ExtremeSwitching™

Release Notes for VSP 8600

Release 4.5.0.1
NN47227-401
Issue 16.02
September 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks’ agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks’ standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: http://www.extremenetworks.com/support under the link ““Policies” or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

“Hosted Service” means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, https://extremeportal.force.com OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE (“EXTREME NETWORKS”).

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at:http://www.extremenetworks.com/support/policies/software-licensing or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at https://gtacknowledge.extremenetworks.com/.

Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: http://documentation.extremenetworks.com, or such successor site as designated by Extreme Networks.

Contact Extreme Networks Support

See the Extreme Networks Support website:http://www.extremenetworks.com/support for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website:http://www.extremenetworks.com/support/contact/ (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Table of Contents

This page is left blank intentionally

Chapter 1: Preface

Disclaimer

On July 15, 2017, Extreme Networks acquired the Networking Business Unit from Avaya. The formerly Avaya products are in the process of being rebranded to Extreme Networks. In some cases the Avaya name is specific to command syntax, in those cases Avaya will continue to appear in the documentation and the operational software until such time that the command has been altered. Where applicable the documentation will continue to use the name of Avaya products that did not transition to Extreme Networks with which the networking products have unique operational capabilities

Purpose

This document describes important information about this release for the Extreme Networks Virtual Services Platform 8600.

These Release Notes include supported hardware and software, scaling capabilities, and a list of known issues (including workarounds, where appropriate). This document also describes known limitations and restrictions.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at www.extremenetworks.com/education/.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.

- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com

Getting Help

Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Product purchased from Avaya

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for previous versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing.

Chapter 2: New in this release

New in Release 4.5.0.1

The following section details what is new in Release 4.5.0.1.

Support for 8606CQ

Support for VSP 8606CQ, 6 port 100 Gbps QSFP28 ports is available. This IOC module is MACsec hardware ready. Software support for MACsec will be available in a future release.

New in Release 4.5.0.0

The following section details what is new in Release 4.5.0.0.

VSP 8600 Series

This release is the first software release for VSP 8608 Chassis model.

Virtual Services Platform 8600 is a next generation high performance and highly scalable chassis based modular Ethernet switching platform that provides multiple interface speeds options from 1G/10G/25G/40G/100G. VSP8600 features four types of IOC (Integrated I/O and Control) modules, which provide network connectivity along with supervisor/controller capabilities.

The following IOC modules are supported in this release:

- 8624XS: 24 port 1/10 Gbps SFP+ fiber ports, MACsec capable
- 8624XT: 24 port 100 Mbps/1 Gbps/10 Gbps RJ–45 copper ports, MACsec capable
- 8616QQ: 16 port 40 Gbps QSFP+ ports

The VSP 8608 chassis provides eight slots for IOC modules and three slots for switch fabric (SF) modules in a 7U vertically oriented configuration. The SF and IOC modules are hot-swappable. The chassis supports four AC or DC power supplies, and includes five preinstalled cooling modules, each with 2x80 mm fans. The IOC modules occupy slots 1 through 4 and slots 5 through 8. The middle 3 slots are used for SF modules.

For more information, see the following documents:

- *Installing VSP 8600 (NN47229-300)*
- *Quick Install for Chassis (NN47229-303)*
- *Quick Install for Modules (NN47229-302)*
- *Installation Job Aid for VSP 8600 (NN47229-301)*

VSP 8600 licensing

The VSP 8600 Series supports a licensing model that has two main categories of licenses: IOC Base License and Feature Pack Licenses. With this model, you can purchase and activate software features as you need to deploy them. The IOC Base License enables base software features and one IOC Base License is required per IOC in the chassis. Additional advanced features such as L3VSN, MACsec are available through Feature Pack Licenses. IOC-Base License is applicable on a per IOC basis and is a mandatory license to enable the IOC and provide Base set of features. Having the Base License applicable on a per IOC basis rather than the chassis, enables a pay as you grow model that avoids large upfront chassis based licensing cost. The Feature Pack Licenses are optional and is applicable on a per chassis basis. In this release, the following feature pack licenses are available:

- L3 Virtualization (L3VSN, >24 VRFs, >16 BGP Peers)
- L3 Virtualization with MACsec (L3VSN, >24 VRFs, >16 BGP Peers, MACsec)

For more information, see *Administering* (NN47227-600)

High Availability-CPU (HA-CPU)

VSP8600 supports controller redundancy, thus enabling High Availability (HA). Each IOC module supports both I/O and supervisor/controller functionality. Any IOC inserted in Slot 1/2 act as the Master/Standby Controller in a HA configuration. In this release, VSP8600 provides two HA modes - Warm Standby and Hot Standby. In Warm Standby mode the configurations are synced between Master and Standby IOCs. In Hot Standby mode, both configurations and protocol state are synced between Master and Standby IOCs.

VSP8600 also provides Switch Fabric redundancy in a N+1 configuration. Power Supply and Cooling units also operate in a redundant fashion. See Installing VSP 8600 (NN47229-300) to refer power supply calculator and determine the power requirements of the chassis based on the number and type of IOC modules used.
For more information about HA, see Administering (NN47227-600).

For a list of features, see Supported Features

Chapter 3: Supported Features

The following table lists the features supported on VSP 8600.

Feature	Release
Access Control List (ACL)-based filtering: - Egress ACLs - Ingress ACLs - Layer 2 to Layer 4 filtering - Port-based - VLAN-based For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.5
Address Resolution Protocol (ARP) - Proxy ARP - Static ARP For more information, see *Configuring IPv4 Routing.*	4.5
All Fabric Connect services with switch cluster For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
Alternative routes for IPv4 For more information, see *Configuring IPv4 Routing.*	4.5
Alternative routes for IPv6 For more information, see *Configuring IPv6 Routing* .	n/a
Automatic QoS (supported only for routed pkt) For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.5
Switch cluster (multi-chassis LAG) Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation , MLT, SMLT, and vIST* .	4.5
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services* .	4.5
BGP+ (BGP for IPv6) For more information, see *Configuring BGP Services* .	n/a
Bridge Protocol Data Unit (BPDU) Guard For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a
Certificate order priority For more information, see *Configuring Security* .	n/a
CFM configuration on C-VLANs For more information, see *Troubleshooting.*	n/a
Channelization of 100 Gbps ports For more information, see the hardware documentation and *Administering.*	n/a
Channelization of 40 Gbps ports For more information, see the hardware documentation and *Administering.*	n/a

Feature	Release
Command Line Interface (CLI) For more information, see *Using CLI and EDM* .	4.5
Configuration and Orchestration Manager (COM) For more information, see Extreme Configuration and Orchestration Manager (COM) documentation. **NOTE:** Only device discovery is supported.	4.5
Domain Name Service (DNS) client (IPv4) For more information, see *Administering.*	4.5
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.5
Directed Broadcast For more information, see *Configuring Security* .	n/a
Distributed Virtual Routing (DvR) controller For more information, see *Configuring IPv4 Routing* .	n/a
Distributed Virtual Routing (DvR) leaf For more information, see *Configuring IPv4 Routing* .	n/a
Domain Name Service (DNS) client (IPv4) For more information, see *Administering.*	4.5
DNS client (IPv6) For more information, see *Administering.*	n/a
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see *Configuring IPv4 Routing.*	4.5
DHCP Snooping and Neighbor Discovery Inspection For more information, see *Configuring Security* .	n/a
DHCPv6 Guard For more information, see *Configuring Security* .	n/a
DHCP Snooping (IPv4) For more information, see *Configuring Security* .	n/a
DHCP Snooping (IPv6) For more information, see *Configuring Security* .	n/a
Digital certificate/PKI For more information, see Configuring Security.	n/a
Dynamic ARP Inspection (DAI) For more information, see *Configuring Security* .	n/a
Egress port mirror For more information, see *Troubleshooting.*	4.5
Egress port shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.5

Feature	Release
Encryption modules - The encryption modules file is included in the runtime software image file; it is not a separate file.	4.5
Enable or disable ICMP Broadcast/Multicast For more information, see *Configuring IPv6 Routing*	n/a
Enable/disable IP Source Routing For more information, see *Configuring IPv6 Routing*	n/a
Enhanced Secure mode for JITC and non-JITC sub-modes. For more information, see *Administering.*	n/a
EDM representation of physical LED status For more information, see *Installing the Virtual Services Platform 8600 Series* , NN47229-300.	4.5
Entity MIB - Physical Table For more information, see *Administering.*	n/a
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see *Configuring IPv4 Routing.*	4.5
ECMP for IPv6 For more information, see the following documents: - *Configuring IPv4 Routing* - *Configuring IPv6 Routing* - *Configuring BGP Services*	n/a
ECMP support for VXLAN Gateway and Fabric Extend For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a
Equal Cost Trees (ECT) For more information, see *Configuring Fabric Basics and Layer 2 Services.*	4.5
E-Tree and Private VLANs For more information about E-Tree, see *Configuring Fabric Connect Basics and Layer 2 Services.* For more information about Private VLANs, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see *Configuring Security* .	n/a
EAPoL MHMA-MV For more information, see *Configuring Security* .	n/a
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN, and others For more information, see *Configuring Security* .	
External BGP (EBGP) For more information, see *Configuring BGP Services.*	4.5
Fabric Attach For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
Fabric Attach Zero Touch Client Attachment For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
Fabric BCB functionality For more information, see *Configuring Fabric Basics and Layer 2 Services* .	4.5

Feature	Release
Fabric BEB functionality For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
Fabric Extend For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
Fabric RSPAN (Mirror to I-SID) For more information, see *Troubleshooting.*	n/a
File Transfer Protocol (FTP) server and client (IPv6) For more information, see *Administering.*	n/a
File Transfer Protocol (FTP) server and client (IPv4) For more information, see *Administering.*	4.5
First Hop Security For more information, see *Configuring Security* . - FHS - DHCPv6 Guard - FHS - DHCP Snooping (IPv4) - FHS - DHCP Snooping (IPv6) - FHS - IP Source Guard (IPv4 and IPv6) - FHS - Neighbor Discovery Inspection (IPv6) - FHS - IPv6 Router Advertisement (RA) Guard	n/a n/a n/a n/a n/a n/a n/a
Flight Recorder for system health monitoring For more information, see *Troubleshooting.*	4.5
Forgiving mode for CWDM and DWDM SFP+ transceivers For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software* , NN47227-301.	4.5
Gratuitous ARP filtering For more information, see *Configuring IPv4 Routing.*	4.5
High Availability For more information, see *Administering.*	4.5
IEEE 802.1ag Connectivity Fault Management (CFM): - Layer 2 Ping - TraceRoute - TraceTree For more information, see *Configuring Fabric Basics and Layer 2 Services.*	4.5
IEEE 802.3X Pause frame transmit For more information, see *Administering.*	n/a
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see *Administering.*	n/a
Ingress dual rate port policers For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.5
Internal BPG (IBGP) For more information, see *Configuring BGP Services.*	4.5
Internet Control Message Protocol (ICMP) For more information, see *Configuring IPv4 Routing.*	4.5
ICMP broadcast and multicast enable or disable For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing.*	4.5

Feature	Release
Internet Group Management Protocol (IGMP), including virtualization For more information, see *Configuring IP Multicast Routing Protocols.*	4.5
Internet Key Exchange (IKE) v2 For more information, see *Configuring Security* .	n/a
Inter-VSN routing For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
IP Multicast over Fabric Connect For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
IP route policies For more information, see *Configuring IPv4 Routing.*	4.5
IP Shortcut routing including ECMP For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
IP Source Guard (IPv4 and IPv6) For more information, see *Configuring Security* .	n/a
IP source routing enable or disable For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing.*	4.5
IPsec for IPv6 For more information, see *Configuring Security.*	n/a
IPv6 (VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing* .	n/a
IPv6 OSPFv3 For more information, see *Configuring IPv6 Routing* .	n/a
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	n/a
IPv6 inter-VSN routing For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
IPv6 mode flag (boot config flags ipv6-mode) For more information, see *Configuring IPv6 Routing* .	n/a
IPv6 Shortcut routing For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
IS-IS accept policies For more information, see *Configuring Fabric Basics and Layer 2 Services.*	n/a
Key Health Indicator (KHI) For more information, see *Monitoring Performance.*	4.5
Layer 2 video surveillance install script For more information, see *Configuring Fabric Basics and Layer 2 Services* .	n/a
Layer 2 to Layer 4 ingress port rate limiter For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	n/a

Feature	Release
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Fabric Basics and Layer 2 Services.*	4.5
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	4.5
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	n/a
Layer 3 VSN For more information, see *Configuring Fabric Basics and Layer 2 Services.* **NOTE:** *Only BCB is supported.*	4.5
linerate-directed-broadcast boot flag (boot config flags linerate-directed-broadcast) For more information, see *Administering* .	n/a
Link Layer Discovery Protocol (LLDP) For more information, see *Administering.*	n/a
Logging to a file and syslog (IPv4) For more information, see *Monitoring Performance* .	4.5
Logging to a file and syslog (IPv6) For more information, see *Monitoring Performance* .	n/a
Logon banner For more information, see *Administering* .	n/a
MAC security (MAC-layer filtering, limit learning) For more information see *Configuring VLANs, Spanning Tree, and NLB.*	n/a
Media Access Control Security (MACsec) 2AN mode For more information, see *Configuring Security.*	n/a
MACsec 4AN mode For more information, see *Configuring Security.*	4.5
Mirroring (port and flow-based) For more information, see *Troubleshooting.*	4.5
Multicast Listener Discovery (MLD) For more information, see *Configuring IP Multicast Routing Protocols* .	n/a
Multicast route (mroute) statistics for IPv4 and IPv6 'For more information, see *Configuring IP Multicast Routing Protocols* .	n/a
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	4.5
Network Load Balancing (NLB) - multicast operation For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a
Network Load Balancing (NLB) - unicast operation For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	4.5
Network Time Protocol (NTP) For more information, see *Administering.*	4.5

Feature	Release
nni-mstp boot flag This flag has special upgrade considerations the first time you upgrade to a release that supports it.	n/a
Non EAPoL MAC RADIUS authentication For more information, see *Configuring Security* .	n/a
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP.*	4.5
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see *Configuring IP Multicast Routing Protocols.*	4.5
PIM-SM and PIM-SSM for IPv6 For more information, see *Configuring IP Multicast Routing Protocols.*	n/a
Power over Ethernet (PoE) For more information, see *Administering.*	n/a
PoE/PoE+ allocation using LLDP For more information, see *Administering.*	n/a
Power Manager For more information, see Administering.	4.5
QoS Access Control Entries (ACE) For more information, see *Configuring QoS and ACL-Based Traffic Filtering* .	n/a
RADIUS (IPv6) For more information, see *Configuring Security* .	n/a
RADIUS, community-based users (IPv4) For more information, see *Configuring Security* .	4.5
RADIUS secure communication using IPSec for IPv4 For more information, see *Configuring Security* .	n/a
RADIUS secure communication using IPSec for IPv6 For more information, see *Configuring Security* .	
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering.*	4.5
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see *Monitoring Performance* .	4.5
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Monitoring Performance* .	n/a
Remote Shell (RSH) server/client For more information, see *Administering.*	4.5
Rlogin server (IPv6) For more information, see *Administering.*	n/a
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP.*	4.5
RIPng For more information, see *Configuring OSPF and RIP.*	n/a

Feature	Release
run spbm installation script For more information, see *Configuring Fabric Connect Basics and Layer 2 Services.*	n/a
run vms endura script For more information, see *Configuring Fabric Connect Basics and Layer 2 Services.*	n/a
Secure Copy (SCP) **Note:** The switch does not support the WinSCP client. For more information, see *Administering.*	4.5
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP* .	4.5
Secure Shell (SSH) (IPv4) For more information, see *Administering.*	4.5
Secure Sockets Layer (SSL) certificate management For more information, see *Administering.*	4.5
Security ACEs For more information, see *Configuring QoS and ACL-Based Traffic Filtering* .	4.5
sFlow For more information, see *Monitoring Performance* .	n/a
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	4.5
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see *Monitoring Performance.*	n/a
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security.*	4.5
SLA Mon For more information, see *Configuring the SLA Mon Agent* .	4.5
SNMP (IPv6) For more information, see *Configuring Security* .	n/a
SoNMP For more information, see *Administering.*	4.5
Spanning Tree Protocol (STP): - Multiple STP (MSTP) - Rapid STP (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	4.5
spbm-config-mode For more information, see *Configuring IP Multicast Routing Protocols.*	4.5
SPB-PIM Gateway controller node *For more information, see Configuring SPB-PIM Gateway.*	n/a
SPB-PIM Gateway interface *For more information, see Configuring SPB-PIM Gateway.*	n/a

Feature	Release
SSH (IPv6) For more information, see *Administering.*	n/a
SSH client disable For more information, see *Administering.*	4.5
SSH key size For more information, see *Administering* .	n/a
SSH rekey For more information, see *Administering.*	4.5
Static routing For more information, see *Configuring IPv4 Routing.*	4.5
Suspend duplicate system ID detection For more information, see *Configuring Fabric Connect Basics and Layer 2 Services* .	n/a
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	n/a
Switched UNI For more information, see *Configuring Fabric Connect Basics and Layer 2 Services.*	n/a
TACACS+ For more information, see *Configuring Security* .	4.5
TACACS+ secure communication using IPSec for IPv4 For more information, see *Configuring Security* .	n/a
Telnet server and client (IPv4) For more information, see *Administering.*	4.5
Telnet server and client (IPv6) For more information, see *Administering.*	n/a
TLS server with secure https For more information, see Using CLI and EDM.	n/a
TLS client for secure syslog For more information, see Troubleshooting.	n/a
Transparent Port UNI (T-UNI) For more information, see *Configuring Fabric Connect Basics and Layer 2 Services.*	n/a
Trivial File Transfer Protocol (TFTP) server and client (IPv4) For more information, see *Administering.*	4.5
TFTP server and client (IPv6) For more information, see *Administering.*	n/a
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see *Configuring Security* . **NOTE**: Supported only on IPv4.	4.5

Feature	**Release**
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and*	4.5
Virtual Router Redundancy Protocol (VRRP) For more information, see *Configuring IPv4 Routing* .	4.5
Virtualization with IPv4 Virtual Routing and Forwarding (VRF) - ARP - DHCP Relay - Inter-VRF Routing (static, dynamic, and policy) - Local routing - OSPFv2 - RIPv1 and v2 - Route policies - Static routing - VRRP For more information, see *Configuring IPv4 Routing* .	4.5
Increased VRF and Layer 3 VSN scaling For more information, see *Configuring IPv4 Routing* .	n/a
VRRPv3 for IPv4 and IPv6 For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing* .	n/a
VXLAN Gateway For more information, see *Configuring VLANs, Spanning Tree, and NLB* .	n/a

Chapter 4: Filenames

To download the software files, use one of the following browsers:

For HTTPS, Microsoft Internet Explorer (IE) 9 and 10, and Mozilla Firefox 44 through 49.
For HTTP, Microsoft IE 11, and Mozilla Firefox 43+

Do not use Google Chrome or Safari to download software files. Google Chrome can change the file sizes. Safari changes the .tgz extension to .tar.

After you download the software, calculate and verify the md5 checksum.
For more information, see *Administering.*

Software filenames and sizes

Description	VSP 8600 Series	File size
SHA512 Checksum files	VOSS8600.4.5.0.1.sha512	1,406 bytes
MD5 Checksum files	VOSS8600.4.5.0.1.md5	542 bytes
MIB - supported object names	VOSS8600.4.5.0.1_mib_sup.txt	883,653 bytes
MIB - zip file of all MIBs	VOSS8600.4.5.0.1_mib.zip	999,543 bytes
MIB - objects in the OID compile order	VOSS8600.4.5.0.1_mib.txt	6,701,493 bytes
EDM plug-in for COM	VOSSv4.5.0.1.zip	5,177,535 bytes
EDM Help files	VOSSv4501_HELP_EDM_gzip.zip	3,269,547 bytes
Logs reference	VOSS8600.4.5.0.1_edoc.tar	62,074,880 bytes
Software images	VOSS8600.4.5.0.1.tgz	138,978,618 bytes

Open Source software files

Master copyright file	Open source base software
VOSS8600.4.5.0.1_oss-notice.html 414,262 bytes	VOSS8600.4.5.0.1_OpenSource.zip 9,5871,740 bytes

The Open Source license text for the switch is included on the product.
You can access it by typing the following command in the CLI:
more release/w.*x.y.z.GA* /release/oss-notice.txt
where w.*x.y.z* represents a specific release number.

Chapter 5: Important Notices

This section provides important information for this release.

100 Gbps ports

Support for the following software features on 100 Gbps ports will be available in a future release:

- Channelization
- MACsec

Fabric Configuration

VSP 8600 can be positioned in a Fabric Connect network as a Backbone Core Bridge (BCB). In the BCB mode, VSP 8600 can transport all types of Fabric services including L2VSN, L3VSN, IP Shortcuts and Multicast over SPB.

In this release, VSP 8600 cannot be provisioned as a Backbone Edge Bridge (BEB). That is, I-SIDs cannot be provisioned on VSP 8600. All types of I-SIDs can still traverse VSP 8600 positioned as a BCB node in a Fabric Connect network. This limitation will be removed in the next VSP 8600 release and the switch can be provisioned as a BEB as well.

In this release, VSP 8600 does not support provisioning of CVLANs on the same physical link as Fabric NNI interface.

vIST Configuration

VSP 8600 supports switch clustering or mLAG using the Simplified vIST configuration. Like other VSP products, for configuring Simplified vIST, the switch must be configured to non-Fabric mode by setting the `spbm-config-mode` boot flag to FALSE. That is, Fabric cannot be provisioned when the switch is operating in non-Fabric mode. Switch clustering and Fabric BCB mode cannot be configured at the same time in this release.

In the next release, VSP 8600 will support VIST configuration in Fabric mode, where a pair VSP 8600s can be provisioned as a switch cluster using vIST and can also be part of Fabric network.

IP Multicast

VSP 8600 supports IP Multicast protocols including IGMP and PIM-SM. However, these protocols are not supported with switch clustering or mLAG. This limitation will be removed in the next release of VSP 8600, where both IGMP and PIM will be supported with VIST.

Network Load balancing

VSP 8600 supports Network Load balancing (NLB) in unicast mode only. Support for Multicast mode will be available in a future release.

High Availability

VSP 8600 supports High Availability in two modes: Warm Standby and Hot Standby. Hot Standby mode is not supported when either Fabric or Switch Clustering (vIST) is provisioned. Fabric or vIST enables network based resiliency for switch or link failures, thus ensuring non-stop forwarding. Hot Standby mode is more relevant when either of these technologies are not deployed. In Hot Standby mode, both configuration and protocol states are synced between Master and Standby IOC, thus ensuring a hitless switchover upon Master IOC failure.

In Warm Standby mode, only the configurations are synced between Master and Standby IOC. In Warm Standby mode, if there is a software failure on the Master IOC, the Standby IOC immediately takes over and reboots all the other IOCs. If Fabric or VIST is provisioned, non-stop forwarding can be achieved by network based resiliency enabled by these technologies.

Filters and QoS

VSP 8600 supports a full range of port based and VLAN based filters functionality including L2, L3 and L4 filters. Due to the architecture difference, there are updates and limitations in the type of filters that can be provisioned on VSP 8600.

In this release, the following qualifiers are not supported on VSP8600 in the egress direction (outPort):

Note: Ingress support (inVlan/InPort) for these qualifiers are available.

- arprequest and arpresponse
- ip-frag-flag
- tcp-flags

Support for ip-options qualifier will not be available in ingress/egress direction.

Support for QoS ACLs, including setting of internal-qos, remark-dscp and remark-dot1p will not be available in this release, but will be available in a future release.

IPv6 filters are not supported in this release. Although the commands are visible, the functionality is available only in Demo mode.

For more information, see *Configuring QoS and ACL-Based Traffic Filtering* , NN47227-502

IPv6

In this release, IPv6 configurations are available only in Demo mode. That is, IPv6 features can be provisioned using command line or network management tools. However, IPv6 is not supported in this release. IPv6 will be fully available in a future release.

Chapter 6: Hardware availability

This section lists the hardware availability.
VSP 8608 Chassis provides 8 slots for IOC modules and 3 slots for SF modules.

Part number	Model name	Description
Chassis bundles		
EC8602002-E6	AC Bundle	VSP 8608 Bundle. Includes 1 Chassis, 3 SF modules, 4 AC PSU
EC8602003-E6	DC Bundle	VSP 8608 Bundle. Includes 1 Chassis, 3 SF modules, 4 DC PSU
Chassis		
EC8602001-E6	VSP 8608	VSP 8608 chassis with 8 IOC module slots
SF and IOC modules		
EC8604001–E6	8600SF	8600SF Switch Fabric module
EC8604002-E6	8624XS	24 port 1/10 Gbps SFP+ IOC module
EC8604003-E6	8624XT	24 port 100 Mbps/1 Gbps/10 Gbps RJ-45 copper IOC module
EC8604004-E6	8616QQ	16 port 40 Gbps QSFP+ IOC module
EC8604005-E6	8606CQ	6 port 100 Gbps QSFP28 IOC module
Accessories		
EC8605A01-E6		3000W 100-240V AC Power Supply (No power cable)
EC8605A02-E6		2500W DC Power Supply for VSP 8608 chassis. (No DC power cable)
EC8611001-E6		Spare fan module for VSP 8608 chassis
EC8611002-E6		Spare IOC module filler panel for VSP 8608 chassis
EC8611003-E6		Spare power supply filler panel for VSP 8608 chassis
EC8611004-E6		Spare Rack Mount Kit for VSP 8608
EC8611005-E6		Spare Cable Guide Kit
EC8611006-E6		PSU cover for VSP 8608 chassis
DC power cable		
AA0020112–E6		DC power cable for EC8602001-E6
AC power cables		
AA0020076-E6		Power cable 20A/125V NEMA 5-20, North America
AA0020077-E6		Power cable 15A/250V NEMA 6-15, North America
AA0020078-E6		Power cable 16A/250V CEE7/7, Continental Europe
AA0020079-E6		Power cable 16A/250V CEI 23-50 S17, Italy
AA0020080-E6		Power cable 16A/250V SI 32, Israel
AA0020081-E6		Power cable 15A/250V BS-546, India / South Africa
AA0020082-E6		Power cable 16A/230V 3-Pin IEC60309, InternatIOCnal
AA0020084-E6		Power cable 15A/250V AS 3112, Australia
AA0020085-E6		Power cable 13A/230V BS 1362, UK and Ireland
AA0020086-E6		Power cable 16A/250V GB 11918-86, Greater China
AA0020087-E6		Power cable 15A/250V NEMA L6-15 Twist Lock, North America. This power cable is used with the 9006AC in 220-240V AC twist-lock applicatIOCns.
AA0020102-E6		Power cable IEC C19 TO NBR 14136 (IEC 60906-1) Brazil (2.5 METER 16A/250V) ERS8800 VSP9000

Chapter 7: Software scaling capabilities

This section lists the maximum scaling capabilities for the switch.

Layer 2	
MAC table size	256,000
MAC table size (with switch clustering)	128,000
Port-based VLANs	4,059
RSTP instances	1
MSTP instances	64
LACP aggregators	192
Ports per LACP aggregator	8
MLT groups	192
Ports per MLT group	8
SLPP VLANs	500
VLACP interfaces	128
Microsoft NLB cluster IP interfaces	200
Layer 3	
IPv4 route table	252,000
IPv4 ARP table	64,000
IP interfaces	4,059
VRRP interfaces	512
VRRP interfaces with fast timers (200ms)	24
Routed Split Multi-LinkTrunking (RSMLT) interfaces	1000
IPv4 VRF instances	512
ECMP groups/paths per group	1,000/8
IPv4 UDP forwarding entries	1,024
IPv4 DHCP Relay forwarding entries	1,024
IPv4 CLIP interfaces	64
IPv4 static ARP entries (per VRF/per switch)	2,000/10,000
IPv4 static routes (per VRF/per switch)	2,000/10,000
IPv4 route policies (per VRF/per switch)	2,000/16,000
IP Unicast	
IPv4 BGP peers	256
IPv4 BGP routes (control plane only)	1.5 M
IPv4 OSPFv2 neighbors (active/passive)	500/2,000
OSPF areas	12 per VRF or GRT/80 per switch
IPv4 OSPF routes	64,000

IPv4 RIP interfaces	200
IPv4 RIP routes (per VRF/per switch)	2,000/16,000
IP Multicast	
IGMP interfaces	4,000
PIM interfaces (Active/Passive)	512/3,000
PIM-SSM static channels	4,000
Multicast routes (per switch) in BCB mode	50,000
Multicast receivers/IGMP receiver entries (per switch)	6,000
Multicast senders/IGMP sender entries (per switch)	6,000
Filters, QoS & Security	
Total ACE - Ingress	4,000
Total ACE - Egress	2,000
Total ACL - Ingress	2,000
Total ACL - Egress	1,000
Fabric	
Number of SPB regions	1
Number of SPB adjacencies	192
Number of B-VIDs	2
SPBM enabled switches per region (BEB + BCB)	800*
****NOTE**: If there are any VSP 4000 switches in the network, then the total number of SPBM enabled switches per region will come down to 550.	
OAM & Diagnostics	
FTP sessions	4
Rlogin sessions	8
SSH sessions	8
Telnet sessions	8
Mirroring ports	191
Mirrored destination ports	4

Chapter 8: Known Issues

Issue number	Description	Workaround
VOSS-4712	When there are broadcast packets in the VLAN, these packets are sent to all ports in the VLAN. The packets get dropped because the port is operationally down. However, outPkts stats increment and the unicast packets are not sent to that port because the port is down.	Ignore the stats counter when port is down.
VOSS-5191	The OSPF MD5 related functionality cannot be enabled from EDM.	Use CLI to configure OSPF MD5 related functionality.
VOSS-5511	Half duplex option is not supported but it can be configured on VSP 8600 port.	Do not configure half-duplex.
VOSS-5702	Multicast traffic will not have DSCP marked (when enabled on incoming port), when IGMP snooping is enabled on the VLAN.	No workaround.
VOSS-5797	Error message appears when SSIO process is terminated.	There is no network or operational impact outside the slot when the ssio process is terminated. All cards function as normal and no workaround or action is needed.
VOSS-6102	`sys action reset counters` command does not reset ISIS control packets.	Use `clear isis` command to reset stats.
VOSS-6103	`sys action reset counters` command does not reset ISIS int-counters.	Use `clear isis` command to reset stats.
VOSS-6104	`sys action reset counters` command does not reset any ISIS system stats.	Use `clear isis` command to reset stats.
VOSS-6565	OSPF High Availability (HA) related errors appear on console when the same route policy is applied twice.	No workaround.
VOSS-6776	The switch EDM cannot be accessed through HTTPS using Mozilla Firefox version 50 and above.	To connect to the switch using EDM with HTTPS, use Mozilla Firefox version 49 or below or another browser that supports RC4 cipher.
VOSS-7006	SMLT MACs are not synced correctly when you create a new VLAN on one of the vIST peers.	After creating the VLAN, enter the following command for synchronizing: `vlan mac-address-entry`
VOSS-7148	EDM: In the **Virtual IF** tab, the options SHA-1 and SHA-2 are not available to configure virtual link authorization.	Use CLI to configure virtual link authorization.
VOSS-7179	EDM: **Device Physical View** tab displays the power supplies but does not show their LED status to determine if it is AC, DC or in a failed state.	In EDM, navigate to Edit > Power Supply tab to check the power supply status.
VOSS-7250	When a card is removed and inserted back, depending on the STP port status, an event is sent from CP to standby to stop the timer that was not started on standby.	No workaround.

Issue number	Description	Workaround
VOSS-7305	In a scaled setup, if thousands of ARP records are getting aged out at the same interval, the TTL value displayed in the `show ip arp` output can go to a negative value. This causes the ARP aging to get delayed.	There is no impact to system.
VOSS-7380	The Management port supports 100/1000 full duplex speeds through auto-negotiation. 10 M half/full and 100 M half duplex speeds are not supported.	No workaround.
VOSS-7399	The inband FTP transfer speed to the VSP 8600 is limited to 1 MBps.	No workaround.
VOSS-7500	COM+ does not display correct number of IP OSPF ECMP routes.	Use CLI and EDM to check IP OSPF ECMP routes.
VOSS-7512	If certain router bgp commands are executed in a VRF context, you must save the configuration and exit CLI, then start a new CLI session for future commands to be executed properly. The following are the router bgp commands: - `ibgp-report-import-rt` - `ignore-illegal-rtrid` - `quick-start` - `traps` - `debug-screen` - `router-id`	No workaround.
VOSS-7709	On the 8608CQ IOC module, the output of the `show interface gigabitEthernet statistics` command does not display a value in IN PACKET for packets that have ethertype/length field of 0.	No workaround.
VOSS-7712	If a 100 Gbps port has a local or remote fault, EDM displays the interface connector color as amber and the link/activity LED is off. The link/activity LED should blink green/amber.	Use the LEDs on the physical switch.
VOSS-7713	The system does not currently restrict the number of NLB virtual IP address ARP entries learned. The following message is logged but does not prevent the addition of new entries in the ARP table: `CP1 [09/15/17 11:34:20.192:EDT] 0x0003c984 00000000 GlobalRouter IP WARNING rcIpAddArp: Maximum number of NLB servers supported has been reached. New NLB server connection requests are ignored.`	No workaround. Do not scale beyond the documented scaling number of 200 NLB servers in a cluster.

Chapter 9: Resolved Issues

Issue number	Description
VOSS-6976	NLB does not work in a Simplified vIST or SMLT environment when the NLB traffic is hashed across the VIST to or from the NLB Servers.
VOSS-7425	When the default routes are learned through BGP and if at least two CPU switchovers are issued in a row, a potential switch reset can appear.
VOSS-7446	When there are more than 50 files in USB, the EDM displays only 50 files and not more than that under Chassis > USB files tab.
VOSS-7450	When there is a fan fault and it stops spinning, the fan speed may not be updated.

Chapter 10: Limitations and expected behaviors

This section lists known limitations and expected behaviors that may first appear to be issues.

Filters

The following are the expected behaviour with filters:

- ACL: The incoming packets must be tagged to hit an entry of port-based ACLs containing a VLAN based qualifier in the ACE.
- ACL: InVlan ACLs can match tagged or untagged traffic, with the port-default VLAN considered if the incoming packet is untagged. However, if an ACE of an InVlan ACL contains the qualifier vlan-tag-prio, it can be used to filter only tagged traffic and not the untagged traffic.
- ACL: The outPort ACLs cannot match on the fields that are changed in the packet during forwarding decisions. Hence, the fields (Destination MAC, Source MAC, VLAN ID, etc.) which get modified during L3 routing cannot be used to match on the new contents of these fields in the outgoing packet.
- ACL: The outPort ACLs cannot match on a destination port that is a member of an MLT. So if port 1/5 is a member of an MLT (static or via LACP), an ACE of an OoutPort filter with member 1/5 will not be hit.
- ACL: In an OutPort ACL, the ACEs containing Layer 3 qualifiers will only be hit for packets that are routed. So the qualifiers such as src-ip and dst-ip (in the `filter acl ace ip <acl><ace>` command) does not work for Layer 2 switched packets.
- ACL: Each filter member port uses a separate TCAM entry, which impacts the overall ACE scaling number. For example, an inPort filter with 5 members that has one ACE configured uses 10 different TCAM entries (with at least 5 each for the user and default ACEs). For inPort filters, the existing XGS-based platforms use a single entry for multiple members, since they have the ability to match on port bitmaps instead of a single port. For outPort filters, the existing XGS based platforms use a separate TCAM entry for each filter member.
- ACL: For outPort ACLs, the use of the “ethertype” qualifier results in two TCAM entries being used internally instead of one (one each for single tagged and untagged packets). The packets with multiple tags are unsupported, i.e., we cannot match on Ethertype field of such packets. If VLAN qualifiers are present in ACE (for example, vlan-id or vlan-tag-prio), the entry for untagged packets is not created internally. So a single TCAM entry is used that matches the tagged packets alone. This impacts the overall ACE scaling number.
- There can be a single ACE hit for a packet. Port-based ACLs have precedence over VLAN based ACLs. However, the default ACEs have a lower priority than the user ACEs.

- There can be a single ACE hit for a packet. Port-based ACLs have precedence over VLAN based ACLs. However, the default ACEs have a lower priority than the user ACEs.
  1. User ACE of InPort ACL
  2. User ACE of InVlan ACL
  3. Default ACE of InPort ACL
  4. Default ACE of InVlan ACL

  NOTE:
  If a packet matches a user ACE in both an inPort and inVLAN ACL, the inVLAN ACL is ignored. If a packet matches a user ACE in VLAN-based ACL and the default ACE of an inPort ACL, the user ACE in the inVLAN ACL is hit and the inPort ACL is ignored.
- ACL: The monitor actions (monitor-dst-port or monitor-dst-mlt) are not supported for outPort ACLs. They are only applicable to Ingress ACLs (InPort or InVlan). For flow-based mirroring, you can configure these monitor actions at the ACE level.
- ACE: When an ACE with action count is disabled, the statistics associated with the ACE are reset.
- For ACEs of port-based ACLs, you can configure VLAN qualifiers. Configuring Port qualifiers are not permitted.
  For ACEs of VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.

Chapter 11: Licenses

Licensing allows switch operators to select the features that best suits their needs.

Product Licensing and Delivery System (PLDS) is used for product licenses. The PLDS portal is a one stop area for ordering, authorizing, and generating licenses. See *Getting Started with Avaya PLDS for Avaya Networking Products* , NN46199-300 for information on using PLDS.

The VSP 8600 Series supports a licensing model that has two main categories of licenses: Base License and Feature Pack Licenses. A Base License enables base software features and one is required per IOC in the chassis. You require a Feature Pack License to enable additional features that are grouped into Feature Packs. These licenses are optional.

Licenses are tied to the switch Base MAC address. After you activate licenses on Avaya PLDS, you can install the license file on the switch.

For example, if a VSP8600 chassis is populated with 4 IOCs, you need to activate 4 IOC Base Licenses for the Chassis Base MAC address.

After the licenses are activated on PLDS portal, a license XML file is generated that can be installed on the switch.

Offer Level	**Period**	**Support**
Factory Default	30-days	Can configure all features, excluding MACsec.
Trial	60 days	Can test licensed features. The following types of Trial Licenses are available: • allows the use of all features excluding MACsec • allows the use of all features including MACsec **Note**: You can activate a Trial License once per switch.
IOC Base License		Can use Base software features on the switch. IOC Base license is required for each IOC module that you plan to install in the chassis. If the number of IOCs exceeds the licensed IOC quantity, the ports on the excess IOCs are license-locked and appear administratively down.
Feature Pack		Features that are not available in the Base License are grouped into Feature Packs based on use case. License is required to use a Feature Pack. A Feature Pack License applies to the entire chassis; you do not need to purchase this license type for each installed IOC module. Feature Pack licenses that the VSP 8600 supports: Layer 3 Virtualization: • Layer 3 Virtual Services Networks (VSNs) • Greater than 24 VRFs • Greater than 16 BGP Peers Layer 3 Virtualization with MACsec: • Layer 3 Virtual Services Networks (VSNs) • Greater than 24 VRFs • Greater than 16 BGP Peers • MACsec **NOTE:** Layer 3 VSN will be supported in forthcoming releases.
Uplift		Converts a non MACsec license to a MACsec equivalent license.

For more information about licenses, see *Administering* .