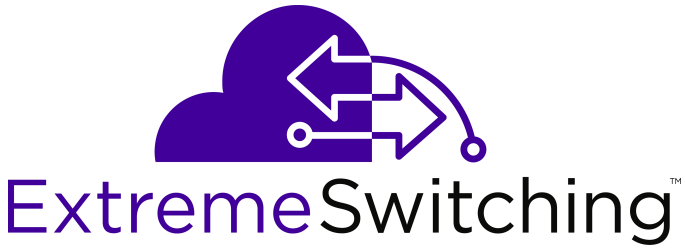

Release Notes for VSP Operating System Software

Release 6.1.2
NN47227-401
Issue 19.04
January 2018

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.

For additional information on Extreme Networks trademarks, please see: http://www.extremenetworks.com/company/legal/

Table of Contents

Click on the hyperlink to open a tab.

New in this release

The following sections detail what is new in Release 6.1.2.

Rebranding

Release 6.1.2 software has been rebranded for Extreme which affects logs, CLI, and EDM.

Entity MIB Enhancements

The Entity MIB assists in the discovery of functional components on the switch. In Release 6.1.2, Entity MIB support has been implemented and enhanced for the following:

- Physical Table — Describes the physical entities managed by a single agent.
- Alias Mapping Table — This table contains mappings between Logical Index, Physical Index pairs, and alias object identifier values. It allows resources managed with other MIB modules (repeater ports, bridge ports, physical and logical interfaces) to be identified in the physical
entity hierarchy.

- Physical Contains Table — This table contains simple mappings between Physical Contained In values for each container or containee relationship in the managed system. The indexing of this table allows a network management station (NMS) to quickly discover the Physical Index values for all children of a given physical entity.

- Last Change Time Table — Represents the value of sysUpTime when the Entity MIB configuration was last changed.

Entity MIB support has been enhanced to provide full basic support for VOSS platforms on Extreme Management Center (XMC).

Backup Configuration

Extreme Management Center (XMC) has a configuration backup feature with a requirement to be able to backup configuration related files. Release 6.1.2 introduces new CLI commands to backup configuration related files and package them into a single zip file, or to restore configuration files that were backed up.

Note: License files are not backed up.

System Logging Enhancements

The Syslog messages with this release conform to RFC5424. The Syslog header now has a timestamp conforming to RFC 3339 which helps to identify the Syslog generation time by indicating the year, milliseconds, and time zone, as well as the Hostname from which the message is generated. The timestamp for the logfiles generated and stored on the device are also compliant with RFC3339 and Hostname of the device. Enhancements also include Log message and SNMP trap generation for unsuccessful logins.

A new boot flag, syslog-ref5424-format, has been introduced with Release 6.1.2 which controls the format of the syslog output and logging. By default, the device uses the RFC5424 format. If the user disables the RFC based format, the older format is used.

Extreme Management Center (XMC) requires the new RFC 5424 format (i.e. syslog-rfc5424-format flag set to enable).

Dot1Q MIB

For Extreme Management Center (XMC) to be able to provision VLAN's, support for the following MIB tables have been added in Release 6.1.2.

- dot1VlanCurrentTable – Contains current configuration information for each VLAN configured on the switch.
- dot1qVlanStaticTable – Contains static configuration information for each VLAN configured on the switch.

• dot1qPortVlanTable – Contains per-port control and status information for VLAN configuration.

• dot1dBasePortEntry – Contains generic information about every port that is associated with this bridge.

• dot1qVlanNumDelete – Indicates the number of times of a VLAN entry was deleted from the dot1qVlanCurrentTable.

P-Bridge MIB

P-Bridge MIB supports the following:

dot1dExtBase Group

dot1dDeviceCapabilities

dot1dTrafficClassesEnabled

dot1dGmrpStatus

dot1dPortCapabilitiesTable

Licensing

Release 6.1.2 supports license files signed using Extreme Networks signature, in addition to existing legacy or PLDS license files signed using Avaya signature.

For a list of features, see Features by Release

Filenames

To download the software files, use one of the following browsers:
IE 9 or later
Mozilla Firefox 37 and later

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.*

Starting in VOSS 4.2, the encryption modules are included as part of the standard runtime software image file.

Prior to VOSS 4.2.1, image filenames began with VSP, for example, VSP4K4.1.0.0.tgz.
In VOSS 4.2.1 and later, image filenames start with VOSS, for example, VOSS8K4.2.1.0.tgz.

Software filenames and sizes

Description	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
SHA512 Checksum files	VOSS4K.6.1.2.0.sha512 1,397 bytes	VOSS7K.6.1.2.0.sha512 1,391 bytes	VOSS8K.6.1.2.0.sha512 2,172 bytes
MD5 Checksum files	VOSS4K.6.1.2.0.md5 533 bytes	VOSS7K.6.1.2.0.md5 527 bytes	VOSS8K.6.1.2.0.md5 527 bytes
MIB - supported object names	VOSS4K.6.1.2.0_mib_sup.txt 1,182,904 bytes	VOSS7K.6.1.2.0_mib_sup.txt 1,186,371 bytes	VOSS8K.6.1.2.0_mib_sup.txt 1,186,371 bytes
MIB - zip file of all MIBs	VOSS4K.6.1.2.0_mib.zip 1,083,041 bytes	VOSS7K.6.1.2.0_mib.zip 1,083,041 bytes	VOSS8K.6.1.2.0_mib.zip 1,083,041 bytes
MIB - objects in the OID compile order	VOSS4K.6.1.2.0_mib.txt 7,180,195 bytes	VOSS7K.6.1.2.0_mib.txt 7,180,195 bytes	VOSS8K.6.1.2.0_mib.txt 7,180,195 bytes
EDM plug-in for COM	VSP4000v6.1.2.0.zip 4,869,205 bytes	VOSSv6.1.2.0.zip 5,176,832 bytes	VOSSv6.1.2.0.zip 5,176,832 bytes
EDM Help files	VSP4000v612_HELP_EDM_gzip.zip 3,282,973 bytes	VOSSv612_HELP_EDM_gzip.zip 3,288,186 bytes	VOSSv612_HELP_EDM_gzip.zip 3,288,186 bytes
Logs reference	VOSS4K.6.1.2.0_edoc.tar 63,979,520 bytes	VOSS7K.6.1.2.0_edoc.tar 63,979,520 bytes	VOSS8K.6.1.2.0_edoc.tar 63,979,520 bytes
Software image	VOSS4K.6.1.2.0.tgz 104,415,587 bytes	VOSS7K.6.1.2.0.tgz 66,411,308 bytes	VOSS8K.6.1.2.0.tgz 120,449,983 bytes

Open Source software files

Description	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
Open source base software	VOSS4K.6.1.2.0_OpenSource.zip 95,871,740 bytes	VOSS7K.6.1.2.0_OpenSource.zip 95,871,740 bytes	VOSS8K.6.1.2.0_OpenSource.zip 95,871,740 bytes
Master copyright file	VOSS4K.6.1.2.0_oss-notice.html 458,318 bytes	VOSS7K.6.1.2.0_oss-notice.html 458,318 bytes	VOSS8K.6.1.2.0_oss-notice.html 458,318 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.

VOSS feature differences

Avaya has implemented feature parity between the VSP Operating System Software (VOSS) platforms in all but a few exceptions. Some features are supported in one platform and not another to maintain compatibility with previous releases. In other cases, the difference is because of the role of the switch in the network.

The following table summarizes the feature differences between the platforms in release 6.1.2.

Feature	VSP 4000 Series	VSP 7200 Series	VSP 8000 Series
CFM CMAC for the CVLAN	Supported	Not supported	Not supported
Channelization of 40 Gbps ports	Not applicable	Supported	Supported
DvR Controller	Not supported	Supported	Supported
Fabric RSPAN	Flow-based Mirroring into single ISID only	Supported	Supported
FDB protected by port (MAC security limit-learning)	Supported	Not supported	Not supported
Ingress Dual Rate Port Policers	Supported	Not supported	Not supported
Layer 2 Video Surveillance install script	Supported	Supported	N/A
Layer 3 Video Surveillance install script (formerly called Endura script)	Supported	N/A	N/A
Multicast Route Statistics for IPv4 and IPv6	Not supported	Supported	Supported
NLB Unicast and Multicast	Not supported	Supported	Supported
PoE/PoE+ Allocation Using LLDP	Supported on VSP 4850GTS-PWR+ and VSP 4450GTX-HT-PWR+	Not supported	Not supported
Port licensing	Not supported	Applicable to Port licensed VSP 7254XSQ fiber switch and VSP 7254XTQ copper switch	Not supported
QoS	Supported	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead	Supported with exceptions: • Classification does not have routed packet classification • No ingress policer- Uses ingress port rate limiting instead
sFlow	Reduced sampling rate	Supported	Supported
Software licensing (Premier)	Supports the Avaya Data Licensing Portal and the Product Licensing & Delivery System (PLDS)	Supports Product Licensing & Delivery System (PLDS) only	Supports Product Licensing & Delivery System (PLDS) only
SPM-PIM GW Controller	Not supported on VSP 4850	Supported	Supported
Use of Open Networking Adapter for Fabric Extend	Required	Not required	Not required
VXLAN Gateway	Not supported	Supported	Supported

Upgrade considerations

The *Administering* document includes detailed image management procedures that includes information about the following specific upgrade considerations:

- Notes for systems using IPv6 static neighbors
- Pre-upgrade instructions for IS-IS metric type
- Upgrade considerations regarding MACsec replay-protect configuration
- Upgrade support for the nni-mstp boot configuration flag
- Upgrade considerations for IS-IS enabled links with HMAC-MD5 authentication
- Considerations for IPv6 VRRP or DHCP Relay configurations saved in VOSS 4.1 or 4.2
- TACACS+ upgrade consideration

If your configuration includes one of the above scenarios, read the upgrade information in*Administering* before you begin an image upgrade.

Supported upgrade paths

This section identifies the software releases for which upgrades to this release have been validated.

Validated upgrade paths are VOSS 6.1.x to VOSS 6.1.2.

VOSS 6.1.0.0 was validated from VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x.

At the time of publishing this document, there were no known restrictions on upgrades. Customers can upgrade directly from other releases to this release (6.1.2). For non-validated upgrade paths, perform the upgrade with one or two switches initially before doing a widespread upgrade.

Upgrading DvR configurations from Releases 6.0.1.1 and earlier to 6.0.1.2 and beyond

All DvR nodes must be upgraded to the same release as quickly as possible. This release includes changes to I-SID ranges that are utilized for DvR communication, and thus introduces an incompatibility with DvR nodes running 6.0.1.1 and earlier, with 6.0.1.2 and beyond.

All DvR Leaf nodes should be upgraded first to minimize the impact of this incompatibility and the resulting loss of connectivity between DvR Controller nodes and Leaf nodes while nodes are at incompatible versions. Once all Leaf nodes have been upgraded, the Controller nodes should then be upgraded, which will then restore DvR connectivity to the already upgraded Leaf nodes.

Note: During the period of time when the Leaf nodes and Controller nodes are running incompatible versions, there will be no DvR connectivity between the Controller and Leaf nodes so this activity should be planned accordingly.

For existing customers with saved configurations prior to 6.1.2.0 who are parsing the non RFC 5424 syslog format, the device defaults to the old format. When XMC registers for syslog, it will set it to the RFC 5424 format and automatically change the syslog and log formats.

Important notices

This section provides important information for this release. Unless specifically stated otherwise, the notices in this section apply to all VOSS platforms.

AES-GCM SSH connection with Open SSH

Switch side encryption and authentication type must be set to the AES-GCM-128/256 methods and needs at least one hmac method in the authentication list in addition for the connection to work.

Auto negotiation settings

VOSS 4.1 and later software requires the same auto negotiation settings on link partners to avoid incorrect declaration of link status. Mismatched settings can cause the links to stay down as well as unpredictable behavior. Ensure the auto negotiation settings between local ports and their remote link partners match before upgrading software to VOSS 4.1 or later.

dos-chkdsk

If at the end of the `dos-chkdsk WORD<1-99>` command output you see:
1) Correct
2) Don't correct
Then, you should run the `dos-chkdsk WORD<1-99>` repair command.

EDM browser support

Use the following recommended browser versions to access Enterprise Device Manager (EDM):
• Microsoft Edge 38.14393
• Microsoft Internet Explorer 11
• Mozilla Firefox 50+

Note: The following earlier browser versions can be used to access EDM (although not recommended):
• Microsoft Internet Explorer 9 and 10
• Mozilla Firefox 37 through 49

Fabric Attach interoperability notes

For Fabric Attach to operate between a VOSS platform and an ERS device, the ERS device must meet minimum software requirements. The following tables identify the minimum GA software releases required to build an FA solution.

Table 1: Extending Fabric using Static FA Proxy configuration (ISID/VLAN is manually configured on FA Proxy)

FA Server		FA Proxy	
Product	**Minimum release**	**Product**	**Minimum release**
VSP 4000	5.0.0.0	ERS 5900	7.0.1
VSP 7200		ERS 5600	6.6.3
VSP 8200		ERS 4800	5.9.2
VSP 8400		ERS 4500	5.7.3

Table 2: Extending Fabric to FA Clients by using FA Proxy

FA Server		FA Proxy		FA Policy	FA Client	
Product	**Minimum release**	**Product**	**Minimum release**		**Product**	**Minimum release**
VSP 4000	5.0.0.0	ERS 5900	7.0.1	IDE Release 9.1 (See Note below)*	AP9100	7.2.5
VSP 7200		ERS 5600	6.6.3			
VSP 8200		ERS 4800	5.9.2			
VSP 8400		ERS 4500	5.7.3			

* Required for AP9100 FA Client. IDE sends FA ISID/VLAN assignment request by using FA Proxy to VOSS FA Server.

IKEv2 digital certificate support with Strong Swan

Strong Swan server must be customized to get IKEv2 Digital Certificate connection between switch and server for RFCs that Strong Swan is compliant and switch is not. This includes SHA256 signing check, IPv6 identifier check and others.

show vlan remote-mac-table command output

- The output for the `show vlan remote-mac-table` command can be different than what appears for the same command on VSP 9000.
- Because all MinM packets that originate from the IST switch use the virtual B-MAC as the source BMAC, the remote BEB learns the C-MAC against the virtual B-MAC.
- Because the remote BEB uses the shortest path to the virtual B-MAC, the remote BEB can show the IST peer as a tunnel in the `show vlan remote-mac-table` command output.

VSP 4000 connecting to an ERS 8800 interoperability notes

- For customers running version 7.1.x:
  The minimum software release is 7.1.3.1, however the recommended ERS 8800 software release is 7.1.5.4 or later.
  On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000, the minimum software version is 7.1.5.4.
  The “spbm version” on the ERS 8800 must be set to “802.1aq”.

- For customers running version 7.2.x:
  The minimum software release is 7.2.0.2, however the recommended ERS 8800 software release is 7.2.1.1 or later.
  On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.2.1.1.

- Diffserv is enabled in the VSP 4000 port settings, and is disabled in the ERS 8800 port settings, by default.

VSP 4000 notes on combination ports

When the VSP 4000 is reset, the peer connections for all ports, including combination ports 47 and 48 on VSP 4450GTX-HT-PWR+, will transition down. During the reset, the fiber ports remain down, but only the copper ports 47 and 48 come up periodically throughout the reset. The copper ports 47 and 48 come up approximately 15 seconds into the reset, remain up for approximately 60 seconds, and then transition down until the boot sequence is complete and all ports come back up.

The following is an example of the status of the combination ports during reset.

```
CP1 [03/18/70 09:55:35.890] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link Down(1/47)
CP1 [03/18/70 09:55:35.903] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link Down(1/48)
CP1 [03/18/70 09:55:49.994] 0x0000c5ec 00300001.239 DYNAMIC CLEAR GlobalRouter HW INFO Link Up(1/48)
CP1 [03/18/70 09:55:50.322] 0x0000c5ec 00300001.238 DYNAMIC CLEAR GlobalRouter HW INFO Link Up(1/47)
CP1 [03/18/70 09:56:43.131] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW INFO Link Down(1/47)
CP1 [03/18/70 09:56:43.248] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW INFO Link Down(1/48)
```

Cabled connections for both copper and fiber ports

The following limitations apply when the combination ports have cabled connections for both the copper and fiber ports.

- Do not use the fiber port and do not insert an SFP into the optical module slot in the following situations:
  - a copper speed setting of either 10M or 100M is required
  - a copper duplex setting of half-duplex is required

Notes:
These limitations are applicable only when auto-negotiation is disabled. To avoid this limitation, use auto-negotiation to determine the speed to 10/100/1000 and to determine the duplex.
The 100M-FX SFP requires auto-negotiation to be disabled. Therefore, auto-negotiation will also be disabled for the copper port. Configure peer switch to disable auto-negotiation.

Hardware compatibility

The following tables list the hardware compatibility for all VOSS platforms and power supplies:

VSP 4000 hardware
VSP 7200 hardware
VSP 8000 hardware
Transceivers
Power supply compatibility

VSP 4000 hardware

Part number	Model number	Initial release	Supported new feature release				
			5.1.1	6.0	6.0.1	6.1	6.1.2
EC4400004-E6	VSP 4450GSX-DC	4.0.50	Y	Y	Y	Y	Y
EC4400A03-E6	VSP 4450GTX-HT-PWR+ (no power cord)	4.0.40	Y	Y	Y	Y	Y
EC4400E03-E6	VSP 4450GTX-HT-PWR+ (NA power cord)	4.0.40	Y	Y	Y	Y	Y
EC4400x05-E6 Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4450GSX-PWR+	4.0	Y	Y	Y	Y	Y
EC4400A05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (no power cord)	4.0.50	Y	Y	Y	Y	Y
EC4400E05-E6GS	VSP 4450GSX-PWR+ TAA Compliant (NA power cord)	4.0.50	Y	Y	Y	Y	Y
EC4800078-E6	VSP 4850GTS DC	3.0	Y	Y	Y	Y	Y
EC4800x78-E6 EC4800x78-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS	3.0	Y	Y	Y	Y	Y
EC4800x88-E6 EC4800x88-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 4850GTS-PWR+	3.0	Y	Y	Y	Y	Y

Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate the desired product nationalization.
See the following for details:
“A”: No power cord included.
“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.
“C”: Includes power cord commonly used in the United Kingdom and Ireland.
“D”: Includes power cord commonly used in Japan.
“E”: Includes North American power cord.
“F”: Includes Australian power cord.

VSP 4000 operational note

Warning:
The USB FLASH drive on all models of VSP 4850 (factory built and converted from ERS 4850) must be treated as a permanent non-removable part of the switch and must NEVER be removed from the switch to ensure proper operation. Additionally, the USB cover must be installed to ensure additional protection against removal. The USB FLASH drive on the VSP 4850 switch is uniquely and permanently bound to the operating system of the switch it is first used on and cannot be transferred to a different switch. Removal (and reinsertion) of the USB FLASH drive from the switch is not supported as it can permanently compromise the switch functionality and render it non-functional.

VSP 7200 hardware

Part number	Model number	Initial release	Supported release				
			5.1.1	6.0	6.0.1	6.1	6.1.2
EC720001F-E6	VSP 7254XSQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y	Y

EC7200x1B-E6 EC7200x1F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XSQ	4.2.1	Y	Y	Y	Y	Y
EC720002F-E6	VSP 7254XTQ DC (Front to back airflow)	4.2.1	Y	Y	Y	Y	Y
EC7200x2B-E6 EC7200x2F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XTQ	4.2.1	Y	Y	Y	Y	Y
EC7200x3B-E6 EC7200x3F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XSQ Port Licensed	5.1	Y	Y	Y	Y	Y
EC7200x4B-E6 EC7200x4F-E6 B represents back to front airflow. F represents front to back airflow. Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 7254XTQ Port Licensed	5.1	Y	Y	Y	Y	Y

Note: The character (x) in the order number indicates the power cord code. Replace the “x” with the proper letter to indicate the desired product nationalization. See the following for details:
“A”: No power cord included.
“B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.
“C”: Includes power cord commonly used in the United Kingdom and Ireland.
“D”: Includes power cord commonly used in Japan.
“E”: Includes North American power cord.
“F”: Includes Australian power cord.

VSP 7200 operational notes

- The VSP 7254XSQ has a PHYless design, which is typical for Data Center top of rack switches. The benefits of a PHYless design are lower power consumption and lower latency. However, due to the PHYless design, the following transceivers are not supported:
  - AA1403017-E6: 1-port 10GBASE-LRM SFP+
  - AA1403016-E6: 1-port 10GBase-ZR/ZW SFP+
    The AA1403165 10GBASE-ZR CWDM DDI SFP+ transceiver can be substituted for AA1403016-E6 10GBASE-ZR/ZW SFP+.

- Software partitions the switch into two logical slots: Slot 1 and Slot 2.
  - Slot 1: 10 Gbps ports: 1 - 48
  - Slot 2: 40 Gbps ports: 1 - 6

- Channelization is supported on the 40 Gbps QSFP+ ports.

- MACsec support:
  - MACsec is only supported on the VSP 7254XTQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XSQ 10 Gbps ports.
  - MACsec is not supported on VSP 7254XTQ and VSP 7254XSQ 40 Gbps ports whether channelization is enabled or not.

• Port licensing support on the port licensed VSP 7254XSQ fiber switch:
  - 24 ports (Slot 1, ports 25 to 48) out of the 48 1/10 GbE SFP/SFP+ ports require a Port License to be unlocked.
  - two ports (Slot 2, ports 5 and 6) out of the six 40 GbE QSFP+ ports require a Port License to be unlocked.

Port licensing support on the port licensed VSP 7254XTQ copper switch:
  - 24 ports (Slot 1, ports 25 to 48) out of the 48 100 Mbps/1 GbE/10 GbE RJ-45 ports require a Port License to be unlocked.
  - two ports (Slot 2, ports 5 and 6) out of the six 40 GbE QSFP+ ports require a Port License to be unlocked.

• 1000BASE-T SFP (AA1419043-E6) will only operate at 1 Gbps speeds when used on a VSP 7254XSQ.

• When you use 1 Gigabit Ethernet SFP transceivers on VSP 7254XSQ, the software disables auto-negotiation on the port:
  - If you use 1 Gbps fiber SFP transceivers, the remote end must also have auto-negotiation disabled.
  - If you use 1 Gbps copper SFP transceivers, the remote end must have auto-negotiation enabled. If not, the link will not be established.

• When a port on VSP 7254XSQ is disabled or enabled, or a cable replaced, or the switch rebooted, the remote link can flap twice.

• Enable auto-negotiation to ensure proper operation at 100 Mbps speeds on VSP 7254XTQ:
  - Link instability will be seen if both ends are set to 100 Mbps auto-negotiation disabled and you use a straight through cable.
  - If Link instability is seen when you use a cross-over cable, a port disable or enable can fix the issue.

For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

VSP 8000 hardware

Part number	Model number	Initial release	Supported release				
			5.3	6.0	6.0.1	6.1	6.1.2
EC8200x01-E6 EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 8284XSQ	4.0	N	Y	Y	Y	Y
EC8200001-E6	VSP 8284XSQ-DC	4.0.50	N	Y	Y	Y	Y
EC8400001-E6	VSP 8404-DC	4.2.1	N	Y	Y	Y	Y
EC8400x01-E6 EC8200x01-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 8404	4.2	N	Y	Y	Y	Y
EC8400002-E6	VSP 8404C-DC	5.3	Y	N	N	Y	Y
EC8400x02-E6 EC8200x02-E6GS Note: Replace the “x” with a country specific power cord code. See the footnote for details.	VSP 8404C	5.3	Y	N	N	Y	Y
Ethernet Switch Modules (ESM) — VSP 8400 only **Important:** Ensure the switch runs, at a minimum, the noted initial software release before you install an ESM.							
EC8404001-E6 EC8404001-E6GS	8424XS	4.2	Y	Y	Y	Y	Y
EC8404002-E6 EC8404002-E6GS	8424XT	4.2	Y	Y	Y	Y	Y
EC8404003-E6 EC8404003-E6GS	8408QQ	4.2	Y	Y	Y	Y	Y
EC8404005-E6 EC8404005-E6GS	8418XSQ	4.2	Y	Y	Y	Y	Y
EC8404006-E6 EC8404006-E6GS	8418XTQ	5.0	Y	Y	Y	Y	Y
EC8404007-E6 EC8404007-E6GS	8424GS	5.0	Y	Y	Y	Y	Y
EC8404008-E6 EC8404008-E6GS	8424GT	5.0	Y	Y	Y	Y	Y

EC8404009-E6 EC8404009-E6GS	8402CQ (supported in VSP 8404C only)	5.3	Y	N	N	Y	Y

Note: The character (x) in the order number indicates the power cord code. Replace the "x" with the proper letter to indicate the desired product nationalization.
See the following for details:
"A": No power cord included.
"B": Includes European "Schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.
"C": Includes power cord commonly used in the United Kingdom and Ireland.
"D": Includes power cord commonly used in Japan.
"E": Includes North American power cord.
"F": Includes Australian power cord.

Transceivers

VSP Operating System software now allows the use of transceivers and direct attach cables from any vendor, which means that the switch will bring up the port operationally when using any transceiver. Avaya does not provide support for operational issues related to the use of non-Avaya branded transceivers and direct attached cables used in the switches.
For more information, see *Installing Transceivers and Optical Components on VSP Operating System Software*, NN47227-301.

Power supply compatibility

You can use certain power supplies in more than one VOSS platform. This section lists the power supplies and indicates the compatible platforms.
For more specific information on each power supply, see the following documents:
• *Installing Avaya Virtual Services Platform 4850GTS Series*, NN46251-300
• *Installing Avaya Virtual Services Platform 4450GTX-HT-PWR+ Switch*, NN46251–304
• *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch*, NN46251-307
• *Installing the Avaya Virtual Services Platform 8000 Series*, NN47227-300
• *Installing the Avaya Virtual Services Platform 7200 Series*, NN47228-302

VSP 4000 Series power supplies

Platform	300 W AC AL1905x08-E5	300 W DC AL1905005-E5	1,000 W AC AL1905x21-E6	1,000 W AC-HT EC4005x03-E6HT
VSP 4850GTS-DC	—	Y	—	—
VSP 4850GTSPWR+	—	—	Y	Y
VSP 4850GTS	Y	—	—	—
VSP 4450GTX-HT-PWR+	—	—	—	Y
VSP 4450GSX-DC	—	Y	—	—
VSP 4450GSXPWR+	—	—	Y	Y

VSP 7200 Series and VSP 8000 Series power supplies

Platform	460 W AC front-to-back EC7205x1F-E6	460 W AC back-to-front EC7205x1B-E6	800 W AC front-to-back EC8005x01-E6	800 W AC front-to-back EC7205x0F-E6	800 W AC back-to-front EC7205x0B-E6	800 W DC front-to-back EC8005001-E6
VSP 8284XSQ	—	—	Y	—	—	—
VSP 8284XSQ-DC	—	—	—	—	—	Y
VSP 8404	—	—	Y	—	—	—
VSP 8404-DC	—	—	—	—	—	Y
VSP 8404C	—	—	Y	—	—	—
VSP 8404C-DC	—	—	—	—	—	Y
VSP 7254XSQ front-to-back	Y	—	—	—	—	—
VSP 7254XSQ back-to-front	—	Y	—	—	—	—
VSP 7254XTQ front-to-back	—	—	—	Y	—	—
VSP 7254XTQ back-to-front	—	—	—	—	Y	—
VSP 7254XSQ-DC	—	—	—	—	—	Y
VSP 7254XTQ-DC	—	—	—	—	—	Y

Note: The character (x) in the order number indicates the power cord code. Replace the "x" with the proper letter to indicate the desired product nationalization.
See the following for details:
"A": No power cord included.
"B": Includes European "Schuko" power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden.
"C": Includes power cord commonly used in the United Kingdom and Ireland.
"D": Includes power cord commonly used in Japan.
"E": Includes North American power cord.
"F": Includes Australian power cord.

Software scaling capabilities

This section lists software scaling capabilities of the following products:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

	Maximum number supported		
	VSP 4000 Series	**VSP 7200 Series**	**VSP 8000 Series**
Layer 2			
Directed Broadcast interfaces	n/a	200 *See NOTE	200 *See NOTE
*** NOTE:** The number of Directed Broadcast interfaces must be less than or equal to 200. However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs.			
MAC table size (without SPBM)	32,000	224,000	224,000
MAC table size (with SPBM)	16,000	112,000	112,000
Port-based VLANs	4,059	4,059	4,059
Private VLANs	1,000	4,059	4,059
Protocol-based VLANs (IPv6 only)	1	1	1
RSTP instances	1	1	1
MSTP instances	12	12	12
LACP aggregators	24	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Ports per LACP aggregator	8 active	8 active	8 active
MLT Groups	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Ports per MLT group	8	8	8
SLPP VLANs	128	128	128
VLACP interfaces	50	54 (up to 72 with channelization)	84 (up to 96 with channelization)
Microsoft NLB cluster IP interfaces	n/a	200 *See NOTE	200 *See NOTE
*** NOTE:** The number of NLB cluster IP interfaces multiplied by the number of configured clusters must be less than or equal to 200. The number of NLB cluster IP interfaces is the key, not the number of VLANs. You can configure 1 VLAN with up to 200 NLB cluster IP interfaces or configure up to 200 VLANs with 1 NLB cluster IP interface per VLAN. For example: 1 virtual interface per cluster x 200 clusters = 200 or 2 virtual interfaces per cluster x 100 clusters = 200 However, if you configure VLANs with both NLB and Directed Broadcast, you can only scale up to 100 VLANs assuming there is only 1 NLB cluster IP interface per VLAN.			
IP Unicast			
IP interfaces (IPv4 or IPv6 or IPv4+IPv6)	256	506 *See NOTE	VSP 8404C = 503 Other VSP 8000 Series platforms = 506 *See NOTE
VRRP interfaces (IPv4 or IPv6)	64	252 *See NOTE	252 *See NOTE
Routed Split Multi-Link Trunking (RSMLT) interfaces (IPv4 or IPv6 or IPv4+IPv6)	252	252 *See NOTE	252 *See NOTE
*** NOTE:** The maximum number of IP interfaces is based on the following formulas: - If you disable the VRF scaling boot configuration flag: = 506 – (# of VRRP IPv4 interfaces) - (# of VRRP IPv6 interfaces) – (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3x(# of VRFs) - If you enable the VRF scaling boot configuration flag: = 506 – (# of VRRP IPv4 interfaces) – (# of VRRP IPv6 interfaces) - (# of RSMLT interfaces) – 2 (if IP Shortcuts is enabled) – 3			
VRRP interfaces with fast timers (200ms) - IPv4/IPv6	24	24	24
DvR Virtual IP interfaces	501 with vIST 502 without vIST	501 with vIST 502 without vIST	501 with vIST 502 without vIST
ECMP groups/paths per group	500/4	1,000/8	1,000/8
OSPF v2/v3 interfaces	100	500	500
OSPF v2/v3 neighbors (adjacencies)	100	500	500
OSPF areas	12 for each VRF 64 for the switch	12 for each VRF 80 for the switch	12 for each VRF 80 for the switch
IPv4 ARP table	6000	32,000	32,000
IPv4 CLIP interfaces	64	64	64
IPv4 RIP interfaces	24	200	200
IPv4 BGP peers	12	12	12
IPv4 VRF instances See VRF scaling note	128 including GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
IPv4 static ARP entries	200 for each VRF 1,000 for the switch	2,000 for each VRF 10,000 for the switch	2,000 for each VRF 10,000 for the switch
IPv4 static routes	1,000 for each VRF 1,000 for the switch	1,000 for each VRF 5,000 for the switch	1,000 for each VRF 5,000 for the switch
IPv4 route policies	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch	500 for each VRF 5,000 for the switch
IPv4 UDP forwarding entries	128	512	512
IPv4 DHCP Relay forwarding entries	128	1024	1024
IPv6 DHCP Snoop entries in Source Binding Table	1,024	1,024	1,024
IPv6 Neighbor table	4,000	8,000	8,000
IPv6 static entries in Source Binding Table	256	256	256
IPv6 static neighbor records	128	256	256
IPv6 CLIP interfaces	64	64	64
IPv6 static routes	1,000	1,000	1,000
IPv6 6in4 configured tunnels	254	506	506
IPv6 DHCP Relay forwarding	128	512	512
IPv6 RIPng interfaces	24	48	48
Layer 3 route table size			
IPv4 RIP routes IPv4 OSPF routes IPv4 BGP routes IPv4 SPB shortcut routes IPv4 SPB Layer 3 VSN routes IPv6 OSPFv3 routes - GRT only IPv6 SPB shortcut routes - GRT only IPv6 RIPng routes	See Route Scaling		
IP Multicast			

Combination of VLANs + number of IPv4 senders + IPv6 senders (non-SPBM mode)	4,059	8,192	8,192
Combination of Layer 2 VSNs + number of IPv4 senders + number of IPv6 senders (SPBM mode)	4,059	8,192	8,192
IGMP/MLD interfaces (IPv4/IPv6)	4,059	4,059	4,059
PIM interfaces (IPv4/IPv6)	128 Active	128 Active	128 Active
PIM Neighbors (IPv4/IPv6) (GRT Only)	128	128	128
PIM-SSM static channels (IPv4/IPv6)	512	4,000	4,000
Multicast receivers/IGMP joins (IPv4/IPv6) (per switch)	1,000	6,000	6,000
Total multicast routes (S,G,V) (IPv4/IPv6) (per switch)	1,000	6,000	6,000
Total multicast routes (S,G,V) (IPv4) on an SPB-PIM Gateway configured switch	1,000	3,000	3,000
Static multicast routes (S,G,V) (IPv4/IPv6)	512	4,000	4,000
Multicast enabled Layer 2 VSN (IPv4)	1,000	2,000	2,000
Multicast enabled Layer 3 VSN (IPv4)	128 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
SPB-PIM Gateway controller S,Gs (source announcements) with MSDP (IPv4)	6,000	6,000	6,000
SPB-PIM Gateway controllers per SPB fabric (IPv4)	5	5	5
SPB-PIM Gateway nodes per SPB fabric (IPv4)	64	64	64
SPB-PIM Gateway interfaces per BEB (IPv4)	64	64	64
PIM neighbors per SPB-PIM Gateway node (IPv4)	64	64	64
Distributed Virtual Routing (DvR)			
DvR Virtual IP interfaces	501 with vIST 502 without vIST	501 with vIST 502 without vIST	501 with vIST 502 without vIST
DvR domains per SPB fabric	16	16	16
Controller nodes per DvR domain	n/a	8	8
Leaf nodes per DvR domain	250	250	250
DvR enabled Layer 2 VSNs	501 with vIST 502 without vIST	501 with vIST 502 without vIST	501 with vIST 502 without vIST
DvR host route scaling	6,000	32,000	32,000
Notes: -On the DvR leaf, you must enable the VRF scaling boot configuration flag if more than 24 VRFs are required in the DvR domain. -Scaling of the VSP 4000 controls the scaling of the DvR domain it is in. For example, if a VSP 4000 is in a DvR domain with other platforms such as VSP 7200s and VSP 8000s, the scaling of the entire domain is limited to the scaling of the VSP 4000.			
VXLAN Gateway			
MAC addresses in base interworking mode	n/a	112,000	112,000
MAC addresses in full interworking mode	n/a	74,000	74,000
VNI IDs per node	n/a	2,000	VSP 8404C = 4,000 Other VSP 8000 Series platforms = 2,000
VTEP destinations per node or VTEP	n/a	500	500
Filters, QoS & Security			
Total IPv4 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	1,020	766	VSP 8404C = 3,070 Other VSP 8000 Series platforms = 766
Total IPv4 Egress rules/ACEs (Port based, Security filters)	255	252	VSP 8404 and 8404C = 251 Other VSP 8000 Series platforms = 252
Total IPv6 Ingress rules/ACEs (Port/VLAN based, Security/QoS filters)	255	256	VSP 8404 = 511 VSP 8404C = 2,047 Other VSP 8000 Series platforms = 256
For more information on filter scaling, see	Filter Scaling		
EAPoL 802.1x (clients per port)	32	32	32
OAM & Diagnostics			
FTP sessions (IPv4/IPv6)	4	4	4
Rlogin sessions (IPv4/IPv6)	8	8	8
SSH sessions (IPv4/IPv6)	8 total (any combination of IPv4 and IPv6)	8 total (any combination of IPv4 and IPv6)	8 total (any combination of IPv4 and IPv6)
Telnet sessions (IPv4/IPv6)	8	8	8
Mirrored ports	49	53 (up to 71 with channelization)	83 (up to 95 with channelization)
Fabric RSPAN Port mirror instances per switch (Ingress only)	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.	Port mirror sessions can be mapped to 24 unique I-SID offsets for Ingress Mirror. Only one I-SID offset for Egress Mirror.
Fabric RSPAN Flow mirror instances per switch (Ingress only)	Filter ACL ACE sessions can be mapped to only 1 mirror I-SID offset.	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.	Filter ACL ACE sessions can be mapped to 24 unique I-SID offsets.
Fabric RSPAN Monitoring I-SIDs (network value)	1,000 Monitoring I-SIDs across SPB network	1000 Monitoring I-SIDs across SPB network	1,000 Monitoring I-SIDs across SPB network
sFlow sampling limit	100 samples per second	3,000 samples per second	3,000 samples per second

VRF scaling note

By default, the system reserves VLAN IDs 4060 to 4094 for internal use.
If you enable both the VRF scaling and the SPBM mode boot configuration flags, the system reserves additional VLAN IDs (3500 to 3998) for internal use.
By default, VRF scaling is disabled and SPBM mode is enabled.

Fabric scaling capabilities

This section lists the fabric scaling information.

Attribute	VSP 4000 Series		VSP 7200 Series		VSP 8000 Series	
	vIST configured	vIST not configured	vIST configured	vIST not configured	vIST configured	vIST not configured
Number of SPB regions	1	1	1	1	1	1
Number of B-VIDs	2	2	2	2	2	2
Maximum number of Physical and Logical (Fabric Extend) NNI interfaces/adjacencies	VSP 4450 = 255 VSP 4850 = 24	VSP 4450 = 255 VSP 4850 = 24	255	255	255	255
SPBM enabled nodes per region (BEB + BCB)	550	550	800	800	800	800
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs, E-Tree, Multicast, Transparent Port UNI). vIST clusters are counted as 3 nodes. Each Fabric Extend IS-IS adjacency or VXLAN remote VTEP reduces this number by 1.	500	500	500	500	500	500
Maximum number of vIST/IST clusters this node can share I-SIDs with	500	500	330	330	330	330
Layer 2 MAC table size (with SPBM)	16,000	16,000	112,000	112,000	112,000	112,000
I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported
Maximum number of Layer 2 VSNs per switch	1,000	1,000	4,059	4,059	4,059	4,059
Maximum number of Switched UNI I-SIDs per switch	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported
Maximum number of Transparent Port UNIs per switch	48	48	54 (up to 72 with channelization)	54 (up to 72 with channelization)	84 (up to 96 with channelization)	84 (up to 96 with channelization)
Maximum number of E-Tree PVLAN UNIs per switch	1,000	1,000	4,059	4,059	4,059	4,059
Maximum number of Layer 3 VSNs per switch See VRF scaling note	128 including mgmt VRF and GRT	128 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT	256 including mgmt VRF and GRT
Maximum number of SPB Layer 2 multicast UNI I-SIDs	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported	See Number of I-SIDs supported
Maximum number of SPB Layer 3 multicast UNI I-SIDs	Maximum 1,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.		Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.		Maximum 6,000 for a BEB: Due to internal resource sharing IP Multicast scaling depends on network topology. Switch will issue warning when 85 and 90% of available resources are reached.	
Maximum number of FA ISID/VLAN assignments per port	94	94	94	94	94	94
Maximum number of IP multicast S,Gs when operating as a BCB	1,000	1,000	16,000	16,000	16,000	16,000

Number of I-SIDs supported for the number of configured IS-IS interfaces and adjacencies (NNIs)

The number of I-SIDs supported depends on the number of IS-IS interfaces and adjacencies (NNIs) configured.

The following table shows the number of UNI I-SIDs supported per BEB. UNI I-SIDs are used for Layer 2 VSN, Layer 3 VSN, Transparent-UNI, E-Tree, Switched-UNI and S, G for Multicast.

Number of IS-IS interfaces (NNIs)	VSP 4000 Series		VSP 7200 Series		VSP 8000 Series	
	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform	I-SIDs with vIST configured on the platform	I-SIDs without vIST configured on the platform
4	1,000	1,000	4,000	4,000	4,000	4,000
6	1,000	1,000	3,500	4,000	3,500	4,000
10	650	1,000	2,900	4,000	2,900	4,000
20	350	700	2,000	4,000	2,000	4,000
48	n/a	n/a	1,000	2,000	1,000	2,000
72	n/a	n/a	750	1,500	750	1,500
100	n/a	n/a	550	1,100	550	1,100
128	n/a	n/a	450	900	450	900
250	n/a	n/a	240	480	240	480

Recommendations

This section provides recommendations that affect feature configuration.

Pay special attention to the expected scaling of routes in the network and the number of OSPF neighbors in a single VRF when you select configuration values for the **isis l1-hellointerval** and **isis l1-hello-multiplier** commands on IS-IS interfaces. The default values for these commands work well for most networks, including those using moderately-scaled routes.

VSP 7200 and VSP 8000 Series

The default values work well for 16,000 routes and 64 OSPF neighbors in a single VRF. However, in highly-scaled networks, you may need to configure higher values for these commands.

For example, if the total number of non IS-IS routes on a given BEB exceeds 16,000 in combination with approximately 128 OSPF neighbors in a single VRF, you should configure a value of 12 for **isis l1-hellomultiplier**, instead of using the default value of 3.

VSP 4000 Series

If the total number of non IS-IS routes on a given BEB exceeds 25,000 in combination with approximately 60,000 IS-IS routes that the BEB receives from other BEBs in the network, you should configure a value of 12 for **isis l1-hellomultiplier**, instead of using the default value of 3.

Interoperability considerations for IS-IS external metric

BEBs running VOSS 5.0 can advertise routes into IS-IS with the metric type as external. They can also correctly interpret route advertisements with metric type external received via IS-IS. In an SPB network with a mix of products running different versions of software releases, you must take care to ensure that turning on the ability to use metric-type external does not cause unintended loss of connectivity.

Note the following before turning on IS-IS external metric if the SPB network has switches running a release prior to VOSS 5.0:

- There are no special release or product type implications if the switch does not have IP Shortcuts or Layer 3 VSN enabled. For example, this applies to Layer 2 only BEBs and BCBs.

z

- There are no special release or product type implications if the Layer 3 VSN in which routes are being advertised with a metric-type of external is not configured on the switch.

- If a switch running a VOSS release that is prior to VOSS 5.0 but VOSS 4.2.1 or later, it will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.

- Switches running VSP 9000 release 4.1.0.0 or later will treat all IS-IS routes as having metric-type internal, regardless of the metric-type (internal or external) used by the advertising BEB in its route advertisement.

- Switches running VOSS releases prior to 4.2.1.0 may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to the GRT.

- Switches running VSP 9000 releases prior to 4.1.0.0 may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

- Switches running any ERS 8800 release may not correctly install IS-IS routes in a Layer 3 VSN if any routes advertised with metric-type external are advertised in that Layer 3 VSN by other BEBs in the network. Layer 3 VSNs in which there are no routes with an external metric-type will not be impacted. Similar note applies to GRT.

Route scaling capabilities

The following table provides information on IPv4 and IPv6 route scaling.

The route scaling does not depend on the protocol itself, but rather the general system limitation in the following configuration modes:

- URPF check mode - Enable this boot configuration flag to support Unicast Reverse Path Forwarding check mode.
- IPv6 mode - Enable this boot configuration flag to support IPv6 routes with prefix-lengths greater than 64 bits. When the IPv6-mode is enabled, the maximum number of IPv4 routing table entries decreases. This flag does not apply to all hardware platforms.

		VSP 4000 Series			VSP 7200 Series and VSP 8000 Series		
URPF mode	IPv6 mode	IPv4	IPv6		IPv4	IPv6	
			Prefix less than 64	Prefix greater than 64		Prefix less than 64	Prefix greater than 64
No	No	15,744	7,887	256	15,488	7,744	n/a
No	Yes	n/a	n/a	n/a	7,488	3,744	2,000
Yes	No	7,744	3,872	256	7,488	3,744	n/a
Yes	Yes	n/a	n/a	n/a	3,488	1,744	1,000

Filter scaling

This section provides filter scaling numbers for the following platforms:
Filter scaling for VSP 4000 Series
Filter scaling for VSP 7200 Series and VSP 8000 Series
Filter scaling for the VSP 8404C

Filter scaling for the VSP 4000 Series

This section provides more details on filter scaling numbers for the VSP 4000 Series.

The switch supports the following maximum limits:
- 220 IPv4 ingress ACLs
- 50 IPv4 egress ACLs
- 128 IPv6 ingress ACLs
- 1,020 IPv4 ingress ACEs
- 255 IPv4 egress ACEs
- 255 IPv6 ingress ACEs

Filter scaling for the VSP 7200 Series and VSP 8000 Series

This section provides more details on filter scaling numbers for the VSP 7200 Series and VSP 8000 Series.

The switch supports the following maximum limits:
- 256 ingress ACLs (see Note 1)
- 126 egress ACLs (see Note 2)
- 766 ingress ACEs (see Note 3)
- 252 egress ACEs (see Note 4)

Note 1: Regarding ingress ACLs (inPort or inVlan), the switch supports:
- 256 ACLs with 1 security ACE each, or
- 128 ACLs with 1 QoS ACE each, or
- a combination based on this rule:
((num ACLs + num security ACEs) <= 512) && ((num ACLs + num QoS ACEs) <= 256)
This maximum implies a VLAN member count of 1 for inVlan ACLs

Note 2: Regarding egress ACLs (outPort only), the switch supports:
- 126 ACLs with 1 security ACE each (one of these ACLs can have 2 ACEs)
This maximum implies a port member count of 1 for outPort ACLs.

Note 3: Theoretical maximum of 766 implies 1 ingress ACL with 511 security ACEs and 255 QoS ACEs.
- Ingress ACEs supported: (512 (security) - # of ACLs) + (256(QoS) - # of ACLs).
This maximum also implies a VLAN member count of 1 for an inVlan ACL.

Note 4: Theoretical maximum of 252 implies 1 egress ACL with 252 security ACEs.
- Egress ACEs supported: 253 - # of ACLs.
This maximum also implies a port member count of 1 for the outPort ACL.

Filter scaling for the VSP 8404C

This section provides more details on filter scaling numbers for the VSP 8404C.

The switch supports a maximum 3070 non-IPv6 ingress ACEs, 2047 IPv6 ingress ACEs, and 251 non-IPv6 egress ACEs.

IPv6 ingress QoS ACL/Filters and IPv6 egress security with QoS ACL/Filters are not supported. If you disable an ACL, the ACL state affects the administrative state of all of the ACEs within it.

ACL scaling

The switch supports the following maximum limits:
• 1024 non-IPv6 ingress ACLs (see Note 1)
• 1024 IPv6 ingress ACLs (see Note 2)
• 126 non-IPv6 egress ACLs (see Note 3)

Note 1: For 1024 non-IPv6 ingress ACLs (inPort or inVlan), the maximum is:
• 1024 ACLs with 1 security ACE each OR
• a combination based on the following rule:
  num of ACLs <= 1024 AND
  (num of ACLs + Security ACEs) <= 2048 AND
  (num of ACLs + QoS ACEs) <= 1024
This maximum implies a VLAN member count of 1 for inVlan ACLs.

Note 2: For 1024 IPv6 ingress ACLs (inPort), the maximum is:
• 1024 IPv6 ACLs with 1 security ACE each OR
• a combination based on the following rule:
  num of IPv6 ACLs <= 1024 AND
  (num of IPv6 ACLs + Security ACEs) <= 2048

Note 3: For 126 non-IPv6 egress ACLs (outPort), the maximum is:
• 126 ACLs with 1 Security ACE each OR
• a combination based on the following rule:
  num ACLs <= 126 AND
  (num ACLs + num security ACEs) <= 252
This maximum implies a port member counter of 1 for outPort ACLs.

ACE scaling

The switch supports the following maximum limits:
• 3070 non-IPv6 ingress ACEs (see Note 4)
• 2047 IPv6 ingress ACEs (see Note 5)
• 251 non-IPv6 egress ACEs (see Note 6)

Note 4: For 3070 non-IPv6 ingress ACEs, the theoretical maximum implies the following configuration:
• 1 non-IPv6 ingress ACL with 2047 security ACEs and 1023 QoS ACEs.
• a VLAN member count of 1 for inVlan ACLs
• Non-IPv6 Ingress ACEs supported:
  [2048(security) - (num of ACLs)] + [1024(QoS) - (num of ACLs)]

Note 5: For 2047 IPv6 ingress ACEs, the theoretical maximum implies the following configuration:
• 1 IPv6 ingress ACL with 2047 security ACEs
• IPv6 Ingress ACEs supported:
  [2048(security) - (num of ACLs)]

Note 6: For 251 non-IPv6 egress ACEs, the theoretical maximum implies the following configuration:
• 1 egress ACL with 251 security ACEs
• a port member count of 1 for outPort ACLs
• Non IPv6 egress ACEs supported:
  252 - (num egress ACLs)

Known Issues

Issue number	Description	Workaround
VOSS-1265	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to default.
VOSS-1278	SLA Mon™ tests fail (between 2% and 8% failure) between devices when you have too many agents involved with scaled configurations.	This happens only in a scaled scenario with more than seven agents, otherwise the failure does not occur. The acceptable failure percentage is 5%, but you may see failure of up to 8%.
VOSS-1279	The command sys shutdown does not change the STATUS LED.	None. This issue does not impact any functionality.
VOSS-1280	The following error message occurs when performing shutdown/no-shutdown commands continuously: `IO1 [05/02/14 06:59:55.178:UTC] 0x0011c525 00000000 GlobalRouter COP-SW ERROR vsp4kTxEnable Error changing TX disable for SFP module: 24, code: -8`	None. When this issue occurs, the port in question can go down, then performs a shutdown/no-shutdown of the port to bring it up and resumes operation.
VOSS-1284	On a fresh boot, peer ports connected to ports 1/49 and 1/50 bounce and can cause additional transitions in the network.	None.
VOSS-1285	CAKs are not cleared after setting the device to factory-default.	None. Currently this is the default behavior and does not affect functionality of the MACsec feature.
VOSS-1287	A reboot with verbose configuration does not allow you to delete a VRF.	This issue occurs only if you save the configuration file in verbose mode and reboot the switch in that configuration. This situation is unlikely to exist; verbose mode is used more as a diagnostic tool. This issue does not impact functionality.
VOSS-1288	Shutting down the T1 link from one end of the link does not shut down the link at the remote end. You may experience traffic loss if the remote side of the link is not shut down.	This issue occurs only when a T1 SFP link from one end is shutdown. Enable a dynamic link layer protocol such as LACP or VLACP on both ends to shut the remote end down too. As an alternative, administratively disable both ends of the T1 SFP link to avoid the impact.
VOSS-1289	On a MACsec enabled port, you can see delayed packets when the MACsec port is kept running for more than 12 hours. This delayed packet counter can also increment when there is complete reordering of packets so that the application might receive a slow response. But in this second case, it is a marginal increase in the packet count, which occurs due to PN mismatch sometimes only during Key expiry, and does not induce any latency.	None.
VOSS-1309	You cannot use EDM to issue ping or traceroute commands for IPv6 addresses.	Use CLI to initiate ping and traceroute.
VOSS-1310	You cannot use EDM to issue ping or traceroute commands for IPv4 addresses.	Use CLI to initiate ping and traceroute.
VOSS-1312	On the 40-gigabit ports, the small metallic fingers that surround the ports are fragile and can bend out of shape during removal and insertion of the transceivers. When the fingers are bent, they prevent the insertion of the QSFP+ transceiver.	Insert the QSFP+ carefully. If the port gets damaged, it needs to be repaired.
VOSS-1335	In an IGMP snoop environment, after dynamically downgrading the IGMP version to version 2 (v2), when you revert back to version 3 (v3), the following is observed: - The multicast traffic does not flow. - The sender entries are not learned on the local sender switch. - The Indiscard packet count gets incremented on the **show int gig error** statistics command.	Use a v3 interface as querier in a LAN segment that has snoop-enabled v2 and v3 interfaces.
VOSS-1340	From EDM, you cannot perform a Layer 2 IP ping for an IPv6 address. EDM displays the following error: `No next Hop address found for ip address provided`	Use the CLI to perform a Layer 2 IP ping.
VOSS-1344	In EDM, you cannot select multiple 40 gigabit ports or a range of ports that includes 40 gigabit ports to graph or edit. You need to select them and edit them individually.	None.
VOSS-1348	In the COM EDM Plugin command, the Layer 2 Traceroute IPv6 does not work properly and gives the error,`No Such Name`.	Use the ACLI to initiate the Layer 2 Traceroute for IPv6.
VOSS-1349	On EDM, the port LED for channelized ports only shows the status of sub-port #1, but not the rest of the sub-ports. When you remove sub-port #1, and at least one other sub-port is active and online, the LED color changes to amber, when it should be green because at least one other sub-ports is active and online. The LED only shows the status of sub-port #1.	None.
VOSS-1354	An intermittent link-flap issue can occur in the following circumstance for the copper ports. If you use a crossover cable and disable auto-negotiation, the port operates at 100 Mbps. A link flap issue can occur intermittently and link flap detect will shutdown the port.	Administratively shutdown, and then reenable the port. Use auto-negotiation. Disabling auto-negotiation on these ports is not a recommended configuration.
VOSS-1358	Traffic is forwarded to IGMP v2 SSM group, even after you delete the IGMP SSM-map entry for the group.	If you perform the delete action first, you can recreate the SSM-map record, and then disable the SSM-map record. The disabled SSM-map record causes the receiver to timeout because any subsequent membership reports that arrive and match the disabled SSM-map record are dropped. You can delete the SSM-map record after the receivers time out.
VOSS-1359	The 4 byte AS confederation identifier and peers configuration are not retained across a reboot. This problem occurs when 4 Byte AS is enabled with confederation.	Reconfigure the 4 byte AS confederation identifier and peers on the device, and reboot.
VOSS-1360	After you enable enhanced secure mode, and log in for the first time, the system prompts you to enter a new password. If you do not meet the minimum password requirements, the following system output message appears: `Password should contain a minimum of 2 upper and lowercase letters, 2 numbers and 2 special characters like !@#$%^*().  Password change aborted. Enter the New password:` The system output message does not display the actual minimum password requirements you need to meet, which are configured on your system. The output message is an example of what the requirements may need to mee The actual minimum password requirements you need to meet are configured on your system by the administrator.	None.
VOSS-1363	The switch provides an NTP log message that indicates that the NTP server did not synchronize, even though one of the NTP servers synchronized correctly and the NTP stats show that it did.	None.
VOSS-1367	The `router ospf` entry always appears in the configuration file regardless of whether OSPF is configured. This line does not perform any configuration and has no impact on the running software.	None.
VOSS-1368	When you use Telnet or SSH to connect to the switch, it can take up to 60 seconds for the login prompt to appear. However, this situation is very unlikely happen, and it does not appear in a standard normal operational network.	Do not provision DNS servers on a switch to avoid this issue altogether.
VOSS-1370	If you configure egress mirroring on NNI ports, you do not see the MAC-in-MAC header on captured packets.	Use an Rx mirror on the other end of the link to see the packets.
VOSS-1371	A large number of IPv6 VRRP VR instances on the same VLAN can cause high CPU utilization.	Do not create more than 10 IPv6 VRRP VRs on a single VLAN.
VOSS-1389	If you disable IPv6 on one RSMLT peer, the switch can intermittently display `COP-SW ERROR` and `RCIP6 ERROR` error messages. This issue has no impact.	None.

VOSS-1390	If you delete the SPBM configuration and re-configure SPBM using the same nickname but a different IS-IS system ID without rebooting, the switch displays an error message.	Reboot the switch after you delete the SPBM configuration.
VOSS-1402	You cannot use EDM to configure SSH rekey, or to enable or disable SFTP.	Use CLI to configure SSH rekey, and to enable or disable SFTP.
VOSS-1403	EDM displays the user name as Admin, even though you login using a different user name.	None.
VOSS-1404	You cannot use EDM to view the IPv6 DHCP relay counters.	Use CLI to view the IPv6 DHCP relay counters.
VOSS-1406	When you re-enable insecure protocols in the CLI SSH secure mode, the switch does not display a warning message.	None.
VOSS-1418	EDM displays the IGMP group entry that is learned on a vIST MLT port as TX-NNI.	Use CLI to view the IGMP group entry learned on a vIST MLT port.
VOSS-1428	When port-lock is enabled on the port and re-authentication on the EAP client fails, the port is removed from the RAIUS-assigned VLAN. This adds the port to the default VLAN and displays an error message. This issue has no impact.	The error message is incorrect and can be ignored.
VOSS-1431	When IS-IS is disabled on one of the vIST peer nodes with RSMLT interfaces and it has ECMP routes with the RSMLT peer as the next hop, the ECMP routes that are being replaced during the transition of the IS-IS state now will have a next hop of the local interface. This results in an error message:`COP-SW ERROR ercdProcIpRecMsg: Failed to Replace IP Records.`	Enable IS-IS on both vIST peers.
VOSS-1433	When you manually enable or disable IS-IS on 40 Gbps ports with CR4 direct attach cables (DAC), the port bounces once.	Configure IS-IS during the maintenance period. Bring the port down, configure the port and then bring the port up.
VOSS-1438	In a rare scenario in Simplified vIST configuration when vIST state is toggled immediately followed by vIST MLT ports are toggled, one of the MLT ports will go into blocking state resulting in failure to process data packets hashing to that link.	Before enabling vIST state ensure all vIST MLT ports are shut and re-enabled after vIST is enabled on the DUT.
VOSS-1440 VOSS-1441	When you configure a scaled Layer 3 VSN (24 Layer 3 VSN instances), route leaking from GRT to VRF on the local DUT does not happen. The switch displays an incorrect error message:`Only 24 L3 VSNs can be configured.`	None.
VOSS-1459 VOSS-1463 VOSS-1471	When you use Fabric Extend over IP (FE-IP) and Fabric Extend over Layer 2 VLAN (FE-VID) solution, if you change the ingress and egress .1p map, packet may not follow correct internal QoS queues for FE tunnel to FE tunnel, or FE tunnel to regular NNI traffic.	Do not change the default ingress and egress .1p maps when using Fabric Extend. With default ingress and egress .1p maps, packets follow the correct internal QoS when using the Fabric Extend feature.
VOSS-1470	You cannot use EDM to enable or disable ASG. You can only view ASG status	Use the CLI to enable or disable ASG.
VOSS-1473	If the I-SID associated with a Switched UNI or Fabric Attach port does not have a platform VLAN association and you disable Layer 2 Trusted, then the non IP traffic coming from that port does not take the port QoS and still uses the .1p priority in the packet.	None.
VOSS-1530	If you improperly close an SSH session, the session structure information does not clear and the client can stop functioning.	Disable and enable SSH.
VOSS-1560	If you apply an ipv6-out-route-map on a BGP peer to filter a particular IPv6 prefix range with a match network condition, it does not filter the full prefix range.	Configure the incoming policy to filter incoming advertised routes on BGP+ peers.
VOSS-1584	The **show debug-file all** command is missing	None.
VOSS-1585	The system does not generate a log message, either in the log file or on screen, when you run the **flight-recorder** command.	None.
VOSS-1608	If you use an ERS 4850 FA Proxy with a VOSS FA Server, a mismatch can exist in the show output for tagged management traffic. The ERS device always sends traffic as tagged. The VOSS FA Server can send both tagged and untagged. For untagged, the VOSS FA Server sends VLAN ID 4095 in the management VLAN field of the FA element TLV. The ERS device does not recognize this VLAN ID and so still reports the traffic as tagged.	There is no functional impact.
VOSS-1706	EAPOL: Untagged traffic is not honoring the port QOS for Layer 2 trusted/ Layer 3 untrusted. This issue is only seen on EAPOL enabled ports.	None.
VOSS-2014	IPV6 MLD Group is learned for Link-Local Scope Multicast Addresses. This displays additional entries in the Multicast routing tables.	None.

VOSS-2033	The following error messages appear when you use the **shutdown** and **no shutdown** commands on the MLT interface with ECMP and BGP+ enabled:
	`CP1 [01/23/16 11:10:16.474:UTC] 0x00108628 00000000 GlobalRouter RCIP6 ERROR rcIpReplaceRouteNotifyIpv6:FAIL ReplaceTunnelRec conn_id 2`
	`CP1 [12/09/15 12:27:02.203:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 201:6:604:0:0:0:0:0, mask: 96, nh: 0:0:0:0:0:0:0:0 cid 6657 owner BGP`
	`CP1 [12/09/15 12:20:30.302:UTC] 0x00108649 00000000 GlobalRouter RCIP6 ERROR ifyRpcOutDelFibEntry: del FIB of Ipv6Route failed with 0: ipv6addr: 210:6:782:0:0:0:0:0, mask: 96, nh: fe80:0:0:0:b2ad:aaff:fe55:5088 cid 2361 owner OSPF`
		Disable the alternate path.

VOSS-2036	IPsec statistics for the management interface do not increment for inESPFailures or InAHFailures.	None.
VOSS-2117	If you configure static IGMP receivers on an IGMPv3 interface and a dynamic join and leave are received on that device from the same destination VLAN or egress point, the device stops forwarding traffic to the static receiver group after the dynamic leave is processed on the device. The end result is that the IGMP static groups still exist on the device but traffic is not forwarded.	Disable and re-enable IGMP Snooping on the interface.
VOSS-2128	EAP Security and Authentication EDM tabs display additional information with internal values populated, which is not useful for the end user.	There is no functional impact. Ignore the additional information in EDM. Use the CLI command **show eapol port interface** to see port status.
VOSS-2207	You cannot configure an SMTP server hostname that begins with a digit. The system displays the following error: `Error: Invalid IP Address or Hostname for SMTP server`	None.
VOSS-2208	While performing CFM Layer 2 traceroute between two BEBs via a transit BCB the transit BCB hop is not seen, if the transit BCB has ISIS adjacencies over FE l3core with both source BEB and destination BEB.	None.
VOSS-2253	Trace level command does not list module IDs when **?** is used.	To get the list of all module IDs, type **trace level,** and then press **Enter.**
VOSS-2270	The packet internal CoS is derived incorrectly for packets sourced from a brouter port when the CoS should be derived from the port level QoS. The following list identifies scenarios that derive the internal CoS from the port QoS: - Untagged non-IP packet - Untagged IP packet, and the source port is Layer 3 untrusted - Tagged non-IP packet and the source port is Layer 2 untrusted - Tagged IP packet and the source port is Layer 3 untrusted and Layer 2 untrusted	Use the port default QoS configuration for the brouter port. The port default configuration is Layer 2 trusted and Layer 3 trusted, and under this configuration, only the first scenario in the list is still an issue. The other scenarios do not occur.
VOSS-2279	When an IPv6 neighbor device boots, the following error message occurs in the peer device console: `GlobalRouter COP-SW ERROR ercdProcIpv6RouteMsg: Failed to Delete IPV6 Record - Ip: fe80:0:0:8dc:b2ad:aaff:fe55:1b91, NextHop:0:0:0:0:0:0:0:0, mask: 128`	There is no functional impact. Port **shutdown** and **no shutdown** commands, which recovers the traffic, works even when the switch is in an error state.

VOSS-2285	When on BEB, continuously pinging IPv6 neighbor address using CLI command **ping -s**, ping packets do not drop, but instead return `no answer` messages.	Restart the ping. Avoid intensive CPU processing.
VOSS-2333	Layer 2 ping to Virtual BMAC (VBMAC) fails, if the VBMAC is reachable via Layer 2 core.	None.
VOSS-2397	If you configure a channelized port in EDM by using the **Configuration > Edit > Port > General** or **Configuration > Edit > Port > IP** or **IPv6** navigation paths, you can only see and configure the first sub-port.	In the Device Physical View, right-click the port and use the General, IP, or IPv6 sub-menu to configure all sub-ports.
VOSS-2411	On a VSP 4450GSX-DC device, the https-port info is not displayed or saved into the config.	None.
VOSS-2415	There is no option in the **Insert V3 Interface** screen of EDM to insert a VRRPv3 interface for IPv6. The two check boxes in the screen are disabled.	There is no functional impact. EDM has two menus of IP and IPv6 and this functionality available there along with other features.
VOSS-2418	When you configure and enable the SLA Mon agent, the SLA Mon server is able to discover it but the agent registration on the switch does not occur.	None.
VOSS-2422	When a BGP Neighbor times out, the following error message occurs: `CP1 [03/11/16 13:43:39.084:EST] 0x000b45f2 00000000 GlobalRouter SW ERROR ip_rtdeleteVrf: orec is NULL!`	There is no functional impact. Ignore the error message.
VOSS-2859	You cannot modify the port membership on a protocol-based VLAN using EDM after it has been created.	Use CLI to provision the port membership on the protocol-based VLAN or delete the protocol-based VLAN, and then re-create it with the correct port member setting.
VOSS-3393	When the SLA Mon agent IP is created on a CLIP interface, the switch provides the CLIP-id as the agent MAC.	There is no functional impact. Use different clip-id's to differentiate the SLA Mon agents from the SLA Mon server.
VOSS-4255	If you run IP traceroute from one end host to another end host with a DvR Leaf in between, an intermediate hop will appear as not responding because the Lea does not have an IP interface to respond. The IP traceroute to the end host will still work.	None.
VOSS-4728	If you remove and recreate an IS-IS instance on an NNI port with autonegotiation enabled in addition to vIST and R/SMLT enabled, it is possible that the NNI port will briefly become operationally down but does recover quickly. This operational change can lead to a brief traffic loss and possible reconvergence if non-ISIS protocols like OSPF or BGP are also on the NNI port.	If you need to remove and recreate an IS-IS instance on an autonegotiation enabled NNI port that also has non-ISIS traffic, do so during a maintenance window to minimize possible impact to other non-ISIS traffic.
VOSS-4840	If you run the **show fulltech** command in an SSH session, do not disable SSH on the system. Doing so can block the SSH sessior	None.
VOSS-4912	The VSP 4000 does not advertise an LLDP Management TLV.	None.
VOSS-5130	Disabling and immediately enabling IS-IS results in the following log message: `PLSBFIB ERROR: /vob/cb/nd_protocols/plsb/lib/ plsbFib.cpp(line 1558) unregisterLocalInfo() local entry does not exist. key(0xfda010000fffa40)`	There is no functional impact. Ignore the error message.
VOSS-5159 & VOSS-5160	If you use a CLIP address as the management IP address, the switch sends out 127.1.0.1 as the source IP address in both SMTP packets and TACACS+ packets.	None.
VOSS-5173	A device on a DvR VLAN cannot authenticate using RADIUS if the RADIUS server is on a DvR VLAN on a DvR Leaf using an in-band management IP address.	Place the RADIUS server in a non-DvR VLAN off a DvR Leaf or DvR Controller.
VOSS-5197	A BGP peer-group is uniquely identified by its name and not by its index. It is possible that the index that is configured for a peer-group changes between system reboots; however this has no functional impact.	None.
VOSS-5331	When you enable FHS ND inspection on a VLAN, and an IPv6 interface exists on the same VLAN, the IPv6 host client does not receive a ping response from the VLAN.	None.
VOSS-5467	If a MinM Unicast packet (destined to a virtual BMAC) is sent over an FE tunnel to a vIST paired BEB, and that destination BEB has not yet learned the customer destination MAC, then the flooded packet is not received by its vIST peer.	Ensure that you flush the customer MAC addresses in the particular VLAN or I-SID on both the vIST peer BEBs on which the FE tunnel is terminated.
VOSS-5603	In a scaled DvR environment (scaled DvR VLANs), you may see a higher CPU utilization while deleting a DvR leaf node from the DvR domain (`no dvr leaf`). The CPU utilization stays higher for several minutes on that node only and then returns to normal after deleting all the internal VLANs on the leaf node.	It is recommended to use a maintenance window when removing leaf(s) from a DvR domain.
VOSS-5627	The system does not currently restrict the number of VLANs on which you can simultaneously configure NLB and Directed Broadcast, resulting in resource hogging.	Ensure that you configure NLB and Directed Broadcast on not more that 100 VLANs simultaneously, assuming one NLB cluster for each VLAN. Also, ensure that you configure NLB on a VLAN first, and then Directed Broadcast, so as to not exhaust the NLB and Directed Broadcast shared resources. The shared resources are NLB interfaces and VLANs with Directed Broadcast enabled. The permissible limit for the shared resources is 200.
VOSS-5650	Radius assigned priority for EAP clients' traffic should be configured per MAC address and not per interface.	None.
VOSS-5982	When using Microsoft Edge to login to EDM, the first attempt fails if you use `http`.	Use `https`, another browser (Firefox or Internet Explorer), or login a second time.
VOSS-6189	When you connect to EDM using HTTPS in Microsoft Edge or Mozilla FireFox, the configured values for the RADIUS KeepAliveTimer and CFM SBM MepId d not appear.	Use Internet Explorer when using an HTTPS connection.
VOSS-6822	If the IPsec/IKE software used in the Radius server side is strongSwan, there is a compatibility issue between VOSS and strongSwan in terms of IPv6 Digicert (IKEv1/v2) authentication.	None.
VOSS-6928	On VSP 8000 Series platforms IPv4 Filters with redirect next hop action is not forwarding when a default route is not present or a VLAN common to ingress VLAN of the filtered packet is not present.	Configure a default route if possible.
VOSS-6959	On VSP 4000 platforms, if you configure an ACL with `default-action deny` and `control-packet-action deny`, it causes all packets to be dropped including packets matching ACEs with `permit` action.	Do not configure the ACL `control-packet-action deny` option on VSP 4000 platforms.
VOSS-7006	SMLT MACs are not synced correctly when you create a new VLAN on one of the vIST peers.	After you create a VLAN, enter the following command: **vlan mac-address-entry <vlan id> re-sync**
VOSS-7058	Redirect to the next-hop ACL takes longer than expected to become active afte a link down/link up scenario.	Configure a dummy static route pointing to the next-hop.
VOSS-7139	DHCPv6 Snooping is not working in an SPB network as the DHCPv6 Snooping entries are not being displayed.	Administrator should add manual entries.
VOSS-7396	After EAP is globally enabled, RADIUS Reachability is triggered. It will take a few seconds until RADIUS Response packet is received and RADIUS Server is declared reachable. NEAP authentication will not be possible in this very short period of time, as RADIUS Server reachability is not known.	If this situation occurs, for NEAP authentication to work properly, MAC should be aged and learned again. Any of the following commands should be used: - **clear mac-address-table port 1/1 address <MAC-Addr>** - **vlan action <VLAN-ID> flush** - **vlan mac-address-entry <VLAN-ID> flush**
VOSS-7439	When the RADIUS server changes the reachability state, no log message is generated. The switch sends a trap.	None.
VOSS-7443	You may detect MHMV ports in the NULL VLAN.	Manually change the VLAN membership.
VOSS-7445	If global EAPOL is disabled while NEAP clients are authenticated, error message "`CP1 [06/26/17 11:36:57.998:UTC] 0x000e8590 00000000 GlobalRouter EAP ERROR Unable to restore port 1/4 to Vlan 1`" will indicate that VLAN membership or default-vlan-id has been affected.	Manually configure VLAN membership of default-vlan-id.

VOSS-7457	The switch can experience an intermittent traffic loss after you disable a Fabric Extend tunnel.	Bounce the tunnel between the devices.
VOSS-7471	EDM does not provide a menu for valid TCP flag options when configuring an ACL/ACE filter. You cannot see what flags are supported for eq and mask.	Use CLI, which shows the valid TCP flag options.
VOSS-7472	EDM shows incorrect guidance for ACL TCP flag mask. EDM reports 0…63 as hexadecimal. CLI correctly shows <0-0x3F | 0-63> Mask value <Hex | Decimal>. This is a display issue only with no functional impact.	Use CLI to see the correct unit values.
VOSS-7495	The VSP 4000 CLI Help text shows an incorrect port for **boot config flags linerate-directed-broadcast** The Help text shows 1/48. The correct port is 1/46.	None
VOSS-7504	A port is not removed from a RADIUS assigned VLAN (RAV) when you disable EAP (RAV and egress attribute are returned by the RADIUS server). VLAN membership is not restored but traffic is still blocked for unauthenticated clients so there is no functional impact. This issue is observed when both the RAV and egress VLAN attributes are received with the same value from the RADIUS server.	1. Disable EAP. 2. Add the port to the RAV, and then remove it.
VOSS-7520	The switch can experience an intermittent traffic loss where an autolearned client behind an authenticated client (EAP/NEAP) will have its traffic filtered. This issues occurs if the following conditions are met: -NEAP authentication configured. - one MAC to learn before the main MHSA client so a NEAP RADIUS authentication must be tried. - RADIUS response for the main client to be received before the other one, even if it is learned later.	Clear the MAC address that lost connectivity.
VOSS-8560	Inband brouter RADIUS server - first RADIUS reachability request is not sent immediately after reboot.	
VOSS-8876	On bootup COP-SW ERROR lcdPimPortToMac: invalid PIM_PORT[255] sometimes observed.	This message can be safely ignored and will not impact the system. The message will be removed in a future release.
wi01208650	The console gets disconnected frequently when you enable screen trace. The error displayed is `Forced log-out after 65535 secs`	None.
wi01217871	If you attach the QSFP+ end of a passive breakout cable to a VSP 4000 or VSP 7200 Series or VSP 8000 Series switch, and the SFP+ ends of the cable to a VSP 9000 running Release 4.0.1, the output for the show pluggable-optical-modules basic command on the VSP 9000 shows an incorrect vendor name and part number. The incorrect information also appears in EDM under the Edit > Port > General menu path.	None.
-	HTTPS connection fails for CA-signed certificate with certificate inadequate type error on FF.	Ensure End-Entity, Intermediate CA and Root CA certificates are all SHA256 based and RSA2048 key signed, and Extended key usage field is set to TLS webserver Auth only for subject and root. For intermediate, it must be set with other required bits to avoid this issue. Add the root, intermediate CAs in the trust store of the browser for accessing the EDM with HTTPS.
-	VRF provisioning is restricted to 127 VRFs on VSP 4000.	None.

Limitations and expected behaviors

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

Limitations for VSP 4450GTX-HT-PWR+

Caution: The VSP 4450GTX-HT-PWR+ has operating temperature and power limitations. For safety and optimal operation of the device, ensure that the prescribed thresholds are strictly adhered to.

The following table provides a description of the limitation or behavior and the work around, if one exists.

Behavior	Description	Workaround
For high-temperature threshold	The VSP 4450GTX-HT-PWR + supports a temperature range of 0°C to 70°C. In the alpha release, power supply does not shut down at an intended over-temperature threshold of 79°C.	To prevent equipment damage, ensure that the operating temperature is within the supported temperature range of 0°C to 70°C.
For power supply wattage threshold	Software functionality to reduce the POE power budget based on the number of operational power supplies and operating temperature is not available in the Alpha SW image.	Ensure that the POE device power draw is maintained at the following when the device is at temperatures between 61°C and 70°C: • 400W — with 1 operational power supply • 832W — with 2 operational power supplies
For inoperable external USB receptacle	The VSP 4450GTX-HT-PWR+ has an empty external USB receptacle that was not available in GTS models. Software to support the use of the external USB receptacle is not yet available in the Alpha SW image. Therefore the USB port is inoperable.	No workarounds are provided with the alpha image.

General limitations and expected behaviors

The following table provides a description of the limitation or behavior.

Issue number	Description	Workaround
VOSS-7	Even when you change the LLDP mode of an interface from CDP to LLDP, if the remote side sends CDP packets, the switch accepts them and refreshes the existing CDP neighbor entry.	Disable LLDP on the interface first, and then disable CDP and re-enable LLDP.
VOSS-687	EDM and CLI show different local preference values for a BGP IPv6 route. EDM displays path attributes as received and stored in the BGP subsystem. If the attribute is from an eBGP peer, the local preference appears as zero. CLI displays path attributes associated with the route entry, which can be modified by a policy. If a route policy is not configured, the local preference shows the default value of 100.	None.
VOSS-1954	After you log in to EDM, if you try to refresh the page by clicking on the refresh button in the browser toolbar, it will redirect to a blank page. This issue happens only for the very first attempt and only in Firefox.	To refresh the page and avoid this issue, use the EDM refresh button instead of the browser refresh button. If you do encounter this issue, place your cursor in the address bar of the browser, and press **Enter.** This will return you to the EDM home page.
VOSS-2166	The IPsec security association (SA) configuration has a NULL Encryption option under the **Encrpt-algo** parameter. Currently, you must fill the **encrptKey** and **keyLength** sub-parameters to set this option; however, these values are not used for actual IPsec processing as it is a NULL encryption option. The NULL option is required to interoperate with other vendors whose IPsec solution only supports that mode for encryption.	There is no functional impact due to this configuration and it only leads to an unnecessary configuration step. No workaround required.
VOSS-2185	MAC move of the client to the new port does not automatically happen when you move a Non-EAP client authenticated on a specific port to another EAPoL or Non-EAP enabled port.	As a workaround, do one of the following: - Clear the non-EAP session on the port that the client is first authenticated on, before you move the client to another port. - Create a VLAN on the switch with the same VLAN ID as that dynamically assigned by the RADIUS server during client authentication. Use the command **vlan create <2-4059> type port-mstprstp <0–63>**. Ensure that the new port is a member of this VLAN.

wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example: Switch:1(config)#**isis apply redistribute direct vrf 2**	n/a
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.	n/a
wi01122478	Stale SNMP server community entries for different VRFs appear after reboot with no VRFs. On a node with a valid configuration file saved with more than the default vrf0, SNMP community entries for that VRF are created and maintained in a separate text file, snmp_comm.txt, on every boot. The node reads this file and updates the SNMP communities available on the node. As a result, if you boot a configuration that has no VRFs, you may still see SNMP community entries for VRFs other than the globalRouter vrf0 .	n/a
wi01137195	A static multicast group cannot be configured on a Layer 2 VLAN before enabling IGMP snooping on the VLAN. After IGMP snooping is enabled on the Layer 2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that Layer 2 VLAN.	n/a
wi01138851	Configuring and retrieving licenses using EDM is not supported.	n/a
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or Telnet session stops responding and SNMP requests time out for up to 2 minutes.	n/a
wi01142142	When a multicast sender moves from one port to another within the same BEB or from one vIST peer BEB to another, with the old port operationally up, the source port information in the output of the **show ip igmp sender** command is not updated with new sender port information.	You can perform one of the following workarounds: - On an IGMP snoop-enabled interface, you can flush IGMP sender records. **CAUTION:** Flushing sender records can cause a transient traffic loss. - On an IGMP-enabled Layer 3 interface, you can toggle the IGMP state. **CAUTION:** Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01145099	IP multicast packets with a time-to-live (TTL) equal to 1 are not switched across the SPB cloud over a Layer 2 VSN. They are dropped by the ingress BEB.	To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL greater than 1.
wi01159075	**VSP 4450GSX-PWR+**: Mirroring functionality is not working for RSTP BPDUs.	None.
wi01171670	Telnet packets get encrypted on MACsec enabled ports.	None.
wi01198872	A loss of learned MAC addresses occurs in a vIST setup beyond 10k addresses. In a SPB setup the MAC learning is limited to 13k MAC addresses, due to the limitation of the internal architecture when using SPB. Moreover, as vIST uses SPB and due to the way vIST synchronizes MAC addresses with a vIST pair, the MAC learning in a vIST setup is limited to 10K Mac addresses.	None.
wi01210217	The command **show eapol auth-stats** displays LAST-SRC-MAC for NEAP sessions incorrectly.	n/a
wi01211415	In addition to the fan modules, each power supply also has a fan. The power supply stops working if a power supply fan fails, but there is no LED or software warning that indicates this failure. Try to recover the power supply fan by resetting the switch. If the fan does not recover, then replace the faulty power supply.	n/a
wi01212034	When you disable EAPoL globally: - Traffic is allowed for static MAC configured on EAPoL enabled port without authentication. - Static MAC config added for authenticated NEAP client is lost.	n/a
wi01212247	BGP tends to have many routes. Frequent additions or deletions impact network connectivity. To prevent frequent additions or deletions, reflected routes are not withdrawn from client 2 even though they are withdrawn from client 1. Disabling route-reflection can create a black hole in the network.	Bounce the BGP protocol globally.
wi01212585	LED blinking in EDM is representative of, but not identical to, the actual LED blinking rates on the switch.	n/a
wi01213040	When you disable auto-negotiation on both sides, the 10 Gbps copper link does not come up.	n/a
wi01213066 wi01213374	EAP and NEAP are not supported on brouter ports.	n/a

wi01213336	When you configure tx mode port mirroring on T-UNI and SPBM NNI ports, unknown unicast, broadcast and multicast traffic packets that ingress these ports appear on the mirror destination port, although they do not egress the mirror source port. This is because tx mode port mirroring happens on the mirror source port before the source port squelching logic drops the packets at the egress port.	n/a
wi01219658	The command **show khi port-statistics** does not display the count for NNI ingress control packets going to the CP.	n/a
wi01219295	SPBM QOS: Egress UNI port does not follow port QOS with ingress NNI port and Mac-in-Mac incoming packets.	n/a
wi01223526	ISIS logs duplicate system ID only when the device is a direct neighbor.	n/a
wi01223557	Multicast outage occurs on LACP MLT when simplified vIST peer is rebooted.	You can perform one of the following work arounds: - Enable PIM on the edge. - Ensure that IST peers are either RP or DR but not both.
wi01224683 wi01224689	Additional link bounce may occur on 10 Gbps ports when toggling links or during cable re-insertion.	n/a
wi01224683 wi01224689	Additional link bounce may occur with 40 Gbps optical cables and 40 Gbps break-out cables, when toggling links or during cable re-insertion.	n/a
wi01229417	Origination and termination of IPv6 6-in-4 tunnel is not supported on a node with vIST enabled.	None.
wi01232578	When SSH keyboard-interactive-auth mode is enabled, the server generates the password prompt to be displayed and sends it to the SSH client. The server always sends an expanded format of the IPv6 address. When SSH keyboard-interactive-auth mode is disabled and password-auth is enabled, the client itself generates the password prompt, and it displays the IPv6 address format used in the **ssh** command.	None.
wi01234289	HTTP management of the ONA is not supported when it is deployed with a VSP 4000 Series device.	None.

SSH connections

VOSS 4.1.0.0 and VOSS 4.2.0.0 SSH server and SSH client support password authentication mode.

VOSS 4.2.1.0 changed the SSH server from password authentication to keyboard-interactive. VOSS 4.2.1.0 changed the SSH client to automatically support either password authentication or keyboard-interactive mode.

In VOSS 4.2.1.0, you cannot configure the SSH server to support password authentication. This limitation creates a backward compatibility issue for SSH clients that do not support keyboardinteractive mode, including SSH clients that are part of pre-VOSS 4.2.1.0 software releases. For example, VOSS 4.1.0.0 SSH clients, VOSS 4.2.0.0 SSH clients, and external SSH clients that only support password authentication cannot connect to VOSS 4.2.1.0 SSH servers.
This issue is addressed in software release VOSS 4.2.1.1 and later. The default mode of the SSH server starting from VOSS 4.2.1.1 is changed back to password authentication. Beginning with VOSS 5.0, you can use an ACLI command to change the SSH server mode to keyboard-interactive.
For more information about how to configure the SSH server authentication mode, see *Administering.*
Note: If you enable the ASG feature, the SSH server must use keyboard-interactive.

See the following table to understand SSH connections between specific client and server software releases.

Client software release	Server software release	Support
VOSS 4.1.0.0	VOSS 4.2.0.0	Supported
VOSS 4.1.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.2.0.0	VOSS 4.2.1.0	Not supported
VOSS 4.1.0.0	VOSS 4.2.1.1	Supported
VOSS 4.2.0.0	VOSS 4.2.1.1	Supported

SSL certificates

The switch uses the Avaya SSL certificate by default.

For more information about SSL certificates, see *Administering.*

Fabric Extend IP over ELAN/VPLS

This feature allows multiple switches running Fabric Extend IP to be directly connected over a Layer 2 broadcast domain without the need for loopback VRFs in Release 6.0 or later.

Releases earlier than 6.0 have a single next hop/ARP restriction that require the use of loopback VRFs to deploy Fabric Extend IP over ELAN/VPLS.

For more information, see *Configuring Fabric Basics and Layer 2 Services* .

Redirect next-hop filter limitations

This feature does not behave the same way on all platforms. See the appropriate section below for your platform.

VSP 4000 limitation:
The redirect next-hop filter redirects packets with a time-to-live (TTL) of 1 rather than sending them to the CPU where the CPU would generate ICMP TTL expired messages. IP Traceroute does not correctly report the hop. For more information, see Configuring QoS and ACL-Based Traffic Filtering.

VSP VSP 7200/8000 limitation:
The redirect next-hop filter does not redirect packets with a time-to-live (TTL) of 1 nor does it send them to the CPU where the CPU would generate ICMP TTL expired messages. IP Traceroute reports a timeout for the hop. For more information, see Configuring QoS and ACL-Based Traffic Filtering.

Filter limitations

The following table identifies known limitations.

Applies To	Limitation
VSP 4000 VSP 7200 VSP 8000	The switch does not support logging and PCAP with filters.
ACL limitations	
VSP 4000 VSP 7200 VSP 8000	Only Port-based ACLs are supported on egress. VLAN-based ACLs are not supported.
VSP 4000 VSP 7200 VSP 8000	IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported.
VSP 4000 VSP 7200 VSP 8000	Control packet action is not supported on IPv6 filters.
VSP 4000 VSP 7200 VSP 8000	IPv4/IPv6 VLAN based ACL filters will be applied on traffic received on all the ports if it matches VLAN ID associated with the ACL.
VSP 7200 VSP 8000	VLAN ID and VLAN_DOT1p attributes for untagged traffic are not supported for ingress/egress filters.
VSP 4000 VSP 7200 VSP 8000	Scaling numbers are reduced for IPv6 filters.
ACE limitations	
VSP 4000 VSP 7200 VSP 8000	When an ACE with action count is disabled, the statistics associated with the ACE are reset.
VSP 4000 VSP 7200 VSP 8000	Only security ACEs are supported on egress. QoS ACEs are not supported.
VSP 4000 VSP 7200 VSP 8000	ICMP type code qualifier is supported only on ingress filters.
VSP 4000 VSP 7200 VSP 8000	For port-based ACLs, you can configure VLAN qualifiers. Configuring Port qualifiers are not permitted.
VSP 4000 VSP 7200 VSP 8000	For VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.
VSP 4000 VSP 7200 VSP 8000	Egress Security/QoS filters are not supported for IPv6 filters.
VSP 4000 VSP 7200 VSP 8000	Ingress QoS filters are not supported for IPv6 filters.
VSP 4000 VSP 7200 VSP 8000	Source/Destination MAC addresses cannot be added as attributes for IPv6 filters ACEs.
VSP 4000 VSP 7200 VSP 8000	If more than 256 IPv6 filters are configured, number of IPv4 filters will get reduced.

Resolved Issues

Fixes from previous releases

VOSS 6.1.2 incorporates all fixes from prior releases, up to and including VOSS 6.1.1.0.

The following table identifies the issues resolved in Release 6.1.2.

Fixed in Release 6.1.2.

Issue number	Description
VOSS-1363	Getting NTP log message that server did not sync up even though NTP stats show it did
VOSS-5935	Added Log when duplicate IP address detected.
VOSS-6799	Boot Config Host option should be present in Boot Config tab in EDM
VOSS-7386	Disabling auto-neg 10G copper SFP+ causes operating speed display to full 10 instead of full 1000
VOSS-7397	VSP8400 platform was not supporting "match route-dest" or "match route-type".
VOSS-7514	OSPF IPv6 Prefixes with LA-bit set were not considered in processing. Thus, routes derived from these prefixes with LA-bit set were not added to the routing table.
VOSS-7805	Mibwalk fails, Error: OID not increasing, stuck on mcast streams 228.19.15.1
VOSS-7944	SMLTSYSID is Blank in EDM (Firefox/Edge) over HTTPS
VSP4000-160	RSMLT not forwarding on behalf of its peer if the ingress vlan goes down and comes back up after the IST is lost.
VSP4000-173	ISIS adjacency between two VSP4850 goes down during an ARP storm. Reduced the maximum ARPs per second allowed for VSP4800 platform.
VSP4000-182	Fixed snmp-server authentication trap control.
VSP4000-186	Problem with Solarwinds switch port mapper since upgrade from 6.0.1.2
VSP4000-187	Set Interface default Ingress peak-rate and svc-rate to 0.
VSP4000-188	Switch doesn't authenticate after the eapol re-auth timer sent via Radius is expired.
VSP4000-190	SSH Session stops working after closing the maximum allowed session on a box abruptly (by disabling the NIC or disconnecting the PC LAN cable).
VSP4000-194	Switch hangs with 'ISIS ERROR isisCheckAndSlide: TLV overflow del tlv 184' condition repeatedly
VSP7200-40	Switch Reboots Intermittently With Error Process ssio (5304) died, exit status: uncaught signal: 6
VSP8000-222	SNMP access-policy with group restrictions did not work.
VSP8000-227	After changing an OSPF area from NSSA to stub, some Type7 LSA entries were not cleaned up.
VSP8000-238	After a loop condition, peer switch local MAC is allowed to be learned on none VIST/IST port/tunnel on a different vlan.
VSP8000-245	Able to add Simplified IST MLT ports in other VLAN at the time of that VLANs creation through EDM.
VSP8000-246	Traffic loss and node sluggishness when node is hit with large ICMP packets destined for the VRRP address.
VSP8000-247	Switch provides an NTP Log Message as if the Server did not sync up even after successfull synchronization

Fixes from previous releases

VOSS 6.1 incorporates all fixes from prior releases, up to and including VOSS 5.1.1.6 and VOSS 6.0.1.2.

Issue number	Description
VOSS-1420	On an untagged ARP packet, ingressing on a Layer 2 VSN interface will honor default the port QoS. Changing port QoS value will not be honored.
VOSS-1430	When an operational SMLT is removed from a T-UNI ISID and is not added to any other VLAN or T-UNI ISID, then Spanning Tree is enabled on this SMLT interface. Spanning Tree is disabled when added to a VLAN or T-UNI ISID. This issue has no impact.
VOSS-1499	You cannot use EDM to clear Fabric Attach statistics.
VOSS-1545	The switch does not Support Fabric Extend over Layer 2 VLAN (FE-VID) logical interface configuration over an MLT interface.
VOSS-1747	On a VSP 8404 with MLT on 10G ports on an 8424XT or 8424XTQ module, multiple VLANs that have the MLT as a member of the VLAN, there is a possibility that a copy of the IP multicast traffic may not be sent on all VLANs that have a receiver on the MLT.

VOSS-2444	The output of the **show ip mroute stats [group address]** command wraps to an additional line. Four columns of data are on one line and the fifth column, `AverageSize,` wraps to an additional line. There is also an extra line feed in the column header.
VOSS-2792	Untagged (access) ports drop 9600 byte packets when the system MTU is set to 9600. (9596 byte packets are accepted.) The same packets are not dropped if ingressing on a tagged port.
VOSS-3546 VOSS-4918	VSP8404 was unresponsive after reboot.
VOSS-4114, VOSS-4116, VOSS-4972 & VOSS-5258	You cannot use FireFox 50 or newer to connect to EDM using HTTPS.
VOSS-4505	EDM-DDI tab displays all ports on system instead of single channelized ports for 40G channelized ports
VOSS-4554 & VOSS-4910	The **show ip vrrp address** command does not accurately display the value of the holddown timer remaining.
VOSS-4627	The **qos if-policer** allows configuration of **peak-rate** and **svc-rate** in the range 64 - 10000000 Kbps. However on 1G and 10G links, the effective policer rate is on the nearest 500 Kbps boundary (approximately), with a minimum policer rate of 500 Kbps. For example, configuring both peak-rate and svc-rate at 900 will result in an effective policer rate of 1000 (Kbps). This limitation does not apply to 10M and 100M negotiated links. On 10M and 100M links, the effective policer rate is close to any configured rate in the advertised range. **Note:** Due to a related issue, the minimum rate of 64 should not be used on any link.
VOSS-4724	Inter-VRF static route where next-hop address is in another VRF was not being cleaned up properly when the nexthop is removed.
VOSS-4843	CDP packet is sending prompt for Device ID and Platform.
VOSS-4856	On a DvR Leaf, you cannot configure an sFlow agent IP address to use one of the subnets that is DvR enabled or a DvR controller.
VOSS-4908	When a tunnel to a VTEP goes down on a vIST peer, the MAC address is not relearned during the first mac-aging timer interval. The VTEP continues to flood traffic ensuring there is no traffic loss. The MAC address is synchronized at the next mac-aging timer trigger.
VOSS-4935	The system will display unnecessary `rcdRadixLookup failed` messages if you perform any of the following functions simultaneously in both vIST peers: - Delete a VLAN. - Delete ISID of a VLAN. - Disable DvR. - Reboot the switch.
VOSS-4986, VOSS-5030, VOSS-5046 & VOSS-5065	You can experience MIB walk failures on the following tables: - `rcIgmpSenderTable` - `rcIsisPlsbIpUnicastFibTable` - `rcIsisPlsbMcastFibTable` - the interface table (`IF-MIB`) on a DvR leaf - `rcIpRedistributeInterVrfTable` if you use DvR and route redistribution
VOSS-5076	When using EDM, changing the VLAN configuration of a Tagged MLT composed of multiple vlans results in only the last VLAN being selected.
VOSS-5161	If you configure a DvR Leaf for in-band management (**inband-mgmt-ip**), SNMP and SYSLOG protocols send out the DvR Gateway IP as the source address of packets.
VOSS-5256	Add support for new extended range SR4 40G module AA1404006 from Finissar
VOSS-5274	CFM L2 ping/traceroute from a VOSS device towards an end device is failing when there are two ECMP paths on different SPBM vlans. Return path is selecting wrong interface.
VOSS-5413	LSDB detail sometimes incorrectly populating TLV 147 chassis mac with chassis mac associated with another nodes LDP information

VOSS-5602	Enhance SPB L3 Unicast to support overload bit for IP shortcut and IPv6 Routes.
VOSS-5670	In an SPBM environment, when you execute the traceroute command to a destination IP address learned using inter-VRF routing, the traceroute fails.
VOSS-5855	You cannot use SFTP to download the alarm log files or the output of the `show fulltech file <filename>` command.
VOSS-6377	Traffic loss between VOSS systems that have adjacent FE tunnels.
VOSS-6443	Using SPB nickname of 3.33.33 causes issues forwarding broadcast and subnet multicast packets..
VOSS-6702 & VOSS-6848	Redistributed Default route learnt via ISIS is not learnt correctly.
VOSS-6895	Reserved ISIDs for DVR have been changed to match DVR functionality in 6.1.0.0 and beyond. This requires that if any DVR node is upgraded to 6.0.1.2 or higher, all nodes running DVR need to be running 6.0.1.2 or higher. Also a consistency check was added to prevent the entire reserved ISID range greater than or equal to16,000,000 from being configured. See the following section: Upgrade considerations
VOSS-6994	DVR host entry is not relearnt after clearing ARP(manual forced clear)from controllers connected to SMLT host with continuous bi-directional traffic.
VOSS-7124	ARP learnt on one IST peer is not learnt by the other IST peer.
VSP4000-58	VSP4000 tagged ARP packets are allowed to CP for processing even if that tagged packet ingresses a port that is not a vlan member.
VSP4000-118 VSP4000-126	Watchdog coredump collection enhanced to collect more information for state of the IO
VSP4000-125	SNMP MIB walk does not return complete set of objects for dot1dBasePortTable
VSP4000-129	Netboot process fails for Apple Mac PC when DHCP-relay is configured on VSP 4450 switches running SPBM-L2VSN
VSP4000-133	Inconsistency in EDM LED Status With Physical Device LED Status
VSP4000-134	ISIS logical adjacency does not re-establish when the physical port containing the IP tunnel is bounced. In this scenario, the ISIS control packets are sent with a source mac of all zeros, leading to any intermediate L2 devices between the logical adjacency endpoints dropping the packet.
VSP4000-135	Syslog showed passwords and SNMP community strings in the clear.
VSP4000-138	Trace level 125 is defaulted to very terse. This results in a large number of PLSB/ISIS related messages in the trace file.
VSP4000-144	VSP4000 datapath support of IP Directed Broadcast using port 1/46
VSP4000-141	Duplicate Nickname connected to existing SPBM topology caused network outage. SPBM ISIS Duplicate System Id/Nickname Detection. Enhancements were made to the SPBM code in all products to help prevent network outages caused by duplicate misconfigurations of Nickname and/or System-id. - The upgraded code has algorithms to detect duplicate system-id and/or Nickname when a node is introduced into the SPB network. When duplication is detected the newly added duplicate system is isolated from the SPBM network by automatically disabling ISIS and the existing SPBM nodes perform clean-up activities for the corruption introduced. - The recovery procedure is as follows depending on which entity was duplicated: a. If both the Nickname and System-id were duplicated, then both need to be made unique and ISIS re-enabled b. If only the System-id was duplicated then the Nickname needs to be changed, the System-id needs to be made unique and ISIS re-enabled c. If only the Nickname was duplicated then: 1. Either wait 20 minutes for the LSPs from that System-id to age out of the network, make the Nickname unique and re-enable ISIS 2. Or if the node needs to be introduced into the network immediately, make the Nickname unique, change the System-id and re-enable ISIS - A CLI consistency check was introduced to prevent a virtual BMAC being erroneously configured equal to the “system-id” or the “IST peer’s system-id”. - To help administrators identify and avoid introducing a duplicate, the existing CLI command “show isis spbm nick-name” was augmented to include all system identifications that need to be unique: LSP-id /system-id, Nickname, Virtual BMAC and Host name. - Filtering by nick-name, smlt-virtual-bmac and sysid options were added to the "show isis spbm nick-name" command.

VSP4000-146	ISIS logical adjacency does not re-establish when the physical port containing the IP tunnel is bounced. In this scenario, the ISIS control packets are sent with a source mac of all zeros, leading to any intermediate L2 devices between the logical adjacency endpoints dropping the packet.
VSP4000-150	Changes to an OSPF interface metric via EDM are not reflected in the running config
VSP4000-160	If a VLAN becomes active on the local node while our IST peer is down, the RSMLT for that VLAN was being kept in holddown state for 60 secs, preventing the local node from forwarding on behalf of the downed peer during this period.
VSP4000-161	BGP adjacency fails to re-establish after a port bounces multiple times in succession.
VSP4000-163	On a VSP 4000 platform pair, users are able to set port operation to 10M-half duplex on either side and able to see the link is running at 10M-half duplex. However, when configuration save and reboot action is performed, the operation will revert back to 10M-full duplex.
VSP4000-171	FE-ONA Tunnels not coming up with VOSS 6.0.x.x.
VSP7200-14	L3VSN traffic destined for routes within a VRF context that learned any routes via ISIS accept policies may get dropped.
VSP7200-16	L3VSN traffic destined for routes within a VRF context that learned any routes via ISIS accept policies may get dropped
VSP7200-20	Following messages seen when PLSB FIB DB exceeded. “Failed to insert VpnIdBmacEntry: vpnId(0x16f) bvlan(4052) bmac(0xbb00000200) index(64385) PLSBFIB ERROR: /vob/cb/nd_protocols/plsb/lib/spbRemotePort.cpp(line 815) addBmacBVlanToVpnId() Failed to insert VpnIdBmacEntry: vpnId(0x182) bvlan(4052) bmac(0xbb00000200) index(64403)”
VSP7200-22	'SW ERROR Invalid tPORT: 81 for getLpidFromPort conversion!!' error started appearing in system logs without any functional impact
VSP7200-23	“CP1 [02/02/17 12:26:34.774:UTC] 0x00010870 00400028.1 DYNAMIC SET GlobalRouter HW WARNING Fans airflow direction mismatch” log message seen after upgrade to 6.0.1.0
VSP7200-24	For a VIST cluster with asymmetric SMLT traffic flows, MAC aging and re-ARPing logic causes extended period of traffic loss. ARPs can be seen pointing to TX-NNI for extended times and the peer has ARP pointing to the SMLT port, however no MAC is present. Fix detects the condition and re-initiates MAC learning so packets may flow correctly.
VSP8000-130	Show running config command incorrectly shows truncated display of software version information
VSP8000-144	EDM/SNMP Walk of IP DHCP Relay global table does not show up entries for VRF
VSP8000-145	Route map deletion causes crash after removing OSPF instance in VRF
VSP8000-157	VRRP Hold-down timers do not come into effect at the same time for multiple VRRP instances during failover tests.
VSP8000-162	Traps not sent on GBIC insertion and GBIC removal.
VSP8000-166	ARP table Entry maybe learned in wrong VRF context after disabling an NNI Link.
VSP8000-168	Switch may reset when deleting a VRF and a static route which has a next hop in the deleted VRF. Consistency check added to not allow VRF deletion until all routes that refer to the VRF are deleted.
VSP8000-171	VSP 8000 crash during a FTP upload
VSP8000-173	Inconsistent ARP table Entry noticed after disabling NNI Link
VSP8000-178	SPBM-ISIS Configuration Not Displayed with 'show run' Config.
VSP8000-182	MIB “ifSpeed” for 10G/40G ports returns 1,345,294,336.
VSP8000-183	Adding a new SPB node into network causes OSPF adjacencies to fail on interfaces where ISIS adjacency is okay. This is a symptom of generic SPB network node scaling limits exceeded. Increased scaling limits. See the following section: Fabric Scaling
VSP8000-184	SPBM-ISIS Configuration Not Displayed with 'show run' Config.
VSP8000-187	"AggregateOrIndividual” column in EDM is misleading. Column is removed.
VSP8000-188	If a VRRP mac is learned via an SMLT port, then moves to a different port (VIST port, another SMLT), the mac is not completely cleaned up from the original SMLT port. If the original SMLT port bounces, the VRRP mac is incorrectly re-tied to the original port, resulting in routing issues for packets sent to the VRRP mac address.

VSP8000-189	Prevent internal IP addresses (127.x.x.x) from being returned in SNMP requests for the ipNetToMediaTable.
VSP8000-195	GlobalRouter SNMP INFO Duplicate IP address message should be set as WARNING, not just INFO.
VSP8000-196	VSP 8000: Switch Erases The Route Policy Config Parameter "Match Route-Type ExternalType-2" Post The Device Reboot.
VSP8000-197	Unable to SSH to switch with error message "sshError: SSH: Server is shutting down. Please try after some time".
VSP8000-199	SCP does not work with DSA/RSA certificate authentication methods.
VSP8000-202	High CPU utilization and memory leak when responding to large ICMP echo request packets that required fragmentation.
VSP8000-208	MIB ifOperStatus is reported down on a SPB VLAN with no UNI local port assigned to that VLAN.
VSP8000-214	OSPF statically configured neighbors on NBMA circuits are lost after a reboot if the nbma circuit is configured on a brouter port.
VSP8000-215	Port statistics show zero in EDM for attributes that are not valid for 1 Gig ports.
VSP8000-218	Connectivity issue reaching L3VSN ECMP routes to a node with an ISIS system ID having the 0x020000000000 bit set (locally administered bit). Problem appears when the route using the secondary bvid is removed or replaced.

Feature licensing

The VSP 4000, VSP 7200, VSP 8200, and VSP 8400 series support a licensing model that includes Base and Premier licenses. The Base License, which is included with the purchase of the switch, enables the basic networking capabilities of the device. You can purchase Premier Licenses separately to enable advanced features on the switch.

Premier Licenses enable advanced features not available in the Base License. The following table provides information on the Premier Licenses that the switch supports.

License type	Supported features
Premier License	- Fabric Connect Layer 3 Virtual Services Networks (VSNs) - DvR - VXLAN Gateway - Greater than 24 VRFs and Layer 3 VSNs
Premier with MACsec License	- Fabric Connect Layer 3 Virtual Services Networks (VSNs) - DvR - VXLAN Gateway - Greater than 24 VRFs and Layer 3 VSNs - IEEE 802.1AE MACsec

For information about licensing including how to load a license file, see *Administering.*

Features by Release

The following table identifies the release that first introduced feature support on a hardware platform.
Each new release includes all the features from previous releases unless specifically stated otherwise.

NOTE:
- Release 4.1 was the first VOSS release. Release numbers earlier than 4.1 are releases specific to the particular platform.

	Release introduced (by platform series)			
Features	**VSP 4000**	**VSP 7200**	**VSP 8200**	**VSP 8400**
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.*	3.0	4.2.1	4.0	4.2
Address Resolution Protocol (ARP) - Proxy ARP - Static ARP For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2
All Fabric Connect services with switch cluster For more information, see the Fabric Connect documents: • *Configuring Fabric Basics and Layer 2 Services* • *Configuring Layer 3 Fabric Services* • *Configuring Fabric Multicast Services*	4.1	4.2.1	4.0	4.2
Alternative routes for IPv4 For more information, see *Configuring IPv4 Routing*.	3.1	4.2.1	4.0	4.2
Alternative routes for IPv6 For more information, see *Configuring IPv6 Routing*.	5.1	5.1	5.1	5.1
Automatic QoS For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	3.0	4.2.1	4.0	4.2
Backup Configuration	6.1.2	6.1.2	6.1.2	6.1.2
Border Gateway Protocol (BGP) for IPv4 For more information, see *Configuring BGP Services*.	3.1	4.2.1	4.1	4.2
BGP+ (BGP for IPv6) For more information, see *Configuring BGP Services*.	5.0	5.0	5.0	5.0
Bridge Protocol Data Unit (BPDU) Guard For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	6.0	6.0	6.0	6.0
CFM configuration on C-VLANs For more information, see *Troubleshooting.*	3.1	n/a	n/a	n/a
Certificate order priority **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security*.	5.1.2	5.1.2	5.1.2	5.1.2
Channelization of 40 Gbps ports For more information, see the hardware documentation and *Administering.*	n/a	4.2.1	4.2	4.2
Channelization of 100 Gbps ports For more information, see the hardware documentation and *Administering.*	n/a	n/a	n/a	n/a
Command Line Interface (CLI) For more information, see *Using CLI and EDM*.	3.0	4.2.1	4.0	4.2
Configuration and Orchestration Manager (COM) For more information, see Avaya Configuration and Orchestration Manager (COM) documentation, http://support.avaya.com/.	3.0	4.2.1	4.0	4.2
DHCPv6 Guard For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0

DHCP Snooping (IPv4) For more information, see *Configuring Security*.	6.1	6.1	6.1	6.1
DHCP Snooping (IPv6) For more information, see *Configuring Security*.	5.1	5.1	5.1	5.1
Digital certificate/PKI **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security*.	5.1.2	5.1.2	5.1.2	5.1.2
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	3.0	4.2.1	4.0	4.2
Directed Broadcast For more information, see *Configuring Security*.	5.1.1	5.1.1	5.1.1	5.1.1
Distributed Virtual Routing (DvR) controller For more information, see *Configuring IPv4 Routing*.	n/a	6.0.1	6.0.1	6.0.1
Distributed Virtual Routing (DvR) leaf For more information, see *Configuring IPv4 Routing*.	6.1	6.0.1	6.0.1	6.0.1
Domain Name Service (DNS) client (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Dot1Q MIB • dot1VlanCurrentTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1dBasePortEntry • dot1qVlanNumDelete	6.1.2	6.1.2	6.1.2	6.1.2
DNS client (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
Dynamic ARP Inspection (DAI) For more information, see *Configuring Security*.	6.1	6.1	6.1	6.1
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see *Configuring IPv4 Routing.*	3.0	4.2.1	4.0	4.2
Egress port mirror For more information, see *Troubleshooting.*	4.0	n/a	n/a	n/a
Egress port shaper For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	3.0	4.2.1	4.0	4.2
Encryption modules - The encryption modules file is included in the runtime software image file; it is not a separate file.	4.2	4.2.1	4.2	4.2
Enhanced Secure mode For more information, see *Administering.*	4.2	4.2.1	4.2	4.2
Enhanced Secure mode for JITC and non-JITC sub-modes. For more information, see *Administering.*	5.1	5.1	5.1	5.1
Enterprise Device Manager (EDM) For more information, see *Using CLI and EDM*.	3.0	4.2.1	4.0	4.2
EDM representation of physical LED status For more information, see the following documents: • *Installing Avaya Virtual Services Platform 4850GTS Series* , NN46251-300 • *Installing Avaya Virtual Services Platform 4450GTX-HTPWR+ Switch* , NN46251–304 • *Installing Avaya Virtual Services Platform 4450GSX-PWR+ Switch* , NN46251-307 • *Installing the Avaya Virtual Services Platform 7200 Series* , NN47228-302 • *Installing the Avaya Virtual Services Platform 8000 Series* , NN47227-300	3.0	4.2.1	4.2	4.2
Entity MIB - Physical Table For more information, see *Administering.*	6.0	6.0	6.0	6.0
Entity MIB enhancements and integration for the following: • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time Table	6.1.2	6.1.2	6.1.2	6.1.2
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see *Configuring IPv4 Routing*.	3.0	4.2.1	4.0	4.2

ECMP for IPv6 For more information, see the following documents: • *Configuring IPv4 Routing* • *Configuring IPv6 Routing* • *Configuring BGP Services*	5.1	5.1	5.1	5.1
ECMP support for VXLAN Gateway and Fabric Extend For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a	6.0	6.0	6.0
Equal Cost Trees (ECT) For more information, see *Configuring Fabric Basics and Layer 2 Services.*	3.0	4.2.1	4.0	4.2
E-Tree and Private VLANs For more information about E-Tree, see *Configuring Fabric Basics and Layer 2 Services.* For more information about Private VLANs, see *Configuring VLANs, Spanning Tree, and NLB.* For information about how to configure MLT and Private VLANs, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	3.0.1	4.2.1	4.1	4.2
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see *Configuring Security*.	4.1	4.2.1	4.1	4.2
EAPoL MHMA-MV For more information, see *Configuring Security*.	5.1	5.1	5.1	5.1
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN, and others For more information, see *Configuring Security*.	6.1	6.1	6.1	6.1
External BGP (EBGP) For more information, see *Configuring BGP Services.*	3.1	4.2.1	4.1	4.2
Fabric Attach For more information, see *Configuring Fabric Basics and Layer 2 Service*.	5.0	5.0	5.0	5.0
Fabric Attach Zero Touch Client Attachment For more information, see *Configuring Fabric Basics and Layer 2 Service*.	6.0	6.0	6.0	6.0
Fabric BCB mode For more information, see *Configuring Fabric Basics and Layer 2 Service*.	3.0	4.2.1	4.0	4.2
Fabric BEB mode For more information, see *Configuring Fabric Basics and Layer 2 Service*.	3.0	4.2.1	4.0	4.2
Fabric Extend For more information, see *Configuring Fabric Basics and Layer 2 Service*. All platforms require an Open Networking Adapter (ONA).	5.0	5.0	5.0	5.0
Fabric RSPAN (Mirror to I-SID) For more information, see *Troubleshooting.*	6.0 Flow-based mirroring into single I-SID only	6.0	6.0	6.0
FDB protected by port (MAC security limit-learning) For more information see *Configuring VLANs, Spanning Tree, and NLB.*	3.0	n/a	n/a	n/a
File Transfer Protocol (FTP) server and client (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
File Transfer Protocol (FTP) server and client (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
First Hop Security (FHS) For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0
- FHS - DHCPv6 Guard	5.0	5.0	5.0	5.0
- FHS - DHCP Snooping (IPv4)	6.1	6.1	6.1	6.1
- FHS - DHCP Snooping (IPv6)	5.1	5.1	5.1	5.1
- FHS - IP Source Guard (IPv4 and IPv6)	6.1	6.1	6.1	6.1
- FHS - Neighbor Discovery Inspection (IPv6)	5.1	5.1	5.1	5.1
- FHS - IPv6 Router Advertisement (RA) Guard	5.0	5.0	5.0	5.0
Flight Recorder for system health monitoring For more information, see *Troubleshooting.*	3.0	4.2.1	4.0	4.2
Gratuitous ARP filtering For more information, see *Configuring IPv4 Routing.*	4.2	4.2.1	4.2	4.2

High Availability For more information, see *Administering.*	n/a	n/a	n/a	n/a
IEEE 802.1ag Connectivity Fault Management (CFM): - Layer 2 Ping - TraceRoute - TraceTree For more information, see *Configuring Fabric Basics and Layer 2 Services.*	3.1	4.2.1	4.0	4.2
IEEE 802.3X Pause frame transmit For more information, see *Administering.*	6.0	6.0	6.0	6.0
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see *Administering.*	6.0	6.0	6.0	6.0
Ingress dual rate port policers For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	3.0	n/a	n/a	n/a
Internal BPG (IBGP) For more information, see *Configuring BGP Services.*	4.2	4.2.1	4.2	4.2
Internet Control Message Protocol (ICMP) For more information, see *Configuring IPv4 Routing.*	3.0	4.2.1	4.0	4.2
ICMP broadcast and multicast enable or disable For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing.*	5.1	5.1	5.1	5.1
Internet Group Management Protocol (IGMP), including virtualization For more information, see *Configuring IP Multicast Routing Protocols.*	3.0	4.2.1	4.0.1	4.2
Internet Key Exchange (IKE) v2 **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security*.	5.1.2	5.1.2	5.1.2	5.1.2
Inter-VSN routing For more information, see *Configuring Layer 3 Fabric Services.*	3.0	4.2.1	4.0	4.2
IP Multicast over Fabric Connect For more information, see *Configuring Fabric Multicast Services.*	3.1	4.2.1	4.1	4.2
IP route policies For more information, see *Configuring IPv4 Routing.*	3.0	4.2.1	4.0	4.2
IP Shortcut routing including ECMP For more information, see *Configuring Layer 3 Fabric Services*.	3.0	4.2.1	4.0	4.2
IP Source Guard (IPv4 and IPv6) For more information, see *Configuring Security*.	6.1	6.1	6.1	6.1
IP Source Routing enable or disable For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing.*	5.1	5.1	5.1	5.1
IPsec for the Out-of-band management port (IPv4) For more information, see *Configuring Security.*	4.2	4.2.1	4.2	4.2
IPsec for the Out-of-band management port (IPv6) For more information, see *Configuring Security.*	6.0	6.0	6.0	6.0
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see *Configuring IPv6 Routing*.	4.1	4.2.1	4.1	4.2
IPv6 ACL filters For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	4.1	4.2.1	4.1	4.2
IPv6 inter-VSN routing For more information, see *Configuring Layer 3 Fabric Services*.	4.1	4.2.1	4.1	4.2
IPv6 mode flag (boot config flags ipv6-mode) For more information, see *Configuring IPv6 Routing*.	n/a	4.2.1	4.1	4.2
IPv6 Router Advertisement (RA) Guard For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0
IPv6 Shortcut routing For more information, see *Configuring Layer 3 Fabric Services*.	4.1	4.2.1	4.1	4.2

IS-IS accept policies For more information, see *Configuring Layer 3 Fabric Services* .	4.1	4.2.1	4.1	4.2
Key Health Indicator (KHI) For more information, see *Monitoring Performance.*	3.0	4.2.1	4.0	4.2
Layer 2 video surveillance install script For more information, see *Configuring Fabric Basics and Layer 2 Services* .	6.1	6.1	6.1	6.1
Layer 2 Virtual Service Network (VSN) For more information, see *Configuring Fabric Basics and Layer 2 Services* .	3.0	4.2.1	4.0	4.2
Layer 3 switch cluster (Routed SMLT) with Simplified vIST For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	4.1	4.2.1	4.0.1	4.2
Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	4.1	4.2.1	4.0	4.2
Layer 3 video surveillance install script (formerly known as the run vms endura script) For more information, see *Configuring Layer 3 Fabric Services* .	4.1	n/a	n/a	n/a
Layer 3 VSN For more information, see *Configuring Layer 3 Fabric Services.*	3.0	4.2.1	4.1	4.2
linerate-directed-broadcast boot flag (`boot config flags linerate-directed-broadcast`) For more information, see *Administering.*	6.1	n/a	n/a	n/a
Link Layer Discovery Protocol (LLDP) For more information, see *Administering.*	6.0	6.0	6.0	6.0
Logging to a file and syslog (IPv4) For more information, see *Monitoring Performance* .	3.0	4.2.1	4.0	4.2
Logging to a file and syslog (IPv6) For more information, see *Monitoring Performance* .	4.1	4.2.1	4.1	4.2
Logon banner **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Administering* .	5.1.2	5.1.2	5.1.2	5.1.2
MACsec 2AN mode **Note:** VOSS 5.0 officially removes the replay protection commands. Do not use replay protection in earlier releases. For more information, see *Configuring Security.*	4.0	4.2.1	4.1	4.2
MACsec 4AN mode For more information, see *Configuring Security.*	6.0	6.0	6.0	6.0
Mirroring (port and flow-based) For more information, see *Troubleshooting.*	3.0	4.2.1	4.0	4.2
Multicast Listener Discovery (MLD) For more information, see *Configuring IP Multicast Routing Protocols* .	5.1	5.1	5.1	5.1
Multicast route (mroute) statistics for IPv4 and IPv6 'For more information, see *Configuring IP Multicast Routing Protocols* .	n/a	5.1	5.1	5.1
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	3.0	4.2.1	4.0	4.2
Neighbor Discovery Inspection (IPv6) For more information, see *Configuring Security* .	5.1	5.1	5.1	5.1
Network Load Balancing (NLB) - multicast operation For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a	6.0	6.0	6.0
Network Load Balancing (NLB) - unicast operation For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	n/a	4.2.1	4.0	4.2
Network Time Protocol (NTP) v3 For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
NTPv3 with SHA Authentication For more information, see *Administering.*	5.1	5.1	5.1	5.1

nni-mstp boot flag This flag has special upgrade considerations the first time you upgrade to a release that supports it. For more information, see *Administering.*	6.0	6.0	6.0	6.0
Non EAPoL MAC RADIUS authentication For more information, see *Configuring Security* .	4.2.1	4.2.1	4.2.1	4.2.1
Open Shortest Path First (OSPF) For more information, see *Configuring OSPF and RIP.*	3.1	4.2.1	4.0	4.2
P-Bridge MIB Adds support for: - dot1dExtBase Group - dot1dDeviceCapabilities - dot1dTrafficClassesEnabled - dot1dGmrpStatus - dot1dPortCapabilitiesTable	6.1.2	6.1.2	6.1.2	6.1.2
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see *Configuring IP Multicast Routing Protocols.*	4.1	4.2.1	4.0.1	4.2
PIM over IPv6 For more information, see *Configuring IP Multicast Routing Protocols.*	5.1	5.1	5.1	5.1
Power Management For more information, see *Administering.*	n/a	n/a	n/a	n/a
Power over Ethernet (PoE) For more information, see *Administering.*	3.0	n/a	n/a	n/a
PoE/PoE+ allocation using LLDP For more information, see *Administering.*	5.1	n/a	n/a	n/a
QoS Access Control Entries (ACE) For more information, see *Configuring QoS and ACL-Based Traffic Filtering* .	3.0	4.2.1	4.0	4.2
QoS ingress port rate limiter For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	n/a	4.2.1	4.0	4.2
QoS per queue rate limiting For more information, see *Configuring QoS and ACL-Based Traffic Filtering.*	5.1	5.1.1	5.1.1	5.1.1
RADIUS (IPv6) For more information, see *Configuring Security* .	4.1	4.2.1	4.1	4.2
RADIUS, community-based users (IPv4) For more information, see *Configuring Security* .	3.0	4.2.1	4.0	4.2
RADIUS secure communication using IPSec for IPv4 **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security* .	5.1.2	5.1.2	5.1.2	5.1.2
RADIUS secure communication using IPSec for IPv6 **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security* .	5.1.2	5.1.2	5.1.2	5.1.2
Remote Login (Rlogin) server/client (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Rlogin server (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see *Monitoring Performance* . **Note:** Release 5.0 and 5.1 do not support RMON1.	3.0	4.2.1	4.0	4.2
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see *Monitoring Performance* .	4.2	4.2.1	4.2	4.2
Remote Shell (RSH) server/client For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Route Information Protocol (RIP) For more information, see *Configuring OSPF and RIP.*	3.1	4.2.1	4.0	4.2
Route metric for BGP route redistribution For more information, see *Configuring BGP Services.*	6.1	6.1	6.1	6.1
RIPng For more information, see *Configuring IPv6 Routing.*	5.0	5.0	5.0	5.0
run spbm installation script For more information, see *Configuring Fabric Basics and Layer 2 Services.*	4.1	4.2.1	4.1	4.2

Russia summer time zone change For more information, see *Administering.*	4.2	4.2.1	4.2	4.2
Secure Copy (SCP) **Note:** The switch does not support the WinSCP client. For more information, see *Administering.*	3.0	5.0	4.0	5.0
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see *Configuring OSPF and RIP* .	4.2	4.2.1	4.2	4.2
Secure Shell (SSH) (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Secure Sockets Layer (SSL) certificate management For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
Security ACEs For more information, see *Configuring QoS and ACL-Based Traffic Filtering* .	3.0	4.2.1	4.0	4.2
sFlow For more information, see *Monitoring Performance* .	6.0	6.0	6.0	6.0
Simple Loop Prevention Protocol (SLPP) For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	3.0	4.2.1	4.0	4.2
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see *Monitoring Performance.*	6.0	6.0	6.0	6.0
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see *Configuring Security.*	3.0	4.2.1	4.0	4.2
SLA Mon For more information, see *Configuring the SLA Mon Agent* .	4.1	6.0	4.1	4.2
SLPP Guard For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST* .	6.1	6.1	6.1	6.1
SNMP (IPv6) For more information, see *Configuring Security* .	4.1	4.2.1	4.1	4.2
SoNMP For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Spanning Tree Protocol (STP): - Multiple STP (MSTP) - Rapid STP (RSTP) For more information, see *Configuring VLANs, Spanning Tree, and NLB.*	3.0	4.2.1	4.0	4.2
spbm-config-mode For more information, see *Configuring IP Multicast Routing Protocols.*	4.1	4.2.1	4.0.1	4.2
SPB-PIM Gateway controller node For more information, *see Configuring Fabric Multicast Services.*	6.0	6.0	6.0	6.0
SPB-PIM Gateway interface For more information, see *Configuring Fabric Multicast Services.*	6.0	6.0	6.0	6.0
SSH (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
SSH client disable For more information, see *Administering.*	6.0	6.0	6.0	6.0
SSH key size **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Administering.*	5.1.2	5.1.2	5.1.2	5.1.2
SSH rekey For more information, see *Administering.*	5.1	5.1	5.1	5.1
Static routing For more information, see *Configuring IPv4 Routing.*	3.0	4.2.1	4.0	4.2
Suspend duplicate system ID detection For more information, see *Configuring Fabric Connect Basics and Layer 2 Services.*	6.1	6.1	6.1	6.1
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	4.1	4.2.1	4.0	4.2
Switched UNI For more information, see *Configuring Fabric Basics and Layer 2 Services.*	5.0	5.0	5.0	5.0
System Logging compliance with RFC5424 and RFC3339.	6.1.2	6.1.2	6.1.2	6.1.2

TACACS+ For more information, see *Configuring Security*.	4.0	4.2.1	4.1	4.2
TACACS+ secure communication using IPSec for IPv4 **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Configuring Security*.	5.1.2	5.1.2	5.1.2	5.1.2
Telnet server and client (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
Telnet server and client (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
TLS server with secure https **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Using CLI and EDM.*	5.1.2	5.1.2	5.1.2	5.1.2
TLS client for secure syslog **NOTE:** Releases 6.0 and 6.0.1 do not support this feature. For more information, see *Troubleshooting.*	5.1.2	5.1.2	5.1.2	5.1.2
Transparent Port UNI (T-UNI) For more information, see *Configuring Fabric Basics and Layer 2 Services.*	3.1	4.2.1	4.2.1	4.2.1
Trivial File Transfer Protocol (TFTP) server and client (IPv4) For more information, see *Administering.*	3.0	4.2.1	4.0	4.2
TFTP server and client (IPv6) For more information, see *Administering.*	4.1	4.2.1	4.1	4.2
Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6) For more information, see *Configuring Security*.	5.0	5.0	5.0	5.0
Virtual Link Aggregation Control Protocol (VLACP) For more information, see *Configuring Link Aggregation, MLT, SMLT, and vIST.*	3.0	4.2.1	4.0	4.2
Virtual Router Redundancy Protocol (VRRP) For more information, see *Configuring IPv4 Routing.*	3.0	4.2.1	4.0	4.2
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.*	3.0	4.2.1	4.0	4.2
Increased VRF and Layer 3 VSN scaling For more information, see *Configuring IPv4 Routing.*	6.0	6.0	6.0	6.0
VRRPv3 for IPv4 and IPv6 For more information, see *Configuring IPv4 Routing* and *Configuring IPv6 Routing*.	5.1	5.1	5.1	5.1
VXLAN Gateway For more information, see *Configuring VLANs, Spanning Tree, and NLB*.	n/a	6.0	6.0	6.0

MIB changes in this release

The following tables identify when MIB objects are first deprecated, added, or made obsolete.

Deprecated MIBs
New MIBs
Obsolete MIBs

Deprecated MIBs

Object Name	Object OID	Deprecated in Release
rcVlanIpsecEnable	1.3.6.1.4.1.2272.1.3.2.1.64	6.1
rcPortIpsecEnable	1.3.6.1.4.1.2272.1.4.10.1.1.113	6.1

New MIBs

Object Name	Object OID	New in Release
rcIkeProfileTable	1.3.6.1.4.1.2272.1.86.1	6.1
rcIkeProfileEntry	1.3.6.1.4.1.2272.1.86.1.1	6.1
rcIkeProfileName	1.3.6.1.4.1.2272.1.86.1.1.1	6.1
rcIkeProfileHashAlgorithm	1.3.6.1.4.1.2272.1.86.1.1.2	6.1
rcIkeProfileEncryptionAlgorithm	1.3.6.1.4.1.2272.1.86.1.1.3	6.1
rcIkeProfileEncryptKeyLen	1.3.6.1.4.1.2272.1.86.1.1.4	6.1
rcIkeProfileDHGroup	1.3.6.1.4.1.2272.1.86.1.1.5	6.1
rcIkeProfileExchangeMode	1.3.6.1.4.1.2272.1.86.1.1.6	6.1
rcIkeProfileLifetimeSeconds	1.3.6.1.4.1.2272.1.86.1.1.7	6.1
rcIkeProfileRowStatus	1.3.6.1.4.1.2272.1.86.1.1.8	6.1
rcIkePolicyTable	1.3.6.1.4.1.2272.1.86.2	6.1
rcIkePolicyEntry	1.3.6.1.4.1.2272.1.86.2.1	6.1
rcIkePolicyLocalIfIndex	1.3.6.1.4.1.2272.1.86.2.1.1	6.1
rcIkePolicyLocalAddrType	1.3.6.1.4.1.2272.1.86.2.1.2	6.1
rcIkePolicyLocalAddr	1.3.6.1.4.1.2272.1.86.2.1.3	6.1
rcIkePolicyRemoteAddrType	1.3.6.1.4.1.2272.1.86.2.1.4	6.1
rcIkePolicyRemoteAddr	1.3.6.1.4.1.2272.1.86.2.1.5	6.1
rcIkePolicyName	1.3.6.1.4.1.2272.1.86.2.1.6	6.1
rcIkePolicyProfileName	1.3.6.1.4.1.2272.1.86.2.1.7	6.1
rcIkePolicyAuthenticationMethod	1.3.6.1.4.1.2272.1.86.2.1.8	6.1
rcIkePolicyPSKValue	1.3.6.1.4.1.2272.1.86.2.1.9	6.1
rcIkePolicyDPDTimeout	1.3.6.1.4.1.2272.1.86.2.1.10	6.1
rcIkePolicyP2PFS	1.3.6.1.4.1.2272.1.86.2.1.11	6.1
rcIkePolicyP2PfsUseIkeGroup	1.3.6.1.4.1.2272.1.86.2.1.12	6.1
rcIkePolicyP2PfsDHGroup	1.3.6.1.4.1.2272.1.86.2.1.13	6.1
rcIkePolicyAdminState	1.3.6.1.4.1.2272.1.86.2.1.14	6.1
rcIkePolicyOperStatus	1.3.6.1.4.1.2272.1.86.2.1.15	6.1
rcIkePolicyRowStatus	1.3.6.1.4.1.2272.1.86.2.1.16	6.1
rcIkePolicyRevocationCheckMethod	1.3.6.1.4.1.2272.1.86.2.1.17	6.1
rcIkePolicyProfileVersion	1.3.6.1.4.1.2272.1.86.2.1.18	6.1
rcIkePolicyPeerName	1.3.6.1.4.1.2272.1.86.2.1.19	6.1
rcIkeActiveSATable	1.3.6.1.4.1.2272.1.86.4	6.1
rcIkeActiveSAEntry	1.3.6.1.4.1.2272.1.86.4.1	6.1
rcIkeActiveSAId	1.3.6.1.4.1.2272.1.86.4.1.1	6.1
rcIkeActiveSALocalIfIndex	1.3.6.1.4.1.2272.1.86.4.1.2	6.1
rcIkeActiveSALocalAddrType	1.3.6.1.4.1.2272.1.86.4.1.3	6.1
rcIkeActiveSALocalAddr	1.3.6.1.4.1.2272.1.86.4.1.4	6.1
rcIkeActiveSARemoteAddrType	1.3.6.1.4.1.2272.1.86.4.1.5	6.1
rcIkeActiveSARemoteAddr	1.3.6.1.4.1.2272.1.86.4.1.6	6.1
rcIkeActiveSAName	1.3.6.1.4.1.2272.1.86.4.1.7	6.1
rcIkeActiveSAAuthenticationMethod	1.3.6.1.4.1.2272.1.86.4.1.8	6.1
rcIkeActiveSADPDTimeout	1.3.6.1.4.1.2272.1.86.4.1.9	6.1
rcIkeActiveSAHashAlgorithm	1.3.6.1.4.1.2272.1.86.4.1.10	6.1
rcIkeActiveSAEncryptionAlgorithm	1.3.6.1.4.1.2272.1.86.4.1.11	6.1
rcIkeActiveSAEncryptKeyLen	1.3.6.1.4.1.2272.1.86.4.1.12	6.1
rcIkeActiveSADHGroup	1.3.6.1.4.1.2272.1.86.4.1.13	6.1
rcIkeActiveSAExchangeMode	1.3.6.1.4.1.2272.1.86.4.1.14	6.1
rcIkeActiveSALifetimeSeconds	1.3.6.1.4.1.2272.1.86.4.1.15	6.1
rcIkeActiveSAStatus	1.3.6.1.4.1.2272.1.86.4.1.16	6.1
rcIkeActiveSAInitiator	1.3.6.1.4.1.2272.1.86.4.1.17	6.1

rcIkeV2ProfileTable	1.3.6.1.4.1.2272.1.86.5	6.1
rcIkeV2ProfileEntry	1.3.6.1.4.1.2272.1.86.5.1	6.1
rcIkeV2ProfileName	1.3.6.1.4.1.2272.1.86.5.1.1	6.1
rcIkeV2ProfileHashAlgorithm	1.3.6.1.4.1.2272.1.86.5.1.2	6.1
rcIkeV2ProfileEncryptionAlgorithm	1.3.6.1.4.1.2272.1.86.5.1.3	6.1
rcIkeV2ProfileEncryptKeyLen	1.3.6.1.4.1.2272.1.86.5.1.4	6.1
rcIkeV2ProfileDHGroup	1.3.6.1.4.1.2272.1.86.5.1.5	6.1
rcIkeV2ProfileExchangeMode	1.3.6.1.4.1.2272.1.86.5.1.6	6.1
rcIkeV2ProfileLifetimeSeconds	1.3.6.1.4.1.2272.1.86.5.1.7	6.1
rcIkeV2ProfileIntegrityAlgorithm	1.3.6.1.4.1.2272.1.86.5.1.8	6.1
rcIkeV2ProfileRowStatus	1.3.6.1.4.1.2272.1.86.5.1.9	6.1
rcIkeV2SATable	1.3.6.1.4.1.2272.1.86.6	6.1
rcIkeV2SAEntry	1.3.6.1.4.1.2272.1.86.6.1	6.1
rcIkeV2SAId	1.3.6.1.4.1.2272.1.86.6.1.1	6.1
rcIkeV2SALocalIfIndex	1.3.6.1.4.1.2272.1.86.6.1.2	6.1
rcIkeV2SALocalAddrType	1.3.6.1.4.1.2272.1.86.6.1.3	6.1
rcIkeV2SALocalAddr	1.3.6.1.4.1.2272.1.86.6.1.4	6.1
rcIkeV2SARemoteAddrType	1.3.6.1.4.1.2272.1.86.6.1.5	6.1
rcIkeV2SARemoteAddr	1.3.6.1.4.1.2272.1.86.6.1.6	6.1
rcIkeV2SAName	1.3.6.1.4.1.2272.1.86.6.1.7	6.1
rcIkeV2SAAuthenticationMethod	1.3.6.1.4.1.2272.1.86.6.1.8	6.1
rcIkeV2SADPDTimeout	1.3.6.1.4.1.2272.1.86.6.1.9	6.1
rcIkeV2SAHashAlgorithm	1.3.6.1.4.1.2272.1.86.6.1.10	6.1
rcIkeV2SAEncryptionAlgorithm	1.3.6.1.4.1.2272.1.86.6.1.11	6.1
rcIkeV2SAEncryptKeyLen	1.3.6.1.4.1.2272.1.86.6.1.12	6.1
rcIkeV2SADHGroup	1.3.6.1.4.1.2272.1.86.6.1.13	6.1
rcIkeV2SAExchangeMode	1.3.6.1.4.1.2272.1.86.6.1.14	6.1
rcIkeV2SALifetimeSeconds	1.3.6.1.4.1.2272.1.86.6.1.15	6.1
rcIkeV2SAStatus	1.3.6.1.4.1.2272.1.86.6.1.16	6.1
rcIkeV2SAInitiator	1.3.6.1.4.1.2272.1.86.6.1.17	6.1
rcIkeV2SAIntegrityAlgorithm	1.3.6.1.4.1.2272.1.86.6.1.18	6.1
rcIpConfIpsecEnable	1.3.6.1.4.1.2272.1.8.1.1.1.32	6.1
rcWebTlsMinimumVersion	1.3.6.1.4.1.2272.1.18.31	6.1
rcWebMinimumPasswordLength	1.3.6.1.4.1.2272.1.18.32	6.1
rcIpv6InterfaceIpsecEnable	1.3.6.1.4.1.2272.1.62.1.1.2.1.30	6.1
rcSyslogHostSecureForwardingTcpPort	1.3.6.1.4.1.2272.1.22.2.1.23	6.1
rcSyslogHostSecureForwardingMode	1.3.6.1.4.1.2272.1.22.2.1.24	6.1
rcSyslogHostSecureForwardingServerCertName	1.3.6.1.4.1.2272.1.22.2.1.25	6.1
rcSyslogRootCertificateTable	1.3.6.1.4.1.2272.1.22.5	6.1
rcSyslogRootCertificateEntry	1.3.6.1.4.1.2272.1.22.5.1	6.1
rcSyslogRootCertificateFilename	1.3.6.1.4.1.2272.1.22.5.1.1	6.1
rcSyslogRootCertificateAction	1.3.6.1.4.1.2272.1.22.5.1.2	6.1
rcSyslogRootCertificateRowStatus	1.3.6.1.4.1.2272.1.22.5.1.3	6.1
rcSshAuthType	1.3.6.1.4.1.2272.1.34.1.21	6.1
rcSshEncryptionType	1.3.6.1.4.1.2272.1.34.1.22	6.1
rcSshKeyExchangeMethod	1.3.6.1.4.1.2272.1.34.1.23	6.1
rcDigitalCert	1.3.6.1.4.1.2272.1.222	6.1
rcDigitalCertMib	1.3.6.1.4.1.2272.1.222.1	6.1
rcDigitalCertNotifications	1.3.6.1.4.1.2272.1.222.1.0	6.1
rcDigitalCertObjects	1.3.6.1.4.1.2272.1.222.1.1	6.1
rcDigitalCertScalars	1.3.6.1.4.1.2272.1.222.1.1.1	6.1
rcDigitalCertSubjectCommonName	1.3.6.1.4.1.2272.1.222.1.1.1.1	6.1
rcDigitalCertSubjectEmailAddress	1.3.6.1.4.1.2272.1.222.1.1.1.2	6.1
rcDigitalCertSubjectOrganizationalUnit	1.3.6.1.4.1.2272.1.222.1.1.1.3	6.1
rcDigitalCertSubjectOrganization	1.3.6.1.4.1.2272.1.222.1.1.1.4	6.1
rcDigitalCertSubjectLocality	1.3.6.1.4.1.2272.1.222.1.1.1.5	6.1
rcDigitalCertSubjectProvince	1.3.6.1.4.1.2272.1.222.1.1.1.6	6.1
rcDigitalCertSubjectCountry	1.3.6.1.4.1.2272.1.222.1.1.1.7	6.1
rcDigitalCertInstallFile	1.3.6.1.4.1.2272.1.222.1.1.1.8	6.1
rcDigitalCertInstallFileName	1.3.6.1.4.1.2272.1.222.1.1.1.9	6.1
rcDigitalCertUninstallFile	1.3.6.1.4.1.2272.1.222.1.1.1.10	6.1
rcDigitalCertUninstallFileName	1.3.6.1.4.1.2272.1.222.1.1.1.11	6.1
rcDigitalCertGenerateCsr	1.3.6.1.4.1.2272.1.222.1.1.1.12	6.1
rcDigitalCertKeyTable	1.3.6.1.4.1.2272.1.222.1.1.2	6.1

rcDigitalCertKeyEntry	1.3.6.1.4.1.2272.1.222.1.1.2.1	6.1
rcDigitalCertKeyType	1.3.6.1.4.1.2272.1.222.1.1.2.1.1	6.1
rcDigitalCertKeySize	1.3.6.1.4.1.2272.1.222.1.1.2.1.2	6.1
rcDigitalCertKeyName	1.3.6.1.4.1.2272.1.222.1.1.2.1.3	6.1
rcDigitalCertKeyRowStatus	1.3.6.1.4.1.2272.1.222.1.1.2.1.4	6.1
rcDigitalCertCaTable	1.3.6.1.4.1.2272.1.222.1.1.3	6.1
rcDigitalCertCaEntry	1.3.6.1.4.1.2272.1.222.1.1.3.1	6.1
rcDigitalCertCaName	1.3.6.1.4.1.2272.1.222.1.1.3.1.1	6.1
rcDigitalCertCaCommonName	1.3.6.1.4.1.2272.1.222.1.1.3.1.2	6.1
rcDigitalCertCaKeyName	1.3.6.1.4.1.2272.1.222.1.1.3.1.3	6.1
rcDigitalCertCaCaUrl	1.3.6.1.4.1.2272.1.222.1.1.3.1.4	6.1
rcDigitalCertCaAction	1.3.6.1.4.1.2272.1.222.1.1.3.1.5	6.1
rcDigitalCertCaActionChallengePassword	1.3.6.1.4.1.2272.1.222.1.1.3.1.6	6.1
rcDigitalCertCaLastActionStatus	1.3.6.1.4.1.2272.1.222.1.1.3.1.7	6.1
rcDigitalCertCaLastActionFailureReason	1.3.6.1.4.1.2272.1.222.1.1.3.1.8	6.1
rcDigitalCertCaInstallRootCaFileName	1.3.6.1.4.1.2272.1.222.1.1.3.1.9	6.1
rcDigitalCertCaSubjectCertificateValidityDays	1.3.6.1.4.1.2272.1.222.1.1.3.1.10	6.1
rcDigitalCertCaUsePost	1.3.6.1.4.1.2272.1.222.1.1.3.1.11	6.1
rcDigitalCertCaRowStatus	1.3.6.1.4.1.2272.1.222.1.1.3.1.12	6.1
rcDigitalCertTable	1.3.6.1.4.1.2272.1.222.1.1.4	6.1
rcDigitalCertEntry	1.3.6.1.4.1.2272.1.222.1.1.4.1	6.1
rcDigitalCertType	1.3.6.1.4.1.2272.1.222.1.1.4.1.1	6.1
rcDigitalCertVersionNumber	1.3.6.1.4.1.2272.1.222.1.1.4.1.2	6.1
rcDigitalCertSerialNumber	1.3.6.1.4.1.2272.1.222.1.1.4.1.3	6.1
rcDigitalCertIssuerName	1.3.6.1.4.1.2272.1.222.1.1.4.1.4	6.1
rcDigitalCertValidStartPeriod	1.3.6.1.4.1.2272.1.222.1.1.4.1.5	6.1
rcDigitalCertValidEndPeriod	1.3.6.1.4.1.2272.1.222.1.1.4.1.6	6.1
rcDigitalCertCertificateSignatureAlgorithm	1.3.6.1.4.1.2272.1.222.1.1.4.1.7	6.1
rcDigitalCertCertificateSignature	1.3.6.1.4.1.2272.1.222.1.1.4.1.8	6.1
rcDigitalCertSubject	1.3.6.1.4.1.2272.1.222.1.1.4.1.9	6.1
rcDigitalCertSubjectPublicKeyAlgorithm	1.3.6.1.4.1.2272.1.222.1.1.4.1.10	6.1
rcDigitalCertSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.4.1.11	6.1
rcDigitalCertHasBasicConstraint	1.3.6.1.4.1.2272.1.222.1.1.4.1.12	6.1
rcDigitalCertHasKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.4.1.13	6.1
rcDigitalCertIsCa	1.3.6.1.4.1.2272.1.222.1.1.4.1.14	6.1
rcDigitalCertKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.4.1.15	6.1
rcDigitalCertStatus	1.3.6.1.4.1.2272.1.222.1.1.4.1.16	6.1
rcDigitalCertInstalled	1.3.6.1.4.1.2272.1.222.1.1.4.1.17	6.1
rcDigitalCertCdpUrl	1.3.6.1.4.1.2272.1.222.1.1.4.1.18	6.1
rcDigitalCertOcspUrl	1.3.6.1.4.1.2272.1.222.1.1.4.1.19	6.1
rcDigitalCertExtendedKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.4.1.20	6.1
rcDigitalCertStoreTable	1.3.6.1.4.1.2272.1.222.1.1.5	6.1
rcDigitalCertStoreEntry	1.3.6.1.4.1.2272.1.222.1.1.5.1	6.1
rcDigitalCertStoreType	1.3.6.1.4.1.2272.1.222.1.1.5.1.1	6.1
rcDigitalCertStoreCommonName	1.3.6.1.4.1.2272.1.222.1.1.5.1.2	6.1
rcDigitalCertStoreVersionNumber	1.3.6.1.4.1.2272.1.222.1.1.5.1.3	6.1
rcDigitalCertStoreSerialNumber	1.3.6.1.4.1.2272.1.222.1.1.5.1.4	6.1
rcDigitalCertStoreIssuerName	1.3.6.1.4.1.2272.1.222.1.1.5.1.5	6.1
rcDigitalCertStoreValidStartPeriod	1.3.6.1.4.1.2272.1.222.1.1.5.1.6	6.1
rcDigitalCertStoreValidEndPeriod	1.3.6.1.4.1.2272.1.222.1.1.5.1.7	6.1
rcDigitalCertStoreCertificateSignatureAlgorithm	1.3.6.1.4.1.2272.1.222.1.1.5.1.8	6.1
rcDigitalCertStoreCertificateSignature	1.3.6.1.4.1.2272.1.222.1.1.5.1.9	6.1
rcDigitalCertStoreSubject	1.3.6.1.4.1.2272.1.222.1.1.5.1.10	6.1
rcDigitalCertStoreSubjectPublicKeyAlgorithm	1.3.6.1.4.1.2272.1.222.1.1.5.1.11	6.1
rcDigitalCertStoreSubjectPublicKey	1.3.6.1.4.1.2272.1.222.1.1.5.1.12	6.1
rcDigitalCertStoreHasBasicConstraint	1.3.6.1.4.1.2272.1.222.1.1.5.1.13	6.1
rcDigitalCertStoreHasKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.5.1.14	6.1
rcDigitalCertStoreIsCa	1.3.6.1.4.1.2272.1.222.1.1.5.1.15	6.1
rcDigitalCertStoreKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.5.1.16	6.1
rcDigitalCertStoreStatus	1.3.6.1.4.1.2272.1.222.1.1.5.1.17	6.1
rcDigitalCertStoreInstalled	1.3.6.1.4.1.2272.1.222.1.1.5.1.18	6.1
rcDigitalCertStoreCdpUrl	1.3.6.1.4.1.2272.1.222.1.1.5.1.19	6.1
rcDigitalCertStoreOcspUrl	1.3.6.1.4.1.2272.1.222.1.1.5.1.20	6.1
rcDigitalCertStoreExtendedKeyUsage	1.3.6.1.4.1.2272.1.222.1.1.5.1.21	6.1

rcDigitalCertStoreCaFileName	1.3.6.1.4.1.2272.1.222.1.1.5.1.22	6.1
rcPrFilterAceRedirectNextHopVrfName	1.3.6.1.4.1.2272.1.202.1.1.2.4.1.1.36	6.1
rcRadiusSupportedVendorIds	1.3.6.1.4.1.2272.1.29.1.25	6.1
rcIsisLSPSmltBmac	1.3.6.1.4.1.2272.1.63.11.1.7	6.1
rcnDigitalCertStatusTrap	1.3.6.1.4.1.2272.1.21.0.336	6.1
rcnDvrVistPeerDomainMismatchErrorTrap	1.3.6.1.4.1.2272.1.21.0.341	6.1
rcnDvrVistPeerDomainMismatchErrorClearTrap	1.3.6.1.4.1.2272.1.21.0.342	6.1
bayStackArpInspection.mib	-	6.1
bayStackDhcpSnooping.mib	-	6.1
bayStackSourceGuard.mib	-	6.1
dot1VlanCurrentTable	1.3.6.1.2.1.17.7.1.4.2	6.1.2
dot1qVlanStaticTable	1.3.6.1.2.1.17.7.1.4.3	6.1.2
dot1qPortVlanTable	1.3.6.1.2.1.17.7.1.4.5	6.1.2
dot1dBasePortEntry	1.3.6.1.2.1.17.1.4	6.1.2
dot1qVlanNumDelete	1.3.6.1.2.1.17.7.1.4.1	6.1.2
dot1dExtBase	1.3.6.1.2.1.17.6.1.1	6.1.2
dot1dDeviceCapabilities	1.3.6.1.2.1.17.6.1.1.1	6.1.2
dot1dTrafficClassesEnabled	1.3.6.1.2.1.17.6.1.1.2	6.1.2
dot1dGmrpStatus	1.3.6.1.2.1.17.6.1.1.3	6.1.2
dot1dPortCapabilitiesTable	1.3.6.1.2.1.17.6.1.1.4	6.1.2
dot1dPortCapabilitiesEntry	1.3.6.1.2.1.17.6.1.1.4.1	6.1.2
dot1dPortCapabilities	1.3.6.1.2.1.17.6.1.1.4.1.1	6.1.2
entPhysicalIndex	1.3.6.1.2.1.47.1.1.1.1.1	6.1.2
entAliasLogicalIndexOrZero	1.3.6.1.2.1.47.1.3.2.1.1	6.1.2
entAliasMappingIdentifier	1.3.6.1.2.1.47.1.3.2.1.2	6.1.2
entPhysicalChildIndex	1.3.6.1.2.1.47.1.3.3.1.1	6.1.2
entLastChangeTime	1.3.6.1.2.1.47.1.4.1	6.1.2

Obsolete MIBs

Object Name	Object OID	Obsolete in Release
rcIsisPlsbIpUnicastFibTable	1.3.6.1.4.1.2272.1.63.12	6.1
rcIsisPlsbIpUnicastFibEntry	1.3.6.1.4.1.2272.1.63.12.1	6.1
rcIsisPlsbIpUnicastFibVrfId	1.3.6.1.4.1.2272.1.63.12.1.1	6.1
rcIsisPlsbIpUnicastFibDestinationIpAddrType	1.3.6.1.4.1.2272.1.63.12.1.2	6.1
rcIsisPlsbIpUnicastFibDestinationIpAddr	1.3.6.1.4.1.2272.1.63.12.1.3	6.1
rcIsisPlsbIpUnicastFibDestinationMask	1.3.6.1.4.1.2272.1.63.12.1.4	6.1
rcIsisPlsbIpUnicastFibNextHopBmac	1.3.6.1.4.1.2272.1.63.12.1.5	6.1
rcIsisPlsbIpUnicastFibVlan	1.3.6.1.4.1.2272.1.63.12.1.6	6.1
rcIsisPlsbIpUnicastFibIsid	1.3.6.1.4.1.2272.1.63.12.1.7	6.1
rcIsisPlsbIpUnicastFibNextHopName	1.3.6.1.4.1.2272.1.63.12.1.8	6.1
rcIsisPlsbIpUnicastFibOutgoingPort	1.3.6.1.4.1.2272.1.63.12.1.9	6.1
rcIsisPlsbIpUnicastFibPrefixCost	1.3.6.1.4.1.2272.1.63.12.1.10	6.1
rcIsisPlsbIpUnicastFibSpbmCost	1.3.6.1.4.1.2272.1.63.12.1.11	6.1