



OcNOS[®]

**Open Compute Network Operating System
for Data Centers**

Release Notes

Version 7.0.0

March 2026

©2026 IP Infusion Inc. All Rights Reserved.

This documentation is subject to change without notice. The software described in this document and this documentation are furnished under a license agreement or nondisclosure agreement. The software and documentation may be used or copied only in accordance with the terms of the applicable agreement. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of IP Infusion Inc.

IP Infusion Inc.

3979 Freedom Circle, Suite 900

Santa Clara, CA 95054

+1 408-400-1900

<http://www.ipinfusion.com/>

For support, questions, or comments via E-mail, contact:

support@ipinfusion.com

Trademarks:

IP Infusion and are trademarks or registered trademarks of IP Infusion. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Use of certain software included in this equipment is subject to the IP Infusion, Inc. End User License Agreement at <http://www.ipinfusion.com/license>. By using the equipment, you accept the terms of the End User License Agreement.

| CONTENTS

Contents	3
Preface	6
About this Guide	6
Audience	6
Conventions	6
IP Infusion Product Release Version	6
Related Documentation	7
Feature Availability	7
Migration Guide	7
IP Maestro Support	7
Technical Support	7
Technical Sales	7
Technical Documentation	7
Documentation Disclaimer	8
Comments	8
Overview	9
Target Users	9
Key Capabilities	9
Quick Links	9
OcNOS Data Center	10
Key Benefits of OcNOS	10
Release 7.0.0	11
Routing and Security Enhancements	13
BGP VRF Export-Map Enhancement	13
BGP RT-Filter Visibility Enhancements	13
IGMP Offlink Log Suppression	13
BGP Labeled Unicast Next Hop in Route-Map	13
Optimized Debug Logging via Background Debug Recording (BDR)	13
EVPN L3 Gateway with VXLAN Stitching	14
Route Maps in BGP EVPN	14
EVPN L3 Gateway with VXLAN Stitching	14
Layer 2 Service Enhancements	15
Enhanced LACP Force-up Behavior	15
Added Clear LLDP Neighbors	15
Disable MAC Learning on Layer 2 Protocol Packets	15
HPC or Artificial Intelligence Networking	16
Dynamically Adjusts Explicit Congestion Notification Marking Threshold Values	16
PFC Deadlock Detection and Recovery	16
PFC Frames and ECN Packets Monitoring	16

Switch Packet Buffer Tuning	17
ECN and PFC Support for Lossless VxLAN Transport	17
Layer 2 or Layer 3 Overlay Networking	18
Layer 3 Sub-Interface Support in OcNOS-DC	18
Route Distinguisher (RD) Configuration Restriction	18
VxLAN Software Forwarding on Demo VM	18
Network Management and Automation	19
Mandatory Migration of Service Template Configuration before Upgrade	19
RBAC Access to System Bootup Logs	19
NetConf Access Control Model User Guide	19
Event Manager Action Script Validation Enhancement	19
sFlow - Sample Packet Monitoring for Multiple Interfaces	19
Secure Upgrade and Downgrade Using HTTPS	20
Support for USB-Based Backup and Restore	20
SNMP SysOID Support for Vendor and Model Identification	20
Enhanced Alarm Support in the Fault Management System	20
Support for CLI-Script and CLI-Shell Commands	21
sFlow Port PVID Update Support for Sampled Traffic	21
Enhanced DHCP Snooping and Relay Option 82 Support	21
SNMP Configuration for ALARM-MIB Support	21
System Limits and Counters – Show and NetConf Enhancement	22
sFlow - Ingress and Egress Interface Indexes for Sample Packets	22
Streaming Telemetry Enhancements	22
On-Change Stream Mode Support	22
Enhanced gNMI Authentication and Certificate Management	22
Enhanced Port Configuration	22
IPv6 Interface Support Update	23
Data Model Support	23
Mirror Filtered Packets to CPU	23
VxLAN OAM for Overlay Networks	23
Image Upgrade by Traffic Diversion (IUTD)	23
Deprecation of commit dry-run Command	24
Support for Custom GET/SET RPCs	24
Enhanced Security and Performance	25
Per-Core CPU Average Setting	25
SNMPv3 User Password Encryption	25
Enhanced SSH HostKey Algorithm	25
Network Resilience	26
EVPN Multihoming and MC-LAG Hybrid Deployment Support	26
Hardware Platform	27
Multi Firmware Update Version Display	27
Transceivers	27
Smartoptics IPI-SO-TD8002-S31C-SO	27
ATOP IPI-AT-APQD85KCDMS8C	28
E.C.I.Networks IPI-EN-QDD800-2LR4-2CS	28
E.C.I.Networks IPI-EN-QDD800DAC-xM	28
Accelink IPI-AL-RTXM600-411	29

Accelink IPI-AL-RTXM600-2004	29
Accelink IPI-AL-RTXM-600-2001	29
Smartoptics IPI-SO-TQ2031-TUNC-SO	30
Smartoptics IPI-SO-TQ2025-TUNC-SO	31
Smartoptics IPI-SO-TOC003-SC4C-SO	32
Smartoptics IPI-SO-TOC004-SC4C-SO	32
Smartoptics IPI-SO-DOC001-003C-SO	33
Security Updates	34
OcNOS End-of-Sale Notice	34

PREFACE

About this Guide

This guide describes how to configure Release Notes in OcNOS.

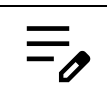
Audience

This guide is intended for network administrators and other engineering professionals who configure OcNOS.

Conventions

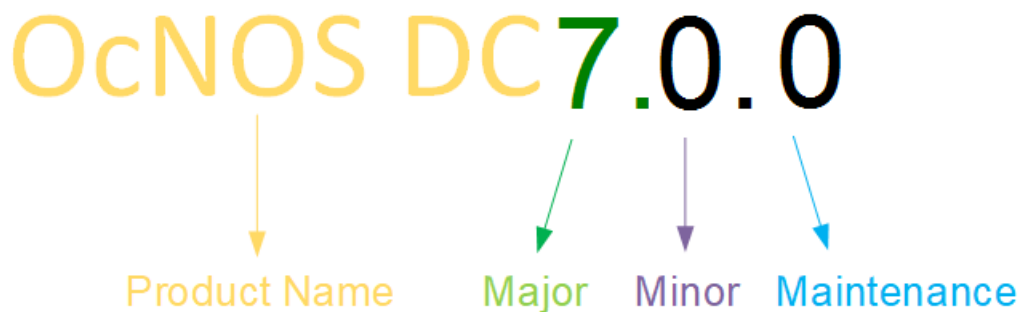
The [Table 1](#) table shows the conventions used in this guide.

Table 1. Conventions

Convention	Description
Italics	Emphasized terms; titles of books
 Note:	Special instructions, suggestions, or warnings
<code>monospaced type</code>	Code elements such as commands, parameters, files, and directories

IP Infusion Product Release Version

Each integer in release numbers indicates Major, Minor, and Maintenance release versions. Build numbers that follow the release 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; including a significant marketing change or direction in the product.

Minor Version: Enhancements or extensions to existing features, changes to address external needs, or internal improvements to satisfy new sales regions or marketing initiatives.

Maintenance Version: A collection of product bugs or issues usually scheduled every 30 or 60 days, based on the number of issues.

Related Documentation

For information about installing OcNOS, see the *Installation Guide* for your platform.

Feature Availability

Each OcNOS SKU contains a set of supported features. For a list of available features based on the SKU that you purchased, refer to the [Feature Matrix](#) .

Migration Guide

Check the *Migration Guide* for necessary configuration changes before migrating from one version of OcNOS to another.

IP Maestro Support

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

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 Sales

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

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](#).

Documentation Disclaimer

The global documentation site is evolving to provide an enhanced website user experience for select topics included in this release. Some guides are now available outside the existing documentation library and can be accessed directly from custom documentation landing pages. These guides offer robust in-built search functionality.

For the latest documentation, visit the product-specific documentation landing page and select the relevant guide.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

OVERVIEW

The Open Compute Network Operation System Data Center (OcNOS) Release Notes provide a consolidated summary of all new features, enhancements, hardware additions, and optics support introduced in a specific release. This document serves as the primary reference for understanding the scope and impact of changes delivered in that release.

Release Notes present high-level feature summaries and platform updates. Detailed configuration and operational information is available in the respective module guides within the documentation library.

Target Users

This guide is intended for:

- Network architects evaluating release readiness
- Operations teams planning upgrades
- Technical planners assessing feature availability
- Sales and solution teams aligning capabilities to customer requirements

Key Capabilities

This guide enables users to:

- Quickly identify new features and enhancements introduced in a release
- Review added hardware and optics support
- Assess release impact before upgrade planning
- Navigate to corresponding module documentation for detailed implementation

Quick Links

- [Routing and Security Enhancements \(page 13\)](#)
- [Layer 2 Service Enhancements \(page 15\)](#)
- [HPC or Artificial Intelligence Networking \(page 16\)](#)
- [Layer 2 or Layer 3 Overlay Networking \(page 18\)](#)
- [Network Management and Automation \(page 19\)](#)
- [Enhanced Security and Performance \(page 25\)](#)
- [Network Resilience \(page 26\)](#)
- [Hardware Platform \(page 27\)](#)
- [Security Updates \(page 34\)](#)
- [OcNOS End-of-Sale Notice \(page 34\)](#)

| OCNOS DATA CENTER

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 softwarebased 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.

RELEASE 7.0.0

OcNOS DC Release 7.0.0 introduces several software features, product enhancements, and support for new optics and hardware devices.

Routing and Security Enhancements	13
BGP VRF Export-Map Enhancement	13
BGP RT-Filter Visibility Enhancements	13
IGMP Offlink Log Suppression	13
BGP Labeled Unicast Next Hop in Route-Map	13
Optimized Debug Logging via Background Debug Recording (BDR)	13
EVPN L3 Gateway with VXLAN Stitching	14
Route Maps in BGP EVPN	14
EVPN L3 Gateway with VXLAN Stitching	14
Layer 2 Service Enhancements	15
Enhanced LACP Force-up Behavior	15
Added Clear LLDP Neighbors	15
Disable MAC Learning on Layer 2 Protocol Packets	15
HPC or Artificial Intelligence Networking	16
Dynamically Adjusts Explicit Congestion Notification Marking Threshold Values	16
PFC Deadlock Detection and Recovery	16
PFC Frames and ECN Packets Monitoring	16
Switch Packet Buffer Tuning	17
ECN and PFC Support for Lossless VxLAN Transport	17
Layer 2 or Layer 3 Overlay Networking	18
Layer 3 Sub-Interface Support in OcNOS-DC	18
Route Distinguisher (RD) Configuration Restriction	18
VxLAN Software Forwarding on Demo VM	18
Network Management and Automation	19
Mandatory Migration of Service Template Configuration before Upgrade	19
RBAC Access to System Bootup Logs	19
NetConf Access Control Model User Guide	19
Event Manager Action Script Validation Enhancement	19
sFlow - Sample Packet Monitoring for Multiple Interfaces	19
Secure Upgrade and Downgrade Using HTTPS	20
Support for USB-Based Backup and Restore	20
SNMP SysOID Support for Vendor and Model Identification	20
Enhanced Alarm Support in the Fault Management System	20
Support for CLI-Script and CLI-Shell Commands	21

sFlow Port PVID Update Support for Sampled Traffic	21
Enhanced DHCP Snooping and Relay Option 82 Support	21
SNMP Configuration for ALARM-MIB Support	21
System Limits and Counters – Show and NetConf Enhancement	22
sFlow - Ingress and Egress Interface Indexes for Sample Packets	22
Streaming Telemetry Enhancements	22
Mirror Filtered Packets to CPU	23
VxLAN OAM for Overlay Networks	23
Image Upgrade by Traffic Diversion (IUTD)	23
Deprecation of commit dry-run Command	24
Support for Custom GET/SET RPCs	24
Enhanced Security and Performance	25
Per-Core CPU Average Setting	25
SNMPv3 User Password Encryption	25
Enhanced SSH HostKey Algorithm	25
Network Resilience	26
EVPN Multihoming and MC-LAG Hybrid Deployment Support	26
Hardware Platform	27
Multi Firmware Update Version Display	27
Transceivers	27
Security Updates	34
OcNOS End-of-Sale Notice	34

Routing and Security Enhancements

BGP VRF Export-Map Enhancement

OcNOS now supports route-map–based export filtering and attribute modification at the VRF level. Administrators can apply route-maps to VRFs to filter exported routes using match conditions and adjust key BGP attributes with set clauses before the routes leave the VRF. This provides more granular control over inter-VRF route export policies, enhances security, and improves traffic engineering.

For more details, refer to the [export map](#) command in the *OcNOS Layer 3 Guide*, Release 7.0.0.

BGP RT-Filter Visibility Enhancements

OcNOS introduces two new commands, `show ip bgp rtfilter neighbors <prefix> advertised-routes` and `show ip bgp rtfilter neighbors <prefix> received-routes`, to display BGP Route-Target (RT) filter routes advertised to or received from a specific neighbor. These commands enhance visibility and make troubleshooting RT-filter route exchanges easier.

For more details, refer to the `show ip bgp rtfilter neighbors` command in the *OcNOS Layer 3 Guide*, Release 7.0.0.

For more details, refer to the [show ip bgp rtfilter neighbors](#) command in the *OcNOS Layer 3 Guide*, Release 7.0.0.

IGMP Offlink Log Suppression

OcNOS adds a new per-interface CLI option `log-suppress` to the `ip igmp offlink` command. When configured, warning messages for IGMP reports from non-local subnets are suppressed entirely, reducing log volume in environments with many offlink receivers.

For more details, see the [ip igmp offlink](#) command in the *OcNOS Multicast Guide*, Release 7.0.0.

BGP Labeled Unicast Next Hop in Route-Map

BGP Labeled Unicast Next Hop in Route-Map provides the ability to selectively set the next hop value to self, and the label attributes of the matched routes are replaced with the local BGP peer address and the local label.

For more information, refer to the [BGP Labeled Unicast Next Hop in Route-Map](#) section in the *OcNOS Layer 3 Guide*, Release 7.0.0.

Optimized Debug Logging via Background Debug Recording (BDR)

Introduced the Background Debug Recording (BDR) feature to optimize debug logging performance by storing debug logs in an in-memory buffer instead of writing them directly to disk, and periodically or manually flushing them to log files to reduce I/O overhead. This enables users to keep debugging active during testing without impacting system performance or requiring test reruns. In the event of a crash, in-memory logs can be retrieved for analysis. The feature supports configurable buffer sizes (1–10 MB), module-based logging, severity level selection, and optional suppression of non-BDR logs. BDR must be explicitly enabled and configured per module.

For more details, see the [Background Debug Recording](#) section of the *OcNOS System Management Guide*, Release 7.0.0.

EVPN L3 Gateway with VXLAN Stitching

OcNOS supports Layer 3 EVPN Gateway Stitching, enabling seamless IP connectivity between independent VXLAN EVPN domains or VRFs without merging their control planes or Layer 2 broadcast domains. The feature uses EVPN Type-5 route stitching at border leaf or spine devices to facilitate scalable and secure inter-domain routing across multi-site data centers, multi-PoD fabrics, and hybrid cloud environments.

For more details, refer to the [EVPN L3 Gateway with VXLAN Stitching](#) section in *OcNOS Virtual Extensible LAN Guide*, Release 7.0.0.

Route Maps in BGP EVPN

Enables operators to apply route maps for the EVPN address family, including BGP L2VPN unnumbered mode. Allows matching on EVPN route-type and MAC lists to filter routes in IN and OUT directions, providing fine-grained policy control, selective advertisement of Type-5 prefixes, and flexible route management across EVPN networks.

For more information, refer to the section in the *OcNOS Layer 3 Guide*, Release 7.0.0.

EVPN L3 Gateway with VXLAN Stitching

OcNOS supports Layer 3 EVPN Gateway Stitching, enabling seamless IP connectivity between independent VXLAN EVPN domains or VRFs without merging their control planes or Layer 2 broadcast domains. The feature uses EVPN Type-5 route stitching at border leaf or spine devices to facilitate scalable and secure inter-domain routing across multi-site data centers, multi-PoD fabrics, and hybrid cloud environments.

For more details, refer to the [EVPN L3 Gateway with VXLAN Stitching](#) section in *OcNOS Virtual Extensible LAN Guide*, Release 7.0.0.

Layer 2 Service Enhancements

Enhanced LACP Force-up Behavior

OcNOS introduces the 90-second activation delay timer for LACP force-up links. A link enters the force-up state after 90 seconds without PDUs on all member links and immediately exits when PDUs are received. The timer restarts when a member link flaps.

For more details, refer to the [LACP Aggregator Force-up](#) section in the *OcNOS Layer 2 Guide*, Release 7.0.0.

Added Clear LLDP Neighbors

Introduced a new CLI command `clear lldp neighbors` to allow operators to dynamically clear LLDP neighbor information. This enhancement enables users to remove all learned LLDP neighbors at once or selectively clear entries associated with a specific interface, providing operational flexibility for troubleshooting neighbor discovery, validating link changes, and refreshing LLDP state without requiring a system or process restart. The feature is available in both Exec and Privileged Exec modes and helps maintain accurate and up-to-date LLDP topology information.

For more details, refer to the [Link Layer Discovery Protocol Commands](#) section of the *OcNOS Layer 2 Guide*, Release 7.0.0.

Disable MAC Learning on Layer 2 Protocol Packets

Introduced a new CLI `l2protocol all learn-disable` command to disable MAC address learning from all Layer 2 protocol data units (BPDU) received on the device. When configured, the device does not learn the source MAC addresses of Layer 2 control protocol packets, including xSTP, LACP, EAP, LLDP, EFM, SyncE, and ELMI, on any interface.

For more details, see the [l2protocol all learn-disable](#) topic in the *OcNOS System Management Guide*, Release 7.0.0.

HPC or Artificial Intelligence Networking

Dynamically Adjusts Explicit Congestion Notification Marking Threshold Values

OcNOS is enhanced to support lossless Ethernet fabrics for AI/ML workloads through Dynamic Explicit Congestion Notification (D-ECN) method on Broadcom Tomahawk5 platforms.

D-ECN allows users to adjust the ECN thresholds using D-ECN-ON-Offset and D-ECN-OFF-Offset settings that provides capability to enable precise congestion marking based on shared buffer usage.

Unlike traditional methods that depend on packet drops, D-ECN enhances efficiency by marking IP headers to indicate congestion, prompting receivers to signal senders to adjust transmission rates.

For further details, refer to [Dynamic ECN Marking](#) section in the *OcNOS Quality of Service Guide*, Release 7.0.0.

PFC Deadlock Detection and Recovery

OcNOS now supports Priority Flow Control (PFC) Deadlock Detection and Recovery. It prevents network congestion and improves performance in data transmission. It works by allowing the transmitter to dynamically adjust the amount of data sent to the receiver based on the receiver's ability to process the data.

This enhancement introduces mechanisms to detect and recover from PFC deadlocks, ensuring traffic flows are restored automatically without manual intervention. It provide the following capabilities:

- Per-interface enablement of PFC deadlock detection and recovery.
- Timer-based monitoring to identify persistent XOFF conditions.
- PFC State XON mode to restore traffic once congestion clears.
- Global action mode to automatically drop traffic in deadlock scenarios if configured.

For more details, refer to the Priority-based [PFC Deadlock Detection and Recovery](#) section in the [OcNOS Layer 2 Guide](#), Release 7.0.0.

For more details, refer to the [PFC Deadlock Detection and Recovery](#) topic in the OcNOS Layer 3 Guide, Release 7.0.0.

PFC Frames and ECN Packets Monitoring

OcNOS now supports monitoring of Priority-based Flow Control (PFC) pause frames and Explicit Congestion Notification (ECN) marked packets.

PFC (IEEE 802.1Qbb) provides per-priority flow control by pausing traffic for specific classes, preventing congestion and improving link utilization.

ECN (RFC 3168) enables end-to-end congestion signaling in TCP/IP networks by marking packets instead of dropping them, prompting the sender to reduce its transmission rate until congestion clears.

It supports the following capabilities:

- Monitoring of ECN-marked packets on an interface.
- Monitoring of PFC pause frames on an interface.

For more details, refer to the [PFC Frames and ECN Packets Monitoring](#) section in the [OcNOS Layer 2 Guide](#), Release 7.0.0.

For more details, refer to the [PFC Frames and ECN Packets Monitoring](#) topic in the OcNOS Layer 3 Guide , Release 7.0.0.

Switch Packet Buffer Tuning

This release introduces Network Switch Packet Buffer Tuning, a system designed to enhance network switch performance by avoiding congestion and packet drops. This feature allows for the allocation of packet buffer size based on traffic priority classes, known as Priority Groups (PGs), instead of physical ports.

Key Enhancements Include:

- Custom device responses to Priority-based Flow Control (PFC) pause storms, enabling precise control over when the switch transmits pause frames to prevent packet loss.
- Priority Group (PG) configuration with specific limits on shared memory and the ability to set PFC X-OFF and X-ON offsets to trigger pause frames during congestion.
- Queue-specific buffer limits using a dynamic threshold (alpha value) for fine-grained control over buffer consumption from the shared pool.
- Global adjustment of buffer limits, simplifying configuration.

Supported Platforms: This feature is intended for LTSW chipsets (Tomahawk4 (TH4) platforms, Tomahawk5 (TH5) platforms, Trident4 (TD4) platforms) and DC chipsets (Tomahawk3 (TH3) platforms, Trident3 (TD3) platforms).

For more details, refer to the [Switch Packet Buffer Tuning](#) section in *OcNOS Quality of Service Guide*, Release 7.0.0.

ECN and PFC Support for Lossless VxLAN Transport

OcNOS 7.0 enables Explicit Congestion Notification (ECN) and Priority Flow Control (PFC) operation over VxLAN overlays, allowing operators to extend lossless transport capabilities across multi-tenant AI fabrics and frontend network.

These enhancements provides:

- Scalable Layer 2 and Layer 3 multi-tenancy.
- End-to-end lossless transport across overlay networks.
- Seamless integration of AI workload isolation with high-performance GPU fabric requirements.

For more details, refer to the [Unified ECN and PFC Support for Lossless VxLAN Transport](#) section in the *OcNOS Virtual Extensible LAN Guide*, Release 7.0.0.

Layer 2 or Layer 3 Overlay Networking

Layer 3 Sub-Interface Support in OcNOS-DC

OcNOS-DC now supports Layer 3 (L3) subinterfaces. An L3 subinterface is a logical interface created on a physical port, allowing multiple IP networks or VLANs to share the same physical interface while maintaining separate routing domains. This feature enables efficient inter-VLAN routing, scalability, and reduced port usage, especially for WAN uplinks.

For more details, see the [Layer 3 Sub-interface Configuration](#) section in the *OcNOS Layer 3 Guide*, Release 7.0.0.

Route Distinguisher (RD) Configuration Restriction

Manual configuration of the Route Distinguisher (RD) is restricted within the reserved range vtepip.64512 to vtepip.64532, where vtepip represents the globally configured VTEP IP address. This reservation prevents conflicts with system-generated RD values that are automatically derived from the global VTEP IP, ensuring consistent and reliable operation of EVPN and VXLAN services.

For more details, see the [rd \(route distinguisher\)](#) topic in the *OcNOS Layer 3 Guide*, Release 7.0.0.

VxLAN Software Forwarding on Demo VM

VxLAN Software Forwarding on OcNOS DEMO VM enables L2 and L3 VxLAN forwarding on OcNOS-x86-based platforms. The feature supports Static VxLAN BGP, VxLAN IRB (Asymmetric and symmetric) deployments using a software data path.

For more details, refer to the [OcNOS VXLAN Guide](#), Release 7.0.0.

Network Management and Automation

Mandatory Migration of Service Template Configuration before Upgrade

After the upgrade to OcNOS 7.0.0 Release, the Service Template CLI commands will be hidden. It is recommended to migrate all Service Template configurations to sub-interface-based commands prior to performing the upgrade.

The following CLI commands are deprecated and no longer supported:

- `mpls-l2-circuit <NAME> service-template <NAME> ((primary|secondary))`
- `vc-mode (standby|revertive) service-template <NAME>`
- `mpls-vpls <NAME> service-template <NAME>`
- `service-template <NAME>`

RBAC Access to System Bootup Logs

RBAC users with privilege levels below 15 can now execute the `show system bootup-log` command, enabling secure access without elevated privileges. Previously, RBAC users were unable to run this command due to file permission restrictions. OcNOS now allows RBAC users to view system bootup logs, enhancing troubleshooting and operational visibility while maintaining secure access controls.

For more details, see the [RBAC Bootup Log Access](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

NetConf Access Control Model User Guide

OcNOS introduces the NetConf Access Control Model (NACM) feature, which provides an access control mechanism for the protocol operations and content layers of NetConf. This feature enables administrators to configure and manage permissions for different authorized users, allowing them to control, modify, and access network resources based on defined rule types and modules.

For more details, refer to [NetConf Access Control Model User Guide](#) section in the *OcNOS NetConf User Guide*, Release 7.0.0.

Event Manager Action Script Validation Enhancement

Event Manager action scripts now require `execute` permission and a Shebang (`#!`) line at the beginning of the script to indicate the interpreter. This ensures compatibility and correct execution of the configured scripts.

For more details, refer to [Event Manager](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

sFlow - Sample Packet Monitoring for Multiple Interfaces

The sFlow feature has been enhanced to support multiple collectors to monitor multiple interfaces. This functionality is enabled by default.

When more than one collector is configured and sFlow is enabled on an interface, samples from the interface are sent to all configured collectors.

To disable the sending of samples from an interface to a specific collector or to multiple collectors, a new command `no sflow collector-id` has been introduced at the interface level.

The `show sflow detail` CLI command output has also been updated to display all active collectors for each interface.

For more details, refer to the [sFlow - Sample Packet Monitoring for Multiple Interfaces](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Secure Upgrade and Downgrade Using HTTPS

This enhancement introduces HTTPS protocol support for performing system upgrades and downgrades in OcNOS. It enables secure transfer of OcNOS images and licenses through HTTPS URLs, ensuring integrity and confidentiality during version and license updates.

Installing OcNOS using HTTPS through ONIE is not supported.

For more information, refer to the [Install, License, and Upgrade Configuration](#) section in the *OcNOS Licensing Guide*, Release 7.0.0.

Support for USB-Based Backup and Restore

OcNOS introduces support for backing up and restoring critical system files using a USB drive, enabling network administrators to store configurations, images, and licenses on a USB drive and restore them when needed. This functionality streamlines the recovery and the return merchandise authorization (RMA) processes by verifying and preserving the integrity of the stored data through validation mechanisms.

For more information, refer to the [System Backup and Restore from USB Commands](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

SNMP SysOID Support for Vendor and Model Identification

This feature enables device identification based on the SNMP System Object Identifier (SysOID). It allows the retrieval of vendor and hardware model details through SNMP, simplifying device classification and verification in network management environments.

For more information, refer to the [Simple Network Management Protocol](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Enhanced Alarm Support in the Fault Management System

OcNOS introduces new alarm types in the Fault Management System (FMS). This enhances the network monitoring capability. It also enables precise tracking of critical system components, improving fault detection and operational reliability. The new alarms include:

- `LDP_SESSION_DOWN`: Indicates that an established LDP neighborhood session has transitioned to a down state.

- `LDP_SESSION_UP`: Indicates that a LDP neighborhood session has successfully transitioned to an up state. `LDP_SESSION_FAILURE`: Indicates that a failure has been detected within an active LDP session. `LDP_INTERNAL_ERR`: Indicates that an internal error has occurred within the LDP process or component. `ISIS_OPR_ADJ_STATE`: Indicates a change in the operational state of an IS-IS adjacency.
- `ISIS_OPR_INTF`: Indicates a change in the operational state of an IS-IS interface. `ISIS_OPR_INTF_CIRCUIT_STATE`: Indicates a change in the circuit-level operational state of an IS-IS interface.

For more details, refer to the [Fault Management System Configuration](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Support for CLI-Script and CLI-Shell Commands

OcNOS introduces support for the CLI-Script and CLI-Shell commands to enhance automation and operational flexibility. The CLI-Script command enables the creation and execution of predefined sets of configuration and execution mode commands, with support for including delay and message statements within the script.

For more details, refer to the [CLI-Script and CLI-Shell Command](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

sFlow Port PVID Update Support for Sampled Traffic

OcNOS introduces the `sflow sampling update-port-pvid` command to include the bridge port PVID in sampled untagged packets sent to the collector. This enhancement provides the necessary VLAN context for untagged traffic and is applicable specifically to spanning-tree bridge configurations.

For more details, refer to the [sFlow Commands](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Enhanced DHCP Snooping and Relay Option 82 Support

OcNOS enhances DHCP Snooping and Relay Option82 functionality by enabling the user-defined configuration of the Circuit ID and Remote ID sub-options. Using a template-based approach, parameters such as hostname, interface name, and VLAN ID are included within these sub-options.

For more details, refer to the [DHCP Snooping Commands](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

SNMP Configuration for ALARM-MIB Support

This enhancement introduces SNMP interface support for the Alarms feature in OcNOS and extends the Alarms Data Model to support the retrieval of active alarm information through SNMP get operations and trap notifications. Users can now access alarm data using SNMP Get commands and receive alarm notifications through SNMP traps, ensuring improved monitoring and integration with SNMP-based network management systems.

For more details, refer to the [Simple Network Management Protocol](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

System Limits and Counters – Show and NetConf Enhancement

In OcNOS, the System Limits and Counters (Show and NetConf) feature enhances operational visibility by providing real-time access to hardware and software resource utilization through both CLI and management interfaces. It consolidates capacity data for routing, VLANs, MAC, and protocol sessions into a unified view, helping operators validate resource availability before deployment or scaling. Using YANG-based models with NetConf or gNMI, this feature improves troubleshooting accuracy, supports automation, and ensures consistent system capacity monitoring across all platforms.

For more details, refer to the [System Limits and Counters](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

sFlow - Ingress and Egress Interface Indexes for Sample Packets

sFlow provides a view of the traffic by taking periodic snapshots of packets which helps in identifying the exact source and destination of the packets. While the packet header describes the data, the input and output port provides the context on where the data originated and where it is headed within the switch fabric.

For more details, refer to the [sFlow - Sample Packet Ingress and Egress Interface](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Streaming Telemetry Enhancements

On-Change Stream Mode Support

OcNOS now supports On-Change stream mode for gNMI-based telemetry subscriptions. In this mode, the device sends update notifications only when a subscribed data value changes, reducing telemetry traffic and improving operational efficiency. On-Change mode supports container-level, leaf-level, and wildcard sensor-paths, enabling fine-grained monitoring of dynamic operational states such as interface status, BGP peer state, and transceiver attributes.

For more details, refer to the [On-Change Stream Mode](#) section in the *OcNOS Streaming Telemetry Guide*, Release 7.0.0.

Enhanced gNMI Authentication and Certificate Management

OcNOS now supports gRPC-contained user and password authentication for gNMI TLS connections in addition to X.509 certificate Common Name validation. A new exec-mode command, `crypto pki load`, enables loading of server and CA certificates from external sources to simplify ZTP workflows.

For more details, refer to the [User Authentication and Certificate Loading for gNMI TLS Connections](#) section in the *OcNOS Streaming Telemetry Guide*, Release 7.0.0.

Enhanced Port Configuration

Users can now configure the same port number across multiple VRFs using the `port` command. Users can explicitly set the default port value, which is 9339, and this value will now appear in the output of the `show running-config streaming-telemetry` command. Additionally, updated the valid port range for the `tls`

`tls-port` and `port` commands from `<32768-60999>` to `<1024-65535>` to provide flexibility in deployment.

For more details, refer to the [port](#) and [tls tls-port](#) commands in the *OcNOS Streaming Telemetry Guide*, Release 7.0.0.

IPv6 Interface Support Update

Streaming telemetry now supports connections over IPv6 interfaces in Dial-in mode. IPv6 connections remain unsupported in Dial-out mode.

For more details, refer to the [Dial-In Telemetry Connection over IPv6 Interface](#) commands in the *OcNOS Streaming Telemetry Guide*, Release 7.0.0.

Data Model Support

OcNOS adds support for additional IPI data model modules. The new and existing modules `ipi-vlan`, `ipi-acl`, `ipi-qos`, and `ipi-rib` enhance visibility into the operational status and attributes of various components.

For more details, refer to the [IPI Data Models](#) sections in the *OcNOS Streaming Telemetry Guide*, Release 7.0.0.

Mirror Filtered Packets to CPU

Mirroring to the CPU using a filter provides the ability to mirror filtered data plane packets to the CPU. It enables sniffing of selected packets that match the programmed filter condition and real-time monitoring in the Network Operating System.

For more information, refer to the [Mirror Filtered Packets to CPU](#) section in the *OcNOS Layer 2 Guide*, Release 7.0.0.

VxLAN OAM for Overlay Networks

OcNOS supports VxLAN Operations, Administration, and Maintenance (OAM) to enhance visibility and fault management for VxLAN overlays in CLOS data center fabric. Using Maintenance End Points (MEPs) at VxLAN Tunnel End Point (VTEPs) and Spines within VxLAN tunnels, operators can perform the following operations to verify connectivity, and isolate faults.

- Ping /Loopback - Verify reachability to a remote VTEP and that the VxLAN tunnel is operational end-to-end.
- Pathtrace - Discover the full forwarding path inside the VxLAN fabric, hop-by-hop
- Continuity checks - Provide continuous, periodic monitoring of VxLAN tunnel health.

The feature supports both static and dynamic VxLAN tunnels in single- and multi-homed deployments, simplifying troubleshooting and improving operational reliability.

For more details, refer to the [VxLAN Operation Administration Maintenance](#) section in the *OcNOS VxLAN Guide*, Release 7.0.0.

Image Upgrade by Traffic Diversion (IUTD)

In OcNOS, this feature introduces the Image Upgrade by Traffic Diversion (IUTD) method to ensure continuous network operation during critical software installation and upgrade processes. IUTD minimizes traffic loss by manually diverting to the redundant node for update, and restores the flow only after a comprehensive verification of the new OS is complete.

The process relies on a NETCONF client utilizing callhome. It uses a new start-service-tracking RPC to monitor the status (UP/DOWN) of specified services, such as BGP, OSPF, or ISIS, ensuring the network remains stable throughout the maintenance window.

For more details, refer to the [Image Upgrade by Traffic Diversion \(IUTD\)](#) section in the *NetConf User guide*, Release 7.0.0.

Deprecation of commit dry-run Command

The `commit dry-run` command has been deprecated and removed from the Command Reference. It is no longer supported due to inconsistencies with the current commit behavior, leading to incorrect expectations during validation. It is advised to rely on the standard commit work-flow for configuration validation.

Support for Custom GET/SET RPCs

In OcNOS, this feature supports specialized NetConf RPCs (`transceiver-cmis-read` and `transceiver-cmis-write`) to enable direct access to CMIS custom memory pages. These custom GET/SET commands are sent straight to the protocol module (CMMd) for read/write operations, effectively bypassing the OcNOS configuration database on the transceiver hardware.

For more details, refer to the [Backend API-support for Custom GET/SET RPC](#) section in the *OcNOS NetConf User Guide*, Release 7.0.0.

Enhanced Security and Performance

Per-Core CPU Average Setting

OcNOS introduces the `cpu-core-monitor-average interval <60-600>` command to set the averaging interval (in seconds) for CPU per-core usage monitoring. This command sets the average window OcNOS uses to calculate and report CPU usage per core. Configure any value between 60 and 600 seconds; the default is 60 seconds. Use the `no cpu-core-monitor-average interval` command to restore the default.

For more details, refer to the [cpu-core-monitor-average](#) topic in the *OcNOS System Management Guide*, Release 7.0.0.

SNMPv3 User Password Encryption

The SNMPv3 user password is now stored in an encrypted format in the `/etc/snmp/snmp.conf` file. Passwords associated with the `CreateUser` and `trapsess` entries are now stored in encrypted form using either MD5 or SHA encryption methods.

For more details, refer to the [Simple Network Management Protocol](#) section in the *OcNOS System Management Guide*, Release 7.0.0.

Enhanced SSH HostKey Algorithm

After upgrading to 6.6.0, SSH sessions from remote servers fail because OpenSSH was updated to version 9.2p1, which deprecates `ssh-rsa` and `ssh-dsa`. The problem is further caused by the absence of the `HostKeyAlgorithms` in the upgraded `sshd_config`, resulting in rejected connections. This has been addressed in the 7.0.0 release by adding the `HostKeyAlgorithms`, enforcing security with modern algorithms such as Ed25519 and RSA-SHA.

The Key Exchange (KEX) algorithm list was subsequently updated to align with the new OpenSSL package, specifically regarding the `sntrup761x25519-sha512` algorithm.

For more details, refer to the [Secure Shell Commands](#) topic in the *OcNOS System Management Guide*, Release 7.0.0.

Network Resilience

EVPN Multihoming and MC-LAG Hybrid Deployment Support

The Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) network type supported on CLOS fabric devices provides the following capabilities:

1. EVPN Multihoming (EVPN MH) & MC-LAG Coexistence: Enables smooth migration from traditional Multi-chassis Link Aggregation (MC-LAG) to standards-based EVPN multihoming.
2. Ensures redundancy through MC-LAG and dual-homing of hosts to Routers (VTEPs).
3. Equal Cost Multi-Path (ECMP) support from Router (VTEP) to Router (VTEP), enhancing path diversity.
4. Ensures seamless integration into customer environments, existing MC-LAG nodes are treated as single-homed nodes within EVPN, facilitating redundancy and smooth interoperability transition between the two network types.

This capability enables a hybrid deployment model, allowing data centers to protect existing MC-LAG investments while incrementally adopting EVPN multihoming. The approach ensures operational continuity, redundancy, and simplified migration.

CLI Enhancements

To support this feature, the following commands are introduced:

1. **show evpn esi** — Display multihomed segments and their corresponding attached VTEPs
2. **show nvo vxlan vni-tunnel** — Display VPN endpoints
3. **nvo vxlan vtep-info** — Configures the VTEP in vtep-info config mode

For more details, refer to the [VxLAN Command Reference](#) section in *OcNOS Virtual Extensible LAN Guide*, Release 7.0.0.

Hardware Platform

Multi Firmware Update Version Display

OcNOS now integrates the Multi Firmware Update (MFU) version for UfiSpace switches into the existing `show system-information board-info` command. The MFU version displayed in the show output matches the vendor's MFU version and lists firmware details, including ONIE, BMC, CPLD, and BIOS versions.

This enhancement enables quick verification of board firmware versions from the CLI, eliminating the need to cross-check vendor MFU versions.

For more information, refer to the [show system-information board-info](#) command in the *OcNOS System Management Guide*, Release 7.0.0.

Transceivers

OcNOS supports the following transceivers and amplifiers:

Smartoptics IPI-SO-TD8002-S31C-SO

The QSFP-DD 800G 2xDR4 transceiver (IPI-SO-TD8002-S31C-SO) supports 800Gbps Ethernet in data centers, with a reach of up to 500m over single-mode fiber. It features two MPO-12 connectors, supports various electrical interfaces (800GAUI-8, 2x400GAUI-4, 8x100GAUI-1), and complies with CMIS 5.0 for digital diagnostics. The transceiver consumes less than 14W, and operates from 0°C to +70°C. It supports aggregate line rates for 800Gbps, 2x400GbE, and 8x100GbE configurations.

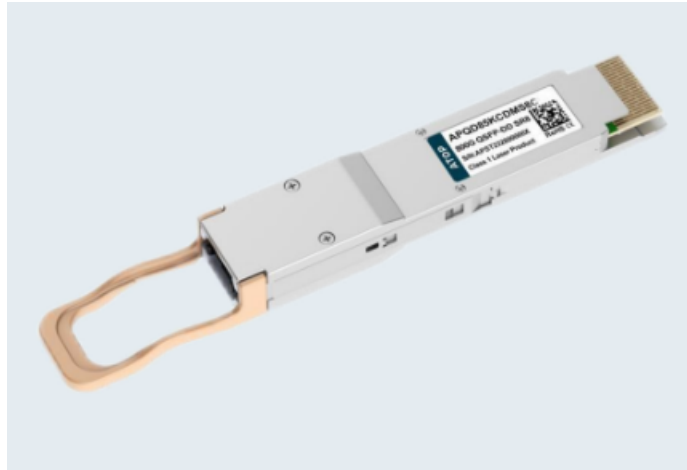
Figure 1. QSFP-DD800 800G-2xDR4 SM Transceiver



ATOP IPI-AT-APQD85KCDMS8C

The ATOP IPI-AT-APQD85KCDMS8C is an 800Gb/s QSFP-DD SR8 optical transceiver. It is designed for 50m OM4/OM5 optical communication, converting 8 channels of 100Gb/s (PAM4) electrical input to 8 parallel 100Gb/s optical signals, and vice-versa, for an aggregate data rate of 800Gb/s. It supports 800GBASE-SR8 and 2x400GBASE-SR4 applications and has an MPO16 connector. Power consumption is less than 15W.

Figure 2. 800G QSFP-DD SR8 Transceiver



E.C.I.Networks IPI-EN-QDD800-2LR4-2CS

The IPI-EN-QDD800-2LR4-2CS is an 800G QSFP-DD 2xLR4 transceiver from E.C.I. NETWORKS, supporting up to 10km transmission on single-mode fiber with duplex LC connector. It handles 8-channel 106.25Gb/s (PAM4) electrical data, converting it into 8-channel 106.25Gb/s optical signals for an aggregated 800G optical transmission. It is specifically designed for 2x400GBASE-LR4 applications, with each lane operating at a signaling rate of 53.125 GBd. Power consumption is less than 16W.

Figure 3. 800G QSFP-DD 2xLR4 Transceiver



E.C.I.Networks IPI-EN-QDD800DAC-xM

The IPI-EN-QDD800DAC-xM is an 800G QSFP-DD Passive DAC TWINAX Cable that provides a high-speed, cost-effective, and power-efficient alternative to fiber optics for short-distance interconnects in data centers and high-

performance computing. It supports an aggregate data rate of 800Gbps (PAM4) over 16 copper pairs, with each lane operating up to 100Gb/s. The cable is powered by a 3.3V supply and is compliant with the IEEE 802.3ck 800G Ethernet standard.

Accelink IPI-AL-RTXM600-411

The 800G QSFP-DD800 2x400G FR4 Transceiver (IPI-AL-RTXM600-411) supports up to 106.25Gbps data rate per channel via PAM4 modulation, enabling 800GBASE 2x400G FR4 Ethernet over 2km of single-mode fiber with dual duplex LC connectors. Each lane operates at a signaling rate of 53.125 GBd. Power consumption is less than 14W.

Figure 4. 800G QSFP-DD800 2x400G FR4 Transceiver



Accelink IPI-AL-RTXM600-2004

The Accelink IPI-AL-RTXM600-2004 is an 800G OSFP Closed TOP DR8 Transceiver with an MPO16 connector, designed for 800GBASE-DR8 Ethernet applications and data centers. It supports data rates up to 106.25 Gbps per channel (PAM4 modulation) across 8 duplex channels over single-mode fiber with a maximum link length of 500m. The selectable data rates are 106.25 Gbps and 53.125 Gbps, with a signaling rate of 53.125 GBd per lane. Power consumption is less than 16W.

Figure 5. 800G OSFP Closed TOP DR8 Transceiver



Accelink IPI-AL-RTXM-600-2001

The Accelink 800G OSFP DR8 Transceiver (IPI-AL-RTXM-600-2001) with dual-LC connector, is designed for 800GBASE-DR8 Ethernet applications and data centers. It transmits and receives serial optical data links at up to

106.25 Gbps per channel (PAM4 modulation) over single-mode fiber. The module's signaling rate is 53.125 GBd. Power consumption is less than 16W.

Figure 6. 800G OSFP DR8 Transceiver



Smartoptics IPI-SO-TQ2031-TUNC-SO

The IPI-SO-TQ2031-TUNC-SO is a high-performance 100G ZR QSFP28 Coherent transceiver. Supporting a 103.12Gbps bit rate via a CAUI-4 (4x25G NRZ) electrical interface, this HP CMIS-compliant module offers versatile long-haul capabilities, reaching up to 120km natively and extending to 300km with amplification.

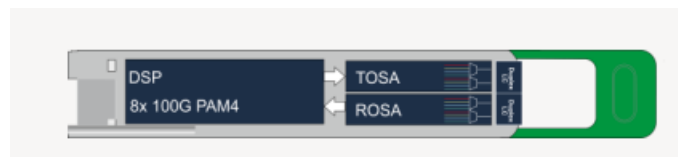
Figure 7. QSFP28 100G Coherent DWDM 120km Transceiver**Smartoptics IPI-SO-TQ2025-TUNC-SO**

The IPI-SO-TQ2025-TUNC-SO is a QSFP28 DWDM transceiver for 100GbE and OTU4 applications with CMIS5.2 and C-CMIS1.2 compliant interface, supporting unamplified reach up to 80km and amplified reach up to 300km. It transmits at a bit rate of 103.12Gbps by splitting the 100Gbps signal into four parallel 25Gbps NRZ electrical streams (CAUI-4). Power consumption is less than 5.5W.

Figure 8. QSFP28 100G Coherent DWDM 80km Transceiver

Smartoptics IPI-SO-TOC003-SC4C-SO

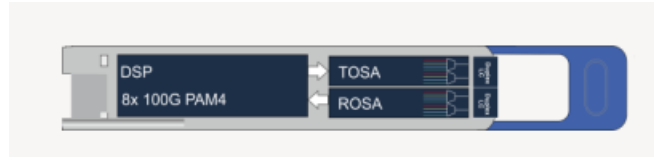
The IPI-SO-TOC003-SC4C-SO is an OSFP112 form-factor transceiver designed for 800Gbps or 2x400G Ethernet applications, compliant with CMIS 5.0. It is intended for use in data center interconnects between switches, routers, and storage equipment, supporting optical distances up to 2km over single-mode fiber (SMF). The electrical interface consists of eight 106.25G signals (800GAUI-8) converted to eight PAM4-modulated channels, while also supporting 2x400GAUI-4 and 2x200GAUI-4 breakout modes. The optical interface features two duplex LC connectors, enabling the aggregation of two 400G-FR4 transceivers. Power consumption for this module is less than 14W.

Figure 9. OSFP112 800G Coherent DWDM 2km Transceiver

Smartoptics IPI-SO-TOC004-SC4C-SO

The IPI-SO-TOC004-SC4C-SO is an OSFP112 form-factor transceiver for 800Gbps or 2x400G Ethernet applications with a CMIS5.0 compliant interface, supporting optical distances up to 10km over single-mode fiber. It transmits at an aggregated bit rate of 800Gbps by converting eight 106.25G electrical signals (800GAUI-8) into eight PAM4-modulated optical channels. The transceiver features two duplex LC connectors and can be configured in 2x400GAUI-4 mode to enable breakout configurations. Power consumption is less than 14W.

Figure 10. OSFP112 800G Coherent DWDM 10km Transceiver



Smartoptics IPI-SO-DOC001-003C-SO

The IPI-SO-DOC001-003C-SO is an OSFP800 Active Electrical Cable (AEC) designed for 800Gbps Ethernet applications, providing a reliable solution for high-density connections within and across adjacent racks. It features a 3-meter reach using AWG32 cabling and is equipped with a CMIS 5.0 compliant management interface.

For more information about the transceivers, contact the IPI sales team.

Security Updates

To ensure product security, OcNOS undergoes rigorous vulnerability scanning and promptly addresses any issues that are found. OcNOS version 7.0.0 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.

OcNOS End-of-Sale Notice

The Edgecore AS7712-32X (TH) platforms have reached End of Sale (EOS). As part of this change, all software updates, enhancements, and technical support for this platform have been discontinued. The platforms are no longer supported for new deployments.

For more details refer [IP Infusion End of Sale and End of Listings](#).