ipinfusion™

OcNOS®

Open Compute Network Operating System for Data Centers Version 6.3.5

Contents

Introduction

Overview

IP Infusion's Open Compute Network Operation System Data Center (OcNOS DC) is used to build both Layer-3 and Layer-2 Data Center fabric as it provides a rich set of control plane features, providing robust quality, ensuring lower costs and, at the same time, providing vendors with a best-of-breed selection for hardware platforms. This release provides support for advanced capabilities, such as EVPN-VXLAN and IP over DWDM.

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 500 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.

OcNOS Software

OcNOS (Open Compute Network Operating System) is a network operating system designed to run on white-box network hardware, 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 and flexible environment and extensive protocol support for software-defined networking (SDN) and disaggregated networks. OcNOS works with applications in diverse network environments, including data centers.

About this Release

This is the OcNOS DC 6.3.5 MR release notes.

OcNOS DC Release 6.3.x provides deployment-ready support to build a hybrid of Layer-3 and Layer-2 Data Centers. Layer 3 routing is used in Tier 1 (core network) and Layer 2 in Tier 3 (access side network). Tier 2 can be based on either Layer 2 or Layer 3. A hybrid model has the advantage of seamless Virtual Machine mobility and requires fewer IP subnets for the data center. Support is provided for following capabilities:

- Comprehensive L2 switching and L3 routing
- EVPN-VXLAN
- Advanced QoS and Data Center Bridging
- SNMP
- Zero Touch Provisioning (ZTP)
- NetConf and, Yang data model

IP Maestro Support

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

IPI Product Release Version

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

- **Product Name:** IP Infusion Product Family
- **Major Version:** New customer-facing functionality represents a significant change to the code base, in other words, a significant marketing change or direction in the product.
- **Minor Version:** Enhancements or extensions to existing features driven by external requirements, such as meeting new sales goals or by internal requirements, such as aligning with a new marketing push.
- **Maintenance Version**: A collection of the product bugs or hotfixes which is scheduled every 60 or 90 days based on the number of hotfixes.

Release 6.3.5

Release 6.3.5 of OcNOS DC introduces the following new software features and enhanced functionalities. This section provides details on these features.

Support BGP MD5 auth for BGP dynamic peer-groups

The BGP dynamic remote neighbor peer authentication is enhanced to accept the request tagged with MD5 signature.

Support ZTP 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 (ZTP1) or after a reboot of the pre-installed OcNOS device (ZTP2). The ZTP1 is supported only on the management interface and the first In-band port. However, the ZTP2 is supported on all out-of-band and in-band interfaces that are UP, but it does not support IPv6 in the 6.3.5 release.

For more information on ZTP, refer to the "*Automatic Install using Zero Touch Provisioning*" section in *OcNOS Installation* Guide, Release 6.3.5.

Support to Add Multiple Tagged VLANs

Supports the addition of multiple tagged VLANs during port security configuration. This enhancement addresses previous database synchronization challenges, ensuring seamless operation and reliability when adding multiple tagged VLANs, saving configurations, and reloading the device.

Support 100G and 200G OFEC in Coherent Optics

The coherent optics module is enhanced to support the following signal modulation formats:

- `dp-qpsk-ofec` Dual polarization quadrature phase shift keying with OFEC

- `8qam-200g-ofec` 8-quadrature amplitude modulation format for 200G with OFEC

Release 6.3.4

Release 6.3.4 of OcNOS DC introduces the following new software features and functionalities. This section provides details on these features.

Modified Extended ACL Deny Rule Behavior in VTY

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

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

- The permit ACL rule remains unchanged.

For more information of the Extended ACL Deny Rule, see the *ACL OVER Virtual Terminal (VTY) Configuration* section in System Management guide.

SFTP and SCP Enhancements

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

For more information, refer to the *Licensing and Upgrade Commands* chapter in the *OcNOS Licensing Guide*, Release 6.3.4.

BGP VPNv4 Route Display Command

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

For more information, refer to the *show ip bgp vpnv4* command section in the *OcNOS Layer 3 Guide*, Release 6.3.4.

Release 6.3.3

Release 6.3.3 of OcNOS DC introduces the following new software features and functionalities. This section provides details on these features.

Custom Syslog Port

Release 6.3.3 enhances the current ability to configure Syslog only on the default port and permits configuration on a custom port. The existing `logging server` CLI command has been enhanced to provide this additional capability. Typically, using the default port in a production network is not recommended. This feature enhancement allows for secure communications using a custom port as opposed to the default port, port 514, that is not considered secure.

Use the revised CLI to configure the custom port within the specified range for Syslog.

New CLI Syntax:

```
logging remote server (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|) (port
<1024-65535>|) (vrf management|)

no logging remote server  (A.B.C.D|X:X::X:X|HOSTNAME) ((0|1|2|3|4|5|6|7)|)
(port|) (vrf     management|)
```

For more information of the Custom Syslog port, see the *Custom Syslog Configuration and Syslog Commands sections* in *System Management* guide.

Release 6.3.2

This release does not introduce any new hardware. This section will present an overview of the latest additions, highlighting their key capabilities and benefits. Below is a summary of the changes and enhancements in this release:

TACACS+ Security: Authorization before Authentication

In this release, the TACACS+ authentication request sequence was modified to improve interoperability with other vendors. Previously, the system would send the authorization request first and then the authentication request, causing compatibility issues with commercial TACACS servers. With the updated sequence, the system sends the authentication packet before the authorization request, ensuring seamless integration and compatibility with commercial TACACS servers from various vendors. This change enhances the overall performance and compatibility of the authentication process.

SNMP Server Engine ID

In this release, extended the Engine ID support, which previously utilized a default value generated from the MAC address. With the introduction of a new CLI, users can now configure the Engine ID to their specific requirements, enhancing customization and flexibility.

Release 6.3.1

Release 6.3.1 continues to support all new hardware offered in Release 6.3.0. However, this release offers a range of new software features and enhancements to our product. This section offers a comprehensive overview of these additions, highlighting their key capabilities and benefits.

VXLAN

Selectively Enabling Multiple IP addresses on IRB Interface for Anycast-gateway

An EVPN-based Integrated Routing and Bridging solution enables communication between two Layer-2 Virtual Network Identifiers (VNIDs) using IP-based Virtual Routing and Forwarding (IP-VRF). This enhancement provides Anycast Gateway Routing support for multiple subnets under the IRB interface (per VNID).

Feature Characteristics

- Connects primary or secondary subnets with either router MAC or Anycast MAC address.
- Supports Anycast Gateway for multiple subnets under the Layer-2 VNID's.
- Subnets A, B, and C can have Anycast Gateway support, while subnet D is reserved for BGP.
- Supports the Interfacefull model for ARP/ND requests and the interfaceless model using the kernel interface with a unique MAC per interface (Router MAC or Anycast MAC) for all subnets.

OcNOS-DC-MGMT SKU

VRRP, MLAG, ZTP, and NetConf functionalities are supported in the current release.

Release 6.3.0

Release 6.3.0 of OcNOS DC introduces the following new hardware, software features and functionalities. This section provides details on these features.

Celestica DS1000

An Open Compute Project (OCP) accepted design, the DS1000 Ethernet switch offers 48 x 10/100/1000Mbps RJ45 ports and 8 SFP+ ports within a 1U form factor.

Figure 1. DS1000 1U 48-port 1GbE Access Switch

This platform provides support for:

- **Interfaces –** 48 x 10/100/1000Base-T RJ45 Copper ports, 8 x SFP+ 10 Gigabit fiber ports, 1 x Console Port base on RJ45, 1 x Out of band management port base on 10/100/1000Mbps RJ45, 2 x Type A USB 2.0 ports

- **Switching Capacity –** 128 Gbps; Packet Buffer of 4MB

- **CPU –** Intel Denverton 4-Core; 4GB ECC DDR4.

Table 1. DS1000 Compatibility

CHIPSET	HARDWARE REVISION	PORT LAYOUT	SKU
Trident III BCM56277_A1	Label Revision: Belgite Board CPLD Version: 2.6	48 x 1G RJ45 8 x 10G SFP+	OcNOS-DC-MGMT

EdgeCore AS5835-54T

This device provides full line-rate switching at Layer 2 or Layer 3 across 48 x10GbE ports and 6 x 100GbE uplinks. The switch can be deployed either as a Top-of-Rack switch or as part of a 40GbE or 100GbE distributed spine, forming a non-blocking folded-Clos data center fabric. The switch is rack mountable in a standard 19-inch rack. It is an ideal Top-of-Rack switch for virtualized data centers with support for VXLAN functions in hardware.

Figure 2. EdgeCore AS5835-54T Switch

Table 2. AS5835-54T Compatibility

CHIPSET	HARDWARE REVISION	PORT LAYOUT	SKU
Trident III BCM56771_A0	Label Revision: R01C CPLD 1 Version: 3 CPLD 2 Version: 2 CPLD 3 Version: 4 Fan CPLD Version: 1	48 x 10G RJ45 6 x 100G QSFP28	OcNOS-DC-IPBASE OcNOS-DC-MPLS

Layer 2

Data Center Bridging (DCB)

Data Center Bridging (DCB) is enhanced to control lossy/lossless settings per port queues in the Ethernet local area network communication protocol used in data center environments.

Priority-based Flow Control (PFC) is a way that provides a link-level flow control mechanism that controls each frame priority independently. This mechanism ensures zero loss (lossless) under congestion in DCB networks.

Quality of service (QoS) works by default with lossy behavior, which is required to function with minimum bandwidth, shaping, and scheduling properly.

This release supports enabling PFC and QoS simultaneously, allowing the ability to control lossy/lossless settings per port queues.

L2CP Tunneling over L2 VXLAN

L2CP tunneling supports the tunneling L2CP frames across L2 VXLAN. When configured, L2CP frames received at the VTEP on an Attachment Circuit (AC) port (VLAN tagged/untagged) will be forwarded to peer VTEP nodes based on corresponding AC port properties. The physical port default behavior is to Tunnel all L2 packets except LACP over the VXLAN network.

Layer 3

ARP ACL

An Access Control List consists of Access Control Entries (ACE). Each ACE in an ACL identifies a trustee and specifies the access rights to allow, deny or update that trustee.

The ARP-based ACL matches ARP packets based on the source or destination IP addresses or source MAC addresses. This release adds ARP ACL support for Trident3, Maverick2, and Hurricane-4 platforms.

Static Route Object Tracking using IP SLA

Static Route Object Tracking with IP SLA is a feature that allows monitoring a static route's reachability status through IP SLA.

Static route object tracking has the following limitations:

- Leaked static routes do not support object tracking.

- Five hundred tracked objects is the maximum supported number.

- When a static route enables BFD and object tracking, the system will not install the route if either BFD or the tracked object goes down

VRRP Route Advertisement for IPv6

As per RFC 5798, the Count IPvX address field in the VRRP packet indicates the number of either IPv4 or IPv6 addresses contained in a VRRP advertisement (the minimum value is 1). In the case of VRRP for IPv6, the first address must be an IPv6 link-local address associated with the virtual router. Supports one additional IPv6 address as a Virtual IP, which becomes a global IPv6 address.

Multi-Protocol Label Switching (MPLS)

RSVP Facility Backup

RSVP supports multiple path protection mechanisms including facility backup. With facility backup protection, N number of LSPs sharing the common path can be protected using one bypass tunnel, which leads to better resource utilization.

RFC 4090 describes the extensions on fast reroute extensions to RSVP-TE for LSP tunnels, which include the facility backup protection mechanism.

VXLAN

IRB Support for Advertising Host Routes

EVPN IRB facilitates communication between two L2VNIs with the help of routing using IP-VRF. This feature provides the host route (/32 or /128) based Symmetric IRB support, which forwards the inter-subnet traffic directly towards the host attached VTEP.

Multicast

PIM ECMP Redirect (IPv4)

Protocol Independent Multicast - Equal-Cost Multipath (PIM ECMP) Redirect enables equal-cost multipath routing for IPv4 multicast traffic. Customers benefit from enhanced performance, load-balancing capabilities, and network resilience. It is used in scenarios with high-volume multicast traffic, the need for network redundancy, and scalable multicast deployments.

System Management

DHCP Server (IPv4 and IPv6)

A Dynamic Host Configuration Protocol (DHCP) server on a network automates the process of assigning IP addresses, default gateways, and other network parameters to client devices. It employs the DHCP as the standard protocol to respond to client queries and provide essential network information. It offers properties to start and stop the DHCP server. OcNOS utilizes the open-source package "isc-dhcpd-4.4.1." In a single VRF instance, run only one IPV4 and one IPv6 DHCP server. An OcNOS router can accommodate a maximum of 256 IPv4 and 256 IPv6 DHCP server instances.

DHCP-Option 82 (IPv4)

While forwarding client-initiated DHCP packets to the server, the DHCP relay agent inserts the relay agent information option, Option 82. Typically, the relay agent removes this option during Reply, yet a configuration option must be available to override this default behavior.

NetConf

Confirmed Commit CLI

The confirm commit feature conforms to NetConf (RFC 6241). This feature commits the configuration on a trial basis. If a customer does not confirm the changes within the default timeout of 300 seconds, the configuration will revert to its previous state. A customer can manually revert the configuration changes before the default timeout.

The confirm commit capability helps mitigate risks, maintain configuration accuracy, and support change control processes. Customers can use it in complex environments, during change management processes, or to meet compliance and auditing requirements.

The confirm commit feature has the following limitations:

- OcNOS-RON supports a maximum of one confirmed commit. It does not support multiple or parallel confirm commit transactions in multiple sessions.

- Confirm commit persistent parameters are not supported. Since it is used to issue a follow-up confirmed commit from any session, transactions do not survive over session disconnects.

- The confirm commit CLI timeout parameter is not supported. Since it is used to reset the timer during transactions, timeout extensions are not supported

Improvements in CLI Error Messages

OcNOS is enhanced to display error messages in Xpath notation or CLI command string. Xpath path notation example is as follows:

```
OcNOS(config-router)#commit
% Configuration " /ospfv2/processes/process[ospf-id='10']/areas/area[area-
id='3.3.3.3']/ interfaces/interface[name='eth3']/vrf-name" depends on
"/ospfv2/global/config/area- interface-config-mode"
% Failed to commit .. As error(s) encountered during commit operation…

CLI command example is as follows:

OcNOS(config-router)#commit
% Configuration " area <value-option> interface <value-option>" depends on " ospf
area- interface-config-mode"
% Failed to commit .. As error(s) encountered during commit operation…
```

OcNOS-DC-MGMT SKU

The new OcNOS-DC-MGMT SKU image provides Layer 2 and Layer 3 switching and routing support for OSPF, IS-IS, and BGP with a perpetual use license (1 license).

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/.

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

Technical Documentation

For information on core commands and configuration procedures, visit
https://www.ipinfusion.com/documentation/ocnos-product-documentation/data-centers/.

Technical Sales

For more information about the OcNOS Data Center solution, contact IP Infusion sales representative.