New Features for VOSS 6.1.2

Release 6.1.2
NN47227-404
Issue 01.01
December 2017

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License type(s)

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

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part,

including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Security Vulnerabilities

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

Downloading Documentation

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

Contact Extreme Networks Support

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

Contact Avaya Support

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

Trademarks

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

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

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

Contents

Chapter 1: Preface

Purpose

This document provides information on the differences in feature support between VOSS 6.1.0.0 and VOSS 6.1.2.0.

VOSS 6.1.2.0 is supported on the following platforms:

- VSP 4000 Series
- VSP 7200 Series
- VSP 8000 Series, which includes VSP 8200 and VSP 8400

Training

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

Providing Feedback to Us

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

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

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

Getting Help

Product purchased from Extreme Networks

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

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

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

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

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

Product purchased from Avaya

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

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

Extreme Networks Documentation

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

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

Open Source Declarations

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

Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

About this task

You can modify your product selections at any time.

Procedure

1. In an Internet browser, go to http://www.extremenetworks.com/support/service-notification-form/ .
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

Chapter 2: Release Overview

Release 6.1.2 software has been rebranded for Extreme which affects logs, CLI, and EDM. Release 6.1.2 also introduces new features that are required for integration with Extreme Management Center (XMC).

For more information on XMC refer to the *Extreme Management Center User Guide* at http://www.extremenetworks.com/support/documentation/.

Important:

Extreme Management Center (XMC) was previously referred to as Extreme Management Center (EMC).

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.

Chapter 3: MIB Enhancements

Release 6.1.2 introduces the following MIBs and MIB enhancements.

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 Extreme Management Center (XMC).

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

Release 6.1.2 adds support for the P-Bridge MIB Table.

- dot1dExtBase Group
  - dot1dDeviceCapabilities
  - dot1dTrafficClassesEnabled
  - dot1dGmrpStatus
  - dot1dPortCapabilitiesTable

Administration Impacts

The following section details new administration tasks for the Entity MIB enhancements in Release 6.1.2.

Viewing Entity Aliases

About this task

Perform this procedure to view the entity aliases on the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Entity**.
3. Click the **Alias** tab.

Alias Field Descriptions

Use the following table to use the Alias tab.

Name	Description
Index	The index of the entry

Table continues…

Name	Description
LogicalIndexOrZero	The index of the entry. The value of this object identifies the logical entity that defines the naming scope for the associated instance of the Mapping Identifier object. This is always 0.
MappingIdentifier	The value of this object identifies a particular conceptual row associated with the indicated Physical Index and Logical Index pair. Because only physical ports are modeled in this table, only entries that represent interfaces or ports are allowed. If an ifEntry exists on behalf of a particular physical port, then this object should identify the associated ifEntry. This is the OID of ifIndex.Port.

Viewing Entity Child Indexes

About this task

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Entity**.
3. Click the **Child Index** tab.

Child Index field descriptions

Use the following table to use the Child Index tab.

Name	Description
Index	Indicates the index of the entry.
ChildIndex	The index of the entry. The value of Physical Index for the contained physical entity.

Documentation Impacts

Use the following Entity MIB sections as a replacement for those found in the *Administering* document in the current documentation suite.

Entity MIB

Entity MIB – Physical Table

The Entity MIB – Physical Table assists in the discovery of functional components on the switch. The Entity MIB – Physical Table supports a physical interface table that includes information about the chassis, power supply, fan, I/O cards, console, and management port.

Some hardware platforms support removable interface modules while others offer a fixed configuration. The names used for these modules can vary depending on the hardware platform.

The following table identifies the entity index range for the switch components.

Component	Entity index range
Chassis	1
Power supply slot	3 to 8
Fan tray and fan slot	9 to 16
I/O slot	17 to 30
SF Slot	31 to 36
I/O card or module	37 to 50
SF Card	51 to 56
Console port	57
Console port 2	58
Management port	64
Management port 2	65
Power supply	68 to 73
Fan tray	74 to 81
Fan module	82 to 105
Port	192 to 1023
Pluggable Module and Sensor	19201 to 102314

For more information about Entity MIB – Physical Table, see Viewing physical entities on page 13.

Viewing physical entities

Perform this procedure to view information about the functional components of the switch.

Procedure

1. In the navigation pane, expand the **Configuration** > **Edit** folders.
2. Click **Entity**.

Physical Entities field descriptions

Use the following table to use the Physical Entities tab.

Name	Description
Index	Indicates the index of the entry.
Descr	Indicates the name of the manufacturer for the physical entity.
VendorType	Indicates the vendor-specific hardware type for the physical entity. Because there is no vendor-specifier registration for this device, the value is 0.
ContainedIn	Indicates the index value for the physical entity which contains this physical entity. A value of zero indicates that this physical entity is not contained in any other physical entity.
Class	Indicates the general hardware type of the physical entity. The value is configured to the standard enumeration value that indicates the general class of the physical entity.
ParentRelPos	Indicates the relative position of the child component among the sibling components.
Name	Indicates the name of the component, as assigned by the local device, and that is suitable to use in commands you enter on the console of the device. Depending on the physical component naming syntax of the device, the name can be a text name such as console, or a component number such as port or module number. If there is no local name, there is no value.
HardwareRev	Indicates the vendor-specific hardware revision string for the physical entity. If no specific hardware revision string is associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
FirmwareRev	Indicates the vendor-specific firmware revision string for the physical entity. If no specific firmware programs are associated with the physical component, or if this information is unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
SoftwareRev	Indicates the vendor-specific software revision string for the physical entity. If no specific software programs are associated with the physical component, or if this information is

Table continues…

Name	Description
	unknown, then this object contains a zero-length string, or there is no value. If there is no information available, there is no value.
SerialNum	Indicates the vendor-specific serial number string for the physical entity. The value is the serial number string printed on the component, if present. If there is no information available, there is no value.
MfgName	Indicates the name of the manufacturer of the physical component. The value is the manufacturer name string printed on the component, if present. If the manufacturer name string associated with the physical component is unknown, then this object contains a zero-length string. If there is no information available, there is no value.
ModelName	Indicates the vendor-specific model name identifier string associated with the physical component. The value is the part number which is printed on the component. If the model name string associated with the physical component is unknown, then this object contains a zero-length string.
Alias	Indicates an alias name for the physical entity that is specified by a network manager, and provides a nonvolatile handle for the physical entity. The software supports read-only and provides values for the port interface only.
AssetID	Indicates a user-assigned asset tracking identifier for the physical entity. This value is specified by a network manager, and provides nonvolatile storage of this information. Because this object is not supported, there is no value.
IsFRU	Indicates whether or not the physical entity is considered a field replaceable unit. • If the value is `true(1)`, then the component is a field replaceable unit. • If the value is `false(2)`, then the component is permanently contained within a field replaceable unit.

Table continues…

Name	Description
MfgDate	Indicates the manufacturing date of the managed entity. If the manufacturing date is unknown, then the value is `'0000000000000000'H`.
Uris	Indicates additional identification information about the physical entity. **Uris** is not supported, therefore there is no value.

Chapter 4: Backup configuration zip file

Backup Configuration Feature Summary

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.

Administration Impacts

The following section details new administration tasks for the Backup Configuration feature in Release 6.1.2.

Backing up Configuration Files

About this task

Use this procedure to backup configuration files.

Important:

Only the RWA user can run the backup command.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Run the backup command.

   ```
   backup configure <filename>
   ```

Example

Restoring Configuration Files

About this task

Use the following procedure to restore previously backed up configuration files.

Before you begin

- Download the backup file to the /intflash directory.
- If restoring the configuration files on a new switch, you must do one of the following:
  - Disable ISIS on the old switch .
  - Power the old switch down.
  - Remove the old switch from the network.
- If restoring the configuration files on a different switch, use the “isis dup-detection-temp-disable “ command on the new switch to suspend duplicate detection prior to its insertion into the existing SPBM topology.

  Important:

  This must be done after the original unit has been completely removed or isolated from the SPBM topology.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Run the restore command to restore the configuration files.

   ```
   restore configure <filename>
   ```

Documentation Impacts

The Backup Configuration feature does not impact the documentation suite.

Chapter 5: System logging

System Logging

Release 6.1.2 introduces a new system logging (syslog) and log file format, which can be enabled or disabled through a new bootflag. If upgrading from 6.1.50 the bootflag is automatically set to use the new format. If upgrading from a release other then 6.1.50 there is no change to the syslog and log message format. To enable the new syslog message format, the bootflag must be set using the following CLI command:

```
boot config flags syslog-rfc5424-format
```

Note:

This also impacts the log message format.

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.

Example

```
RFC Standard: "VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURE-DATA MSG"

Syslog message example:
 1 2017-05-11T08:48:49.482-05:00 switch1 CP1 - 0x00004763 – 00000000 GlobalRouter SNMP
INFO GBIC inserted trap sent from port 2/40.

Interpreting the syslog message:
VERSION = 1
TIMESTAMP = 2017-05-11T08:48:49.482-05:00
HOSTNAME = switch1
APP-NAME = CP1 (or "IO1" depends CP or IO process log the message)
PROCID = - (Proc ID is unknown, it needs to be "-")
MSGID = 0x00004763
STRUCTURE-DATA = - (No structure Data, it needs to be "-")
MSG = 00000000 GlobalRouter SNMP INFO GBIC inserted trap sent from port 2/40
```

Documentation Impacts

System Logging in Release 6.1.2 modifies the following tasks in the current documentation suite.

Configuring boot flags

Before you begin

- If you enable the hsecure flag, you cannot enable the flags for the Web server or SSH password-authentication.

Important:

After you change certain configuration parameters using the **`boot config flags`** command, you must save the changes to the configuration file.

About this task

Configure the boot flags to enable specific services and functions for the chassis.

Note:

The following **`boot config flags`** are not supported on all hardware models:

- ha-cpu flag
- ipv6-mode flag
- linerate-directed-broadcast flag
- savetostandby flag
- vrf-scaling
- vxlan-gw-full-interworking-mode

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Enable boot flags:

```
boot config flags <block-snmp|debug-config [file]|debugmode|dvr-
leaf-mode|enhancedsecure-mode <jitc|non-jitc>|factorydefaults|flow-
control-mode|ftpd|ha-cpu|hsecure|ipv6-mode|linerate-directed-
broadcast|logging|nni-mstp|reboot|rlogind|savetostandby|spanning-
tree-mode <mstp|rstp>|spbm-config-mode|sshd|syslog-rfc5424-format|
telnetd|tftpd|trace-logging|urpf-mode|verify-config|vrf-scaling|
vxlan-gw-full-interworking-mode>
```

3. Disable boot flags:

```
no boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode <jitc|non-jitc>|dvr-leaf-mode |factorydefaults|
flow-control-mode|ftpd|ha-cpu|hsecure|ipv6-mode|linerate-directed-
broadcast|logging|nni-mstp|reboot|rlogind|savetostandby|spanning-
tree-mode <mstp|rstp>|spbm-config-mode|sshd|syslog-rfc5424-format|
telnetd|tftpd|trace-logging|urpf-mode|verify-config|vrf-scaling|
vxlan-gw-full-interworking-mode>
```

4. Configure the boot flag to the default value:

```
default boot config flags <block-snmp|debug-config [file]|debugmode|
enhancedsecure-mode <jitc|non-jitc>|dvr-leaf-mode |factorydefaults|
flow-control-mode|ftpd|ha-cpu|hsecure|ipv6-mode|linerate-directed-
broadcast|logging|nni-mstp|reboot|rlogind|savetostandby|spanning-
tree-mode <mstp|rstp>|spbm-config-mode|sshd|syslog-rfc5424-format|
telnetd|tftpd|trace-logging|urpf-mode|verify-config|vrf-scaling|
vxlan-gw-full-interworking-mode>
```

5. Save the changed configuration.
6. Restart the switch.

Example

```
Switch:1>enable
Switch:1#configure terminal
```

Activate High Secure mode:

```
Switch:1(config)# boot config flags hsecure
Switch:1(config)# save config
Switch:1(config)# reset
```

Activate High Availability mode:

```
Switch:1(config)#boot config flags ha-cpu
Switch:1(config)#save config
```

Variable definitions

Use the data in the following table to use the **`boot config flags`** command.

Variable	Value
block-snmp	Activates or disables Simple Network Management Protocol management. The default value is false (disabled), which permits SNMP access.
debug-config [console] | [file]	Enables you to debug the configuration file during loading configuration at system boot up. The default is disabled. You do not have to restart the switch after you enable debug-config, unless you want to immediately debug the configuration. After you enable debug-config and save the configuration, the debug output either displays on the console or logs to an output file the next time the switch reboots.

Table continues…

Variable	Value
	The options are: • debug-config [console]—Displays the line-by-line configuration file processing and result of the execution on the console while the device loads the configuration file. • debug-config [file]— Logs the line-by-line configuration file processing and result of the execution to the debug file while the device loads the configuration file. The system logs the debug config output to /intflash/debugconfig_primary.txt for the primary configuration file. The system logs the debug config output to /intflash/debugconfig_backup.txt for the backup configuration, if the backup configuration file loads.
debugmode	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging earlier on specified port. It only works on console connection. By default, it is disabled. **Important:** Do not change this parameter unless directed by technical support.
dvr-leaf-mode	Enables an SPB node to be configured as a DvR Leaf. A note that has this flag set cannot be configured as a DvR Controller. Use the no or the default operator to disable this flag. The boot flag is disabled by default. For information on DvR, see *Configuring IPv4 Routing*.
enhancedsecure-mode {jitc | non-jitc}	Enables enhanced secure mode in either the JITC or non-JITC sub-modes. **Note:** It is recommended that you enable the enhanced secure mode in the non-JITC sub-mode, because the JITC sub-mode is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting.

Table continues…

Variable	Value
	When you enable enhanced secure mode in either the JITC or non-JITC sub-modes, the switch provides role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting after the CPU restarts. If you change this parameter, you must restart the switch.
flow-control-mode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames. The default is disabled.
ftpd	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the tftpd flag is disabled.
ha-cpu	Activates or disables High Availability-CPU (HA-CPU) mode. Switches with two CPUs use HA mode to recover quickly from a failure of one of the CPUs. If you enable or disable HA mode, the secondary CPU resets automatically to load settings from the saved configuration file.
hsecure	Activates or disables High Secure mode. The hsecure command provides the following password behavior: • 10 character enforcement • The password must contain a minimum of 2 uppercase characters, 2 lowercase characters, 2 numbers, and 2 special characters. • Aging time • Failed login attempt limitation The default value is disabled. If you enable High Secure mode, you must restart the switch to enforce secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.

Table continues…

Variable	Value
ipv6–mode	Enables IPv6 mode on the swtich. This parameter does not apply to all hardware platforms.
linerate-directed-broadcast {true | false}	Enables or disables support for IP Directed Broadcast in hardware without requiring CPU intervention. Setting this boot flag will put port 1/46 into loopback mode, making it unusable for external connections, so you need to move any existing connections on this port first. After setting this boot flag, save the configuration, and then restart the switch. The default value is disabled. This parameter applies to VSP 4000 Series platforms only. **Important:** The software cannot be upgraded or downgraded to a software release that does not contain this directed broadcast hardware assist functionality without first disabling this feature and saving the configuration.
logging	Activates or disable system logging. The default value is enabled. The system names log files according to the following: • File names appear in 8.3 (log.xxxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. • The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file. The system generates multiple sequence numbers for the same chassis and same slot if the system reaches the maximum log file size.
nni-mstp	Enables MSTP and VLAN configuration on NNI ports. The default is disabled. **Note:** Spanning Tree is disabled on all NNIs.

Table continues…

Variable	Value
	You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN. You cannot add additional C-VLANs to a brouter port. For information on releases that support the nni-mstp boot flag see *Release Notes*.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated. **Important:** Do not change this parameter unless directed by technical support.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby	Activates or disables automatic save of the configuration file to the standby CPU. The default value is enabled. If you operate a dual CPU system, it is recommended that you enable this flag for ease of operation.
spanning-tree-mode <mstp|rstp>	Specifies the Multiple Spanning Tree Protocol or Rapid Spanning Tree Protocol mode. If you do not specify a protocol, the switch uses the default mode. The default mode is mstp. If you change the spanning tree mode, you must save the current configuration and restart the switch.
spbm-config-mode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. Use the no operator so that you can configure PIM and IGMP. The boot flag is enabled by default. To set this flag to the default value, use the default operator with the command.
sshd	Activates or disables the SSHv2 server service. The default value is disabled.
syslog-rfc5424-format	Controls the format of the syslog output and logging. By default, the switch uses the RFC5424 format. If the RFC based format is disabled, the older format is used.
telnetd	Activates or disables the Telnet server service. The default is disabled.
tftpd	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.

Table continues…

Variable	Value
trace-logging	Activates or disables the creation of trace logs. The default value is disabled. **Important:** Do not change this parameter unless directed by technical support.
urpf-mode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you configure it on a port or VLAN. The default is disabled.
verify-config	Activates syntax checking of the configuration file. The default is enabled. • Primary config behavior: When the verifyconfig flag is enabled, the primary config file is pre-checked for syntax errors. If the system finds an error, the primary config file is not loaded, instead the system loads the backup config file. If the verify-config flag is disabled, the system does not pre-check syntax errors. When the verify-config flag is disabled, the system ignores any lines with errors during loading of the primary config file. If the primary config file is not present or cannot be found, the system tries to load the backup file. • Backup config behavior: If the system loads the backup config file, the system does not check the backup file for syntax errors. It does not matter if the verify-config flag is disabled or enabled. With the backup config file, the system ignores any lines with errors during the loading of the backup config file. If no backup config file exists, the system defaults to factory defaults. It is recommended that you disable the verify-config flag.
vrf-scaling	Increases the maximum number of VRFs and Layer 3 VSNs that the switch supports. This flag is disabled by default. **Important:** If you enable both this flag and the spbmconfig-mode flag, the switch reduces the number of configurable VLANs. For more information

Table continues…

Variable	Value
	about maximum scaling numbers, see *Release Notes*.
vxlan-gw-full-interworking-mode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST. By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag. The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments. For more information about feature support, see *Configuring VLANs, Spanning Tree, and NLB*.

Viewing the boot configuration

About this task

View the boot configuration to determine the software version, as well as view the source from which the switch last started.

Procedure

1. On the Device Physical View, select the Device.
2. In the navigation pane, expand the **Configuration** > **Edit** folders.
3. Click **Chassis**.
4. Click the **Boot Config** tab.

Boot Config field descriptions

Use the data in the following table to use the Boot Config tab.

Name	Description
SwVersion	Specifies the software version that currently runs on the chassis.
LastRuntimeConfigSource	Specifies the last source for the run-time image.
PrimaryConfigSource	Specifies the primary configuration source.
PrimaryBackupConfigSource	Specifies the backup configuration source to use if the primary does not exist.
EnableFactoryDefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically reset to the default setting

Table continues…

Name	Description
	after the CPU restarts. If you change this parameter, you must restart the switch.
EnableDebugMode	Enabling the debugmode will provide the opportunity to allow user to enable TRACE on any port by prompting the selection on the console during boot up. This allows the user start trace for debugging earlier on specified port. It only works on console connection. By default, it is disabled. **Important:** Do not change this parameter.
EnableRebootOnError	Activates or disables automatic reboot on a fatal error. The default value is activated. **Important:** Do not change this parameter.
EnableTelnetServer	Activates or disables the Telnet server service. The default is disabled.
EnableRloginServer	Activates or disables the rlogin and rsh server. The default value is disabled.
EnableFtpServer	Activates or disables the FTP server on the switch. The default value is disabled. To enable FTP, ensure that the TFTPD flag is disabled.
EnableTftpServer	Activates or disables Trivial File Transfer Protocol server service. The default value is disabled.
EnableSshServer	Activates or disables the SSH server service. The default value is disabled.
EnableSpbmConfigMode	Enables you to configure SPB and IS-IS, but you cannot configure PIM and IGMP either globally or on an interface. The boot flag is enabled by default.
EnableIpv6Mode	Enable this flag to support IPv6 routes with prefix-lengths greater than 64 bits. This flag is disabled by default. This field does not appear for all hardware platforms.
EnableEnhancedsecureMode	Enables or disables the enhanced secure mode. Select either **jitc** or **non-jitc** to enable the enhanced secure mode in one of these sub-modes. The default is disabled. **Note:** It is recommended that you enable the enhanced secure mode in the non-JITC sub-

Table continues…

Name	Description
	mode because the JITC sub-mode is more restrictive and prevents the use of some troubleshooting utilities.
EnableUrpfMode	Enables Unicast Reverse Path Forwarding (uRPF) globally. You must enable uRPF globally before you configure it on a port or VLAN. The default is disabled.
EnableVxlanGwFullInterworkingMode	Enables VXLAN Gateway in Full Interworking Mode, which supports SPB, SMLT, and vIST. By default, the Base Interworking Mode is enabled and Full Interworking Mode is disabled. You change modes by enabling this boot configuration flag. The no operator is the default Base Interworking Mode. In this mode, VXLAN Gateway supports Layer 2 gateway communication between VXLAN and traditional VLAN environments. For more information about feature support, see *Release Notes*.
EnableFlowControlMode	Enables or disables flow control globally. When disabled, the system does not generate nor configure the transmission of flow control messages. The system always honors received flow control messages regardless of the flow control mode status. You must enable this mode before you configure an interface to send pause frames. The default is disabled.
EnableDvrLeafMode	Enables the switch to be configured as a DvR Leaf. When enabled, you cannot configure the switch to operate as a DvR Controller.
EnablevrfScaling	Changes the maximum number of VRFs and Layer 3 VSNs that the switch supports. If you select this check box, the maximum number increases. The default is disabled. **Important:** If you select both this check box and the **EnableSpbmConfigMode** check box, the switch reduces the number of configurable VLANs. For more information about maximum scaling numbers, see *Release Notes*.
EnableSyslogRfc5424Format	Enable or disable the Rfc5424 syslog format.

Table continues…

Name	Description
	The default is enabled. If the pre-existing config file is for a release prior to 6.1.2.0, then the flag is disabled automatically.
NniMstp	Enables MSTP, and allows non SPBM B-VLAN configuration on SPBM NNI ports.The default is disabled. **Note:** Spanning Tree is disabled on all SPBM NNIs. You cannot add an SPBM NNI port or MLT port to any non SPBM B-VLAN.
MasterCPUSlot	Specifies the slot number, either 1 or 2, for the master CPU. The default value is 1.
EnableHaCpu	Enables or disables the CPU High Availability feature. If you enable or disable HA mode, the secondary CPU automatically resets to load settings from the previously-saved configuration file. The default is enabled.
EnableSavetoStandby	Enables or disables automatic save of the configuration file to the standby CPU. The default value is enabled.
Slot	Specifies the slot number.
TftpHash	Enables TFTP hashing.
TftpRetransmit	Set TFTP retransmit timeout counter.
TftpTimeout	Set TFTP timeout counter.
User	Configure host user.
Password	Configure host password.

Verifying boot configuration flags

Verify the boot configuration flags to verify boot configuration settings. Boot configuration settings only take effect after you reset the system. Verification of these parameters is essential to minimize system downtime and the resets to change them.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the flags:

   ```
   show boot config flags
   ```

Example

```
Switch:1>enable
Switch:1#show boot config flags
flags block-snmp false
flags debug-config file
flags debugmode false
flags dvr-leaf-mode false
flags enhancedsecure-mode false
flags factorydefaults false
flags flow-control-mode false
flags ftpd true
flags ha-cpu true
flags hsecure false
flags linerate-directed-broadcast false
flags ipv6-mode false
flags logging true
flags nni-mstp false
flags reboot true
flags rlogind false
flags savetostandby true
flags spanning-tree-mode mstp
flags spbm-config-mode false
flags sshd true
flags syslog-rfc5424-format true
flags telnetd true
flags tftpd true
flags trace-logging false
flags urpf-mode false
flags verify-config true
flags vrf-scaling false
flags vxlan-gw-full-interworking-mode false
```

Note:

The following **`boot config flags`** are not supported on all hardware models:

- ha-cpu flag
- ipv6-mode flag
- savetostandby flag