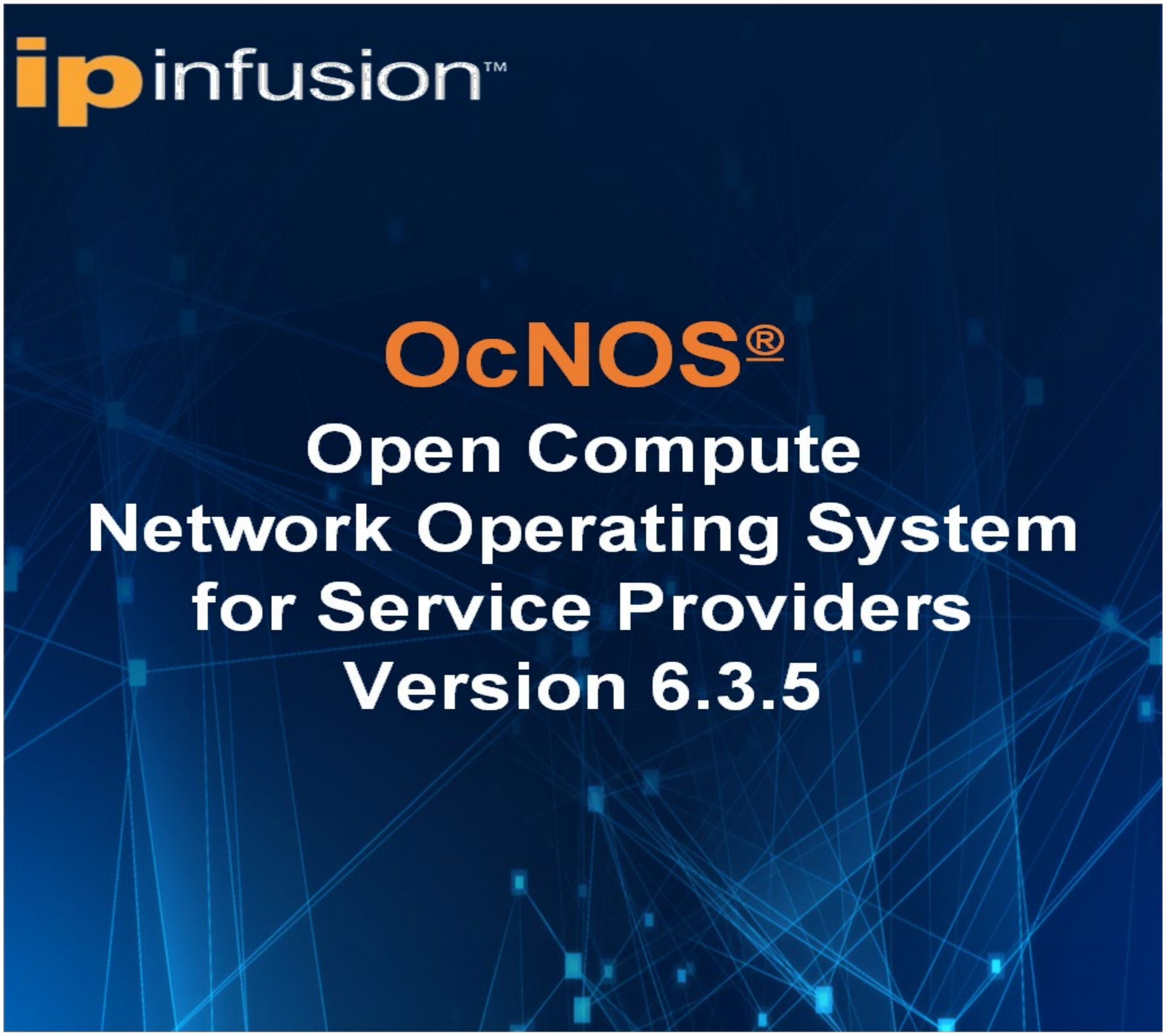


ipinfusion™

OcNOS®

Open Compute Network Operating System for Service Providers Version 6.3.5

Release Notes

19 June 2024

IP Infusion Inc.
3965 Freedom Circle, Suite 200
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:

Contents

Introduction

Overview

The Service Provider mobile and wireline network of the future will not just need to provide exponentially higher bandwidth at lower operating costs but will also have to be capable of enabling new applications such as pervasive mobile broadband, IoT/sensor networks, autonomous vehicles and smart consumer wireless devices. Mobile network operators are actively seeking cost-effective Cell Site Gateway Solutions to accommodate the mass rollout of 4G/5G services to meet this mobile traffic demands. Disaggregated Open Network Solutions benefit operators as they build out 4G/5G infrastructure by reducing costs, expanding the vendor ecosystem and leveraging automation so they are more agile in introducing new services.

The evolution to next-generation 5G networks introduces architectural changes in the radio access network (RAN) and mobile core that will have significant implications for how operators design and provision transport capacity and services. The mobile transport network will need to meet the higher capacity and lower latency demands of 5G, as well as flexibly adapt to diverse traffic flows, to support a growing variety of use cases, from augmented reality to factory automation. A key concept that will enable next generation transport networks is disaggregation, whereby networking software is separated from the switching or routing hardware and partitioned into functional components that can be more efficiently operated. Programmability, automation, and agility with better control of their networks are immediate benefits of disaggregation for operators, besides potential cost savings as well.

Additionally, The exponential growth in network traffic due to digital collaboration offerings for remote work applications has increased the need for managing data and performance efficiently. Evolving data-intensive customer applications require service providers to deliver on-demand high-performance services in a reliable, efficient and secure manner. This drives the need for comprehensive carrier-grade capabilities to enable broadband aggregation and edge routing that provides traffic interfaces necessary to support higher aggregated capacities required for next-generation networks. This functionality provides an ability to manage high volumes of traffic for applications such as mobility, cloud networking, video, and gaming.

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.

About This Release

OcNOS SP provides deployment ready support for low, medium, and high density carrier access/aggregation routing on platforms with aggregation throughput between 32-4800 Gbps with port speeds up to 400Gbps. Support is provided for following capabilities:

- Comprehensive Layer 2 switching including VLAN, Link Aggregation, and xSTP
- Carrier Ethernet-oriented capabilities including Provider Bridging, ERPS, ELPS
- Rich network OAM support including EFM, CFM/Y.1731, BFD, and TWAMP
- Advanced Layer 3 Routing capabilities including BGP, RIP, OSPF, ISIS and VRRP
- Multicast Routing capabilities including PIM, MLDP and IGMP
- Comprehensive Quality of Service support
- Multi-Protocol Label Switch (MPLS) support with LDP, RSVP-TE and MPLS-OAM
- Timing and Synchronization capabilities with Default Profile, IEEE 1588v2, ITU-T G.8262, G.8264, G.8265.1, G.8275.1, G.8275.2
- Management: SNMP: v1, v2, v3, Zero Touch Provisioning, sFlow, NETCONF, OpenConfig,

These combined capabilities enables VXLAN, MPLS, SR-MPLS and SRv6 network transport enabling rich delivery of the following services:

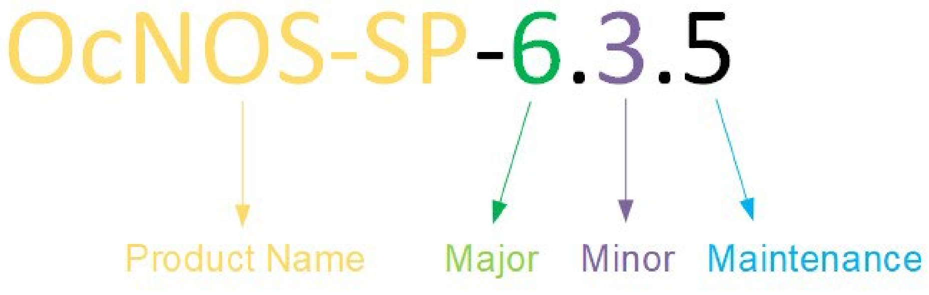
- Layer 2 VPN (L2VPN)
- Layer 3 VPN (L3VPN)
- Virtual Private Wire Service (VPWS)
- Virtual Private LAN Service (VPLS)
- Ethernet VPN (EVPN)

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 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 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 SP introduces the following enhanced software features and functionalities. This section provides details on these features.

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 Instllation* Guide, Release 6.3.5.

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 the addition of 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.

Release 6.3.4

Release 6.3.4 of OcNOS SP 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*, Release 6.3.4.

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 SP 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* section in *System Management* guide.

Release 6.3.2

This release does not introduce any new hardware. In Release 6.3.2, our product introduces new software features and enhancements. This section aims to provide a comprehensive overview of these latest additions, emphasizing their key capabilities and the benefits they bring to our users. Below is a summary of the exciting changes and improvements 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 and software features offered in Release 6.3.0.

New Licenses

In OcNOS SP 6.3.1, IP Infusion offers new licenses to match the switching capacities of devices listed below.

- UfiSpace S9502-12SM and UfiSpace S9502-16SMT at 32 Gbps
- UfiSpace S9501-18SMT and Edgecore AS5915-18X at 64 Gbps

Note: For existing customers, your licenses will continue to work without issue, and no further action is required.

Release 6.3.0

Release 6.3.0 introduces the following new hardware, software features, and enhancements to our product. This section offers a comprehensive overview of these additions, highlighting their key capabilities and benefits.

Edgecore AS7535-28XB

The Edgecore AS7535-28XB is a high-performance open disaggregated cell site gateway platform. It utilizes Qumran family merchant silicon and an Intel Xeon x86 processor for robust performance.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom Q2A BCM88483_B1	24x25G SFP28, 2x100G QSFP28, 2x400G QSFP-DD	Label Revision: R0B CPU CPLD version:11 FPGA1 Version: R0B CPLD Version: 11 BMC: AST2600 BMC Firmware Revision: 0.00	OcNOS-SP-IPBASE-800 OcNOS-SP-MPLS-800 OcNOS-SP-IPADV-CE-AGGR-800 OcNOS-SP-PLUS-800

Edgecore AS7946-30XB

The Edgecore AS7946-30XB is a high-performance aggregation router. It utilizes the latest Qumran2C silicon to deliver a robust performance.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom Q2C BCM88823_A1	4x25G SFP28, 22x100G QSFP28, 4x400G QSFP-DD	Label Revision: R01 CPLD 1 Version: 11 CPLD 2 Version: 11 CPLD 3 Version: 1 CPLD 4 Version: 1 Fan CPLD Version: 2 BMC: AST2600 BMC Firmware Revision: 0.01	OCNOS-SP-IPBASE-2400 OCNOS-SP-MPLS-2400 OCNOS-SP-IPADV-CE-AGGR-2400 OCNOS-SP-PLUS-2400

Edgecore AS7946-74XKSB

Edgecore's AS7946-74XKSB is a high performance 25GbE aggregation router that consists of 64 x 10G/25G SFP28, 8 x 100GE QSFP28, and 2 x 100G QSFP-DD ports.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom Q2C BCM88820_A1	8x 100G QSFP28, 2 x 100G QSFP-DD, 64x 10G/25G SFP28	Label Revision: R01 CPLD 1 Version: 1 CPLD 2 Version: 1 Fan CPLD Version: NA	OCNOS-SP-IPBASE-2400 OCNOS-SP-MPLS-2400 OCNOS-SP-IPADV-CE-AGGR-2400 OCNOS-SP-PLUS-2400

UfiSpace S9502-12SM

The UfiSpace S9502-12SM is a high-performance, fanless router. This utilizes QumranUX silicon and a dual-core processor for better performance.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom QUX BCM88273_A1	8x1GbE SFP, 4x10GbE SFP+	Label Revision: N/A Main board CPLD version: 17 Device Version: 2	OcNOS-CSR-32 OcNOS-SP-IPBASE-32 OcNOS-SP-MPLS-32

UfiSpace S9510-30XC

The UfiSpace S9510-30XC is a high-performance, open networking white box router. It helps telecoms and service providers to deploy disaggregated open network infrastructure efficiently.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom Q2U BCM88284_B1	28 x 1/10/25GE SFP28, 2 x 40/100GE QSFP28 with FlexE support	Label Revision: N/A Main Board CPLD Version: 1 BMC: AST2620 BMC Firmware Revision: 4.04	OCNOS-SP-IPBASE-300 OCNOS-SP-IPADV-300 OCNOS-SP-MPLS-300 OCNOS-SP-PLUS-300

UfiSpace S9600-56DX

UfiSpace's S9600-56DX helps service providers aggregate high throughput and transport services for their networks. The new platform offers highly scaled port density including 8 x 400G QSFP-DD interfaces and 48 x 100G QSFP28 interfaces.

SWITCHING ASIC	PORT CONFIGURATION	HARDWARE REVISION	SKU
Broadcom Q2C BCM88820_A1	48X 100G QSFP28, 8X 400 QSFP-DD	Label Revision: N/A MASTER CPLD version: Beta BMC Firmware Revision: 2.01	OCNOS-SP-IPBASE-4800 OCNOS-SP-MPLS-4800 OCNOS-SP-IPADV-CE-AGGR-4800 OCNOS-SP-PLUS-4800

Access Control List IPv6 128-bit Addresses

This enhancement adds two new hardware- profile filters, supporting up to 128-bit address classification in IPv6 ACL. Before this, IPv6 ACL supported only upper 64-bit address classification. The ACL can be applied on physical interfaces, SVI interfaces, and L3 sub-interfaces.

BGP

BGP Flowspec

The BGP flow specification (flowspec) allows customers to deploy and propagate filtering and policing functionality among a large number of BGP peer routers to mitigate the effects of a Distributed Denial- of-Service (DDoS) attack over a network.

BGP flowspec allows customers to effectively construct instructions to match a particular flow with source, destination, L4 parameters, and packet specifics such as length, fragment, and so on. Flowspec allows for a dynamic installation of an action at border routers to either:

- Drop the traffic
- Inject it in a different VRF for analysis

Or

- Allow it but police it at specifically defined rate

This feature is supported for IPv4 unicast and IPv4 BGP/MPLS VPN service based on RFC 8955. Qumran1 (Q1)/Qumran2(Q2) chipsets have the following limitations:

- For TCP-Flag, the checks of octets 13 stated in RFC 8955 is not supported for Q1 as well as Q2 chipset
- Fragment filter is not supported for Q1 chipset.
- “traffic-rate-packets” and “traffic-action” actions are not supported for Q1 as well as Q2 chipset

BGP On-Demand Nexthop and Auto Steering

Segment Routing On-Demand Next Hop (ODN) or Segment Routing Traffic Engineering (SR-TE) auto steering triggers delegation of computation of an end-to-end LSP using dynamic computation (ISIS/ OSPF/PCEP) including constraints and policies without doing any redistribution. It then installs the reapplied multi-domain LSP for the duration of the service into the local forwarding information base (FIB).

BGP Prefix Independent Convergence (PIC)

BGP Prefix Independent Convergence (PIC) feature improves the BGP convergence after a network failure (Edge failure). This release supports only MPLS-based BGP-PIC for the VPNv4, 6VPE, and 6PE address families.

BGP Large Community

The BGP large communities attribute is an extension to BGP-4 attributes that expands the size of the community attribute (RFC 8092) to support 4-byte AS numbers.

EVPN

EVPN-SRv6 VPWS (ELINE) Multi-Homing

The EVPN-SRv6 VPWS (ELINE) multi-homing feature is used to connect a customer device site to two PE devices, in order to provide redundant connectivity.. A CE device is multi-homed to different PE devices or the same PE device. A redundant PE device can provide network service to the customer device as soon as a failure is detected. Thus, EVPN multi-homing helps maintain EVPN service and traffic forwarding to and from the multi-homed site in the event of network failures.

EVPN-SRv6 VPWS (ELINE) multi-homing has following limitations:

- Support is currently available only for BGP IPv6 peering for EVPN services.
- QoS is not supported for SRv6.

EVPN MPLS Control Word

EVPN MPLS Control Word feature enhances traffic load-sharing by enabling the insertion of a control word (a 4-byte optional field) between the MPLS label stack and payload data in data packets.

Note: Admin must ensure to enable control-word option during creation of EVI instance.

EVPN MPLS L2 and L3 VPN on Qumran2

This release supports EVPN MPLS Layer 2 VPN and Layer 3 VPN for single-homing and multi-homing on Broadcom Qumran2 platforms such as Q2A/Q2C/Q2U. With OcNOS, it allows the usage of a non-IRB interface as an access-side L3 interface while still providing anycast mac-address support.

EVPN SRv6 VPWS (E-LINE) Single-Homing

This release supports EVPN-SRv6 VPWS (ELINE) Single-Homing.

This solution provides a simple Layer 2 packet forwarding mode for the connection between AC interfaces at both ends, avoiding the need to search MAC address entries.

EVPN IRB Support on Qumran2

This release supports IRB ((Integrated Routing/Bridging) for EVPN VXLAN and EVPN MPLS (Single/ Multi Homing) on Broadcom Qumran2 platforms such as Q2A/Q2C/Q2U.

ISIS Microloop Avoidance

During routing convergence in a network, there is a possibility of a packet microloop, as routers receive network updates at different intervals of time. The microloop avoidance feature helps in such scenarios by identifying these events and synchronizing the route installation process. OcNOS has added support for ISIS Microloop Avoidance for Segment Routing.

Microloop avoidance has following limitations:

- Rank computation will not work when there is more than one neighbor in a broadcast link.
- Microloop avoidance feature is supported only for ISIS IPv4 (not supported for ISIS IPv6).

IPv6 Neighbor Discovery Sync for MC-LAG

This release supports the IPv6 Neighbor Discovery Sync and DHCPv6 Prefix Delegation auto route injection sync between MLAG peers.

L2 CE Bridge Dependency Removal

CFM/Y.1731 configurations and show commands are re-structured. Please refer to the migration guide to understand the new CLI syntax.

LDP

LDP ECMP

LDP ECMP performs load balancing for LDP-based LSPs by having multiple outgoing next-hops for a given prefix on ingress and transit LSRs, and follows IGP specified ECMP path.

The default behavior enables LDP ECMP on the ingress node (load balancing is done based on L2/L3/L4 fields). The default behavior disables LDP ECMP on transit nodes. Configurable CLI options enable it. If ECMP is enabled on a transit node, enable LDP entropy for hashing to work. If transit ECMP is enabled, it is recommended not to use PHP.

LDP MD5 Password for Auto-targeted Sessions

This release provides a set of configurable options to associate MD5 passwords to the auto-targeted sessions. In addition, the following are now supported:

- A configurable password to associate with auto-targeted sessions.
- A global configurable password to be used by all other targeted-sessions.
- An exclusion list with prefixes that don’t use the auto-targeted or global passwords.
- Sessions groups with an associated password. For each session group, a prefix list is associated to indicate which prefixes belong to the group.

Maximum MTU Support

Maximum MTU size currently supported for Qumran 1 and Qumran 2 based hardware platforms is 9900 bytes. Earlier, OCNOS supported a maximum MTU of 9216 bytes configuration on Qumran-1 and Qumran-2. In this release, the support is extended up to 9900 bytes.

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 SP 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 displays an error message in Xpath notation or CLI command string. The 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…
```

NetConf Data Model Support

This release now supports the following data models through NetConf:

- Routing Information Protocol (RIP) IPv4
- ipi-rip-types.yang
- ipi-rip-common.yang
- ipi-rip.yang
- ipi-rip-vrf.yang
- Routing Information Protocol Next Gen (RIPng)
- ipi-ripng-types.yang
- ipi-ripng-common.yang
- ipi-ripng.yang
- ipi-ripng-vrf.yang

- Unicast RPF
- ipi-unicast-rpf-types.yang
- ipi-unicast-rpf.yang

OpenConfig Support

New leaves are supported for BGP and OSPFv2 through NetConf with the OpenConfig namespace. . For details, see the *OpenConfig Command Reference*.

PIM

PIM ECMP (IPv4 and IPv6)

Protocol Independent Multicast - Equal-Cost Multipath Redirect (PIM ECMP) enhances IPv4 multicast traffic routing by enabling equal-cost multipath capabilities. This feature provides customers with improved performance, load balancing capabilities, and increased network resilience. It is beneficial in scenarios with high-volume multicast traffic, requirements for network redundancy, and the need for scalable multicast deployments.

PIM ECMP IPv6 is supported only on Qumran2 platforms such as Q2A/Q2C/Q2U.

MLD and PIMv6

This release supports MLD and PIMv6 protocols (except BIDIR) on Broadcom Qumran2 platforms such as Q2A/Q2C/Q2U.

Port Breakout for Q2

The port breakout feature provides flexibility in splitting 100G to 4X10G, and 4X25G,2X50G

When customers do port breakout on a 100g (ce2) port into 4X10g, the original port (ce2) will be removed and four 10g ports added as ce2/1, ce2/2, ce2/3, and ce2/4. On this breakout port customers can do all the L2 and L3 features like a normal port.

Port Breakout for Q2 has the following limitations:

For ports with an external phy, a reboot is needed to support a breakout on 100G interfaces on Qumran2 platforms.

Segment Routing IPv6 Operations, Administration, and Maintenance

Segment Routing IPv6 Operations, Administration, and Maintenance (SRv6 OAM) helps service providers to monitor SRv6 paths and quickly isolate forwarding problems. SRv6 OAM also assists with fault detection and troubleshooting in a network. On ingress, OcNOS initiates a ping to an SRv6 SID/policy to verify whether that SID is reachable and locally programmed at the target node. Traceroute to an SRV6 SID/Policy is used for hop-by-hop fault localization and path tracing to a SID.

SRv6 OAM has the following limitations:

- O-Flag is not supported for this release.
- SRv6 service-related ping and traceroute are not supported.
- SRv6 OAM ping and traceroute is supported only on physical interfaces.

Segment Routing (MPLS Data Plane) User Defined Adjacency SID (OPSFv2)

This release supports customer-configurable adjacency segment identifiers (adj-SIDs) in IPv4 Segment Routing. As part of this, the Segment Routing clients (such as OSPFv2 and ISIS) can configure Segment Routing local block and adj-SIDs. This feature is currently supported only for OSPFv2. Also, in OSPFv2, this feature is supported only for point-to-point links and not for broadcast links.

Smart SFP

The Smart SFP provides OAM functions integrated into the SFP module. The OAM messages are exchanged in a low-speed out-of-band channel between smart transceivers at both ends. Local Smart SFP gets the DDM information and vendor information of remote Smart SFP periodically through 4 OAM data frames and stores the information in its EEPROM. The remote SFP information can be displayed on the local switch by using CLI commands. The administrator can instruct the local SFP to send OAM commands to the remote SFP to enable inner and outer loopbacks, reset, disable tx transmission and more on the remote SFP.

OcNOS has added support for smart SFP transceivers from CIG and Accelink:

- TRS5A21EH02LF000 (CIG)
- RTXM330-8921 (Accelink-WTD)

Split Horizon

VPLS instances can support multiple Attachment Circuits (ACs) configured (such as 50-60 ACs per VPLS instance). Previously for VPLS, AC-AC traffic blocking was not supported. Split horizon allows support where a customer can control if AC-AC traffic needs to be blocked or forwarded. As per this implementation, AC-AC, AC-network filtering is possible.

This feature is supported only for Q1 platforms.

Symmetric IRB Support with Connected 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.

VRRP

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.

VRRP VIPv6

VRRP supports global IPv6 addresses for VIP6.

TWAMP

The OcNOS implementation is based on TWAMP Lite as per the RFC 5357 Appendix A.

TWAMP over L3VPN/EVPN

In general, OcNOS covers:

- CE-CE: overlay only
- CE-PE: overlay only
- PE-PE: both underlay and overlay

TWAMP Server

The TWAMP server starts and the system listens to the configured TCP port. Customers can also specify the list of VRFs where the server starts..

The system accepts connections from TWAMP clients and negotiates the reflector sessions.

Y.1731 SNMP

In this release, the following features have SNMP support:

- Fault Management (FM) MIB - Reference MEF-SOAM-FM-MIB.txt
- Performance Monitoring (PM) MIB - Reference MEF-SOAM-PM-MIB.txt

The following OIDs are supported:

- mefSoamTcMib = 1.3.6.1.4.1.15007.1.1
- mefSoamFmMib = 1.3.6.1.4.1.15007.1.2
- mefSoamPmMib = 1.3.6.1.4.1.15007.1.3

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 or 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/service-providers/

Technical Sales

For more information about the OcNOS Service Providers solution, contact IP Infusion sales representative.