ExtremeWare Release Notes

Software Version 7.1.1b11

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: November 2003
Part Number: 120186-00 Rev 02

Author: Rich Small

Editor: Rich Small

Production: Rich Small

Special Thanks: Mark, Paul

Contents

1 Overview

These Release Notes document ExtremeWare® 7.1.1b11. ExtremeWare 7.1.1 enables new hardware products and software features.

NOTE

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2 (or later). To install ExtremeWare 7.1, see "Upgrading ExtremeWare" on page 17.

This chapter contains the following sections:

New Features in ExtremeWare 7.1

Following are descriptions of features introduced or enhanced in ExtremeWare 7.1.1. These features are documented in detail in the *ExtremeWare Software User Guide* or the *ExtremeWare Software Command Reference Guide*, unless otherwise noted.

You can ignore numbers in parentheses, which are for internal use.

Features Added or Enhanced in ExtremeWare 7.1.1

The following features were added or enhanced in ExtremeWare 7.1.1b8:

- The new MSM-3 provides a more robust switching fabric and supports two new software features: cross-module trunking and T-sync. The MSM-3 is now included in the `show switch`, `show msm-failover`, `show version detail`, and `show log` commands, but does not require new commands or configuration changes.
- BlackDiamond 6804 and BlackDiamond 6808 chassis using MSM-3's now support cross-module trunking. Load-sharing links can now span more than one I/O module for increased availability.
- T-sync is a term used to describe the hitless failover and hitless upgrade features available on the BlackDiamond Management Switch Module 3 (MSM-3). In simple terms, hitless failover transfers switch management control from the master MSM-3 to the slave MSM-3 without causing traffic to be

dropped. Hitless upgrade allows an ExtremeWare software upgrade on a BlackDiamond 6800 series chassis without taking it out of service or losing traffic.

Supported Hardware

Hardware in the following sections listed in *italics* is new for this release.

ExtremeWare 7.0 (and later) supports "*i*" series or "3" series products *only.*

ExtremeWare 7.1.1 requires BootROM 8.1.

Table 1 lists software filenames for the supported hardware that requires software.

Table 1: Software for supported hardware

Extreme Hardware	ExtremeWare Filename	BootROM Filename/Version
BlackDiamond 6816	v711b11.Gxtr or v711b11.SGxtr	Ngboot8.1.bin/8.1
BlackDiamond 6808	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
BlackDiamond 6804	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Alpine 3808	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Alpine 3804	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Alpine 3802	v711b11.xtr or v711b11.Sxtr/EW-70-3802.mig	Ngboot8.1.bin/8.1
Summit7i/7iT	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Summit1i/1iT	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Summit5i/5iT/5iLX	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Summit48i	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
Summit48si	v711b11.xtr or v711b11.Sxtr	Ngboot8.1.bin/8.1
ARM module	v711b11.arm	v711b11.nprom/1.18
OC3 PoS module	v711b11.oc3	v711b11.nprom/1.18
OC12 PoS module	v711b11.oc12	v711b11.nprom/1.18
OC3 ATM module	v711b11.atm3	v711b11.nprom/1.18
MPLS module	v711b11.mpls	v711b11.nprom/1.18
T1 module	v711b11.t1	t1boot28.wr/2.8
E1 module	v711b11.e1	e1boot28.wr/2.8
T3 module	v711b11.t3	t3boot28.wr/2.8

NOTE

The BlackDiamond 6816 requires its own ExtremeWare image. The image that runs on other BlackDiamond, Alpine, or stackable switches does not support the BlackDiamond 6816.

BlackDiamond Component Support

BlackDiamond components supported with ExtremeWare 7.1.1, and the minimum ExtremeWare version required by the chassis to support each component, include:

Table 2: BlackDiamond component support

BlackDiamond Component	ExtremeWare Required
BlackDiamond 6804	6.2.2b56[1]
BlackDiamond 6808	6.2.2b56[1]
BlackDiamond 6816	6.2.2b56[1]
MSM-3	7.1.1
MSM64i	6.2.2b56[1]
G8Xi	6.1.3
G8Ti	6.1.3
G12SXi	6.1.4
G16X[3]	7.0.1
G24T[3]	7.0.1
F32Fi	6.1.8
F48Ti	6.1.2
F96Ti	6.1.8
WDMi	6.1.5
10GLRi	7.0
MPLS	7.0
ARM	7.0
P3cMi	7.0
P3cSi	7.0
P12cMi	7.0
P12cSi	7.0
A3cMi	7.0
A3cSi	7.0
DC Power Supply	6.1.5
110 VAC Power Supply	6.1.5
220 VAC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

NOTE

Do not install mixed versions of the power supplies in the same system. Install power supplies of the same type.

Alpine Component Support

Alpine components supported with ExtremeWare 7.1.1, and the minimum ExtremeWare version required, include:

Table 3: Alpine component support

Alpine Component	ExtremeWare Required
Alpine 3802	6.2.2b56[1]
Alpine 3804	6.2.2b56[1]
Alpine 3808	6.2.2b56[1]
SMMi	6.2.2b56[1]
GM-4Si/Xi/Ti	6.1.5
GM-16X[3]	7.0.1
GM-16T[3]	7.0.1
FM-32Ti	6.1.5
FM-24MFi	6.1.5
FM-24Ti	6.1.7
FM-24SFi	6.1.7
GM-WDMi	6.1.8
WM-4T1i	7.0.1
WM-4E1i	7.0.1
WM-1T3i	7.0.1
FM-8Vi	7.0.1
AC Power Supply	6.1
DC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

Summit Component Support

Summit components supported with ExtremeWare 7.1.1, and the minimum ExtremeWare version required, include:

Table 4: Summit component support

Summit Component	ExtremeWare Required
Summit1i	6.2.2b56[1]
Summit5i	6.2.2b56[1]
Summit7i	6.2.2b56[1]
Summit7i DC Power Supply	6.2.2b56[1]
Summit48i	6.2.2b56[1]
Summit48si	6.2.2b56[1]

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

GBIC Support

GBICs supported with ExtremeWare 7.1.1, and the minimum ExtremeWare version required, include:

Table 5: GBIC support

GBIC	ExtremeWare Required
SX parallel ID	1.0
SX serial ID	2.0
LX parallel ID	1.0
LX serial ID	2.0
ZX	7.0.1b11
ZX Rev 03	7.0.1b11
LX70	2.0
LX100	6.1.9
UTP	6.1.9
SX Mini	7.0.1b11
LX Mini	7.0.1b11
ZX Mini	7.0.1b11

The following table describes how each version of ExtremeWare interprets the media type of the installed GBIC, based on either the Vista web interface, or the `show port configuration` command. All versions correctly identify Parallel ID GBIC types; however, some versions do not correctly identify the Serial ID GBIC type because the Serial ID GBICs were introduced after the software was released.

Table 6: ExtremeWare recognition of GBIC type

ExtremeWare Version	SX Parallel ID	LX Parallel ID	SX Serial ID	LX Serial ID	LX70
1.x	SX	LX	Not Supported	Not Supported	Not Supported
2.x	SX	LX	LX	LX	LX
3.x	SX	LX	CX	CX	CX
4.x	SX	LX	SX	LX	LX
6.x	SX	LX	SX	LX	LX70 (6.1.6 and above)
7.x	SX	LX	SX	LX	LX70

Mini-GBIC Support

Extreme products support the Extreme mini-GBIC only. For reliability and stability reasons, third-party mini-GBICs are not supported at this time.

2 Upgrading to ExtremeWare 7.1

This chapter contains the following sections:

CAUTION

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2b56 (or later).

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site at http://www.extremenetworks.com/go/esupport.htm.

Upgrading ExtremeWare

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2b56 (or later). You can only load ExtremeWare 6.2.2 on a switch running ExtremeWare 6.1.9 (or later). Table 7 lists the BootROM required for each version of ExtremeWare.

Table 7: Required BootROM versions

ExtremeWare Version	BootRom Version
ExtremeWare 7.1.1	BootROM 8.1 (or later)
ExtremeWare 7.0.0 through ExtremeWare 7.1.0	BootROM 7.8 (or later)
ExtremeWare 6.2.2	BootROM 7.6 (or later)
ExtremeWare 6.1.9 through ExtremeWare 6.2.1	BootROM 7.2 (or later)
ExtremeWare 6.1 through ExtremeWare 6.1.8	BootROM 6.5

If your switch is running ExtremeWare 6.1.8 (or earlier), you must first upgrade to ExtremeWare 6.1.9, then upgrade to ExtremeWare 6.2.2b56 (or later). Following are specific instructions on upgrading to, and downgrading from, ExtremeWare 7.1.1 for Summit, Alpine, and BlackDiamond switches.

Upgrading Switches to ExtremeWare 7.1.1

To install ExtremeWare 7.1.1, you must:

1. Save the configuration to a TFTP server.
2. Upgrade the BootROM to Version 8.1 as described on page 19.
3. Upgrade to ExtremeWare 6.1.9 as described on page 19.
4. Upgrade to ExtremeWare 6.2.2b56 as described on page 19.
5. Upgrade to ExtremeWare 7.1.1 as described on page 20.
6. Upgrade ATM, MPLS, ARM, PoS, T1, E1, or T3 Modules as described on page 21.

If you have already installed ExtremeWare 6.1.9 through ExtremeWare 6.2.2b43, you can skip step 3. If you have already installed ExtremeWare 6.2.2b56 through ExtremeWare 7.0.1, you can skip steps 3 and 4.

NOTE

If you are also upgrading your BlackDiamond to MSM-3's, see the MSM-3 Upgrade Note *included with your MSM-3.*

NOTE

The Alpine 3802 requires a different upgrade procedure, described on page 21.

Save the Current Configuration

Before upgrading ExtremeWare, save your configuration using the following steps. This preserves the ability to downgrade should it become necessary.

1. If you are using the Network Login campus mode:
   - **a** Disable Network Login using the `disable netlogin` command to prevent users from re-authenticating during the backup process.
   - **b** Use the `clear netlogin state port` command on all Network Login user ports, causing all Network Login users to be unauthenticated and all client ports to move back to their respective unauthenticated VLAN configuration.
   - **c** Use the `show netlogin` and `show vlan` commands to verify that all Network Login ports are in the unauthenticated state and the client ports are members of their respective unauthenticated VLANs.
2. If you are using ACLs and the CPU DoS protect feature, ensure that the CPU DoS protect filter precedence follows the rules described in "CPU DoS Protect and ACL Precedence" on page 52. If there is a precedence conflict, CPU DoS protect is not enabled.
3. Save the current configuration in both the primary and secondary configuration spaces using the `save configuration primary` and `save configuration secondary` commands.
4. Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use configuration primary` commands.
5. Verify that all of the above procedures were completed successfully with the `show switch` command.

6 Upload the configuration to a TFTP server for safekeeping using the `upload configuration` command.

Upgrade the BootROM to Version 8.1

Before you upgrade ExtremeWare, upgrade to BootROM 8.1 (BootROM 8.1 is compatible with all ExtremeWare versions back to ExtremeWare 6.1.9):

1 Download the BootROM using the `download bootrom [<host_name> | <ip_addr>] <ngboot.bin_name>` command.

2 Reboot the switch using the `reboot` command.

Upgrade to ExtremeWare 6.1.9

If you are running ExtremeWare 6.1.8 (or earlier), upgrade to ExtremeWare 6.1.9:

1 TFTP download ExtremeWare 6.1.9 to the primary image space using the `download image primary` command.

CAUTION

If you do not upgrade to ExtremeWare 6.1.9 before downloading ExtremeWare 6.2.2, the ExtremeWare 6.2.2 download will fail, and the following message will be printed from the system:

```
ERROR: File too large
```

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 Check the log for configuration errors. Manually enter configurations that did not load.

5 If you configured Random Early Drop Probability in ExtremeWare 6.1.8 (or earlier), re-configure the Random Early Drop Probability using the `configure red drop-probability` command.

6 Save the configuration to the primary space.

Upgrade to ExtremeWare 6.2.2b56

If you are running ExtremeWare 6.1.9 to ExtremeWare 6.2.2b43, upgrade to ExtremeWare 6.2.2b56 (you can substitute ExtremeWare 6.2.2 builds 68, 108, 124, and 134 for build 56):

1 TFTP download ExtremeWare 6.2.2b56 to the primary image space using the `download image primary` command.

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

NOTE

ExtremeWare 6.2.2b56 (and later) stores 75 static log entries. Previous versions stored 100 entries. To accommodate the new entry limit, ExtremeWare 6.2.2b56 clears the static log after your first reboot. To preserve your static log entries, use the `show log` *command and save the output.*

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 TFTP download the saved configuration, and answer `y` at the prompt to reboot the switch.

5 Check the log for configuration errors. Manually enter configurations that did not load.

6 Save the configuration.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

NOTE

After upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.2, the IGMP snooping leave time-out value will be changed from 10 seconds to 0. This results in an IGMP snooping membership entry being removed immediately when an IGMP leave is received from a host.

This is good for an environment where only one host is connected. Use the `configure igmp snooping leave-timeout` *command to change the leave time-out value back to 10 seconds.*

Upgrade to ExtremeWare 7.1.1

If you are running ExtremeWare 6.2.2b56 (or later), upgrade to ExtremeWare 7.1.1:

NOTE

If you are upgrading a chassis with MSM64i's to MSM-3's, see the MSM-3 Upgrade Note included with your MSM-3.

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Clear your switch using the `unconfigure switch all` command, and enter `y` at the prompt to reboot the switch.

3 TFTP download ExtremeWare 7.1.1 to the primary image space using the `download image primary` command.

4 Reboot the switch using the `reboot` command.

NOTE

If you have Hitless Failover enabled on your MSM-3, you can use the hitless upgrade procedure.

5 Verify that the correct ExtremeWare version is loaded on the switch using the `show switch` command.

6 TFTP download the configuration you saved in Step 1, and enter `y` at the prompt to reboot the switch.

7 Check the log for configuration errors. Manually enter configurations that did not load.

8 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

9 If you are upgrading a BlackDiamond switch, synchronize the BootROM, image, and configuration across all installed MSM modules using the `synchronize` command. This command reboots the synchronized modules.

You can ignore any diagnostics failure messages generated by the synchronization.

10 Reboot the switch using the `reboot` command.

11 If you are using the Network Login campus mode:

a Manually enable Network Login using the `enable netlogin [web-based | dot1x]` command.

b Verify that users are able to authenticate and successfully access network resources.

Upgrade ATM, MPLS, ARM, PoS, T1, E1, or T3 Modules

If you are using an ATM, MPLS, ARM, PoS, T1, E1, or T3 module, upgrade the module to ExtremeWare 7.1.1:

1 TFTP download the latest ExtremeWare version for the module using the `download image slot` command.

NOTE

T1, E1, and T3 modules must be using ExtremeWare 6.1.8b79 (or later) and BootROM 2.8 (or later) before upgrading to ExtremeWare 7.1.1.

2 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 2 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

3 Download the BootROM using the `download bootrom slot` command.

4 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 4, upgrade every module, then reboot the switch.

Upgrading an Alpine 3802 to ExtremeWare 7.1.1

To upgrade an Alpine 3802 to ExtremeWare 7.1.1:

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Upgrade to BootROM 8.1 using the `download bootrom` command.

3 Reboot the switch using the `reboot` command.

4 TFTP download ExtremeWare 6.1.8w3.0.1 b79 to the primary image space using the `download image primary` command.

5 Verify that the correct BootROM and ExtremeWare versions are loaded on the switch using the `show switch` and `show version` commands.

6 Answer `y` at the prompt to reboot the switch.

7 TFTP download ExtremeWare 7.0.0b46 to the primary image space using the `download image primary` command.

8 Reboot the switch using the `reboot` command.

9 TFTP download the latest ExtremeWare 7.1.1 build to the primary image space using the `download image primary` command.

10 Reboot the switch using the `reboot` command.

11 TFTP download the configuration you saved in Step 1, and enter `y` to reboot the switch.

12 Check the log for configuration errors. Manually enter configurations that did not load.

13 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

Downgrading Switches

Assuming that the previous configuration is in the secondary configuration space and the previous image is in the secondary image space:

1 If you saved an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, configure the switch to use that configuration with the `use configuration secondary` command.

If you did not save an earlier configuration, re-configure the switch or download a configuration at the end of this process.

2 If you did not save the earlier ExtremeWare image in the secondary image space, download the image using the `download image secondary` command.

NOTE

If you downgrade to an ExtremeWare version that does not support software signatures (ExtremeWare 6.2.2b56 or later supports software signatures), you must follow the upgrade procedures in the preceding sections to get back to ExtremeWare 7.1.1. You cannot switch between primary and secondary images on the switch unless they both support software signatures.

3 Use the image in the secondary image space with the `use image secondary` command.

4 Verify that the above procedures were completed successfully with the `show switch` command.

5 Downgrade to the appropriate BootROM version. The `show version` command displays the BootROM version as “Unknown” when the BootROM is downgraded.

6 Reboot the switch.

NOTE

When downgrading to a previous version of ExtremeWare, ensure that the switch configuration matches that version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported. You will get a warning message from the system when attempting to do so.

7 If you did not save an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, re-configure the switch or download a configuration.

3 Supported Limits

This chapter summarizes the supported limits in ExtremeWare.

Supported Limits

The table below summarizes tested metrics for a variety of features. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeWare Software User Guide.*

Table 8: Supported limits

Metric	Description	Limit
Access List rules	Maximum number of Access Lists (best case).	5120
Access List rules—BlackDiamond 6816	Maximum number of BlackDiamond 6816 Access Lists (best case).	3500
Access List rules—Summit	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—Alpine	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—BlackDiamond	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255 per I/O module
Access Profiles	Maximum number of access profiles per switch.	128
Access Profile entries	Maximum number of access profile entries per switch.	256
BGP—Peer Groups	Maximum number of BGP peer groups per switch.	16
BGP—peers	Maximum number of BGP peers per switch.	200
BGP—routes, MSM-3	Maximum number of routes received and contained in the BGP route table (best case).	2,625,000
BGP—routes, MSM64i, Summit7i, Alpine	Maximum number of routes received and contained in the BGP route table (best case).	1,275,000
BGP—routes, Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of routes received and contained in the BGP route table (best case).	180,000
BGP—NLRI filters	Maximum number of NLRI filters per switch.	128
BGP—NLRI filer add entries	Maximum number of NLRI add entries per switch.	256

Table 8: Supported limits (continued)

Metric	Description	Limit
BGP—AS-Path filters	Maximum number of AS-Path filters per switch.	128
BGP—AS-Path filter add entries	Maximum number of AS-Path filter add entries per switch.	256
BGP—network statements	Maximum number of network statements per switch.	256
BGP—aggregate addresses	Maximum number of aggregate routes that can be originated per switch.	256
Jumbo Frame size	Maximum size supported for Jumbo frames, including the CRC.	9216
EAPS—Domains/switch	Maximum number of EAPS domains.	64
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	64
EAPS—VLAN links	Maximum number of Control or Protected VLANs per EAPS domain.	4093
EAPS—Bridge links	Maximum number of EAPS bridge links per switch.	4096
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit
EMISTP & PVST+ — maximum domains, Summit	Maximum number of EMISTP and PVST+ domains.	128
EMISTP & PVST+ — maximum domains, Alpine	Maximum number of EMISTP and PVST+ domains.	256
EMISTP & PVST+ — maximum domains, BlackDiamond	Maximum number of EMISTP and PVST+ domains.	512
EMISTP & PVST+ — maximum ports	Maximum number of EMISTP and PVST+ ports.	3840
EMISTP & PVST+ — maximum domains per port, Summit	Maximum number of EMISTP and PVST+ domains that can be configured per port.	128
EMISTP & PVST+ — maximum domains per port, Alpine	Maximum number of EMISTP and PVST+ domains that can be configured per port.	256
EMISTP & PVST+ — maximum domains per port, BlackDiamond	Maximum number of EMISTP and PVST+ domains that can be configured per port.	512
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum ESRP groups with bi-directional rate shaping	Maximum number of ESRP groups within a broadcast domain when bi-directional rate shaping is enabled.	3
ESRP—maximum VLANs in a single ESRP domain – Summit, Alpine	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain. To obtain higher values see configuration notes.	256 recommended; 3000 max
ESRP—number of VLANs in a single ESRP domain, BlackDiamond	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain. To obtain higher values see configuration notes.	1024 recommended; 3000 max

Table 8: Supported limits (continued)

Metric	Description	Limit
ESRP—Route-track entries, Summit, Alpine, BlackDiamond	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1
FDB—maximum ports for permanent entries	Maximum number of ports supported for permanent FDB entries.	2,000
FDB—maximum L2/L3 entries – BlackDiamond, Summit5i, Summit7i, Alpine 3804, Alpine 3808	Maximum number of MAC addresses/IP host routes for the MSM64i, Summit5i, Summit7i, Alpine 3804, and Alpine 3808.	262,144
FDB—maximum L2/L3 entries – Summit1i, Summit48i, Summit48si, Alpine 3802	Maximum number of MAC addresses/IP host routes for the Summit1i, Summit48i, Summit48si, and Alpine 3802.	131,072
Flow Redirection—maximum redirection rules	Maximum number of rules that can point to the same or separate groups of web cache servers.	64 (8 servers is the maximum)
Flow Redirection—maximum enumeration mode entries	Maximum number of active entries for enumeration mode rules. For example, one /16 rule can take all of the available entries.	64,000
Flow Redirection—maximum subnet mode entries	Maximum number of active entries for subnet mode rules. Each mask can have 1 entry.	64
IP ARP entries	Maximum number of IPARP entries.	20,480
IP ARP Static entries	Maximum number of permanent IP static ARP entries supported.	512
IP ARP Static Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
IP Route Sharing Entries (ECMP)—static or OSPF	Maximum number of static or OSPF routes used in route sharing calculations.	12
IP Route Sharing Entries (ECMP)—IS-IS	Maximum number of IS-IS routes used in route sharing calculations.	8
IP Router interfaces	Maximum number of VLANs performing IP routing - excludes SubVLANs.	512
IP Static Routes	Maximum number of permanent IP routes.	1024
IPX Static Routes and Services (RIP and SAP)	Maximum number of static IPX RIP route and IPX SAP entries.	64 for each
IPX dynamic routes and services	Maximum recommended number of dynamically learned IPX RIP routes and SAP entries.	2000 for each
IPX Router interfaces	Maximum number of IPX router interfaces.	256
IPX Access control lists	Maximum number of Access Lists in which all rules utilize all available options.	worst case: 255
IS-IS—maximum routing interfaces	Maximum IS-IS routing interfaces.	255
IS-IS—maximum routes	Maximum IS-IS routes.	25,000
IS-IS—maximum adjacencies	Maximum IS-IS adjacencies per routing interface.	64
IS-IS—maximum domain summary addresses	Maximum IS-IS domain summary addresses.	32
IS-IS—maximum redistributed routes, regular metric	Maximum IS-IS redistributed routes using the regular metric.	20,000
IS-IS—maximum redistributed routes, wide metric	Maximum IS-IS redistributed routes using the wide metric.	30,000

Table 8: Supported limits (continued)

Metric	Description	Limit
IS-IS—maximum redistributed routes, both metrics	Maximum IS-IS redistributed routes using both metrics.	10,000
Logged Messages	Maximum number of messages logged locally on the system.	1000
MAC-based VLANs—MAC addresses	Maximum number of MAC addresses that can be downloaded to the switch when using MAC-based VLANs.	7000
MAC-based security	Maximum number of MAC-based security policies.	1024
Mirroring—mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8
Mirroring—number of VLANs	Maximum number of VLANs that can be mirrored to the mirror port.	8
NAT—maximum connections	Maximum number of simultaneous connections per switch.	256,000
NAT—maximum rules	Maximum number of rules per switch.	2048
NAT—maximum VLANs	Maximum number of inside or outside VLANs per switch.	The switch's limit
NetFlow—Filters	Maximum number of NetFlow filters in a switch.	128
NetFlow—Groups	Maximum number of NetFlow groups.	32
NetFlow—Hosts	Maximum number of NetFlow hosts.	8/group
Network Login—Maximum clients	Maximum number of Network Login clients per switch.	1024
Network Login—802.1x	Maximum recommended Session-Timeout value returned by RADIUS server.	7200 seconds
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF external routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	130,000
OSPF inter- or intra-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	16,000
OSPF external routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	65,000
OSPF inter- or intra-area routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	8,000
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	200
OSPF interfaces on a single router	Recommended maximum number of OSPF routed interfaces on a switch.	384
OSPF virtual links	Maximum number of OSPF virtual links supported.	32
OSPF adjacencies—Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of OSPF adjacencies on a switch with 128 MB memory.	150

Table 8: Supported limits (continued)

Metric	Description	Limit
OSPF adjacencies—Summit7i, Alpine, BlackDiamond	Maximum number of OSPF adjacencies on a switch with 256 MB memory.	225
Policy Based Routing	Maximum number of policy based routes that can be stored on a switch.	64
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	384
Route Maps	Maximum number of route maps supported on a switch.	128
Route Map Entries	Maximum number of route map entries supported on a switch.	256
Route Map Statements	Maximum number of route map statements supported on a switch.	512
SLB—maximum number of simultaneous sessions	For Transparent and Translational and GoGo modes respectively.	500,000/500,000/ unlimited
SLB—maximum number of VIPs	For Transparent and Translational and GoGo modes respectively.	1000/1000/unlimited
SLB—maximum number of Pools	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of Nodes per Pool	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of physical servers per group	Applies to GoGo mode only; a group shares any number of common VIPs.	8
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—Users	Maximum number of SNMPv3 users.	32
SNMPv3—Groups	Maximum number of SNMPv3 groups.	64
SNMPv3—Accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—Communities	Maximum number of SNMPv3 communities.	64
SNMPv3—Target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—Target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—Notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—Filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—Filters	Maximum number of SNMPv3 notify filters.	400
Spanning Tree—maximum STPDs, Summit	Maximum number of Spanning Tree Domains.	128
Spanning Tree—maximum STPDs, Alpine	Maximum number of Spanning Tree Domains.	256
Spanning Tree—maximum STPDs, BlackDiamond	Maximum number of Spanning Tree Domains.	512
Spanning Tree—minimum STPDs	Minimum number of Spanning Tree Domains.	1
Spanning Tree—802.1d domains	Maximum number of 802.1d domains per port.	1

Table 8: Supported limits (continued)

Metric	Description	Limit
Spanning Tree—number of ports	Maximum number of ports that can participate in a single Spanning Tree Domain.	4096
Spanning Tree—minimum number of ports	Minimum number of ports that can participate in a single Spanning Tree Domain.	1
Spanning Tree—minimum number of domains/port	Minimum number of Spanning Tree Domains that can be configured per port.	1 for default VLAN, 0 for others
Spanning Tree—Spanning Tree modes	Maximum number of Spanning Tree modes per switch.	2 (dot1d and dot1w)
Static MAC FDB entries—Summit, Alpine, BlackDiamond	Maximum number of permanent MAC entries configured into the FDB.	1024
Super-VLAN—number of ports & sub-VLANs	Maximum number of ports and sub-VLANs associated with each super-VLAN.	2550
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
UDP profiles	Number of profiles that can be created for UDP forwarding.	10
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs—Summit, Alpine	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—BlackDiamond 6816 fully populated	Includes all VLANs plus sub VLANs, super VLANs, etc.	681
VLANs—BlackDiamond 6816 with up to 7 I/O modules	Includes all VLANs plus sub VLANs, super VLANs, etc.	1776
VLANs—BlackDiamond	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—maximum active protocol-sensitive filters	The number of simultaneously active protocol filters in the switch.	15
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4
VRRP—maximum VRIDs with bi-directional rate shaping	Maximum number of unique VRID numbers per switch when bi-directional rate shaping is enabled.	3
VRRP—maximum VRIDs/switch	Maximum number of VRIDs per switch.	64
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

4 Clarifications, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification, behaviors that might not be intuitive, and issues that have been resolved since the last release. Numbers in parentheses are for internal reference and can be ignored.

This chapter contains the following sections:

Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 7.1.1. For changes made in previous releases, see the release notes specific to the release.

System Related – All Systems

CAUTION

In order for configuration changes to be retained through a switch power cycle or reboot, you must use the save *command.*

Do Not Use a Port Number as a Display String

Do not use a port number as a display string. For example, if you assign the display string "4" to port 2:4 on a modular switch, you are unable to perform most configurations on ports in slot 4. If you assign the display string "4" to port 4 on a Summit switch, you are unable to perform most configurations on port 4. Changing the display string to an alphanumeric restores complete functionality (PD2-65114851, PD2-65114834).

The show log Command Truncates Long Commands

If you download a configuration, the output of the `show log` command might not completely display commands longer than 240 characters. This is a display problem; the configuration loads correctly (PD2-171470611).

The show log Display Truncates Configuration Parsing

If you download a configuration and use the `show log` command to view the parsing of the configuration, the log does not display the entire parsing. This is a display problem; the configuration parses and loads correctly (PD2-171470601).

Do Not Create Single-Character Names

When you create named components such as VLAN or access group names, do not use single character names. The single character might be interpreted by the switch as a truncated parameter. For example, if you name an SNMPv3 access group "a" and delete that access group using the `configure snmpv3 delete access a` command, the switch might interpret the command as `configure snmpv3 delete access all-non-default` (PD2-152594408).

Smart Redundancy Enabled in Saved Configuration

Smart redundancy is always enabled in a saved configuration. To work around this, disable smart redundancy after downloading a configuration (PD2-128133503).

Microsoft Load Balancing

When using Microsoft load balancing, if you replace existing hardware and use the same IP address on the new hardware (thus associating the same IP address with a new MAC address), IP traffic through the IPFDB is not forwarded. To work around this, manually clear the IPFDB (PD2-124851229).

Telnet and the show ports Command

If you telnet to the switch and use the `show ports info detail` command, the line feeds might not be recognized, resulting in output lines overwriting previous lines (PD2-130127501).

The show configuration Output

After using the `unconfigure switch all` command, the `show configuration` output displays the VLAN *default* without any ports assigned. The ports still belong to the VLAN *default*, as the `show vlan` output correctly displays (PD2-128233941).

Configure Slots or VLANs Before Uploading a Configuration

If you do not configure any slots or VLANs, upload the configuration, reboot the switch, and download the configuration, all ports are deleted from the default VLANs (PD2-110787427). The workaround is to configure slots or create a VLAN before you upload the configuration.

LACP not Supported

Contrary to the information in the *ExtremeWare 7.0 Software User Guide* and *ExtremeWare 7.0 Command Reference Guide*, LACP is not supported.

Upgrading to ExtremeWare 7.0 and Bi-Directional Rate Shaping

When you directly upgrade from ExtremeWare 6.2.2 to ExtremeWare 7.0, bi-directional rate shaping does not work if the loopback ports were in autonegotiation mode. This behavior is not displayed by 10/100Base-T or Gigabit fiber ports. A workaround is to remove and re-add the loopback ports to the VLAN (PD2-107820904).

Upgrading to ExtremeWare 7.0 and Debug-Trace

When you directly upgrade from ExtremeWare 6.2.2 to ExtremeWare 7.0, the debug-trace configuration might change. Verify the debug-trace configuration, if any, after upgrading. Use the `show debug-trace` command to display the configuration. You can either re-configure manually, or download the ExtremeWare 6.2.2 configuration instead of doing a direct upgrade (PD2-106733988).

Upgrading to ExtremeWare 7.0 and OSPF

If you upgrade directly from ExtremeWare 6.2.2 to ExtremeWare 7.0, the OSPF metric for 10 Gigabit interfaces is incorrect. A workaround is to manually configure the OSPF metrics, or to upload the configuration before upgrading and then download the ExtremeWare 6.2.2 configuration (PD2-108161623).

Blank Space in show port info detail Command Output

The output of the `show port info detail` command contains several blank pages. The output still contains all of the requested information (PD2-107800978).

Using an ExtremeWare 7.0 Configuration with an Earlier Image

If you are using an ExtremeWare 7.0 configuration and attempt to use an earlier image, the switch prompts you for confirmation (because this combination is not recommended). If you answer “n” at the prompt, you receive the following error message:

```
Error: bad image.
```

You can safely ignore this message (PD2-110983501).

Console Response with a Large Number of ARP Entries

Console response is slow when the switch is learning 10,000 or more ARP entries. This does not affect performance. Console response returns to normal when the entries are learned (PD2-104103941).

Configuring 1000Base-T Ports for 10,000 Mbps

The switch erroneously allows you to configure a 1000Base-T port to 10,000 Mbps. 1000Base-T ports do not support 10,000 Mbps (PD2-108463706).

The show log chronological Command

When the syslog contains more than 1,000 lines, the `show log chronological` command displays nothing. However, the command `show log` displays correctly (PD2-104062736).

BOOTP-Dependent Routes in Downloaded Configuration not Created

Static and default routes that depend on a BOOTP IP address / subnet are not created when you download a configuration (PD2-86888351).

The disable learning Command and Flooding

The disable learning command does not remove the port from the security flood list. Thus, you cannot disable flooding when learning is disabled (PD2-73199618).

Port Mirroring

Port mirroring is not supported across BlackDiamond modules (PD2-89313413).

Port mirroring is not supported with CPU-generated traffic (1-64H4J).

Port Tag Limitation

There is an absolute limit of 3552 port tags available in a system. The usage of these port tags depends on a combination of factors:

- Installed ATM, MPLS, ARM, and PoS modules
- Mirroring
- IPX routing
- Static FDB entries

If the switch reaches the limit of available port tags, the following messages appear in the syslog:

```
<WARN:HW> tNetTask: Reached maximum otp index allocation
<WARN:HW> tBGTask: Reached maximum otp index allocation
```

If this occurs, you must compromise some features (for example, mirroring) in order to expand your use of other functionality. (1-E5U7Y).

WinSCP2 Not Supported

The application WinSCP2.exe is not supported. Using WinSCP2 does not cause any problems (1-A5C6C).

BlackDiamond

Cross-Module Trunking Module Support

Table 9 lists the modules that support load-sharing across modules.

Table 9: Cross-module trunking module support

Module	CMT Support
G8Xi	Yes
G8Ti	Yes
G12SXi	Yes

Table 9: Cross-module trunking module support (continued)

Module	CMT Support
G16X[3]	Yes
G24T[3]	Yes
F32Fi	Yes
F48Ti	Yes
F96Ti	Yes
WDMi	No
10GLRi	Yes
MPLS	No
ARM	No
P3cMi	Yes
P3cSi	Yes
P12cMi	Yes
P12cSi	Yes
A3cMi	Yes
A3cSi	Yes

Cross module trunking is not supported on WDMi modules (PD2-176314520).

Cross-Module Trunking and Hitless Failover

For traffic load-shared across I/O modules, failover is not hitless; traffic loss occurs for approximately four seconds (PD2-186133901).

Master Slot Must Be Active for CMT

The slot with the master load-sharing port must be populated and active when you configure a cross-module load-sharing group. If the master slot is unavailable at configuration, cross-module load-sharing traffic is not forwarded (PD2-175825901, PD2-175854401).

MSM-3 Log Might Be Out of Chronological Order

Log events are stored independently on the master and slave MSM-3. Thus, a failover might cause the log to appear out of chronological order, or missing information. Concatenating the logs provides all log information (PD2-172852704).

Source Addresses Might Age Out of FDB

If a MAC source address is exclusively sourced on a slave CMT slot, such as with a port-based algorithm, the FDB entry might be aged out. To avoid this, use address-based load sharing on the neighbor switch (PD2-170942776).

Do Not Use Static FDB Entries with CMT

Do not use static FDB entries with CMT. If the CMT master fails, static FDB entries are not transferred to the group members (PD2-170942732, PD2-170942701).

Do Not Reboot Immediately After Synchronizing

Using the `reboot` command immediately after the `synchronize` command, but before the MSM's have finished synchronizing, might corrupt the configuration. To avoid this, wait for the MSM's to synchronize before rebooting. The "state" column in the output of the `show msm-failover` command displays "ready" when the synchronization is complete (PD2-171614101).

RSVP-TE Path Local End Point VLANs

If you specify a VLAN as the local end point for an RSVP-TE path, the switch allows you to change the VLAN's IP address, unconfigure the IP address, or delete the VLAN. No error message is generated. The path remains operational and traffic continues to be forwarded over the associated LSPs, but the current configuration is invalid. To avoid this, use the `show mpls rsvp-te path` command to verify the local end point configuration (PD2-164224901).

RSVP-TE End Point IP Addresses Are Not Verified

An invalid IP address can be configured when creating a new RSVP-TE path. The path might be established to an incorrect end point, causing traffic to be forwarded to the wrong destination. To work around this, use the `show mpls rsvp-te path` command to verify the end point IP address (PD2-162547301).

Saving Health Check Configuration After Failure Causes Console Crash

If an MSM fails a system health check with packet memory errors and is taken offline, the slave becomes the master, but you cannot save the configuration. To avoid this, clear the diagnostics, upload the configuration, and reboot the switch before saving (PD2-171914501).

Diagnostics on MSM-3 with Hitless Failover Causes Failover and Spurious Message

Running diagnostics on the master MSM-3 with hitless failover enabled causes the MSM-3 to fail over to the slave and log a hardware failure message. You can safely ignore this message (PD2-168317013).

Do Not Configure a Port-Based Backplane Algorithm When CMT is Enabled

Do not configure a port-based backplane policy when CMT is enabled. It might cause all egress ports on a given slot to be skipped. To work around this problem, configure an address-based backplane policy. In a similar manner, if a port-based algorithm is selected for the trunk, some egress ports might be skipped. To change the load share policy of a trunk, disable sharing for the port and enable sharing with an address-based policy (PD2-165883601).

Cross-Module Trunking and ACLs

Flooding on a CMT trunk cannot initally be blocked by ACLs. After the remote end responds with a PDU, the destination address is learned via source address learning. Once the address is learned, packets are blocked in hardware by an ACL (PD2-153404501, PD2-115139620, PD2-130299801, PD2-130299807).

ExtremeWare 7.0 (and Later) Does Not Support xmodem

You cannot use xmodem to transfer ExtremeWare 7.0 (or later) to an MSM (PD2-137101701).

4,000 VLANs on a BlackDiamond

If you configure more than 4,000 VLANs, EDP might crash, causing ESRP to fail (PD2-153821210).

E1 Module and the restart port Command

After you use the `restart port` command, E1 modules occasionally fail to establish a physical link (PD2-85857901).

PPP Links Through E1 modules

PPP links through the E1 module are not always re-established after a reboot. To re-establish the PPP link, use the `restart ports` command (PD2-109252301).

Slot Failure Messages During a Broadcast Storm

If you have more than 15 Gigabit Ethernet links between two chassis, all in the same VLAN and generating a broadcast storm, the system health check records slot failures in the log. When the broadcast storm stops, the log messages also stop (PD2-117946811).

No Image Information Reported to SNMP with One MSM

If you only install an MSM in slot B of a BlackDiamond 6804, BlackDiamond 6808, or BlackDiamond 6816, no primary or secondary image information is reported to your SNMP NMS (PD2-129612901).

BlackDiamond 6816 MSM C and D Diagnostics Messages not in Syslog

If you run diagnostics on an MSM in slot C or D of a BlackDiamond 6816, messages are not recorded in the syslog. To view the diagnostics messages, use the `show diagnostics` command (PD2-118049501).

Disabling CLI Paging from the Slave MSM64i

Enabling or disabling CLI paging from the slave MSM64i has no affect on the master MSM64i paging configuration (PD2-104377501).

Limited Commands Mode and the reboot Command

When the BlackDiamond 6816 is in limited commands mode, the `reboot` command does not reboot both MSM64i modules; instead the command causes the master MSM64i to fail over (PD2-107053801).

The unconfig switch all Command

If you use the `unconfig switch all` command and immediately use the `config default vlan delete port all` command, the switch reboots (PD2-105474401). To avoid this situation, after you unconfigure the switch, wait for the switch to completely reboot before you delete the ports.

Dynamic Memory Scanning and Mapping Module Support

BlackDiamond I/O module memory scanning and mapping support is listed in Table 10.

Table 10: Memory scanning and mapping support in BlackDiamond modules

Module	Memory Scanning and Mapping
F32Fi	Yes
F48Ti	Yes
F96Ti	Yes
G12SXi	Yes
G8Ti	Yes
G8Xi	Yes
WDMi	Yes
MSM-3	Yes
MSM64i	Yes

BlackDiamond 6816 MIB Value for Input Power Voltage

On the BlackDiamond 6816, the extremeInputPowerVoltage attribute in extremeSytemCommonInfo is shown as "0" and the extremePowerSupplyInputVoltage in the extremePowerSupplyTable is shown as "unknown." These values cannot be obtained from the switch (1-841J1).

Alpine

Limited Commands Mode

When in limited commands mode, the slot status LED remains orange, though the link is taken down (PD2-99107226).

VDSL Modules in a Half-Duplex Link

A VDSL CPE operating in a half-duplex link can lock up when used with a hub and running wire-rate randomized traffic. This is a hardware limitation. A restart of the VDSL port will recover, but if the traffic continues at wire-rate and is randomized, then the problem will reoccur (PD2-71538118).

Summit

Output of the show log Command

The most common reason for transceiver diagnostics failure is heat. Thus the `show log` output displays the TRXDIAG tag in the temperature log message (PD2-147462529).

The unconfigure switch all Command Clears the Default VLAN from s0

After you reset the switch to the factory defaults using the `unconfigure switch all` command, s0 does not contain the default VLAN. To add the default VLAN to s0, delete then add all ports in the default VLAN (PD2-143709201).

Health Check Error Messages

Error messages from the system health check display the incorrect location (PD2-110132842).

Limited Commands Mode

When in limited commands mode, links remain active (PD2-99220424).

Summit48i Redundant PHY

When the primary port of a redundant pair is disabled and the link removed, the LED for that port continues to flash indicating it has a link and is disabled (9239).

Summit48i Single Fiber Signal Loss

The Summit48i is currently not able to detect a single fiber strand signal loss due to the hardware based Auto Negotiation parameters (10995).

SNMP Results for Power Sources

The inputPower MIB is unable to differentiate between 110 VAC and 220 VAC input on the Summit series switches when accessing this MIB attribute through SNMP (10870).

Summit48si MIB value for Input Power Voltage

On the Summit48si, the extremeInputPowerVoltage attribute in extremeSytemCommonInfo is shown as "0" and the extremePowerSupplyInputVoltage in the extremePowerSupplyTable is shown as "unknown." These values cannot be obtained from the switch (1-841J1).

Command Line Interface (CLI)

SNMP Trap Commands Not Supported

The `disable snmp trap port-up-down port mgmt` and `enable snmp trap port-up-down port mgmt` commands are not supported by the CLI. To enable or disable SNMP port-up-down traps on the management port, use SNMP (PD2-162482918).

The show ports mgmt info Output Missing Flags

The output of the `show ports mgmt info` command does not display the flags (PD2-156475701).

Press [Return] Key Twice With enable temperature-log Command

You must press the [Return] key twice when entering the `enable temperature-log` command. If you only press the [Return] key once, the system does not display the asterisk indicating a configuration change. The log is correctly enabled by pressing the [Return] key once (PD2-152215201).

User Sessions Cannot Enable CLI Paging

You cannot enable CLI paging when logged in to a user account. It is enabled by default (PD2-145565305).

Only US Character Set Supported

The CLI supports only the US character set (2-H1OQC).

Switching and VLANs

Saving ip-mtu Settings

Dynamic TLS (Martini TLS) checks the MTU received from its peer in order for TLS to come to the established state. It compares against the egress VLAN's IP-MTU. If the egress VLAN does not have an IP address defined, any non-default ip-mtu setting will not be saved through a switch reboot (PD2-64084527).

VLAN priority and STP, EDP

STP and EDP (thus ESRP and EAPS) do not transmit packets in the queue specified by the VLAN priority (1-5HOZ9).

Default Routes or Static Routes

If you define a default or static route, and then delete the VLAN on the subnet associated with the default route, the default route entry remains although it is invalid. You must manually delete the configured route.

If you define multiple default routes, the one with the lowest metric is used. If there are multiple routes with the same lowest metric, the switch picks one of the routes.

Configuring a Protocol Filter with 'ffff'

Creating a protocol filter with LLC of value 0xffff and assigning it to a VLAN will not work, and should not be attempted. Doing so will assign all traffic to the VLANs containing that filter and will prevent VLANs with no protocol filter to function properly. If configured and saved, you must issue an `unconfigure switch all` to restore normal operation (2644, 4935).

Deleting Protocols from a VLAN

Adding a protocol to a VLAN may cause an EPC if the protocol was added to the VLAN, deleted from the VLAN, recreated by the user, and re-added to the VLAN (6128).

MAC Based VLANs and DHCP Relay

MAC based VLAN configurations should not be used in conjunction with DHCP. Currently, a host which enters a MAC-based VLAN will not be able to use DHCP to obtain an IP address.

VLAN to VLAN Access Profiles

VLAN to VLAN access profiles are no longer supported on the BlackDiamond switch in ExtremeWare 6.0 or higher (7022).

FDB

Duplicate Entry in show fdb Output

The output of the `show fdb` command displays a duplicate entry (PD2-127001501).

Cannot Add FDB Entry for Management VLAN

You cannot add an FDB entry for the management VLAN (PD2-156475718)

Static FDB Entries and Rate-Shaping

If you create a static FDB entry on a port configured for rate-shaping, the static entry incorrectly ages out. Static entries should not age out (PD2-97150551).

MAC Security

The source FDB address configuration will not discard ICMP packets (16340).

FDB Aging Timer

In ExtremeWare 6.2.0, the default value of the FDB aging timer was set to 1800 seconds on a newly configured ExtremeWare 6.2.0 switch. In ExtremeWare 6.2.1 the default value has been changed back to 300 seconds. However, when upgrading from ExtremeWare 6.2.0 to ExtremeWare 6.2.1, the default value will remain and 1800 seconds. For upgrades from ExtremeWare 6.1.9 (or earlier) the default value will remain 300 seconds. The FDB aging time can still be set to all previous values (1-85QD3).

Configure Less Than 400 Ports in a VLAN

If you use the `clear slot` command (which flushes the FDB) when there are 256,000 or more FDB entries, the watchdog timer can cause the switch to reboot. To avoid this, configure less than 400 ports in a VLAN (PD2-90223209).

Load Sharing

Autonegotiation

Load sharing ports must be configured with autonegotiation set to on. Load sharing ports will not transmit traffic correctly using any other setting (PD2-64617405).

Round Robin Load Sharing

If a port in a round robin load share group is removed, the traffic that was being transmitted on that link will be distributed on only 1 of the other active load share links in the round robin group. The traffic is not distributed evenly between the remaining ports (6977).

Port Based Load Sharing on Summit7i

Port-based load sharing on the Summit7i requires ingress ports to be on the same side of the switch (ports 1 - 4, 9 - 12, 17 - 20, and 25 - 28 on the left, ports 5 - 8, 13 - 16, and 21 - 24 on the right) as the 8 ports in the load share group for all ports in the load share group to transmit/receive traffic (6975).

Alpine and Cross Module Load Sharing

The I/O module configured to contain the “master” port must be physically present in a cross-module load sharing group for the system to pass traffic (8589, PD2-119098401).

Load Sharing and Specific Ports in a Load Share Group

Due to the load sharing algorithm used for round robin load sharing, when using 3, 5, 6 or 7 ports in a load share group packet loss will be observed when sending wire-speed traffic across the load share group. This occurs because some ports will be selected to transmit more packets than other ports resulting in bandwidth over-subscription and subsequent packet loss. This only occurs with round-robin load sharing configurations (10311).

Load Sharing, Software Redundant Ports, and Smart Redundancy

The smart redundancy feature is not supported when using software redundant ports and load sharing (12431).

Disabling Load Sharing if the Master is Down Generates Error

If the load sharing master link goes down, and you disable load sharing, the switch generates a ptag error message (PD2-129379272).

Mirroring

Do Not Configure Port Mirroring While Port is Down

If you reconfigure port mirroring while the physical port is down, switched traffic that crosses a routing boundary is duplicated (PD2-147476551).

Mirroring and Multicast

Mirroring might cause multicast processing to halt and report otpRamBusyWait failures in the log (PD2-133634301).

Mirroring IP Multicast Traffic

Due to IGMP Snooping capabilities, Multicast traffic may cease to be seen on a “mirror port”. If you issue a “restart” command for the mirror port or remove and reinsert the port connection, multicast traffic will resume for the IGMP Host time out period (260 sec) (3534).

Mirroring and Flooding

When a mirrored port is configured, the forwarding database for items being mirrored (e.g. ports or VLANs) are automatically cleared from the forwarding database if the link status on the mirror port changes. This will result in some temporary flooding until the normal learning process completes. Thus, removing or inserting a probe device into the mirror port may appear to cause flooding, however this is expected behavior (5128).

Spanning Tree

Disabling STP Might Display Topology Change

When you disable STP, the output of the `show stpd` command displays a topology change. If there was not actually a topology change, you can safely ignore this indicator (PD2-165211765).

802.1w Topology Change Might Cause FDB Flush of Edge Ports

802.1w topology changes might cause the FDB to flush and re-learn edge ports (PD2-161413529).

FDB Not Flushed After Link Failure with RSTP

When using RSTP, the FDB is not flushed when recovering from a link failure. This is the expected behavior (PD2-143730501).

Do Not Configure All Ports in s0

With all ports on several FM-32 modules in s0 and more than 256,000 FDB entries continuously learning, deleting a range of ports from a VLAN, adding the same range to another VLAN, deleting them from that VLAN, then adding them back to the first VLAN can cause a watchdog reboot. Do not configure all ports in s0 (PD2-118450167).

Error Messages with Topology Changes

If you have STP domains configured on a switch and add active ports to the domain, bringing the links up and down might generate error messages similar to the following (PD2-159834201):

```
<Erro:STP.OutBPDU.Drop> Port=4:13: Illegal message age (21)
```

The “C” Flag Might Be Permanently Set

Occasionally, after an STP topology change, the “C” flag in the output of the `show stp` command might be permanently set. To reset the flag, disable and re-enable STP (PD2-159151212).

Mirroring Does Not Mirror STP BPDUs

Mirroring does not mirror STP BPDUs (PD2-156960212).

Topology Change Counter Might Continuously Increment

After an STP topology change, the Number of Topology Changes counter in the output of the `show stp detail` command might continue to increment (PD2-156960201).

Topology Change Affects All Domains that Share Ports

If you configure the same physical ports on different STP domains, a topology change on one of the domains causes the FDB to flush for all domains sharing those physical ports (PD2-145439733).

Large STPD Configuration Download Might Reboot Switch

If you download a configuration with more than 70 STP domains, and each domain has more than 120 VLANs, the switch might reboot. To avoid this, disable the system watchdog timer, download the configuration, and enable the timer (PD2-136044092).

A Large STP Configuration with 10 Link Transitions

If you have more than 120 802.1w STPDs with more than 2,000 total VLANs, a link failover might form a loop. The loop might last as long as 40 seconds, depending on the number of VLANs configured (PD2-135691018).

Configure Fewer than 4,000 VLANs in an STPD

If you add more than 4,000 VLANs to an STP domain, the switch might run out of memory (PD2-135842818).

The show stpd ports Output Incorrect After Topology Change

Occasionally, after an 802.1w topology change, the flag in the output of the `show stpd ports` command still displays `TC` (PD2-115121007).

802.1w and IGMP Snooping

If you are using 802.1w and IGMP snooping, an 802.1w topology change can interrupt the multicast stream for up to 125 seconds by default (PD2-118511373).

Output of show stpName port detail Command in Hex Format

The output of the `show stpName port detail` command displays the `PortID` in hex format instead of decimal format. If you do not specify the `detail` parameter, the output correctly displays in decimal format (PD2-136044001).

Do Not Re-use VLAN Tags

When you delete a VLAN, the tag is not deleted from the STP domain. If you create a new VLAN with the same tag, you cannot add that VLAN to a different STP domain. You must either add the VLAN to the STP domain associated with the tag, or delete the STP domain associated with the tag, create a new STP domain, and add the VLAN to new STP domain. To avoid this, do not use the same tag (PD2-137137230).

Ensure that a VLAN Contains Active Ports

Before you add a VLAN to an STP domain, ensure that the VLAN contains active ports. Otherwise you must disable STP, remove the VLAN from the STP domain, add the ports to the VLAN, add the VLAN to the STP domain, and enable STP (PD2-137137236).

If You Delete a Port from the STPD, You Cannot Add It Through a VLAN

If you delete a port from the STPD, then add a VLAN containing that port to the STPD, the deleted port is not added. To work around this, add the port back to the STPD (PD2-144382901).

The unconfigure stp Command Does Not Clear All Configurations

The `unconfigure stpd` command does not clear the tag, VLAN, operational mode, rapid root failover, port mode, or port link-type. To clear these configurations, use the `delete stpd` command (PD2-137310575).

Enabling ignore-bpdu or ignore-stp

If you enable ignore-bpdu or ignore-stp on a VLAN and then enable STP, the switch still participates in STP election. To work around this, reboot the switch (PD2-140533593).

High Traffic with 120 STP Instances

If you configure more than 120 STP instances and more than 130 VLANs, and lose a link while forwarding a high traffic load, the port might be unstable (PD2-118500801).

Configuring a VLAN from Vista

If you create an STPD using ExtremeWare 6.1.9 (or earlier), add a VLAN, save the configuration, upgrade to ExtremeWare 6.2.2b68 (or later), and save the configuration, you receive the following error message when you try to modify the VLAN from Vista:

```
ERROR: Cannot assign bridge to stpd! HINT: If a port is part of multiple vlans, the vlans must be in the same Spanning Tree domain.
```

To work around this problem, make configuration changes from the CLI (PD2-118450190).

STP and VLAN Tagging

VLAN tagging is not supported with 802.1d Spanning Tree (STP) BPDUs. Therefore, all BPDUs in a 802.1d STP domain are untagged. However, Extreme Multiple Instance Spanning Tree (EMISTP) and Per-VLAN Spanning Tree (PVST+) do support VLAN tagging of BPDUs.

EMISTP and Ingress Rate Shaping

If a loop exists in your network, but STP is not enabled and Ingress Rate Shaping is, the switches appear to hang and are rebooted by the watch-dog timer. A similar situation exists if a loop is covered by STP on both sides and is disabled on one side; normally the other switch immediately blocks the right port(s), but when Ingress Rate Shaping is present, both switches appear to hang and are rebooted by the watch-dog timer (1-5E9R1).

Upgrading From an ExtremeWare 6.1.9 (or earlier) Configuration

After downloading an ExtremeWare 6.1.9 (or earlier) configuration to an ExtremeWare 6.2.0 (or later) image, a port belonging to a non-default VLAN generates the “Stpd s0, Port 1:1 does not exist” error message because that VLAN does not belong to domain s0 by default (1-BMP5D).

ESRP

The disable slot all Command Generates EDP Errors

If you have ESRP enabled, the `disable slot all` command generates EDP errors. You can safely ignore the error messages (PD2-166105101).

Environmental Tracking on a Chassis with One PSU

If you enable environmental tracking on a BlackDiamond with only one PSU installed, tracking fails. This is by design (PD2-147052232).

Large Configurations Might Lock Console when Enabling and Disabling s0

If you have more than 60 STP domains with more than 200 tagged VLANs between them and more than 6 ports in each, and you enable then immediately disable s0, the console might freeze for up to a minute. Larger networks cause the console to remain locked for longer periods. The switch is still

operating, and the console unlocks after the processing finishes. To work around this, either wait before disabling s0, or wait until the console unlocks (PD2-159834277, PD2-151426418).

Failure of Direct Link Causes Flip

If you have a direct link between the master and slave switch, and that link fails, the master transitions to slave and back to master. To avoid this, configure both load-sharing links to don't count (PD2-157406636, PD2-148539301).

ESRP and Ingress Rate Shaping

Do not use ingress rate shaping on an ESRP-enabled port (PD2-107800933).

ESRP and Protocol-Based VLANs

ESRP-aware switches cannot connect to an ESRP switch through a port configured for a protocol-sensitive VLAN using untagged traffic (PD2-99007701).

ESRP and Load Sharing

If you enable load sharing on ports that belong to more than 200 VLANs, the switch reboots. To avoid this, first enable load sharing, then add the ports to the VLANs (PD2-99259801).

When using load sharing with the ESRP host attach or don't count features, configure *all* ports in the same load-sharing group as host attach ports or don't-count ports (PD2-97342427, PD2-106782876).

Hot-Swapping a Module with 5,000 ACLs

Hot-swapping a module on a switch that has 5,000 or more ACLs configured can cause an ESRP state change (PD2-107800998, PD2-103938301). To avoid the state change, configure the neighbor timeout value to 12 seconds.

Traffic Convergence Time

Traffic convergence after a link failure can take as long as 5 seconds with 2,000 VLANs and 256,000 FDB entries. This delay can cause ESRP state changes as traffic converges (PD2-89915300).

ESRP PDUs on Ports

ESRP PDUs received on ports that do not belong to any VLAN are processed as valid ESRP PDUs and can trigger state changes (PD2-89481346). To avoid this, assign all ports to valid VLANs with matching tags.

Multiple ESRP VLANs

If multiple ESRP VLANs share a host port, each VLAN must be in a different ESRP group.

ELRP

ELRP and Ingress Rate Shaping

Do not use ingress rate shaping on an ELRP-enabled VLAN (PD2-133066184).

VRRP

Backup Transition Creates Duplicate Packets

A VRRP transition from backup to master might cause duplicate data packets to be transmitted for a short period of time. The packets are dropped, so no action is required (PD2-129379226).

QoS

Duplicate Precedence Rules

If you create an ACL rule with the same precedence as an existing rule, an error message warns you of the duplication. However, the rule is still created. You must delete the rule with the duplicate precedence and recreate it with a unique precedence (PD2-116540055).

The qosprofile Accepts a Value Greater than 100%

The `maxbw` parameter in the `configure qosprofile` command incorrectly accepts values greater than 100%; however, the maximum bandwidth is still 100% (PD2-123662004).

Re-Ordering Access List Precedence Numbers

When you add a new ACL rule with a precedence number, the switch re-orders existing rules with lower precedence numbers to make room for the new rule. If, during this re-ordering, two rules have a precedence number difference greater than one, the switch generates an error message similar to the following:

```
<WARN:KERN> Access rule does not exist
```

You can safely ignore this error message (1-FAO8M).

Access List FDB Entries not Cleaned Up

If you delete an access list with the “f” flag (flow rule), the associated FDB entries might not be cleared (PD2-110082518).

Access Lists Using the IP Deny Any Rule

When using an access control list with an IP deny any rule, all ICMP traffic will be blocked within a VLAN (Layer 2). If using an access list with an IP deny any rule across VLANs (Layer 3), ICMP traffic will not be blocked.

Access Lists and IP Fragmentation

When using IP fragmentation, since the TCP header is treated as data and only the IP header information is being replicated in each packet, access-lists that apply to that flow will not apply as the TCP/USP port information is not included after the first fragment (for subsequent fragments).

QoS Configuration Bandwidth Parameters

Minimum and maximum percentage parameters for a specific port on the default VLAN will not be saved across reboots. The configuration change will be applied when configured. This issue only occurs on the BlackDiamond (15500).

Creating Access Lists from Multiple Sessions

When creating or modifying access control lists, please ensure that no other administrator sessions are attempting to create or modify the system access control lists simultaneously. This may result in data corruption (1-579HD).

5,120 Access Lists and SNMP

Although you can configure up to 5,120 ACLs, SNMP only recognizes 1,280. Deleting an ACL that is not recognized by SNMP generates the following error (PD2-64880917):

```
<WARN:SNMP> SNMP IPQOS Could not find entry instance 5083 to delete
```

Monitoring QoS and the show port qos Command

When monitoring QoS, do not use the `show port qos` and `enable qosmonitor` commands on the same port at the same time. These commands in conjunction lock the console session. However, the syslog does capture the output (PD2-64202681, PD2-80836531).

Bi-Directional Rate Shaping

Locking and Unlocking Learning

If you configure a rate shaping port to lock learning and unlock learning, the loopback FDB is not flushed. This causes traffic destined for the port to be flooded. You must manually flush the FDB using the `clear fdb` command (PD2-124568416).

Loopback Port Must be on Same Module

The loopback port must be on the same module as the rate shaped ports. Though you can configure a loopback port on another module, this is still not a supported configuration (PD2-124299901).

1000Base-T Ports as Loopback Ports

If the loopback port for bi-directional rate shaping configurations is configured on 1000Base-T ports, the speed of that port cannot be changed from 1000 Mbps to 100 Mbps as the bandwidth settings will not be accurate when configured in 100 Mbps mode.

EAPS

Do Not Configure a Hello Time of 0

Though the minimum hello time is 1, the switch accepts a hello time of 0. Do not configure the hello time to 0, as this effectively disables EAPS (PD2-119139425).

EAPS Performance Statistics

Table 11 lists the EAPS performance statistics for a single EAPS domain with the default filter.

Table 11: EAPS performance statistics with the default filter

Protected VLANs	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
1	106	101	100	99
500	260	220	170	130
1,000	310	220	170	227
4,000	534	533	675	900

Table 12 lists the EAPS performance statistics for a single EAPS domain with no filters.

Table 12: EAPS performance statistics with no filters

Protected VLANs	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
1	1.9	1.8	1	1
500	54	54	70	100
1,000	106	106	170	226
4,000	415	415	675	900

Table 13 lists the EAPS performance statistics for a single EAPS domain with a single protected VLAN and varying FDB sizes.

Table 13: EAPS performance statistics with varying FDB sizes

FDB Entries	Link Down Convergence Upstream (ms)	Link Down Convergence Downstream (ms)	Link Up Convergence Upstream (ms)	Link Up Convergence Downstream (ms)
2,000	2.4	3.2	1.1	1.2
10,000	2.5	3.5	1.3	1.4
50,000	4	5	2.8	3
100,000	5	6	4	4

ESRP and EAPS Secondary Port

Configuring ESRP Host Attach on an EAPS secondary port causes a broadcast storm (1-B1O4L).

Incorrect show vlan Output

The `show vlan` output incorrectly lists the EAPS secondary port as active with an asterisk (*). The number of active ports is correctly displayed (PD2-59142420).

IP Unicast Routing

Multinetting Enabled by Default

Multinetting is enabled by default (PD2-129703201).

Reset the FDB Aging Timer

When you disable multinetting, you must reset the FDB aging timer to 300 seconds using the `configure fdb agingtime` command (PD2-160697401).

Deleting a Static Entry Using SNMP

If you delete a static IPARP entry using SNMP, the line in the configuration creating that entry is not deleted. Thus, if you reboot, the static entry is again created. To work around this, either edit the configuration or delete static IPARP entries through a direct connection to the switch (PD2-130505418).

The show iproute Output

The output of the show iproute command displays only the first 8 characters of the VLAN name (PD2-128392829).

Traffic Crosses Layer 3 Boundary

If ingress and egress VLANs do not share a port, layer 3 traffic with a broadcast MAC and unicast IP address is incorrectly forwarded to the default route across a layer 3 boundary (PD2-119375325).

No Static ARP Entries

The use of Static ARP entries associated with superVLANs or sub-VLANs is not supported in this release (5106).

ARP Entry Age

The age of ARP entries changes to a large value when system time is changed (1-E7FIV).

Multinetting and the Show VLAN Stats Command

The `show vlan stats <vlan_name>` command is not supported on multinetted VLANs (12196).

Multinetting and VRRP

Multinetting is not supported with VRRP (1-9YG1B).

RIP Routing

RIPv2 Authentication

The authentication feature of RIPv2 is not supported.

RIP in Conjunction with other Routing Protocols

It is recommended that RIP be enabled only on routers running with less than 10,000 routes from other routing protocols, such as BGP or OSPF.

OSPF

AS-external LSAs Might Not Be Regenerated

AS-external LSAs are not regenerated after an active LSA is removed or a neighbor goes down (PD2-149426154).

Do Not Enable originate-router-id when Router ID

Do not enable the OSPF originate-router-id feature when a loopback with the OSPF router ID is configured (PD2-151536301).

Error Message Not Generated

If you configure a low ase-limit with a lot of type-5 LSAs, enabling OSPF causes a database overflow state before OSPF adjacency is built. This should generate a critical error message, but does not (PD2-148164866).

Routes not Installed with Duplicate LSAs

When there are duplicate LSAs in the LSDB from different advertising switches, the route might not be installed in the kernel routing table. To work around this, disable and enable OSPF (PD2-132370484).

Disable OSPF Before Adding or Removing External Area Filters

If you configure an OSPF area external filter on an ABR, and the filter is set to exclude routes that have already been learned, an OSPF failure occurs. A workaround is to disable OSPF before adding or removing OSPF external area filters (PD2-105170634).

IS-IS

Unicast Packets Considered Broadcast

Unicast packets are occasionally considered broadcast packets and dropped (PD2-142499344).

BGP

Large Number of Access Profiles and a Peer Reset

You can add a maximum of 10 BGP community numbers in inbound and/or outbound route updates using access-profiles and/or route-maps. If you add more communities, BGP might crash (PD2-160136950).

Default Route Might Not Be Deleted

If you have the export of static BGP routes enabled, the IP route table has a default static route and BGP is redistributing the default route using the `configure bgp add network` command, then after you delete the default route from BGP using the `configure bgp delete network` command, the default BGP route is not withdrawn from the neighbor's table (PD2-159150038).

BGP Aggregation with a Maximum Prefix of 300,000

Disabling BGP, configuring the maximum prefix to 300,000 or more, enabling BGP aggregation, configuring some aggregate routes, and enabling BGP generates error messages similar to the following (PD2-147347223):

```
<Erro:BGP.Misc.DelAggrtNetErr> Count lost sync for Net 202.7.243.0 Mask 255.255.255.0
```

BGP Loops

If a switch detects a BGP route loop (receives a route with self as the NextHop), it tears down the link to the neighbor that forwarded the route. To avoid this, disable and re-enable BGP (PD2-99209507).

Redistributing BGP Routes to OSPF

Redistributing 70,000 or more BGP routes into OSPF depletes the system resources and the switch might run out of memory, causing task exceptions. Do not redistribute 70,000 or more BGP routes into OSPF (PD2-74932501).

IP Multicast Routing

The unconfigure igmp Command Does Not Unconfigure All Parameters

The `unconfigure igmp` command does not set the `forward-mcrouter-only` or `flood-list` parameters to the default values (PD2-141266115).

Enable or Disable IGMP Snooping on a Sub-VLAN

To disable or enable IGMP snooping on a sub-VLAN, delete the sub-VLAN from the super-VLAN, change the IGMP snooping status, and add the sub-VLAN to the super-VLAN (PD2-136478101).

First Query has Incorrect MAX Response Field

The first query sent in response to a leave message has the MAX response field set to 100, instead of the value in the last member query (PD2-134719211).

Do Not Disable IGMP Snooping with Static Snooping Entries

If you disable IGMP snooping on a VLAN, the configured static IGMP snooping entries do not reply to the IGMP querier, while real hosts attached to the VLAN will (PD2-158477713).

(S,G) Entry Not Created if RP is Rebooted

An (S,G) entry is not created if the RP is rebooted (1-F4YIP).

Cisco Interoperation

For proper Cisco interoperation, use Cisco IOS version 11.3 or better, which supports PIM 2.0. Cisco customer support also recommends using PIM in favor of DVMRP whenever possible on Cisco routers (4669).

Traffic Rate Exceeding Last Hop Threshold

When the traffic rate exceeds the configured last hop threshold, the last hop does not initialize; but if the sending traffic rate is set to 50 Kbps, it switches to STP correctly (1-57NMY).

Security and Access Policies

EAP-Failure Messages Not Sent When Client is Unauthenticated by an Administrator

If an 802.1x supplicant MAC is forced into the unauthenticated state by an administrator, an EAP-Failure message is not sent to the client. Using the `clear netlogin state`, `disable port`, or `restart port` commands can force the client into the unauthenticated state. If this happens, the client is not authenticated, but some 802.1x client applications appear to be authenticated and can cause confusion in troubleshooting. This problem does not occur if the client logs off (PD2-160278605).

Logout Privilege is Enabled in Downloaded Configurations

If you configure web-based network login with the session refresh feature enabled and the logout privilege feature disabled, then download the configuration, the logout privilege feature is automatically enabled. To work around this, download the configuration and manually disable logout privilege (PD2-160278607).

Do Not Upload a Configuration Containing Authenticated Clients

In network login campus mode, do not save and upload a configuration containing authenticated clients. Doing so can corrupt the configuration. To back up a configuration:

1. Disable network login using the `disable netlogin` command.
2. Unauthenticate all client ports using the `clear netlogin state ports vlan` command.
3. Verify that all ports are unauthenticated using the `show netlogin` and `show vlan` commands.
4. Save the configuration using the `save configuration` command.
5. Upload the configuration to your backup server using the `upload configuration` command.

When you download this configuration, remember to enable network login (PD2-142190901).

The show netlogin Output Might Display Wrong Authentication

If you disable network login, the output of the `show netlogin` command incorrectly displays all existing authenticated 802.1x clients as HTTP. If you enable network login again, the display corrects. This is cosmetic, and does not affect the actual authentication (PD2-171477134).

ICMP Access Lists and ignore-overlap

The ignore-overlap feature is not supported with ICMP access lists. Use precedence to manage overlapping. If you specify `ignore-overlap` when you create an ICMP access list but do not specify a precedence number, a precedence of 0 is assigned. In addition, the ICMP access list gives the highest

precedence to the rules created first, instead of giving precedence to the most specific rule (PD2-157416614).

CPU DoS Protect and ACL Precedence

If you configure the CPU DoS protect feature with a filter precedence of x, you cannot create an access list with a precedence of x, x+1, or x+2. All other values are acceptable.

If you configure an access list with a precedence of x, you cannot configure the CPU DoS protect feature with a filter precedence of x, x-1 or x-2. All other values are acceptable (PD2-129163428).

MSM Failover Clears Logins

An MSM failover clears the Network Login state, forcing users to log in again (PD2-109075331).

Network Login RADIUS Server Interoperability

The following RADIUS authentication servers are tested and supported with Network Login:

- Microsoft Windows 2000 Internet Authentication Service
- Funk Steel-Belted-Radius Enterprise Edition version 4.0

The following authentication methods are supported with Network Login:

- PAP (web-based only)
- EAP-MD5 (802.1x only)
- EAP-TLS (802.1x only)
- EAP-TTLS (802.1x only)
- PEAP (802.1x only)

Network Login Supplicant Software Interoperability

The following supplicant software applications are tested and supported with Network Login:

- Web-Based: Internet Explorer 6 web browser
- Web-Based: Netscape Navigator 7 web browser
- 802.1x: Microsoft Windows XP native OS client
- 802.1x: Microsoft Windows 2000 Professional native OS client (patch 313664)
- 802.1x: Funk Odyssey Client, version 2.0
- 802.1x: MeetingHouse Data AEGIS Client for Windows, version 2.0.5
- 802.1x: MeetingHouse Data AEGIS for Windows, version 1.3.6.1
- 802.1x: MeetingHouse Data AEGIS for Linux, version 1.1.2

RADIUS and the BlackDiamond

When RADIUS authentication is configured on a BlackDiamond switch, upon reboot, you will see the following message indicating that the system is initializing before authentication messages will be transmitted to the configured RADIUS server(s) (7046):

```
“Warning: Radius is going to take one minute to initialize.”
```

RADIUS and Telnet

If one of the following two situations occurs:

1. You have a single RADIUS server configured with a RADIUS timeout value of 10 seconds or more
2. Both primary and secondary RADIUS servers lose their connections and the configured RADIUS timeout value is 5 seconds or more

The switch might not be able to fail over to the local user authentication for telnet sessions. If this happens, the switch cannot be accessed via telnet. This does not occur with the default RADIUS timeout configuration of 3 seconds, or when using alternate session types such as console, SSH, or Vista management (PD2-109828821).

The show netlogin Command Output

If you remove a module with configured Network Login ports and reboot the switch, the output of the `show netlogin` command incorrectly omits the configured ports. Network Login remains enabled on the configured ports and operates correctly if you reinstall the module (PD2-92593101).

SLB and Flow Redirection

Do Not Specify a Port Number in the disable slb node Command

If you specify a port number in the `disable slb node` command, the CLI automatically chooses the `tcp-port-check` option. To avoid this, use one of the well known port names (PD2-160291501).

Enumeration Mode Redirects ICMP Packets

When you create a flow redirection rule for source address based on a subnet mask of /24, enumeration mode is selected, and all ICMP packets are redirected to the next hop. To work around this, use a subnet mask of /16 (PD2-118471863).

Cache Servers Set To “Down” Under Sustained High Traffic Loads

Under very high sustained loads flow redirection might fail and set a cache server to the “down” state and then bring it back up. This only occurs during high loads for a duration of more than 2 minutes. The server will come back up immediately; however, during that time connections that were established might be dropped due to a flushing of the associated IP forwarding database entries. A “down” state is depicted in the log with the following message:

```
09/01/2000 10:51.56 <INFO:IPRT> redirect next hop test <ip_addr> changed to down
```

Health Checking Cannot be Disabled

Flow redirection health checking of the next hop address is turned on by default and cannot be disabled.

NAT

If you change the name of a VLAN that is part of your NAT configuration, the NAT rule configuration is not updated. NAT rule matching continues to operate correctly, but if you save or upload the configuration, the rule is saved or uploaded incorrectly (PD2-82963707).

Vista

Cannot Enable STP

You cannot enable a STP domain using Vista. If you try, Vista does not generate an error message, but does not enable STP. (PD2-158471801).

Alpine 3808 Erroneously Displays Four PSUs

Vista displays PSU C and PSU D on an Alpine 3808 chassis. The Alpine 3808 supports only two PSUs, PSU A and PSU B (PD2-135911601)

Cannot Add Trap Receiver or Community String

On the SNMP configuration page, if you add a trap receiver or community string Vista indicates success, but does not make the change to the switch. To successfully add a trap receiver or community string, use the CLI (PD2-120713201).

VLAN Ports Tagging Information Incorrect

In the Virtual LAN Configuration screen, the information for VLAN ports displays incorrect tagging information (PD2-130140999).

Blackhole Flag Missing

The blackhole flag is missing from the FDB statistics screen (PD2-129387401).

Multicast Address Display

If you configure a routing protocol on multiple interfaces, the Vista statistics page displays the wrong Locally Registered Multicast Address (PD2-105094265).

Configuration Statistics PSU Display

The Vista configuration statistics switch display for the BlackDiamond 6808 shows four power supplies when only two are installed (1-D3RSP).

Closing Internet Explorer 4.0

IE 4.0 caches user login information. In some environments, this can be a security issue. As a work-around, it is best to close the browser after logging out of the switch (1873, 1994).

Vista and RADIUS

If a switch configured for RADIUS authentication loses communication with the RADIUS server, subsequent attempts to use the Vista Web application will take a very long time (measured in several minutes). When communication is lost with the RADIUS server, Vista will continue to make authentication requests for every page. Each request has a timer that will expire leading to an excessive amount of time to bring up each page (5144).

Configuration Options with Large Number of Interfaces

When selecting a configuration applet with a large number of configured interfaces, the traversal of the VLAN interfaces by Vista can cause a Watchdog reset due to the task utilization of Vista during the interface data collection. It is recommended that Vista not be used for configurations with Watchdog enabled where the Vista Configuration applet is used with a large number of VLAN interfaces.

SNMP

The trapDestOwner is Required in the trapDestTable

ExtremeWare 7.1 (and later) requires the trapDestOwner in the trapDestTable to send the community, address, owner, and status in the create request for the trapreceiver entry through SNMP (PD2-126200001).

Cannot Delete Default Community Strings

You cannot delete the default community strings (*public* and *private*) using the `configure snmpv3 delete community` command. To delete these strings, use the `configure snmp delete community` command (PD2-153687501).

Do Not Configure an SNMPv3 Community String with more than 32 Characters

You cannot configure an SNMPv3 community string with more than 32 characters. If you download a configuration containing such a string, that line in the configuration fails, returning the following error message to the console (PD2-150132207):

```
ERROR : SNMPV3 Community Creation Failed
```

The rest of the configuration loads correctly.

Modular Switch get Error

A get request from an NMS to a modular switch for the ifMau<object> on the management port returns a “no such instance” error (PD2-124250702).

SNMP v1 Traps

SNMP v1 traps for link up and link down are not supported. ExtremeWare uses SNMP v2 traps (PD2-110113025).

SNMP and ACLs

Polling the ACL table with a network manager can cause high CPU utilization. For example, with 1,000 ACLs, CPU utilization could be as high as 95%, which could make the console unresponsive (PD2-57475201).

Incrementing the Interface Value

With a getnext or bulkget on a non-existent ifIndex of an object ID, the agent returns next OID value instead of incrementing the ifIndex (2-H1OOF, 2-GZ52P).

SNMP ifAdminStatus MIB Value

The SNMP ifAdminStatus MIB value is not saved after a reboot. Ports set to down in the SNMP ifAdminStatus MIB come back up after rebooting. However, if you save the configuration using the CLI or SNMP after changing the port status to down in the ifAdminStatus MIB, the change is saved after a reboot (2-GOQMD).

Trap Receivers as Broadcast Entry

Although it is possible to enter a broadcast or IP multicast address as an SNMP trap receiver, it will not function (2545).

Bridge MIB Attributes

The IEEE Bridge MIB dot1dTpPortEntry PortInDiscards and dot1dBasePortEntry counters do not increment (4937).

SNMP Time-out Setting

SNMP management stations may need to set the SNMP time-out value to 10 seconds as some large configuration operations take longer to perform (7151).

In addition, when using SNMP tools that use the bulk get request function as opposed to generic get next requests, the MIB walk can time out and subsequently fail with the default time-out setting. It is suggested that the default time-out value be increased from 5 seconds to 60 seconds to decrease the frequency of such time-outs when the get bulk request contains a large number of entries (9592).

SNMP Access Profile

The access profile for SNMP read-only or SNMP read-write can be used for permit-mode only, deny-mode is not operational (7153).

SNMP and Auto-negotiation Settings

For 100/1000Base-TX ports, the ifMauAutoNegAdminStatus can only be disabled if the ifMauDefaultType is set to a speed of 100 Mbps. For 10/100Base-TX ports, you must first set the value of ifMauDefaultType to the correct setting before disabling the ifMauAutoNegAdminStatus (9416).

SNMP and the FDB MIB

When exercising the route table in the FDB MIB with dot1dTpFdbTable enabled, high CPU utilization messages might be displayed in the syslog (PD2-102926801). This occurs when there is a large number of FDB entries and has no adverse affects on protocol stability.

Extreme Fan Traps

The `extremeFanOK` and `extremeFanFailed` traps will contain the `extremeFanNumber` indicating which fan has failed (1-7J571).

Extreme Power Supply Traps

A new object was added “extremePowerSupplyNumber” to the power supply traps. The two RPS traps will no longer be sent out. Instead the extremePowerSupplyGood and extremePowerSupplyFail traps will contain the power supply number indicating which power supply has failed (1-7J56T).

DHCP

The DHCP server is not supported as a standalone feature. It is used as part of the Network Login feature only (1-8SAI6).

Diagnostics and Troubleshooting

Event Condition Command Completion

If you enter an event condition using the `show log events` command, press the [Tab] key for command completion, the console displays an “Ambiguous token” message even though the event condition exists. This occurs when there are additional conditions that also match your entry. If you press [Return], the correct log is displayed. For example, if you enter `show log events BGP.Damp.Cfgchg` and press [Tab], the console displays the following (PD2-153433301):

```
Ambiguous token: BGP.Dampening.CfgChg
        <event condition>
          "BGP.Dampening.CfgChg", "BGP.Dampening.CfgChgNullDinfo",
          "BGP.Dampening.CfgChgNullNew", "BGP.Dampening.CfgChgNullOld",
          "BGP.Dampening.CfgChgRt"
```

Entering q Does Not Quit Diagnostics Display

Entering `q` to quit the `show diagnostics sys-health-check` display does not quit the display (PD2-145117543).

Single MSM Not Taken Offline

If you have only one MSM installed in a BlackDiamond chassis, you configure the system health check alarm level to `card-down`, and eight errors are detected, the MSM is not taken offline. The MSM remains fully operational (PD2-143167301).

Automatic Memory Scanning Can Trigger Incorrect Reboot Loop Detection

On Summit and Alpine switches, if memory scanning is automatically initiated via the `auto-recovery` parameter in the `configure sys-health-check` command and the reboot loop detection threshold is 1, the system might incorrectly detect a reboot loop and come up in minimal mode (PD2-140185601).

Packet Diagnostics Display Backplane Incorrectly

When you run packet diagnostics on the Alpine 3804, the console displays the backplane as slot 5. The display is wrong: the diagnostics are correctly running on the backplane. The extended diagnostics console display is correct (PD2-151752701).

Packet Diagnostics Display Wrong Slot Name

When you run packet diagnostics on the MSM in slot B, the console displays the slot as slot 10, instead of MSM-B. The display is wrong: the diagnostics are correctly running on the MSM in slot B. The extended diagnostics console display is correct (PD2-138607801).

Bus-Stats Error Messages

The `show config detail` command output displays the following new commands:

```
disable bus-stats
configure bus-stats window history 3
configure bus-stats window errors 3
configure bus-stats threshold slow-path x
configure bus-stats threshold fast-path y
```

The bus-stats feature helps filter erroneous log messages related to transient hardware errors. It is disabled by default and should only be enabled when troubleshooting transient hardware errors. Enabling this feature requires activation by Extreme Networks personnel.

Spurious Message When system-down is Configured

If you configure the system health check alarm level for system-down and a fault is detected, the switch is turned off but continuously logs the message “Card in slot N is off line.” You can ignore this message (PD2-129386201).

The use configuration Command

When the switch is in minimum mode, the `use configuration` command has no effect on the backup MSM (PD2-129133801).

Output of the show diagnostics Command

The output of the `show diagnostics` command for the CPU system might display negative numbers, and the totals might not add up properly (PD2-128460401).

Configure Auto-Recovery to online or Alarm-Level to traps

If you configure the system health check auto-recovery to `offline`, save the configuration, and configure the alarm-level to `log`, a health check brings the module or switch offline regardless of how many errors the health check detects. To avoid this, either configure auto-recovery to `online`, or configure alarm-level to `traps` (PD2-124368101).

Error Count Not Accurate

If the switch is flooded with heavy traffic for more than 10 minutes, the `CPU System` field in the `show diagnostics` output is not accurate. The display reports up to 20 more errors (PD2-122738701).

Configuring Diagnostics Mode Off

If you configure diagnostics mode OFF, and then execute the `unconfigure switch all` command, when the switch returns to active state the diagnostics mode is still set to OFF. The default diagnostics mode should be `fastpost`. To verify which diagnostics mode is set for the switch, use the `show switch` command (1-97NL1).

Disable Remote Syslog Before Enabling IPARP Debug-Tracing

With remote syslog enabled, if you configure the IPARP debug-trace to level 2 or higher, the switch hangs and is rebooted by the watchdog timer. To avoid this, disable the remote syslog prior to configuring the debug-trace (PD2-110983505).

Documentation

Summit48si LED Behavior Not Correct

The Summit48si LED behavior described in the *Consolidated Hardware Guide* is not correct (PD2-170120478). The actual LED behavior is:

- Green: link is present , port is enabled
- Green blinking: frames are being transmitted and/or received on this port
- Off: link is not present or port is disabled

T-Control Requires Full Layer 3 License

Though not mentioned in the Software Licensing section, the T-control feature does require a full layer 3 license.

Issues Resolved in ExtremeWare 7.1.1b11

The following issues were resolved in ExtremeWare 7.1.1b11. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.1.1b11 includes all fixes up to and including ExtremeWare 6.2.2b108 and ExtremeWare 7.0.1b11. For information on those fixes, see the release notes for those releases.

BlackDiamond

Hitless failover is now supported with the 10GLRi I/O module (PD2-178533101, PD2-176314518).

Hitless failover is now supported on the A3cMi, A3cSi, P3cMi, P3cSi, P12cMi, and P12cSi modules (PD2-178533103).

If you unconfigure hitless failover, you are not required to save the configuration and reboot the switch for this to take effect (PD2-178533105).

If you use the address-based algorithm for a CMT load share group, outbound traffic is now distributed evenly (PD2-160291549).

Summit

Saving the configuration on a Summit48si switch no longer occasionally corrupts the ExtremeWare software image when writing to flash memory (PD2-174291301, PD2-82335602).

STP

When connected to a Catalyst switch running IOS 12.1(8)EA1b no longer generates spurious STP error messages (PD2-177504915).

EAPS

The virtual port state of a shared port that has gone down is now correct, so the EAPS v2 shared port's connectivity is maintained (PD2-175769104).

SNMP

The SNMP v1 EDPneighbor trap agent no longer has the address set to 0.0.0.0 (PD2-180021028).

Issues Resolved in ExtremeWare 7.1.1b10

The following issues were resolved in ExtremeWare 7.1.1b10. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.1.1b10 includes all fixes up to and including ExtremeWare 6.2.2b108 and ExtremeWare 7.0.1b11. For information on those fixes, see the release notes for those releases.

BlackDiamond

If you use ESRP with CMT and all traffic is forwarded through a member link, throughput is no longer limited (PD2-171286201).

SNMP now supports CMT (PD2-163789818, PD2-163789820).

Rebooting the switch no longer might generate an error message similar to (PD2-170077601):

```
<CRIT:SYST> Failed to read card 5 EEPROM.
```

The `keep-links-up` option on an MSM64i now works properly (PD2-171280801).

Alpine

If you have load sharing configured and you hot-swap a module with shared ports, load sharing no longer fails (PD2-171298401).

Issues Resolved in ExtremeWare 7.1.1b8

The following issues were resolved in ExtremeWare 7.1.1b8. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.1.1b8 includes all fixes up to and including ExtremeWare 6.2.2b108 and ExtremeWare 7.0.1b11. For information on those fixes, see the release notes for those releases.

General

Upgrading Summit or BlackDiamond switches to ExtremeWare 7.1 with an existing configuration containing the `disable ipforwarding lpm-routing` command no longer generates “disable lpm” messages in the log (PD2-139986201, PD2-145444601).

BlackDiamond

If you download a configuration containing the `configure ppp mru` command, that command now loads correctly (PD2-158075064).

The output of the `show version` command displays the F48Ti module hardware revision correctly (PD2-165272233).

Hot-swapping a G24Ti module with active traffic no longer generates error messages (PD2-159871401).

If you have a large configuration with the FDB and transceiver diagnostics enabled, rapidly hot-swapping no longer generates false FDB and transceiver diagnostics errors (PD2-158807236).

Downloading an incremental configuration that enables hitless failover when hitless failover is currently disabled, or disabling hitless failover when hitless failover is currently enabled, no longer generates the console message `msgQSend error on hfoDloadDatabase` (PD2-158625526).

The ESRP `remain-esrp-master-in-l2-domains` hitless MSM failover mode now correctly prevents an ESRP master from briefly changing to an ESRP slave (PD2-128792301).

Cross-module trunking is now supported on mismatched I/O module types (PD2-162164501).

Alpine

You can now run extended diagnostics with a VDSL module installed (PD2-116691166).

Software Redundant Ports

If you configure a software redundant port while the master port is ready and the redundant port is active, the redundant port no longer fails (PD2-121674246).

EAPS

EAPS no longer mistakenly reports a disabled port as being up after an MSM failover (PD2-140236701).

IS-IS

If you export static routes into IS-IS, save the configuration, and reboot the switch, the static routes are correctly exported (PD2-142152144).

BGP

BGP routes are correctly advertised to a peer when a peer is bounced in a multihoming topology with more than 120,000 routes (PD2-157777362).

SNMP

If you enable SNMP traps, you no longer have to configure at least one valid trap receiver. SNMP traps are enabled by default (PD2-161413602, PD2-159834250).

If you have one of the following:

- Alpine chassis running ExtremeWare 6.2.2b108
- Alpine chassis running ExtremeWare 6.2.2b134 with transceiver diagnostics enabled

and you upgrade to ExtremeWare 7.1, the SNMPv3 reboot counter is no longer corrupted (PD2-161834101).

Troubleshooting

The `upload configuration` command no longer generates bus-stats error messages when parsing the `disable bus-stats` command (PD2-158075049).

Issues Resolved in ExtremeWare 7.1.0b48

The following issues were resolved in ExtremeWare 7.1.0b48. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.1.0b48 includes all fixes up to and including ExtremeWare 6.2.2b108 and ExtremeWare 7.0.1b11. For information on those fixes, see the release notes for those releases.

General

The `configure ports auto-polarity` command is no longer available on platforms other than the Summit48si (PD2-118503001).

After configuring the time zone, a soft reboot can no longer cause the switch to boot into minimum mode (PD2-109830723).

If you telnet to the switch using port 80 and continuously press keys on your keyboard, the switch no longer has a possibility of rebooting (PD2-129688312).

ZX GBICs are no longer displayed as LX-70 GBICs in the output of the `show ports configuration` command (PD2-131305301).

A VLAN created with the name “mgmt-1” can now be deleted (1-EEUPE).

BlackDiamond

MPLS hello packets are now correctly sent at the configured interval (PD2-131214401).

If you hot-insert a second MSM, IP traffic is correctly forwarded through MPLS and ARM modules (PD2-130167901).

If you enable CPU DoS protect on a BlackDiamond with an MPLS module, ICMP traffic is no longer blocked (PD2-119097601).

If you have the system watchdog timer enabled, executing the `show fdb port` command on an ATM or PoS port no longer causes the system to reboot (PD2-134826401).

Routing entries with a next hop in the management interface subnet are now correctly removed from the routing table based on the MGMT port state (PD2-104430127).

On a BlackDiamond 6816, the `run diagnostics extended msm-d` command no longer generates a system test error (PD2-134478009).

If you hot-swap an F48Ti module, system health check errors are no longer generated (PD2-93060119).

Alpine

T3 modules now properly recover from a failover (PD2-119525910).

If you configure two multilink groups to use the same T1 or E1 module, multilink throughput is no longer degraded slightly (PD2-117966118).

The output of the `show switch` command shows PSU A and PSU B correctly (PD2-129291301, PD2-133156301).

A message similar to the following:

```
12/06/2002 11:58.28 <CRIT:KERN> Restarted fifo on slot 2
```

no longer appears in the log for T1 and E1 slots during the initialization of the T1 or E1 modules (PD2-110059501).

Messages for system health check events are now always logged (PD2-129795601).

When upgrading an Alpine 3802 to full layer 3, ExtremeWare now checks the system ID (SN) for key generation (PD2-97422994).

Summit

The autopolarity detection configuration is now correctly saved and loaded on the Summit48si (PD2-118279201).

Load Sharing

If you configure software redundant ports with load sharing, saved configurations now load properly via TFTP (PD2-130597269).

IP Unicast

BOOTP relay now operates correctly (PD2-147825901).

Multicast

If you use access-profiles to specify another RP for a given multicast group, the local RP now processes joins and prunes correctly (PD2-116382027).

The `enable rip originate-default` command now always advertises the default RIP route to peers (PD2-124368763).

OSPF

After a link transition, entries created by the OSPF originated default route are no longer in the IP FDB (PD2-109830730).

When the LSDB has two as-external LSAs for the same destination with a forwarding address, the best metric route is now selected (PD2-140720001).

BGP

The `configure access-profile add` command now correctly sets the BGP community value (PD2-129638011).

If a new best route comes from an I-BGP peer, an older best route that comes from E-BGP is correctly withdrawn (PD2-108750310).

The BGP Set Community NO_EXPORT_SUBCONFED is no longer advertised to EBGP peers (PD2-120403214).

If a route is received from the same AS via EBGP and the IBGP peer, the switch now compares the multi exist discriminator (PD2-126767407).

If the switch receives a route from an IBGP peer and the first AS number in the AS path sequence is the switch's own AS number, the route is no longer dropped as a loop (PD2-126767401).

Spanning Tree

If you delete a port from the STP domain and save the configuration, that change is now correctly saved (PD2-130809831).

ESRP

A flapping redundant link no longer causes the port counter to increase its count on the neighbor's side (PD2-111264407).

If you configure the neighbor timeout to greater than six times the hello timer, and the link between the master and the slave goes down, the slave might now immediately flushes the FDB table (PD2-124371801).

If you change the priority of the ESRP master to 255, it no longer changes to slave in rare situations (PD2-129379243).

When two switches recover from a dual-master situation, the new master correctly logs the state change (PD2-111406501).

VRRP

In a configuration with more than 20 VLANs, if you use the `show tech-support` command on the backup switch through a telnet connection, the backup no longer transitions to master and back (PD2-128764506).

If you configure the VRRP master priority to 0 (releasing it as the virtual router) and then configure the priority to 255, the master is now released (PD2-127681312).

The track-diagnostic and track-environment features are now supported with VRRP (PD2-127681344).

If you configure a new advertisement interval and then reconfigure the interval back to the default, VRRP no longer elects two master VRRP VLANs (PD2-127681301).

EAPS

EAPS is now supported with WAN modules (PD2-120015201).

You can now change the protected VLAN tag if EAPS is configured and enabled (PD2-121610287).

When configuring EAPS over WAN modules, if the EAPS master is defined with a secondary multilink, then an ARP broadcast storm over the EAPS ring no longer occurs (PD2-110006429).

You can now configure two different EAPS master domains on the same switch, on the same STP or EMISTP VLANs and the same STP or EMISTP domains (PD2-72446883).

The EAPS secondary port now recovers correctly in all cases (1-FY31X).

When ESRP and bi-directional rate shaping are configured simultaneously on the same switch, rate shaping traffic to the ESRP MAC address takes effect immediately (13583).

If you configure a single EAPS ring with 64 domains and more than 3,000 VLANs, a link transition no longer causes a 300 second traffic outage (PD2-119139401).

Ingress QoS

You can not configure ingress QoS on modules other than "3" series modules, as the feature is not supported on other modules and the configuration has no effect (PD2-129625008).

The `Tx Xoff` column in the `show ports ingress stats` command output no longer truncates values to seven characters (PD2-130148001).

Security

When you enable the CPU-DoS-Protect feature in simulated mode, an ACL is no longer created when a DoS attack is simulated, thus traffic is not blocked (PD2-129163414).

If RADIUS is enabled, but access to the RADIUS primary and secondary server fails, the switch no longer uses its local database to authenticate Network Login users (PD2-139715109).

Unauthenticated Network Login HTTP client sessions are no longer temporarily listed as 802.1x sessions in the output of the `show netlogin` command even if the user is HTTP or if 802.1x authentication is disabled (PD2-147036722).

The `clear fdb` command now resets the `Appeared` and `Learnt` counts (PD2-133592701).

When upgrading from ExtremeWare 6.2.2, RADIUS operates correctly (PD2-151787701).

SNMP

Adding or deleting a trapreceiver now detects the correct community string (1-9I5LD).

You can now configure the same community string for both read-only and read-write (PD2-118578301).

Troubleshooting

Output from the `show diagnostics` command now clearly states the number of recoverable and non-recoverable errors found (PD2-142201419).

When a new threshold is configured for reboot loop protection, the time stamp is now cleared (PD2-109830745).

If you configure a large reboot loop protection threshold, you can now configure a count of one (PD2-111222216, PD2-111201401).

If you use SNMP or RMONII to issue the `reboot` command, and reboot loop protection is configured with a threshold of 1, the switch will reboot into minimal mode (PD2-111307101).

The `show diagnostics backplane-utilization` command is no longer available on Alpine or Summit switches. There are no backplane utilization diagnostics available for Alpine or Summit switches (PD2-130597218).

If you configure the `card-down` option in the `configure sys-health-check` command and checksum errors are detected, the MSM is now taken offline as expected (PD2-105991401).