algorithms option using the following newly introduced commands.

- ssh server algorithm encryption
- ssh server algorithm kex
- ssh server algorithm mac
- ssh server default algorithm
- show ssh server algorithm

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

CFM and Y1731 UP-MEP

Connectivity Fault Management (CFM) and Y1731 UP-MEP Qumran1 or Qumran2 CFM (802.1ag) and Y1731 are CE standards which provides CFM functions, such as ContinuityCheck Message (CCM), Loopback Ping (LB), Link-Trace (LT), Loss-Measurement (LM), Delay-Measurement (DM) and Synthetic Loss Measurement (SLM). OcNOS supports all CFM operations using Accelerated UP MEP with Hardware Offload. CFM or Y.1731 function support is extended for below VXLAN feature.

For more details refer to Y.1731 and CFM Over VXLAN ELAN Single Home section and Y.1731 and CFM Over EVPN ELAN Single Home in *Carrier Ethernet Configuration Guide,* Release 6.5.3.

Max Password Age

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

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

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

Removing Users with Expired Passwords

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

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

Improved Routing

Segment Routing ECMP Support for ISIS or OSPF

Multiple outgoing Equal Cost Multi-path (ECMP) next-hops in Segment Routing (SR) for ISIS or OSPF ensures that all the valid next-hop peers of an IP prefix are selected and Incoming Label Maps (ILM) and FEC-to-NHLFE (FTN) entries are created for that prefix with all the identified next-hops in the forwarding plane. Load balancing is used to distribute traffic across multiple equal-cost paths, optimizing resource utilization throughout the network.

Note: Load balancing does not distribute traffic equally across the ECMP paths as it done by hashing of a combination of headers in the traffic streams. The unique combination of such headers may result in the same hash which in turn leads to unequal distribution of traffic in the ECMP next-hop interfaces.

For more information, refer to the Segment Routing ECMP for ISIS or OSPF section in the *OcNOS Segment Routing Guide,* Release 6.5.3.

BGP Additional Paths

The Border Gateway Protocol (BGP) Additional Paths feature allows the advertisement of multiple paths through the same peering session for a given prefix without the new paths implicitly replacing any previous paths. This behavior promotes path diversity and reduces the severity of network failures, thereby improving the control plane convergence in case of network failures.

The following commands are updated with the address family modes.

- `bgp additional-paths`
- `neighbor additional-paths`
- `neighbor advertise additional-paths`
- `bgp additional-paths install`

For more information, refer to the BGP Additional Paths section in the *OcNOS Layer 3 Guide,* Release 6.5.3.

Deep Packet Inspection

For enhanced network load-balancing capabilities, Deep Packet Inspection (DPI) performs a granular check on the inner headers beyond the MPLS bottom of the label stack to load-balance the network traffic. The load balancing key is generated after deep analysis of the MPLS header.

The DPI feature can be configured in the Qumran 1 platforms. In Qumran 2 platforms, it is always enabled by default.

For more information, refer to the Deep Packet Inspection section in the *OcNOS Multi Protocol Label Switching Guide,* Release 6.5.3.

Improved Management

Enhanced System Management Protocols Support for User-Defined VRFs

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

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

SNMP Community String Enhancement

OcNOS software now allows the use of all special characters in the SNMP community string, except for "?". This enhancement improves flexibility when configuring SNMP community strings.

Support for HTTPS and SFTP in NetConf

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

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

Enhanced Maximum Capacity for PTP Clock Ports

The IEEE 1588 v2 Precision Time Protocol (PTP) functionality has been enhanced to support configuration of up to 128 clock ports, provided the physical board has that number of ports. Currently, this enhanced capability is available on UfiSpace and EdgeCore hardware boards.

Modifying Temperature Sensor Threshold Value

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

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

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

Extensions to the CMIS standard - Custom Application

Some transceiver vendors provide a custom extension to the current limitation of having a maximum of 15 applications as imposed by the Common Management Interface Specification (CMIS). In order to provide access to this custom extension the following new CLIs are introduced:

```
custom-app-host-id
```

```
custom-app-media-id
```

For more details, refer to Custom Application section in *OcNOS System Management Configuration Guide,* Release 6.5.3.

Enhanced Egress Queue to Exp Mapping (Q2)

Updated the egress queue to Exp mapping to improve efficiency in handling MPLS encapsulations. Introduced a new CLI command "mpls lsp-encap-dscp-preserve" to preserve DSCP on egress traffic.

For more details refer to the mpls lsp-encap-dscp-preserve command in the *OcNOS Multi-Protocol Label Switching Configuration Guide*, Release 6.5.3.

Improved SNMP Trap Forwarding Mechanism for Network Element Reboots

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

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

User Confirmation Prompt Added for License Release Command

Introduced a confirmation command that prompts users with the message:

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

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

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

New MIBs for Enhanced SNMP Functionality

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

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

Hardware Platform

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

Ciena transceivers

OcNOS supports WaveLogic 5 Nano (WL5n) Standard Amplified 400ZR QSFP-DD transceiver.

IPI-CI-176-3360-900

This is an advanced power-efficient coherent single-carrier transceiver with 100, 200, and 400Gbps transmission for 100G or 200G access and multi-span transport. This QSFP-DD transceiver has an in-built Erbium-Doped Fiber Amplifier (EDFA) with an integrated Tunable Optical Filter (TOF) that supports high Tx launch power for the service provider requirements.

IPI-CI-176-3370-900

This is an advanced power-efficient coherent single-carrier transceiver with 100, 200, 300, and 400Gbps transmission for multi-span metro packet, multi-span regional packet, 100G or 200G access and multi-span, multi-span metro transport, and multi-span regional transport. This QSFP-DD transceiver has an in-built Erbium-Doped Fiber Amplifier (EDFA) with an integrated Tunable Optical Filter (TOF) that supports high Tx launch power for the service provider requirements.

For more details on the PLATFORM MODEL, OPTICS PART NUMBER, MAKE, TRANSCEIVER CATEGORY, TYPE, INTERFACE (G), REACH, and TEMP, refer to the Cables and Transceivers List.

Release 6.5.2

Enhanced Security and Performance

Clock Data Recovery Bypass

Higher data rate transceivers are equipped with Clock Data Recovery (CDR) to ensure the transmitted and received signals are synchronized for optimal transmission.

Some higher data rate transceivers running at a lower data rate are not supported because the clock fails to lock, causing an unstable link. To mitigate jitter generation, the CDR (Clock and Data Recovery) must be bypassed. For instance, on a 100G-LR4 transceiver that supports 4 lanes at 25Gbps, reducing the lane speed to 10Gbps results in jitters. This occurs when the clock tries to lock onto 25Gbps, while the actual data rate is 10Gbps. In these cases, the RX and TX CDR must be bypassed on both connected devices.

- tx cdr-bypass
- rx cdr-bypass

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

Multiple Tagged VLANs to Port Security

Multiple tagged VLANs help address previous database synchronization challenges. It ensures seamless operation and reliability when adding multiple tagged VLANs, saving configurations, and reloading the device.

Zero Touch Provision on Data Ports

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

The following is not supported in ZTP:

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

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

BGP MD5 Authentication for BGP Dynamic Peer-Groups

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

MPLS VPLS LDP Signaling

VPLS LDP signaling happens when each Provider Edge (PE) discovers the endpoints of the VPLS instance. Pseudowires (PWs) are then established over MPLS tunnels between VPN sites to transparently transmit Layer 2 packets between these sites. Users can configure the VPLS type per peer, and the configured VPLS type is forwarded to LDP. This occurs only when there is a change in the VPLS type at the VPLS instance and per peer level.

For more information, refer to the Virtual Private LAN Service Configuration section in the *MPLS Guide*, Release 6.5.2.

Discard Unknown Multicast Traffic

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

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

This feature enables the option to drop the unknown multicast traffic in any snooping configurations. For example, execute the command in the IGMP Snooping Configuration or MLD Snooping Configuration.

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

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

Restricted Access to Privilege Mode based on User Role

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

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

AAA Support for Serial Console Connection in VRF Management

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

sFlow Supported with Multiple Collector

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

IP Unreachable

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

For more information, refer to the No IP Unreachable section in the *System Management Guide*, Release 6.5.2.

CFM and Y1731 UP-MEP

CFM and Y1731 UP-MEP Qumran1 or Qumran2 CFM (802.1ag) and Y1731 are CE standards which provides Connectivity Fault Management functions, such as ContinuityCheck (CCM), Loopback Ping (LB), Link-Trace (LT), Loss-Measurement (LM), Delay-Measurement (DM) and Synthetic Loss Measurement (SLM). OcNOS supports all CFM operations using Accelerated UP Mep with Hardware Offload. CFM or Y.1731 function support is extended for below features:

- VPLS
- EVPN-MPLS E-LAN or E-LINE (Single-Homing and Multi-Homing)
- Cross-connect

For more information, refer to the Y.1731 and CFM Over EVPN ELINE Single Home, Y.1731 and CFM Over EVPN-ELINE Multi-home, Y.1731 and CFM Over VPWS Sub-interface, Y.1731 and CFM Over EVPN ELAN Single Home, Y.1731 and CFM Over EVPN-ELAN Multi-home, Y.1731 and CFM Over VPLS Sub-Interface, and Y.1731 and CFM Over Cross-connect Sub-interface sections in the *Carrier Ethernet Guide*, Release 6.5.2.

Improved Network Resilience

Hierarchical VPLS

Hierarchical VPLS (H-VPLS) introduces a hierarchical approach using a spoke-PW (pseudowire) type for large networks dependent on multipoint communication. Unlike the standard mesh-PW, the spoke-PW facilitates traffic between hierarchical levels, offering a more scalable solution for VPLS networks.

For more information, refer to the Hierarchical VPLS section in the *MPLS Guide*, Release 6.5.2.

H-VPLS Spoke Split Horizon

With the introduction of HVPLS, additional split-horizon combinations are now supported, including:

- spoke-AC
- spoke-spoke
- spoke-hub

Auto-Bandwidth with RSVP-TE

OcNOS introduces the RSVP auto-bandwidth support to monitor the traffic rate on RSVP tunnels at regular intervals. When the traffic variation surpasses the threshold value for more than the threshold limit, as specified in the auto-bandwidth profile, a Make-Before-Break (MBB) session is initiated with the adjusted bandwidth requirement. This guarantees that the tunnel's bandwidth resource allocation matches the traffic flow, preventing the unnecessary reservation of resources.

For more information, refer to the Auto-Bandwidth with RSVP-TE section in *MPLS Guide*, Release 6.5.2.

LDP Tunneling Over RSVP

OcNOS introduces the RSVP auto-bandwidth support to monitor the traffic rate on RSVP tunnels at regular intervals. When the traffic variation surpasses the threshold value for more than the threshold limit, as specified in the auto-bandwidth profile, a Make-Before-Break (MBB) session is initiated with the adjusted bandwidth requirement. This guarantees that the tunnel's bandwidth resource allocation matches the traffic flow, preventing the unnecessary reservation of resources.

For more information, refer to the LDP Tunneling over RSVP-TE section in the *MPLS Guide*, Release 6.5.2.

LACP Aggregator Force-up

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

For more information, refer to the LACP Aggregator Force-up section in the *Layer 2 Guide*, Release 6.5.2.

Load Balancing - Deep Packet Inspection

Deep Packet Inspection (DPI) for Load Balancing on the Qumran 2 series platform enhances load balancing capabilities by enabling DPI on Qumran 2 series devices. With this new implementation, more effective traffic distribution is achieved among the members of port channels, leading to optimized network performance and improved efficiency.

Enhanced Ping CLI with More Options

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

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

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

Configurable Password Policy

A password is a sequence of characters utilized to confirm a user's identity in the authentication procedure. A strong password helps to protect user accounts and prevents unauthorized access. Strong passwords are the first defense against cyberattacks. Hackers commonly use automated tools to crack passwords.; Weak passwords are easily guessed or cracked. Every organization encourages its users to use long passwords combining alphanumeric and special characters. A lengthy password is more complex for hackers, who also need to invest a lot of time to hack the system

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

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

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

EVPN E-Tree

OcNOS enhances Ethernet VPN Ethernet-Tree (EVPN E-Tree) to manage communication within broadcast domains, incorporating redundancy through multi-homing. It optimizes traffic routing and control by categorizing network nodes based on predefined definitions of EVPN instances as Leaf or Root nodes. OcNOS VXLAN and MPLS EVPN E-Tree supports efficient traffic control, enhances security by isolating Leaf hosts, provides scalability across network sizes, and improves network performance.

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

RSVP-TE Dynamic Facility Backup LSP (RSVP Auto Bypass)

IResource Reservation Protocol (RSVP) auto bypass component within Facility Backup enhances fast-reroute protection and operates by establishing bypass tunnels for protected sessions at each PLR node. It serves as a local safeguard for sessions on every PLR. Configuring bypass tunnels manually on each PLR, particularly in larger topologies, presented challenges in configuration management. The RSVP auto bypass functionality ensures creation of bypass tunnels when enabled and sessions request facility backup protection.

For more information, refer to the RSVP-TE Dynamic Facility Backup LSP (RSVP Auto Bypass) section in the *MPLS Guide*.

Commit Configuration Management

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

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

Multi-Line Banner Support

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

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

Global Navigation Satellite System Configuration Command

OcNOS introduces the command `gps satellite-system` to configure the global navigation satellite system (GNSS). GNSS satellites transmit navigation and timing data to GNSS receivers.

For more information, refer to the command reference page for the gps satellite-system in *OcNOS Timing and Synchronization Guide,* Release 6.5.2.

Improved Routing

Multi Topology Routing in ISIS

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

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

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

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

OSPFv2 Multi-Area Adjacency with Multiple Interfaces

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

For more information on OSPFv2 Multi-Area Adjacency, refer to the following RFC: https://datatracker.ietf.org/doc/html/rfc5185.

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

BGP Labeled Unicast - Assign Null Label 3 to Local Routes

The BGP Labeled Unicast (LU) functionality is enhanced to assign an implicit NULL LABEL 3 specifically for locally originated or redistributed IPv4 routes from other protocols. This functionality can be enabled using a new BGP implicit-null CLI introduced in the BGP address-family IPv4 labeled-unicast configuration mode. Enabling this mode from the BGP router automatically adds implicit-null CLI to the existing configuration.

Limitation:
Configuring BGP implicit null among network peers running different OcNOS version earlier than 6.5.x causes traffic drops. To restore traffic flow, remove the implicit null configuration. Additionally, to implement this feature, ensure all peers are using version 6.5.x or higher.

For configuration information, refer to the BGP Labeled Unicast with Implicit Null Label for Local Routes in the *OcNOS Layer 3 Configuration Guide*, Release 6.5.2.

Single Home EVPN-ELAN over SRv6

The Single Home EVPN-ELAN over SRv6 solution provides seamless scalability, simplified management, and enhanced performance. Experience flexible, secure, and future-ready network infrastructure with Single Home EVPN-ELAN over SRv6.

For more information, refer to the Configure SRv6 with EVPN ELAN section in the *OcNOS Key Feature document*, Release 6.5.2.

Improved Management

PTP Support in S9600-28DX Platform

OcNOS provides support for the UfiSpace S9600-28DX a platform that enables multiple application architectures required for high traffic loading in a 5G mobile Ethernet network.

For more information, refer to the S9600-28DX Port Mapping in the *OcNOS UfiSpace Installation Guide*, Release 6.5.2.

hardware-profile seamless-bfd

When downgrading to version 6.3.0 from a higher build version configure the "`hardware-profile seamless-bfd disable`" command.

For more information, refer to the Bidirectional Forwarding Commands section in the *OcNOS Layer3 Guide*, Release 6.5.2.

LLDP Support on VLAN and Sub-interface

The management addresses and interface index associated with SVI, Subinterface, and LAG interface are encapsulated in Management Address TLV and communicated to the LLDP peer system.

For more information, refer to the Link Layer Discovery Protocol Configuration in the *OcNOS Layer 2 Guide*, Release 6.5.2.

BFD Support on LAG Interface

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

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

DHCPv6 Prefix Relay Delegation

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

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

Event Manager

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

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

Enhanced Streaming Telemetry

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

Dial Out Mode

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

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

Poll Mode Subscription

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

Once Mode Subscription

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

OpenConfig and IPI Data Model Support

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

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

PROTO or JSON Encoding

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

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

gNMI In-Band Support

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

Port Number Change for gNMI Server

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

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

Update to gNMI Source Field

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

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

IPFIX

OcNOS introduces the Internet Protocol Flow Information Export (IPFIX) Exporter, which enhances network traffic analysis through real-time flow monitoring and sampling. The IPFIX Exporter enables administrators to select and export flow records containing traffic information, facilitating insights into network behavior and patterns. It streamlines network management tasks, optimizes resource utilization, and provides visibility into network traffic for improved monitoring and troubleshooting capabilities.

For more information, refer to the IP Flow Information Export section in the *OcNOS System Management Guide*, Release 6.5.2.

OpenConfig Support for 400G ZR/ZR+

OcNOS extends support for 400G ZR/ZR+ OpenConfig Translation. ZR/ZR+ provides a flexible and interoperable solution for both long-haul networks and Data Center Interconnection (DCI) needs. It allows seamless data transfer between long distances with signals that are resilient to degradation and ensures high bandwidth and low latency support for applications requiring real-time data transfer.

For more information, refer to the OpenZR+ OpenConfig Translation *OcNOS OpenConfig Command Reference*, Release 6.5.2.

BGP ORF Support for VPNv4

Introduces the Router Address Family mode and provides support for IPv4 unicast, IPv4 multicast, IPv4 labeled-unicast, VPNv4 unicast, IPv4 unnumbered, IPv6 unicast, IPv6 labeled-unicast, and VPNv6 unicast..

For more information, refer to the BGP ORF Prefix-List VPNV4 Address section in the *OcNOS Layer 3 Guide*, Release 6.5.2.

Dynamic Port Breakout

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

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

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

Signal Integrity in QSFP-DD

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

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

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

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

Modification of OPER_LOG to Debug Log for EVPN Module

The operational log (OPER_LOG) for the EVPN module has been modified to a debug log. This enhancement increases logging granularity for better debugging and troubleshooting of EVPN operations.

HSL Oper Log Changed to HSL Debug Log for EVPN

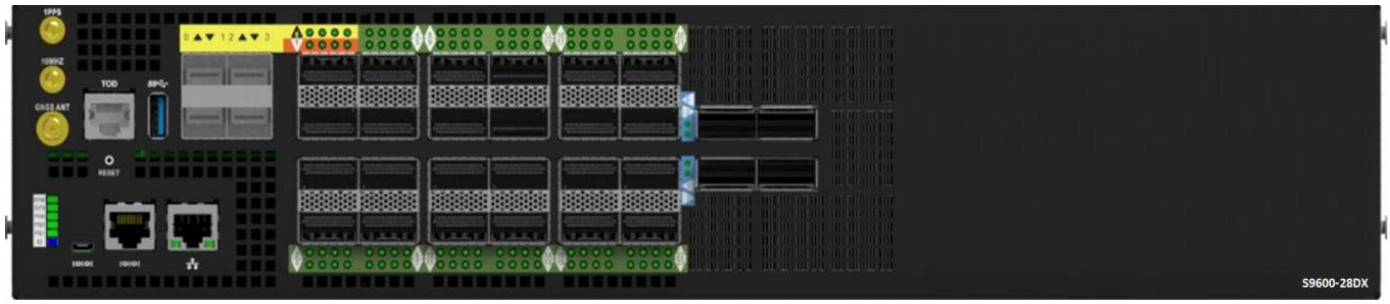
The HSL operational log has been changed to the HSL < debug-info > log specifically for the EVPN module. This change improves the detail and clarity of logs for more effective diagnosis of issues within the EVPN environment.

Hardware Platform

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

UfiSpace S9600-28DX

OcNOS provides support for the UfiSpace S9600-28DX, a platform that enables multiple application architectures required for high traffic loading in a 5G mobile Ethernet network.

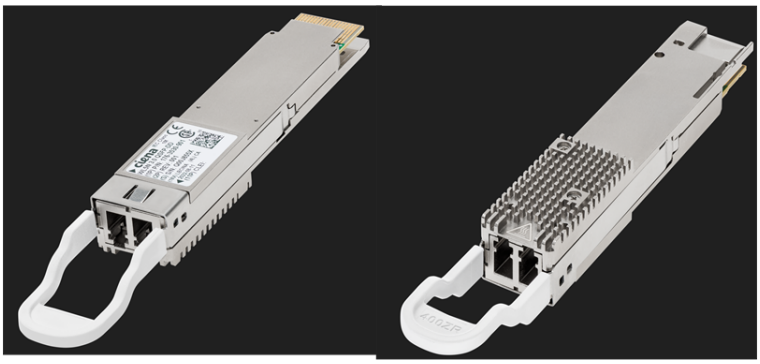


Back and Front Panel View

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

Ciena ZR 176-3530-901

OcNOS supports WaveLogic 5 Nano (WL5n) 400ZR QSFP-DD transceiver. The use cases for the WL5n 400ZR transceiver are the Data Center Interconnect (DCI) and metropolitan area supporting the speed of 400Gbps and 4x100Gbps. The coherent silicon photonics technology combined with optimized electro-optic components and an advanced 7nm DSP provides high performance, micro scale, low power, and cost-effective solution.



WaveLogic 5 Nano 400ZR QSFP-DD Transceiver

For more details on the PLATFORM MODEL, OPTICS PART NUMBER, MAKE, TRANSCEIVER CATEGORY, TYPE, INTERFACE (G), REACH, and TEMP, refer to the Cables and Transceivers List.

Security Update

To ensure product security, OcNOS undergoes rigorous vulnerability scanning, and any issues found are promptly addressed. To review the OcNOS security profile, request a detailed OcNOS Security Report from IP Infusion sales team.

Technical Support

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

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: https://www.ipinfusion.com/documentation/ocnos-product-documentation/data-centers/release-6-5/.

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

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

Technical Sales

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