OcNOS®

Open Compute
Network Operating System
for Routed Optical Networking
Version 6.4.2

Release Notes

07 March 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

Contents

Introduction

Overview

The OcNOS Routed Optical Networking (RON) product is a specialized solution based on the OcNOS network operating system. Leveraging the robust OcNOS network operating system, OcNOS RON combines IP routing and optical transport technologies to deliver a comprehensive solution for converged network environments. With advanced features and capabilities tailored for routed optical networks, OcNOS RON empowers organizations to build high-performance, scalable, and efficient optical networks while benefiting from the flexibility and programmability of IP routing.

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, flexible environment and extensive protocol support for software-defined networking (SDN) and disaggregated networks.

About this Release

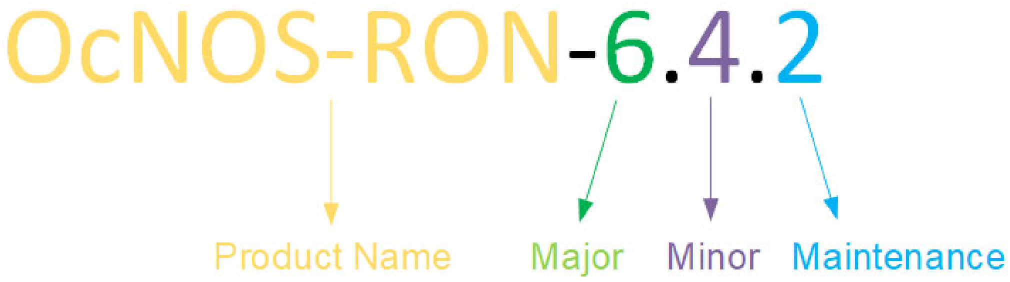
OcNOS-RON Release 6.4.1 introduces several software features, and product enhancements. This section provides a high-level overview of these additions, highlighting their main capabilities and benefits.

IP Maestro Support

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

IP Infusion Product Release Version

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



Product Name: IP Infusion Product Family

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

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

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

Release 6.4.2

Enhanced Security and Performance

Support for RADIUS Authorization

The current implementation of Remote Authentication Dial-In User Service (RADIUS) authentication assigns network-admin role to any user irrespective of the privilege-level. This behavior is modified in the current release. The RADIUS server is enhanced with an authorization service to assign the role to the authenticated users based on the privilege level specified in the RADIUS server.

For more information on RADIUS Client Configuration refer to *System Management Guide, Release 6.4.2.*

Release 6.4.1

Enhanced Security and Performance

NetConf Port Access Control and TCP Port Closure

The NetConf subsystem runs on the default access port 830 over SSH and port 6513 over TLS. Typically, these default access ports are not configurable and are always open. Hence, the NetConf port access control feature enhancement ensures that the Netconf-SSH and NetConf-TLS port access can be controlled and configurable through the new CLIs introduced in the 6.4.1 release.

This feature supports the following:

- Allows access control capabilities for the NetConf-SSH and NetConf-TLS ports.
- Enables/disables the port.
- Allows changing the default port.
- Provides access and control for NetConf services through Inband and Outband.
- Applies ACL rules to the NetConf port to control its access
- Provides the ability to disable the TCP ports not in use

For more information, see the NetConf Port Access Control section in the OcNOS Key Feature document, Release 6.4.1.

Hide the Remote AS using neighbor local-as CLI

The `neighbor local-as` command has been enhanced to hide the Autonomous System (AS) number of remote router from the external connected BGP peer. The `local-as` CLI command has been modified to add new options `no-prepend` and `replace-as`. These options replace the remote AS number with the configured alternate AS in the AS_PATH and BGP OPEN message sent from the remote router. Hence, the remote AS is unknown to the external neighbor peer. This makes the neighbor believe that the received routes are from the alternate AS number included in the AS_PATH and BGP OPEN messages. Thus, the AS number of the remote BGP router is unknown to the external peer.

For more information, see the Hide the Remote AS using the neighbor local-as Command section in the *OcNOS Key Feature document*, Release 6.4.1.

TCP MSS for BGP neighbors

The manual configuration between the routing devices establishes the BGP peer that creates a Transmission Control Protocol (TCP) session. This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session. A TCP segment is a unit of data transmitted in a TCP connection.

TCP MSS configuration per BGP neighbor adjusts the BGP Update Packet Size according to the configured value, which prevents the BGP update packet from getting dropped in transit. The configurable MSS range is from 40-1440. Configure TCP MSS per BGP neighbor using the CLI or NetConf interface.

For more information, refer to the TCP MSS configuration for BGP neighbors section in the *OcNOS Key Feature document*, Release 6.4.1.

TCP MSS Configuration for LDP sessions

Label Distribution Protocol (LDP) uses Transmission Control Protocol (TCP) to establish sessions between the devices. This feature enables the configuration of TCP Maximum Segment Size (MSS) that defines the maximum segment size in a single TCP segment during a communication session. The configuration of the TCP MSS for LDP neighbors helps the neighbors adjust the MSS value of the TCP SYN packet. The configurable MSS range is from 560 to 1440. Configure the TCP MSS through the CLI and NetConf interface.

For more information, refer to the TCP MSS configuration for LDP sessions section in the *OcNOS Key Feature document*, Release 6.4.1.

Increase the Limit of BGP peers in a Peer-Group

The number of BGP peers in a Peer-Group is limited to 32. This means that every time the number of peer members exceeded 32, a new Peer-Group has to be created.

To circumvent this need, the feature has been enhanced to increase the members in a peer group from 32 to 255.

Password Strength Enhancements

OcNOS has now included enhancements to password strength requirements, and the password must adhere to the following criteria:

- Length: Passwords must be 8-32 characters.
- Character Types: Passwords must contain at least one of each of the following:
    - One uppercase letter
    - One lowercase letter
    - One digit
    - One special character (acceptable special characters: ~`!@#$%^&*(){}'[],."</+-_:;)

Note: The following characters are not acceptable in passwords: '=?|>.

For more information, refer to the username command in the *OcNOS System Management Guide*, Release 6.4.1.

RADIUS Server Authentication failure and Fallback

In the event of a RADIUS server authentication failure, this feature provides the ability to fallback to the local authentication server. This occurs in the following two scenarios:

- When the user is not present in the RADIUS server
- When authentication fails from the RADIUS server

To implement the above requirements, the existing `aaa authentication login default fallback error local non-existent-user vrf management` command is used to enable fallback to local authentication server. This is disabled by default.

By default, the fallback to local authentication is applied when the RADIUS server is unreachable.

For more information, see the Fall Back Option for RADIUS Authentication section in the OcNOS Key Feature document, Release 6.4.1.

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, see the Modified Extended ACL Deny Rule Behavior in VTY section in the OcNOS Key Feature document, Release 6.4.1.

Enhanced EVPN Route Show Command

The enhanced EVPN route show command now includes prefix-route details for in-depth insights. It tailors the output to specific requirements, streamlining network management and decision-making with precise and customized data for efficient troubleshooting and enhanced control.

For more information, refer to the show bgp l2vpn evpn section in the *VXLAN Commands* document, Release 6.4.1.

Improved Network Resilience

RSVP Detour Over Ring Topology

In OcNOS, this feature enhances the routing experience by forming a detour in a ring topology. When a failure or congestion occurs in the primary Label Switched Path (LSP), the detour protects data traffic. The detour formation is a local protection mechanism to minimize data traffic loss.

For more information, see the RSVP Detour Over Ring Topology section in the *OcNOS Key Feature document*, Release 6.4.1.

Commit Rollback

Execution of the Commit Rollback functionality within Common Management Layer Commands (CMLSH) allows for the rollback of configurations previously committed. To support this functionality, introduced the following CLIs:

- show commit list
- commit-rollback to WORD (description LINE|)
- clear cml commit-history (WORD|)
- cml commit-history (enable | disable)
- cml commit-id rollover (enable | disable)
- show cml commit-history state

For more information, refer to the Commit Rollback section in the OcNOS Key Feature document, Release 6.4.1.

Improved Management

Route Monitor

The Route Monitor feature in OcNOS introduces a standalone tracking mechanism designed to be used by various processes. It monitors the reachability state of an object through IP SLA.

With Route Monitor, multiple tracked objects can be configured on one or more interfaces, collectively influencing the interface's operational state.

For more information, refer to the Route Monitor section in the *OcNOS Key Feature document*, Release 6.4.1.

Enhancements for OpenConfig Translation

OcNOS extended support for ISIS, LDP, and Bridge-Domain OpenConfig Translation. This enhancement enables network administrators to manage these additional components using standardized YANG models. This promotes consistency and simplifies network management. This extension also offers network operators flexibility and comprehensive error reporting through OpenConfig paths, which can be valuable for troubleshooting and diagnostics.

The OpenConfig Translation feature provides the ability to manage multi-vendor networks through a unified interface, reducing operational costs and complexity for network operators.

In previous OcNOS versions, the network-instance type determination on OcNOS was based on the `type` leaf and some configurations that relied on the presence of the number of interfaces or endpoints. However, starting from the

OcNOS 6.4.1 release version, the network-instance type determination is based on the `/oc-netinst:network-instances/network-instance/config/type` and `/oc-netinst:network-instances/network-instance/encapsulation/config/encapsulation-type` leaves.

For more information, refer to the ISIS OpenConfig Translation, LDP Openconfig Translation, VLAN OpenConfig Translation, and Network-instance Object Values for “type” Attribute sections in the *OcNOS OpenConfig Command Reference Guide*, Release 6.4.1.

NetConf “remove” Operation

The `remove` operation in Netconf is supported under the `edit-config` category. Users can execute this operation using either the `merge` or `replace` operation types. The `remove` operation functions similarly to the `delete` operation, with one crucial difference. In cases where the requested data is not present in the running configuration, instead of displaying a `data-missing` error, it will ignore this error and continue further processing.

For more information, refer to the Supported Operations chapter in the *OcNOS NetConf User Guide*, Release 6.4.1.

DHCP Server Group

Dynamic Host Control Protocol (DHCP) Group provides the capability to specify multiple DHCP servers as a group on the DHCP relay agent and to correlate a relay agent interface with the server group.

This feature helps one configure the DHCP IPv4 and IPv6 groups and attach server IP addresses to the group. Creating a maximum of 32 IPv4 and 32 IPv6 groups per VRF is allowed, and configuring eight DHCP servers is permitted for each DHCP server group.

The DHCP relay agent forwards the request message from the DHCP client to multiple DHCP servers in the group. Forwarding the request message to multiple DHCP servers increases the reliability of obtaining network configuration information.

For more information, refer to the DHCP group section in the *OcNOS Key Feature document*, Release 6.4.1.

Custom Syslog

Release 6.4.1 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 is 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.

For more information, refer to the Custom Syslog Port Configuration and Syslog chapters in the *OcNOS System Management Guide*, Release 6.4.1.

Enhanced VE-ID Range

In OcNOS, the Virtual Ethernet Identifier (VE-ID) range is increased from `1-64` to `1-65535`. This allows network operators to configure and manage Virtual Private LAN Service (VPLS) instances. The VE-ID must be unique for the VPLS peers in a VPLS instance.

For more information, refer to the command reference page for ve-id in the Virtual Private LAN Service Commands chapter in the *OcNOS Multi-Protocol Label Switching Guide,* Release 6.4.1.

VRRP over MLAG with Custom VRF

OcNOS provides the capability to configure the Virtual Router Redundancy Protocol (VRRP) over Multi-Chassis Link Aggregation (MLAG) feature for custom Virtual Routing and Forwarding (VRF).

Custom Virtual routing and forwarding (VRF) isolates and virtualizes the network at Layer 3 of the OSI model, as Virtual Local Area Network (VLAN) serves similarly at Layer 2. The VRFs are used to separate the network traffic and efficiently use the routers. VRF can also create Virtual Private Network (VPN) tunnels dedicated to a single network or a client.

For more information, refer to the Custom VRF Configuration section of the VRRP Configuration chapter in the *OcNOS Layer 3 Guide,* Release 6.4.1.

Enhanced Graceful Restart

Executing the graceful restart CLI commands for BGP, ISIS, RSVP and OSPF modules, deletes in progress configurations if not saved and requires manual restart of the devices running these protocols. To address this issue, the following existing graceful restart CLI commands are enhanced to notify the user to save the configurations before executing them.

- restart bgp graceful
- restart ospf graceful
- restart isis graceful
- restart ipv6 ospf graceful
- IS-IS Graceful Restart Configuration
- OSPFv3 Graceful Restart Configuration
- RSVP Graceful Restart Configuration

For more information, refer to the *Layer 3 Configuration Guide,* Release

6.4.1

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 6.4.1.

Remove “tech-support” file

When the “`show techsupport`” command is executed, a log file is generated in the “`/var/log`” directory.

Currently, there is no way to delete this file. Now the operator has access to a new CLI to remove the log file from the `/var/log` directory.

Introduced the following new CLI command that enables operators to remove files:

remove file (techsupport)

For more information, refer to Software Monitoring and Reporting O*cNOS System Management Guide*, Release 6.4.1.

Improved Routing

Static Route Tracking using Object Tracking (IP SLA)

OcNOS has extended support for IPv6 in Static Route Object Tracking using the Internet Protocol Service Level Agreement (IP SLA), enhancing the management and monitoring of IPv6 traffic. Using the capabilities of IP SLA, the feature continuously assesses IP service quality by employing ICMP pings to detect link failures and promptly notify registered clients of any events. The outcome is a resilient network infrastructure, empowering administrators to quickly respond to changes in tracked object values, ensuring network stability and network reliability across IPv4 and IPv6 networks.

For more information, refer to the Static Route Object Tracking using IP SLA chapter in the *OcNOS Layer 3 Guide*, Release 6.4.1.

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 6.4.1.

Increase the limit of BGP peers in a Peer-Group

The number of BGP peers in a Peer-Group is limited to 32. This require creation of a new Peer-Group every time the number of member peers exceed 32.

New requirement is to increase the members in a peer group from 32 to 255.

Inbound Route Filter for EVPN

The inbound route filtering is available for Ethernet Virtual Private Network (EVPN) address families. By default, Layer 2 Virtual Private Network (L2VPN) EVPN routes are not installed into the VRF BGP table without the matching import route target. This matching mechanism prevents saving the unmatched routes in the remote Route Distinguisher (RD) BGP table and reduces memory consumption.

For more information, see the command reference page for bgp inbound-route-filter in the BGP Virtual Private Network Commands chapter in *OcNOS Layer 3 Configuration guide*, Release 6.4.1.

UDLD Support on Layer 3 Interface

Layer 3 Unidirectional Link Detection protocol (UDLD) support has been enabled.

The UDLD protocol enables to monitor the physical links and detect when a unidirectional link exists. Upon detection user can either block the port or notify the link status based on the network administration configuration.

UDLD works in two different modes:

- Normal mode
- Aggressive mode

For more information, see the Unidirectional Link Detection Configuration section in the *OcNOS Layer 3 Configuration guide*, Release 6.4.1.

Technical Support

IP Infusion maintains an online technical support site that provides a variety of technical support programs for licensed OcNOS customers at http://www.ipinfusion.com/customer-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 core commands and configuration procedures, visit: https://docs.ipinfusion.com/routed-optical-networking/.

Technical Sales

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