



Release Notes for XA1400 Series

Release 8.0.50 (VOSS for XA1400 Series)
9035640-02 Rev AA
August 2019

© 2019, Extreme Networks
All Rights Reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

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

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document	4
Purpose.....	4
Conventions.....	4
Text Conventions.....	4
Documentation and Training.....	8
Getting Help.....	8
Providing Feedback to Us.....	9
Chapter 2: New in this release	11
New in this Release.....	11
Filenames for this Release.....	12
Chapter 3: XA1400 Series Hardware and Software Compatibility	14
Chapter 4: Software Scaling	15
Layer 2.....	15
IP Unicast.....	15
Layer 3 Route Table Size.....	17
IP Multicast.....	17
Filters, QoS, and Security.....	17
Fabric Scaling.....	18
OAM and Diagnostics.....	18
Chapter 5: Important Notices	19
Subscription Licensing for XA1400 Series.....	19
Supported Browsers.....	21
Chapter 6: Known Issues and Restrictions	22
Known Issues and Restrictions.....	22
Filter Restrictions and Expected Behaviors.....	25
Chapter 7: Related Information	27
Features by Release.....	27
MIB Changes.....	41

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document describes important information about this release for supported VSP Operating System Software (VOSS) platforms.

This document includes the following information:

- supported hardware and software
- scaling capabilities
- known issues, including workarounds where appropriate
- known restrictions

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons



Icon	Alerts you to...
 Important:	A situation that can cause serious inconvenience.
 Note:	Important features or instructions.

Table continues...





Icon	Alerts you to...
 Tip:	Helpful tips and notices for using the product.
 Danger:	Situations that will result in severe bodily injury; up to and including death.
 Warning:	Risk of severe personal injury or critical loss of data.
 Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Notice Icons









Icon	Alerts you to...
 Important:	Key information that does not carry with it the risk of personal injury, death, system failure, service interruption, loss of data, damage to equipment, or electrostatic discharge.
 Note:	Important features or instructions.
 Tip:	Helpful tips and notices for using the product.
 Voltage:	An immediate hazard exists that, if not avoided, can result in serious personal injury or death through high voltage or electric shock.
 Danger:	An immediate hazard exists that, if not avoided, can result in minor or moderate personal injury.
 Warning:	A potential hazard exists that, if not avoided, can result in harm to hardware or equipment.
 Caution:	Practices that are not safe or are potential hazards not covered by danger or warning messages.
 Electrostatic alert:	The risk of electrostatic discharge from electrostatic-discharge sensitive (ESDS) devices. It cautions the user to observe precautions for handling ESDS devices.

Table 3: Notice Icons





Icon	Alerts you to...
 Important:	Key information that does not carry with it the risk of personal injury, death, system failure, service interruption, loss of data, damage to equipment, or electrostatic discharge.
 Note:	Important features or instructions.
 Tip:	Helpful tips and notices for using the product.
 Warning:	A potential hazard exists that, if not avoided, can result in harm to hardware or equipment.

Table continues...


Icon	Alerts you to...
 Caution:	Practices that are not safe or are potential hazards not covered by danger or warning messages.

Table 4: Text Conventions

Convention	Description
Angle brackets (< >)	<p>Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command.</p> <p>If the command syntax is <code>cfm maintenance-domain maintenance-level <0-7></code>, you can enter <code>cfm maintenance-domain maintenance-level 4</code>.</p>
Bold text	<p>Bold text indicates the GUI object name you must act upon.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Click OK. • On the Tools menu, choose Options.
Braces ({ })	<p>Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command.</p> <p>For example, if the command syntax is <code>ip address {A.B.C.D}</code>, you must enter the IP address in dotted, decimal notation.</p>
Brackets ([])	<p>Brackets ([]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command.</p> <p>For example, if the command syntax is <code>show clock [detail]</code>, you can enter either <code>show clock</code> or <code>show clock detail</code>.</p>
Ellipses (...)	<p>An ellipsis (...) indicates that you repeat the last element of the command as needed.</p> <p>For example, if the command syntax is <code>ethernet/2/1 [<parameter> <value>]...</code>, you enter <code>ethernet/2/1</code> and as many parameter-value pairs as you need.</p>
<i>Italic Text</i>	<p>Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.</p>

Table continues...

Convention	Description
Plain Courier Text	<p>Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.</p> <p>Examples:</p> <ul style="list-style-type: none"> • <code>show ip route</code> • <code>Error: Invalid command syntax</code> <code>[Failed][2013-03-22 13:37:03.303</code> <code>-04:00]</code>
Separator (>)	<p>A greater than sign (>) shows separation in menu paths.</p> <p>For example, in the Navigation tree, expand the Configuration > Edit folders.</p>
Vertical Line ()	<p>A vertical line () separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command.</p> <p>For example, if the command syntax is <code>access-policy by-mac action { allow deny }</code>, you enter either <code>access-policy by-mac action allow</code> or <code>access-policy by-mac action deny</code>, but not both.</p>

Table 5: Text Conventions

Convention	Description
Angle brackets (< >)	<p>Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command.</p> <p>If the command syntax is <code>cfm maintenance-domain maintenance-level <0-7></code>, you can enter <code>cfm maintenance-domain maintenance-level 4</code>.</p>
Bold text	<p>Bold text indicates the GUI object name you must act upon.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Click OK. • On the Tools menu, choose Options.
<i>Italic Text</i>	<p>Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.</p>

Table continues...

Convention	Description
Plain Courier Text	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: <ul style="list-style-type: none">• <code>show ip route</code>• <code>Error: Invalid command syntax [Failed][2018-09-12 13:37:03.303 -04:00]</code>
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the Configuration > Edit folders.

Documentation and Training

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

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
--------------------------------	---

The Hub A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

*** Note:**

You can modify your product selections or unsubscribe at any time.

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.

About this Document

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

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this release

New in this Release

The following sections detail what is new in VOSS Release 8.0.50. For a full list of features, see [Features by Release](#) on page 27.

XA1440 and XA1480 devices

ExtremeAccess Platform 1400 Series (XA1400 Series) are compact general-purpose hardware appliances intended for remote site or branch deployments. Designed for use with Fabric Connect VPN (FCVPN) software, the XA1400 Series enhances the value of an existing Extreme Networks automated campus deployment by expanding the reach of Fabric Connect services to remote sites while delivering a consistent and uniform experience. FCVPN software transparently extends Fabric Connect services, such as L2/L3 VSNs, over third-party provider networks, including MPLS-based WANs or the Internet. In addition to secure Fabric segmentation over the WAN, FCVPN software also supports IPsec for end-to-end traffic encryption.

Two models of the XA1400 Series are available, both are x86 based hardware appliances which provide:

- Six 1000BASE-T Gigabit Ethernet RJ45 copper ports
- Two 10 Gigabit enhanced small form-factor pluggable (SFP+) fiber ports
- Two serial console interface ports (one micro USB and one RJ45)
- Two USB 2.0 ports

The ExtremeAccess Platform 1440 (XA1440) model is intended for small site or branch applications where up to 100 Mbps aggregate WAN throughput is required. The XA1440 includes a quad core Intel x86 CPU, 8GB RAM, and 32GB SSD storage.

The ExtremeAccess Platform 1480 (XA1480) model is intended for mid-sized site or head-end appliance use cases where up to 500 Mbps aggregate WAN throughput is required. The XA1480 includes an octa core Intel x86 CPU, 8GB RAM, and 64GB SSD storage.

Fabric Connect VPN Application Software and Licensing

VOSS on the XA1400 Series platforms is licensed as a Fabric Connect VPN (FCVPN) application software. The primary difference between VOSS software on VSP switches vs XA1400 Series is the VSP platforms support ASIC based packet forwarding, and the XA1400 Series support software based packet forwarding on the x86 processor. The XA1400 Series software image supports a subset of VOSS features, for more information see [Features by Release](#) on page 27. FCVPN software is offered as a term-based subscription license. A one, three, or five year subscription license is required for each XA1400 Series hardware appliance. The FCVPN application software subscription is available in three service entitlement tiers: ExtremeWorks (EW), PartnerWorks (PW), and ExtremeWorks Premier (EWP), each includes a right-to-use license, software services, and GTAC support for the term. Two bandwidth tiers of licenses are available. A 100 Mbps connectivity

license available for both XA1440 and XA1480 models. A 500 Mbps connectivity license is available for XA1480 model. The bandwidth license tiers only affect aggregate Wide Area Network (WAN) throughput on the XA1400 Series hardware appliance.

Fabric Extend over IPsec

You can use Fabric Extend over IPsec for site-to-site connections, such as connecting remote sites to the core network. Since IPsec works at the network layer, this type of configuration is not limited or dedicated to a particular application. IPsec Tunnel mode is required to support Fabric Extend over IPsec.

Egress Tunnel Shaping

 **Note:**

DEMO FEATURE - Egress Tunnel Shaping is a demonstration feature. Demonstration features are provided for testing purposes. Demonstration features are not for use in a production environment.

Egress Tunnel Shaping is a feature used to shape traffic on a Fabric Extend (FE) tunnel. Egress Tunnel Shaping limits transmission rate by shaping the output load. Egress Tunnel Shaping differs from Port Egress Shaping. Port Egress Shaping limits transmission rate by port and by queue. Egress Tunnel Shaping operates on VXLAN virtual ports and shapes the traffic on each FE tunnel.

Filenames for this Release

 **Important:**

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 VOSS](#).

The following table provides the filenames and sizes for this release.

Table 6: Software Filenames and Sizes

Description	XA1400 Series	File size
SHA512 Checksum files	VOSS1400.8.0.50.0.sha512	1107 bytes
MD5 Checksum files	VOSS1400.8.0.50.0.md5	435 bytes
MIB - supported object names	VOSS1400.8.0.50.0_mib_sup.txt	1030166 bytes
MIB - zip file of all MIBs	VOSS1400.8.0.50.0_mib.zip	1145492 bytes
MIB - objects in the OID compile order	VOSS1400.8.0.50.0_mib.txt	7597433 bytes
Open source software notice	VOSS1400.8.0.50.0_oss-notice.html	2766416 bytes

Table continues...

Description	XA1400 Series	File size
EDM Help files	VOSS1400v8050_HELP_EDM_gzip.zip	4119378 bytes
Logs reference	VOSS1400.8.0.50.0_edoc.tar	65597440 bytes
Software image	VOSS1400.8.0.50.0.tgz	322632449 bytes

The Open Source license text for the switch is included on the product. You can access it by entering the following command in the CLI:

```
more release/w.x.y.z.GA /release/oss-notice.txt
```

where *w.x.y.z* represents a specific release number.

Chapter 3: XA1400 Series Hardware and Software Compatibility

Part number	Model number	Initial release	Supported new feature release
			8.0.50
XA1440	ExtremeAccess Platform 1440 (XA1440)	8.0.50	Y
XA1480	ExtremeAccess Platform 1480 (XA1480)	8.0.50	Y

For a list of XA1400 Series supported optics and SFP transeivers, see <https://www.extremenetworks.com/support/compatibility-matrices/vsp-components-sfp-qsfq28/>

Chapter 4: Software Scaling

This section lists software scaling capabilities for the XA1400 Series.

Layer 2

Table 7: Layer 2 Maximums

LACP aggregators	8
Layer 2 VSNs	124
MAC table size	2,000 for XA1440 4,000 for XA1480
Microsoft NLB cluster IP interfaces	N/A
MLT groups	8
MSTP instances	12
Port-based VLANs	500
Ports per LACP aggregator	8
Ports per MLT group	8
RSTP instances	1
SLPP VLANs	128
VLACP interfaces	8

IP Unicast

Table 8: IP Unicast Maximums

BGP+ peers	N/A
DHCP Relay forwarding entries (IPv4)	128
ECMP groups/paths per group	500/8

Table continues...

IP interfaces (IPv4)	500
IPv4 ARP table	2000 for XA1440 4000 for XA1480
IPv4 BGP peers	12
IPv4 CLIP interfaces	64
IPv4 RIP interfaces	200
IPv4 route policies (per VRF/per switch)	500/5,000
IPv4 static ARP entries (per VRF/per switch)	200/1,000
IPv4 static routes (per VRF/per switch)	1,000/5,000
IPv4 UDP forwarding entries	128
IPv4 VRF instances	24 including GRT
IPv6 CLIP interfaces	N/A
IPv6 Ingress ACEs (Security and QoS)	N/A
IPv6 Neighbor table	N/A
IPv6 OSPFv3 routes - GRT only	N/A
IPv6 RIPng peers	N/A
IPv6 RIPng routes	N/A
IPv6 Route Table size	N/A
IPv6 static neighbor records	N/A
IPv6 static routes	N/A
Layer 3 VSNs	23
OSPFv2 interfaces	48
OSPF v2 neighbors (adjacencies)	24
OSPF v2 areas (per VRF/per switch)	12/64
OSPF v3 areas	N/A
Routed Split Multi-LinkTrunking (RSMLT) interfaces	N/A
VRRP interfaces (IPv4)	64
VRRP interfaces with fast timers (200ms)	24
VRRP VRIDs	8
Manually configured 6-in-4 tunnels	N/A

Layer 3 Route Table Size

Table 9: Layer 3 Route Table Size Maximums

IPv4 BGP routes (control plane only)	15,488
IPv4 OSPF routes	15,488
IPv4 RIP routes	15,488
IPv4 routes	15,488
IPv4 SPB Shortcut routes	15,488

IP Multicast

Table 10: IP Multicast Maximums

IGMP interfaces	N/A
PIM interfaces (Active/Passive)	N/A
Multicast receivers/IGMP receiver entries (per switch)	N/A
Multicast senders/IGMP sender entries (per switch)	N/A
PIM-SSM static channels	N/A
Total multicast routes (S,G,V) (per switch)	N/A

*** Note:**

IPv4 Routes, IPv4 SGV sender records, IPv6 Routes and IPv6 neighbor records reside in the same shared hardware table. If records of all 4 types are present together in this shared table, then the actual numbers that can be supported might be less than the scaling numbers indicated in the above tables.

Filters, QoS, and Security

Table 11: Filters, QoS, and Security Maximums

Total ACE - Ingress	500
Total ACE - Egress	500
Total ACL - Ingress	500
Total ACL - Egress	500

Fabric Scaling

Table 12: Fabric Scaling Maximums

Number of SPB regions	1
Number of B-VIDs	2
Number of SPB adjacencies	64
SPBM enabled nodes per region (BEB + BCB)	550*
* NOTE : If there are VSP 4000 switches in the network, then the total number of SPBM enabled switches per region is reduced to 550.	
Maximum number of IP multicast S,Gs when operating as a BCB	2000
Number of BEBs this node can share services with (Layer 2 VSNs, Layer 3 VSNs)	N/A**
** NOTE : vIST clusters are counted as 3 nodes.	
Maximum number of SPB Layer 2 multicast UNI I-SIDs	N/A
Maximum number of SPB Layer 3 multicast UNI I-SIDs	N/A
Maximum number of IP multicast S,Gs when operating as a BCB	2000

OAM and Diagnostics

Table 13: OAM and Diagnostics Maximums

EDM sessions	5
FTP sessions	4
Mirrored destination ports	4
Mirrored source ports	7
Rlogin sessions	8
sFlow sampling rate	N/A
SSH sessions	8
Telnet sessions	8

Chapter 5: Important Notices

Unless specifically stated otherwise, the notices in this section apply to all XA1400 Series platforms.

Subscription Licensing for XA1400 Series

Each XA1400 Series device requires a subscription license.

Licenses are tied to the switch Base MAC address and switch model type. After you generate the license through Extreme Networks Support Portal at <https://extremeportal.force.com/ExtrLicenseLanding>, you can install the license on the switch.

*** Note:**

VOSS Release 8.0.50 or later is required to support subscription licenses generated through the Extreme Networks Support Portal.

The following sections detail the different categories of licenses supported on the XA1400 Series switch.

Factory Default Trial License

A new switch includes a 60-day Factory Default Trial License starting from the time the switch is first booted. You can configure all features (except MACsec), without restrictions and save the configuration. No license file is required.

The system generates warning messages to inform you about the time remaining in the license period. The alerts appear once every 5 days for the first 55 days, and then once daily for the last 5 days. If you reboot the switch after the 60-day period, and a valid software license is not present, the licensed features in the configuration are not loaded. You must install a valid license to enable the licensed features.

Subscription License

All subscription licenses support all VOSS features on the switch, plus software upgrades and technical support services entitlement during the license term. A one, three, or five year subscription license is required for each XA1400 Series device. Three services entitlement tiers of license are available: ExtremeWorks, PartnerWorks, and ExtremeWorks Premier.

A Subscription License is available in two bandwidth tiers of licenses: Small License and Medium License. A Small License enables up to 100 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity, and a Medium License enables up to 500 Mbps aggregate throughput Fabric Extend WAN tunneling connectivity.

License expiry notifications are sent to the console and management station every 30 days until the last 30 days of the subscription. Then every 5 days until the last 9 days of the subscription, and then daily until the Subscription License expires.

Once the Subscription License expires, you get a limited 30 day grace period. When a subscription expires, notification messages are shown as the grace period counts down. Messages are shown on the console and in the alarms database indicating that the license is expired. If the system reboots after a license expiration, the grace period immediately ends and the system does not load or support any saved configurations or software services. License expired messages continue to show on the console and in the alarms database until a valid subscription license is installed.

! Important:

The 30 day grace period is lost if the system reboots after a license expires. You must renew your Subscription License to allow the software features to continue to function.

XA1400 Series License Types and Part Numbers

The following table provides the part numbers for the various licenses the XA1400 Series supports.

Table 14: Supported licenses

Small Subscription Licenses (up to 100 Mbps)	Part number/ Order code
1 year, ExtremeWorks	FCVPN-100-EW-1Y
1 year, PartnerWorks	FCVPN-100-PW-1Y
1 year, ExtremeWorks Premier	FCVPN-100-EWP-1Y
3 years, ExtremeWorks	FCVPN-100-EW-3Y
3 years, PartnerWorks	FCVPN-100-PW-3Y
3 years, ExtremeWorks Premier	FCVPN-100-EWP-3Y
5 years, ExtremeWorks	FCVPN-100-EW-5Y
5 years, PartnerWorks	FCVPN-100-PW-5Y
5 years, ExtremeWorks Premier	FCVPN-100-EWP-5Y

Medium Subscription Licenses (up to 500 Mbps)	Part number/ Order code
1 year, ExtremeWorks	FCVPN-500-EW-1Y
1 year, PartnerWorks	FCVPN-500-PW-1Y
1 year, ExtremeWorks Premier	FCVPN-500-EWP-1Y
3 years, ExtremeWorks	FCVPN-500-EW-3Y
3 years, PartnerWorks	FCVPN-500-PW-3Y
3 years, ExtremeWorks Premier	FCVPN-500-EWP-3Y
5 years, ExtremeWorks	FCVPN-500-EW-5Y
5 years, PartnerWorks	FCVPN-500-PW-5Y
5 years, ExtremeWorks Premier	FCVPN-500-EWP-5Y

*** Note:**

500 Mbps Subscription Licenses are only supported on XA1480 devices.

Limitations on license filename size

When you dynamically load a named license file, ensure that the file name has a maximum of 42 characters *including* the .xml extension. In other words, the length of the file name must be less than or equal to 42 characters, including the extension.

Otherwise, the license file does not load successfully on system reboot.

Supported Browsers

Use the following recommended browser versions to access Enterprise Device Manager (EDM):

- Microsoft Edge 41.16299.15.0
- Microsoft Internet Explorer 11
- Mozilla Firefox 59.x
- Google Chrome 66.x

*** 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 57

Chapter 6: Known Issues and Restrictions

This section details the known issues and restrictions found in this release. Where appropriate, use the workarounds provided.

Known Issues and Restrictions

This chapter details the known issues and restrictions found in this release. Where appropriate, use the workarounds provided.

General Issues and Restrictions

Issue number	Description	Workaround
VOSS-13463	Out port statistics for MLT port interfaces are not accurate.	Use the command <code>show io nic-counters</code> to display detailed port stats and error info on XA1400 Series.
VOSS-13680	Interface error statistics display is inaccurate in certain scenarios.	Use the command <code>show io nic-counters</code> to display detailed port stats and error info on XA1400 Series.
VOSS-13681	QoS: show qos cosq-stats cpu-port command output is not supported.	Use the command <code>show io cpu-cosq-counters</code> to display detailed cosq-stats on XA1400 Series.
VOSS-13693	QoS: Traffic can egress out of the queue at a different ratio than the default configuration. After the guaranteed traffic rate is served to all egress port queues, any excess bandwidth is shared equally to all queues instead of distributing on weight assigned to each queue.	None.
VOSS-13717 VOSS-14393 VOSS-14972	Link on remote side doesn't go down after admin shut on XA1400 while using 10G DAC or a 4x10 - 40 G breakout DAC. On the XA1400 side link goes down but Link LED shows as up. Both 10G and 4x10G DAC are not fully supported because of this issue	None for DAC and breakout cables. Because of this issue, the following optical transceivers are not supported: <ul style="list-style-type: none">• AA1404036-E6

Table continues...

Issue number	Description	Workaround
		<ul style="list-style-type: none"> AA1404042-E6 C9799X4-5M
VOSS-13768	Fabric Extend tunnel flapping can occur when IPSEC is enabled with F&R with IMIX traffic. Issue is seen only on XA1440 device.	Tunnel flaps can be averted by fine tuning the ISIS hello timers.
VOSS-14104	Packets are dropped on Fabric Extend logical interface if the packet size is larger than the tunnel MTU. This scenario can occur if there are devices such as firewalls placed in front of XA1400 Series devices, which performs bracket reassembly to detect possible anomalies.	Configure the MTU on Firewall router interface to match the tunnel MTU.
VOSS-14150	CLI remote console might stop wrapping text after some usage.	Reset the CLI window or open a new remote console window.
VOSS-14494	<p>Layer 2 VSN and Layer 3 VSN UNI to NNI traffic between two Backbone Edge Bridges does not hash to different ports of a MLT network-to-network interface. MLT hashing for XA1400 devices occurs after the mac-in-mac encapsulation is done. The hash keys used are the Backbone destination and Backbone source MAC addresses (BMAC DA and BMAC SA) in the Mac-in-Mac header.</p> <p>Even for the Transit BCB case on XA 1400 devices for NNI to NNI traffic, the MLT hash keys used are the Backbone destination and Backbone source MAC addresses (BMAC DA and BMAC SA) in the Mac-in-Mac header.</p>	None.
VOSS-14515	<p>Console output errors and warnings are shown during an XA1400 Series reboot, such as:</p> <ul style="list-style-type: none"> error: no such device: ((hd0,gpt1)/EFI/BOOT)/EFI/BOOT/grub.cfg. error: file `/EFI/BOOT/grubenv' not found error: no suitable video mode found. vfiopci 0000:05:00.0: Invalid PCI ROM header signature: expecting 0xaa55, got 0xbeef [0.727012] ACPI: No IRQ available for PCI Interrupt Link [LNKS]. Try pci=noacpi or acpi=off exportfs: can't open /etc/exports for reading KCORE: WARNING can't find /boot/b/ulmage-gemini.bin. No kexec kernel will be configured. 	None. The errors or warnings are host OS or guest OS related with no functional impact and can be ignored.

Table continues...

Known Issues and Restrictions

Issue number	Description	Workaround
VOSS-14590	ISIS logical-interface displays the same egress port for different tunnels when the underlay reachability is from different port interfaces.	None.
VOSS-14592	Operation down log messages display on console for an already shutdown port. Log messages are printed whenever a shut CLI command executes even if the port was previously shutdown.	None.
VOSS-14597	Ping (originated from local CP) fails for jumbo frames on Layer 3 VSN interface.	None.
VOSS-14607	When inserting an optical transceiver into an XA1400 the destination connection flaps once before remaining up.	None.
VOSS-14616	Seeing Queue buffer usage logs when changing the logical interface source IP with 64 tunnels. When changing the source IP with 64 tunnels, seeing "GlobalRouter CPU INFO CPP: 60 percent of fbufs are in use: 0 in Tx queue,1843 in RxQueue0 0 in RxQueue1 0 in RxQueue2 0 in RxQueue3 0 in RxQueue4 0 in RxQueue5 0 in RxQueue6 0 in RxQueue7".	None.
VOSS-14639	Packets ingressing on the front panel ports with source mac as switch's local VLAN MAC are forwarded instead of being dropped.	You can create an ACL filter rule to match packets based on the source MAC and drop the packets when this condition is encountered.
VOSS-14656	Console output "ErrLog: Error Level=2 [(null)] seen during OpenVas testing. No functional impact.	None.
VOSS-14672	Recovery of Fabric Extend tunnel adjacency can be 4 to 5 minutes after changing a tunnel source IP address.	None.
VOSS-15016	SFP+ ports do not power down if 'shut' command is issued without inserting a supported optical transceiver. If you insert a non-DAC optical transceiver on an admin down port 1/5 or 1/6, the peer end link still comes up and port status and activity LED on the XA1400 is on. The root cause is port 1/5,1/6 does not power down if the 'shut' command is issued without first inserting a supported optical transceiver on that port.	You can issue a port 'no shut' and 'shut' command after you insert a supported optical transceiver to have both the local and peer end port link and LED status corrected.

Table continues...

Issue number	Description	Workaround
	<p>When an optical transceiver is inserted on a admin down port, the peer end link still comes up in the following two scenarios:</p> <ul style="list-style-type: none"> • Bootup - inserting optics with default config, when port is in admin shut state. • Run time - in link up state remove existing optics, shut the port and re-insert the optic. When a optics is inserted in above scenario, the peer end link still comes up and local side link LED glows. <p>With 10G optics the issue is seen in both scenarios. With 1G optics the issue is seen only during run time insertion of optics and not at bootup</p>	

Filter Restrictions and Expected Behaviors

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

The following list describes the expected behavior with filters:

- ACL: InVlan ACLs can match tagged or untagged traffic, with the port-default VLAN considered if the incoming packet is untagged. However, if an ACE of an InVlan ACL contains the qualifier `vlan-tag-prio`, it can be used to filter only tagged traffic and not the untagged traffic.
- ACL: The outPort ACLs cannot match on the fields that are changed in the packet during forwarding decisions. Hence, the fields (Destination MAC, Source MAC, VLAN ID, etc.), which get modified during Layer 3 routing, cannot be used to match on the new contents of these fields in the outgoing packet.
- ACL: The outPort ACLs cannot match on a destination port that is a member of an MLT. So if port 1/5 is a member of an MLT (static or via LACP), an ACE of an outPort filter with member 1/5 will not be hit.
- ACL: The outPort ACLs do not apply to mirrored ports.
- There can be a single ACE hit for a packet. Port-based ACLs have precedence over VLAN based ACLs. However, the default ACEs have a lower priority than the user ACEs.
 1. User ACE of InPort ACL
 2. User ACE of InVlan ACL
 3. Default ACE of InPort ACL
 4. Default ACE of InVlan ACL

*** Note:**

If a packet matches a user ACE in both an inPort and inVLAN ACL, the inVLAN ACL is ignored.

If a packet matches a user ACE in VLAN-based ACL and the default ACE of an inPort ACL, the user ACE in the inVLAN ACL is hit and the inPort ACL is ignored.

- ACL: The monitor actions (monitor-dst-port or monitor-dst-mlt) are not supported for outPort ACLs. They are only applicable to Ingress ACLs (InPort or InVlan). For flow-based mirroring, you can configure these monitor actions at the ACE level. ACL global mirroring action is not supported.
- ACE: When an ACE with action count is disabled, the statistics associated with the ACE are reset.
- For ACEs of port-based ACLs, you can configure VLAN qualifiers. Configuring Port qualifiers are not permitted.

For ACEs of VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.

Filters and QoS

Note the following filters:

- XA1400 Series does not support the following qualifiers in the egress direction (outPort). However, ingress support (inVlan/InPort) for these qualifiers are available.
 - `arprequest` and `arpresponse`
 - `ip-frag-flag`
 - `tcp-flags`
- The `ip-options` qualifier is not supported.

For more information, see [Configuring QoS and ACL-Based Traffic Filtering for VOSS](#).

Chapter 7: Related Information

The following section contains information related to the current release.

Features by Release

The following table identifies the release that first introduced feature support on the XA1400 Series. Each new release includes all the features from previous releases unless specifically stated otherwise.

Feature	Release
Access Control List (ACL)-based filtering: <ul style="list-style-type: none">• 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 for VOSS .	8.0.50
Address Resolution Protocol (ARP): <ul style="list-style-type: none">• Proxy ARP• Static ARP For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
Alternative routes for IPv4 For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
Alternative routes for IPv6 For more information, see Configuring IPv6 Routing for VOSS .	Not supported
Application Telemetry For more information, see Monitoring Performance for VOSS .	Not supported
Automatic QoS	8.0.50

Table continues...

Related Information

Feature	Release
For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	
Border Gateway Protocol for IPv4 (BGPv4) For more information, see Configuring BGP Services for VOSS .	8.0.50
BGP+ (BGPv4 for IPv6) For more information, see Configuring BGP Services for VOSS .	Not supported
BGPv6 For more information, see Configuring BGP Services for VOSS .	Not supported
Bridge Protocol Data Unit (BPDU) Guard For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	8.0.50
Certificate order priority For more information, see Configuring Security for VOSS .	8.0.50
CFM configuration on C-VLANs For more information, see Troubleshooting VOSS .	Not supported
Channelization of 40 Gbps ports For more information, see the hardware documentation and Administering VOSS .	Not supported
Channelization of 100 Gbps ports For more information, see the hardware documentation and Administering VOSS .	Not supported
Command Line Interface (CLI) For more information, see Configuring User Interfaces and Operating Systems for VOSS .	8.0.50
Differentiated Services (DiffServ) including Per-Hop Behavior For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	8.0.50
Digital Certificate/PKI For more information, see Configuring Security for VOSS .	8.0.50
Directed Broadcast For more information, see Configuring Security for VOSS .	Not supported
Distributed Virtual Routing (DvR) controller For more information, see Configuring IPv4 Routing for VOSS .	Not supported
Distributed Virtual Routing (DvR) leaf For more information, see Configuring IPv4 Routing for VOSS .	Not supported
Domain Name Service (DNS) client (IPv4)	8.0.50

Table continues...

Feature	Release
For more information, see Administering VOSS .	
DNS client (IPv6) For more information, see Administering VOSS .	Not supported
Dot1Q MIB <ul style="list-style-type: none"> • dot1VlanCurrentTable • dot1qVlanStaticTable • dot1qPortVlanTable • dot1dBasePortEntry • dot1qVlanNumDelete 	8.0.50
Dynamic Host Configuration Protocol (DHCP) Relay, DHCP Option 82 For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
DHCP Snooping (IPv4) For more information, see Configuring Security for VOSS .	8.0.50 (FlexUNI not supported)
DHCP Snooping (IPv6) For more information, see Configuring Security for VOSS .	Not supported
DHCPv6 Guard For more information, see Configuring Security for VOSS .	Not supported
Dynamic ARP Inspection (DAI) For more information, see Configuring Security for VOSS .	Not supported
Egress port mirror For more information, see Troubleshooting VOSS .	8.0.50
Egress port shaper For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	8.0.50
Egress Tunnel Shaping (DEMO) For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	8.0.50
Encryption modules The encryption modules file is included in the runtime software image file; it is not a separate file.	8.0.50
Enhanced Secure mode for JITC and non-JITC sub-modes. For more information, see Administering VOSS .	Not supported
EDM representation of physical LED status For more information, see XA1400 Series Switches: Hardware Installation Guide .	Not supported

Table continues...

Related Information

Feature	Release
Entity MIB enhancements and integration for the following: <ul style="list-style-type: none"> • Physical Table • Alias Mapping Table • Physical Contains Table • Last Change Time Table For more information, see Administering VOSS .	8.0.50
Equal Cost Multiple Path (ECMP) for IPv4 For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
ECMP for IPv6 For more information, see the following documents: <ul style="list-style-type: none"> • Configuring IPv4 Routing for VOSS • Configuring BGP Services for VOSS • Configuring IPv6 Routing for VOSS 	Not supported
ECMP support for VXLAN Gateway and Fabric Extend For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	8.0.50 (Fabric Extend only) Not supported for VXLAN Gateway
Equal Cost Trees (ECT) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
E-Tree and Private VLANs For more information about E-Tree, see Configuring Fabric Basics and Layer 2 Services for VOSS . For more information about Private VLANs, see Configuring VLANs, Spanning Tree, and NLB for VOSS . For information about how to configure MLT and Private VLANs, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	Not supported
Extensible Authentication Protocol (EAP) and EAP over LAN (EAPoL) For more information, see Configuring Security for VOSS .	Not supported
EAPoL MHMA-MV For more information, see Configuring Security for VOSS .	Not supported
EAPoL enhancements: Enhanced MHMV, Fail Open VLAN, Guest VLAN For more information, see Configuring Security for VOSS .	Not supported
External BGP (EBGP) For more information, see Configuring BGP Services for VOSS .	8.0.50

Table continues...

Feature	Release
Extreme Management Center backup configuration ZIP file For more information, see Extreme Management Center documentation.	8.0.50
Fabric Attach For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	Not supported
Fabric Attach Zero Touch Client Attachment For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	Not supported
Fabric BCB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
Fabric BEB mode For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
Fabric Connect services with switch cluster For more information, see the Fabric Connect documents: <ul style="list-style-type: none"> • Configuring Fabric Basics and Layer 2 Services for VOSS • Configuring Fabric Layer 3 Services for VOSS • Configuring Fabric Multicast Services for VOSS 	Not supported
Fabric Extend For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
Fabric Extend over IPsec For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
Fabric RSPAN (Mirror to I-SID) For more information, see Troubleshooting VOSS .	Not supported
File Transfer Protocol (FTP) server and client (IPv4) For more information, see Administering VOSS .	8.0.50
File Transfer Protocol (FTP) server and client (IPv6) For more information, see Administering VOSS .	Not supported
First Hop Security (FHS) For more information, see Configuring Security for VOSS .	Not supported
FHS - DHCPv6 Guard	Not supported
FHS - DHCP Snooping (IPv4)	Not supported
FHS - DHCP Snooping (IPv6)	Not supported

Table continues...

Related Information

Feature	Release
FHS - IP Source Guard (IPv4 and IPv6)	Not supported
FHS - Neighbor Discovery Inspection (IPv6)	Not supported
FHS - IPv6 Router Advertisement (RA) Guard	Not supported
Flight Recorder for system health monitoring For more information, see Troubleshooting VOSS .	8.0.50
Forgiving mode for CWDM and DWDM SFP+ transceivers For more information, see Extreme Networks Pluggable Transceivers Installation Guide .	8.0.50 (Not supported on SFP+ ports 5 and 6.)
Gratuitous ARP filtering For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
High Availability CPU (HA-CPU) for a standalone switch For more information, see Administering VOSS .	Not supported
High Availability CPU (HA-CPU) for Simplified vIST	Not supported
IEEE 802.1AG Connectivity Fault Management (CFM): <ul style="list-style-type: none"> • Layer 2 Ping • TraceRoute • TraceTree For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50 (Layer 2 TraceRoute, Layer 2 TraceTree, and Layer 2 Trace Multicast route are not supported)
IEEE 802.3X Pause frame transmit For more information, see Administering VOSS .	Not supported
Industry Standard Discovery Protocol (ISDP) (CDP compatible) For more information, see Administering VOSS .	Not supported
Ingress dual rate port policers For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	Not supported
Internal BPG (IBGP) For more information, see Configuring BGP Services for VOSS .	8.0.50
Internet Control Message Protocol (ICMP) For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
ICMP broadcast and multicast enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS .	Not supported
Internet Group Management Protocol (IGMP), including virtualization	Not supported

Table continues...

Feature	Release
For more information, see Configuring IP Multicast Routing Protocols for VOSS .	
Internet Key Exchange (IKE) v2 For more information, see Configuring Security for VOSS .	8.0.50
Inter-VSN routing For more information, see Configuring Fabric Layer 3 Services for VOSS .	8.0.50
IP Multicast over Fabric Connect For more information, see Configuring Fabric Multicast Services for VOSS .	Not supported
IP route policies For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
IP Shortcut routing including ECMP For more information, see Configuring Fabric Layer 3 Services for VOSS .	8.0.50 (IPv4 support only)
IP Source Guard (IPv4 and IPv6) For more information, see Configuring Security for VOSS .	8.0.50 (IPv4 support only)
IP Source Routing enable or disable For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS .	Not supported
IPsec for IPv6 For more information, see Configuring Security for VOSS .	Not supported
IPv6 (OSPFv3, VRRP, RSMLT, DHCP Relay, IPv4 in IPv6 tunnels) For more information, see Configuring IPv6 Routing for VOSS .	Not supported
IPv6 ACL filters For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	Not supported
IPv6 inter-VSN routing For more information, see Configuring Fabric Layer 3 Services for VOSS .	Not supported
IPv6 mode flag (<code>boot config flags ipv6-mode</code>) For more information, see Configuring IPv6 Routing for VOSS .	Not supported
IPv6 Shortcut routing For more information, see Configuring Fabric Layer 3 Services for VOSS .	Not supported
IPv6 Virtualization for the following features and functions: <ul style="list-style-type: none"> • IPv6 Interfaces and IPv6 Static Routes in VRFs and Layer 3 VSNs • ECMP and Alternative route • VRRPv3 for IPv6 • DHCP Relay 	Not supported

Table continues...

Related Information

Feature	Release
<ul style="list-style-type: none"> • IPv6 Reverse Path Forwarding • ICMP Ping and Traceroute <p>For more information, see Configuring IPv6 Routing for VOSS.</p>	
<p>IS-IS accept policies</p> <p>For more information, see Configuring Fabric Layer 3 Services for VOSS.</p>	8.0.50 (IPv4 only)
<p>IS-IS authentication with SHA-256</p> <p>For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.</p>	Not supported
<p>Key Health Indicator (KHI)</p> <p>For more information, see Monitoring Performance for VOSS.</p>	8.0.50 (Some limitations apply.)
<p>Layer 2 Video Surveillance install script</p> <p>For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.</p>	Not supported
<p>Layer 3 Video Surveillance install script (formerly known as the run vms endure script)</p> <p>For more information, see Configuring Fabric Layer 3 Services for VOSS.</p>	Not supported
<p>Layer 2 Virtual Service Network (VSN)</p> <p>For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS.</p>	8.0.50
<p>Layer 3 switch cluster (Routed SMLT) with Simplified vIST</p> <p>For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.</p>	Not supported
<p>Layer 3 switch cluster (Routed SMLT) with Virtual Inter-Switch Trunk (vIST)</p> <p>For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS.</p>	Not supported
<p>Layer 3 VSN</p> <p>For more information, see Configuring Fabric Layer 3 Services for VOSS.</p>	8.0.50
<p>linerate-directed-broadcast boot flag (<code>boot config flags linerate-directed-broadcast</code>)</p> <p>For more information, see Administering VOSS.</p>	Not supported
<p>Link Layer Discovery Protocol (LLDP)</p> <p>For more information, see Administering VOSS.</p>	8.0.50
<p>Logging to a file and syslog (IPv4)</p> <p>For more information, see Monitoring Performance for VOSS.</p>	8.0.50
<p>Logging to a file and syslog (IPv6)</p> <p>For more information, see Monitoring Performance for VOSS.</p>	Not supported

Table continues...

Feature	Release
Logon banner For more information, see Administering VOSS .	8.0.50
MAC security (MAC-layer filtering, limit learning) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	Not supported
MACsec 2AN mode For more information, see Configuring Security for VOSS .	Not supported
MACsec 4AN mode For more information, see Configuring Security for VOSS .	Not supported
Mirroring (port and flow-based) For more information, see Troubleshooting VOSS .	8.0.50
Multicast Listener Discovery (MLD) For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
Multicast route (mroute) statistics for IPv4 and IPv6 For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
MultiLink Trunking (MLT) / Link Aggregation Group (LAG) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	8.0.50
Neighbor Discovery Inspection (IPv6) For more information, see Configuring Security for VOSS .	Not supported
Network Load Balancing (NLB) - multicast operation For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	Not supported
Network Load Balancing (NLB) - unicast operation For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	Not supported
Network Time Protocol version 3 (NTPv3) For more information, see Administering VOSS .	8.0.50
nmi-mstp boot flag (<code>boot config flags nmi-mstp</code>) ! Important: This flag has special upgrade considerations the first time you upgrade to a release that supports it. For more information, see Administering VOSS .	Not supported
Non EAPoL MAC RADIUS authentication	Not supported

Table continues...

Related Information

Feature	Release
For more information, see Configuring Security for VOSS .	
Open Shortest Path First (OSPF) For more information, see Configuring OSPF and RIP for VOSS .	8.0.50
P-Bridge MIB Adds support for: <ul style="list-style-type: none"> • dot1dExtBase Group • dot1dDeviceCapabilities • dot1dTrafficClassesEnabled • dot1dGmrpStatus • dot1dPortCapabilitiesTable 	8.0.50
Protocol Independent Multicast-Sparse Mode (PIM-SM), PIM-Source Specific Mode (PIM-SSM) for IPv4 For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
PIM and PIM-SSM over IPv6 For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
Power Management For more information, see Administering VOSS .	Not supported
Power over Ethernet (PoE) For more information, see Administering VOSS .	Not supported
PoE/PoE+ allocation using LLDP For more information, see Administering VOSS .	Not supported
QoS Access Control Entries (ACE) For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	8.0.50 (Not all features are supported. Refer to the documentation for additional details.)
QoS ingress port rate limiter For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	Not supported
RADIUS (IPv6) For more information, see Configuring Security for VOSS .	Not supported
RADIUS, community-based users (IPv4) For more information, see Configuring Security for VOSS .	8.0.50 (IPv4 support only)
RADIUS secure communication using IPSec for IPv4 For more information, see Configuring Security for VOSS .	8.0.50

Table continues...

Feature	Release
RADIUS secure communication using IPSec for IPv6 For more information, see Configuring Security for VOSS .	Not supported
Remote Login (Rlogin) server/client (IPv4) For more information, see Administering VOSS .	8.0.50
Rlogin server (IPv6) For more information, see Administering VOSS .	Not supported
Remote Monitoring 1 (RMON1) for Layer 1 and Layer 2 For more information, see Monitoring Performance for VOSS .	Not supported
Remote Monitoring 2 (RMON2) for network and application layer protocols For more information, see Monitoring Performance for VOSS .	Not supported
Remote Shell (RSH) server/client For more information, see Administering VOSS .	8.0.50
Route Information Protocol (RIP) For more information, see Configuring OSPF and RIP for VOSS .	8.0.50
RIPng For more information, see Configuring IPv6 Routing for VOSS .	Not supported
run spbm installation script For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	Not supported
Secure Copy (SCP)  Note: The switch does not support the WinSCP client. For more information, see Administering VOSS .	8.0.50
Secure hash algorithm 1 (SHA-1) and SHA-2 For more information, see Configuring OSPF and RIP for VOSS .	8.0.50
Secure Shell (SSH) (IPv4) For more information, see Administering VOSS .	8.0.50
Secure Sockets Layer (SSL) certificate management For more information, see Administering VOSS .	Not supported
Security ACEs For more information, see Configuring QoS and ACL-Based Traffic Filtering for VOSS .	8.0.50 (Not all features are supported. Refer to the documentation for additional details.)
sFlow For more information, see Monitoring Performance for VOSS .	Not supported

Table continues...

Related Information

Feature	Release
sFlow collector reachability on user-created VRFs For more information, see Monitoring Performance for VOSS .	Not supported
Simple Loop Prevention Protocol (SLPP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	8.0.50 (FlexUNI not supported)
Simple Mail Transfer Protocol (SMTP) for log notification For more information, see Monitoring Performance for VOSS .	8.0.50
Simple Network Management Protocol (SNMP) v1/2/3 (IPv4) For more information, see Configuring Security for VOSS .	8.0.50
SLA Mon For more information, see Configuring the SLA Mon Agent for VOSS .	Not supported
SLPP Guard For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	8.0.50 (FlexUNI not supported)
SNMP (IPv6) For more information, see Configuring Security for VOSS .	Not supported
SoNMP For more information, see Administering VOSS .	8.0.50
Spanning Tree Protocol (STP): <ul style="list-style-type: none"> • Multiple STP (MSTP) • Rapid STP (RSTP) For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	8.0.50
spbm-config-mode (<code>boot config flags spbm-config-mode</code>) For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
SPB-PIM Gateway controller node For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
SPB-PIM Gateway interface For more information, see Configuring IP Multicast Routing Protocols for VOSS .	Not supported
SSH (IPv6) For more information, see Administering VOSS .	Not supported
SSH client disable	8.0.50

Table continues...

Feature	Release
For more information, see Administering VOSS .	
SSH key size For more information, see Administering VOSS .	Not supported
SSH rekey For more information, see Administering VOSS .	Not supported
Static routing For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
Subscription Licensing For more information, see Administering VOSS .	8.0.50
Suspend duplicate system ID detection For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	8.0.50
Switch cluster (multi-chassis LAG) -Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	Not supported
Switched UNI For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	Not supported
TACACS+ For more information, see Configuring Security for VOSS .	8.0.50
TACACS+ secure communication using IPSec for IPv4 For more information, see Configuring Security for VOSS .	8.0.50
Telnet server and client (IPv4) For more information, see Administering VOSS .	8.0.50
Telnet server and client (IPv6) For more information, see Administering VOSS .	Not supported
TLS server for secure HTTPS For more information, see Configuring User Interfaces and Operating Systems for VOSS .	8.0.50
TLS client for secure syslog For more information, see Troubleshooting VOSS .	8.0.50
Transparent Port UNI (T-UNI) For more information, see Configuring Fabric Basics and Layer 2 Services for VOSS .	Not supported
Trivial File Transfer Protocol (TFTP) server and client (IPv4)	8.0.50

Table continues...

Related Information

Feature	Release
For more information, see Administering VOSS .	
TFTP server and client (IPv6) For more information, see Administering VOSS .	Not supported
<p>Unicast Reverse Path Forwarding (URPF) checking (IPv4 and IPv6)</p> <p>* Note: Supported on IPv4 only.</p> <p>For more information, see Configuring Security for VOSS.</p>	Not supported
Virtual Inter-Switch Trunk (vIST) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	Not supported
Virtual Link Aggregation Control Protocol (VLACP) For more information, see Configuring Link Aggregation, MLT, SMLT and vIST for VOSS .	8.0.50
Virtual Router Redundancy Protocol (VRRP) For more information, see Configuring IPv4 Routing for VOSS .	8.0.50
<p>Virtualization with IPv4 Virtual Routing and Forwarding (VRF)</p> <ul style="list-style-type: none"> • ARP • DHCP Relay • Inter-VRF Routing (static, dynamic, and policy) • Local routing • OSPFv2 • RIPv1 and v2 • Route policies • Static routing • VRRP <p>For more information, see Configuring IPv4 Routing for VOSS.</p>	8.0.50
<p>Increased VRF and Layer 3 scaling</p> <p>(The VSP 8600 automatically supports the maximum number of VRFs without additional VLAN reservation.)</p> <p>For more information, see Configuring IPv4 Routing for VOSS.</p>	Not supported
VRRPv3 for IPv4 and IPv6 For more information, see Configuring IPv4 Routing for VOSS and Configuring IPv6 Routing for VOSS .	8.0.50 (IPv4 support only.)
VXLAN Gateway For more information, see Configuring VLANs, Spanning Tree, and NLB for VOSS .	Not supported

MIB Changes

Modified MIBs

Object Name	Object OID	Modification in Release 8.0.50
rcIscircuitPlsbState	1.3.6.1.4.1.2272.1.63.5.1.4	Changed default value from disable to enable
XA1400 Series:		
rcIsglobalIpTunnelMtu	1.3.6.1.4.1.2272.1.63.1.20	Changed range from 750..1950 to 0 750..1950
rcSysMTUSize	1.3.6.1.4.1.2272.1.1.55	Supports MTU frame size 9000 value 2 (instead of 9600 MTU)
rcVlanType	1.3.6.1.4.1.2272.1.3.2.1.10	Supports only byPort(1) and spbm-bvlan(11) values
rcVlanProtocolId	1.3.6.1.4.1.2272.1.3.2.1.15	Supports only none(0) value
rcPlsbGlobalEtherType	1.3.6.1.4.1.2272.1.78.1.4	Supports only default value (0x8100)
rcIcidServiceType	1.3.6.1.4.1.2272.1.87.2.1.2	Supports only I2vsn(4) value
rcPrFilterAclType	1.3.6.1.4.1.2272.1.202.1.1.2.3.1.1.4	Supports only inVlan(1), inPort(3) and outPort(4) values
rcIscLogicalInterfaceType	1.3.6.1.4.1.2272.1.63.26.1.3	Supports only ip(2) value
rc2kCpuSerialPortBaudRate	1.3.6.1.4.1.2272.1.100.3.1.6	Supports only baud115200 value

New MIBs

Object Name	Object OID
rcLicenseDisplayType	1.3.6.1.4.1.2272.1.56.13
rcIscLogicalInterfaceIpssecEnable	1.3.6.1.4.1.2272.1.63.26.1.14

Table continues...

Related Information

Object Name	Object OID
rclsisLogicalInterfaceAuthenticationKey	1.3.6.1.4.1.2272.1.63.26.1.15
rclsisLogicalInterfaceShapingRate	1.3.6.1.4.1.2272.1.63.26.1.16