ExtremeWare Release Note

Software Version 6.2.2 b108

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

Published: April 2003
Part Number: 120156-00 Rev 09

Author: Rich Small

Editor: Rich Small

Production: Rich Small

Special Thanks: Quazi, Qing, Ying

Contents

1 Overview

These Release Notes document ExtremeWare 6.2.2b108. ExtremeWare 6.2.2 introduces new hardware products and software features.

This chapter contains the following sections:

For information on issues resolved from previous releases, you can obtain previous versions of release notes through a login account on the Extreme Networks Support web site at http://www.extremenetworks.com/support/support.asp.

New Features in ExtremeWare 6.2

Following are descriptions of features introduced or enhanced in ExtremeWare 6.2.0 and subsequent releases. These features are documented in detail in the *ExtremeWare Software User Guide* or the *ExtremeWare Software Command Reference Guide* for the relevant software version, unless otherwise noted.

Numbers in parentheses are for internal use and can be ignored.

Features Added or Enhanced in ExtremeWare 6.2.2b108

- You can now debug link detection (PD2-126693610). To enable debug-trace for link detection, use the following command:

  ```
  configure debug-trace debug-link 1
  ```

  To disable debug-trace for link detection, use the following command:

  ```
  configure debug-trace debug-link 0
  ```

  Unlike other debug-trace commands, higher levels do not produce additional output. To see the current setting, use the following command:

  ```
  show debug-trace debug-link
  ```

- The `show port info detail` command output now displays a new field: Link Filter Counter. This link filter counter is calculated at the middle layer on receiving an event. The link filter up counter

indicates the number of link transitions from down to up at the middle layer filter. The link filter down counter indicates the number of link transitions from up to down at the middle layer filter.

A new MIB is also available (PD2-127397901).

- The system health checker now also checks the integrity of the FDB (PD2-127089001). If you enable the system health checker, a section of the FDB memory on each module's switching fabric is non-intrusively compared to the software copy of the FDB. The switch takes one of the following actions if it suspects a bad entry:

  a If the entry is not in use—remap around the suspect entry

  b If the entry is in use, but is safely removable (most MAC and IP-DA entries)—remove the suspect entry and allow the table to be rebuilt naturally

  c If the entry is in use and is *not* safely removable (MAC_NH, IPSA, IPMCDA, IPDP, IPSP, IPXSN)—send a warning message to the log

  If more than eight suspect entries are detected, the switch executes the configured failure action and stops remapping on that switch fabric. To see the suspect entries, use the `show fdb` command. Suspect entries are marked with "S", remapped entries are marked with "R", and a total count is provided. To clear the suspect entries, use the following command:

  ```
  clear fdb remap
  ```

  In addition, the FDB scan statistics are included in the output of the `show diagnostics sys-health-check` command.

  To enable FDB scanning on a slot independent of the system health check configuration, use the following command:

  ```
  enable fdb-scan slot
  ```

  To disable FDB scanning on a slot independent of the system health check configuration, use the following command:

  ```
  disable fdb-scan slot
  ```

  These commands do not affect the system health check configuration or status. If you disable FDB scanning for a slot and the system health check is enabled, that slot is still scanned by the system health check. To set the interval between FDB scans, use the following command:

  ```
  con fdb-scan period
  ```

  The default is 30 sec. The range is 1 - 60 seconds. If you configure less than 15 seconds, you are asked to confirm. We recommend a period of at least 15 seconds.

- You can now test the integrity of the transceivers used for communication between the ASICs and the CPU on an MSM or SMMi (PD2-126594501). To enable the test, use the following command:

  ```
  enable transceiver-test [all | slot]
  ```

  The transceiver test is enabled by default two minutes after the switch boots, or immediately after you enable it. To disable the test, use the following command:

  ```
  disable transceiver-test [all | slot]
  ```

  To configure how often the test is run, use the following command:

  ```
  configure transceiver-test period <1-60>
  ```

  The default is 12 seconds, and the range is 1 - 60. To configure how many errors are acceptable before an action is taken, use the following command:

  ```
  configure transceiver-test threshold <1-8>
  ```

  The default threshold is 3, the range is 1 - 8. To configure the number of 20 second windows within which the configured number of errors can occur, use the following command:

```
configure transceiver-test window <1-8>
```

The default number of windows is 8, and the range is 1 - 8. This configuration provides a sliding window. If you configure the window to 8, the switch checks for errors within the *last* eight 20 second windows.

NOTE

Extreme Networks does not recommend changing the default period, threshold, or window.

To configure the action the switch takes if too many failures are detected within the specified window, use the following command:

```
configure transceiver-test failure-action [log | sys-health-check]
```

If you select `log`, messages are sent to the syslog. Only one instance of an error message is logged at this level. If you select `sys-health-check`, which is the default, the configured system health check action is taken. To view the statistics, use the following command:

```
show diagnostics
```

To clear the statistics, use the following command:

```
clear transceiver-test
```

You can also configure debug tracing for the transceiver test. To enable debug-trace for transceiver testing, use the following command:

```
configure debug-trace transceiver-test 1
```

To disable debug-trace for link detection, use the following command:

```
configure debug-trace transceiver-test 0
```

Debug messages can continue to appear in the log for up to 30 seconds after you disable the debug-trace. Unlike other debug-trace commands, higher levels do not produce additional output. To see the current setting, use the following command:

```
show debug-trace transceiver-test
```

- You can now configure the system health check recovery behavior per slot (PD2-127914846). To configure the behavior for a module, use the following command:

  ```
  configure packet-mem-scan-recovery-mode [offline | online] slot
  ```

  This command is only effective if the system health check is configured for auto-recovery. To return to the behavior configured for the system, use the following command:

  ```
  unconfigure packet-mem-scan-recovery-mode [offline | online] slot
  ```

  To see the settings for each slot, use the following command:

  ```
  show packet-mem-scan-recovery-mode
  ```

- You can now record the system temperature for BlackDiamond and Alpine systems, in celsius, in the syslog (PD2-118826201). To record the temperature, use the following command:

  ```
  enable log temperature
  ```

  To stop recording the temperature, use the following command:

  ```
  disable log temperature
  ```

- You can now disable auto-polarity detection on the Summit48si (PD2-102329001). The Summit48si automatically detects and corrects the polarity of cables, simplifying installation and maintenance. You can disable this feature using the following command:

  ```
  configure ports <all | portlist> auto-polarity <on | off>
  ```

The default setting is on. The `show ports {portlist | all} info detail` command displays the autopolarity setting.

This command is not documented in the *ExtremeWare 6.2.2 Command Reference Guide*.

- You can now block the SQL Slammer DoS attack. SQL Slammer causes high CPU utilization on the next-hop switch servicing multicast requests as IGMP sender entries are quickly populated into the multicast sender list. This leads to a high number of multicast entries in the IGMP snooping entry table, and a message similar to the following in the system log (PD2-118292101):

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

  To block and clean up after this attack:

  a Block the attack by creating an ACL to block port 1434 using the following command:

  ```
  create access-list UDP dest any ip-port 1434 source any ip-port any
  ```

  b Remove affected SQL servers from the network (you can simply disable the port connecting the server).

  c Clean up the existing IGMP snooping entries and IPMC cache using the following commands:

  ```
  igmp snooping
  clear ipmc cache
  ```

  d Disable IGMP snooping on the affected switches. Disabling IGMP snooping affects routing protocols using multicast addresses and multicast traffic on that switch.

  This feature is not documented in the *ExtremeWare 6.2.2 Command Reference Guide* or the *ExtremeWare 6.2.2 User Guide*.

Features Added or Enhanced in ExtremeWare 6.2.2b56

- Software signatures: each ExtremeWare image now contains a unique signature. The BootROM checks for signature compatibility and denies an incompatible software upgrade. In addition, the software checks both the installed BootROM and software and also denies an incompatible upgrade (PD2-92081601).

  NOTE

  ExtremeWare 6.2.2b56 is the first ExtremeWare release to incorporate software signatures. Thus, you must upgrade to ExtremeWare 6.2.2b56 (or ExtremeWare 6.2.2b68) before upgrading to later ExtremeWare 6.2.2 builds or ExtremeWare 7.0.

- The following five messages (recorded in the system log) have been added to provide you with more information on where data corruption is occurring within the switch:
  - CPU PKT ERROR—corrupted packets destined for the CPU
  - CPU DIAG PKT ERROR—corrupted packets across the switch backplane
  - EDP PKT ERROR—corrupted ExtremeWare Discovery Protocol packets in bound to the CPU
  - PBUS EXTERNAL MAC ERROR—user traffic is corrupted in packet memory in bound to the switching fabric or I/O module
  - PBUS INTERNAL MAC ERROR—user traffic is corrupted in packet memory out bound from the switching fabric or I/O module
- You can now control the number of BGP routes that are deleted and reinstalled with a new gateway using the following command (PD2-103735201):

  ```
  configure ipfdb route-add [clear-all | clear-subnet]
  ```

The `clear-all` option clears all IPFDB entries associated with a route if a more specific route is installed. This is the default option.

The `clear-subnet` option clears only the IPFDB entries associated with the new route's subnet.

To see the current setting, use the `show ipconfig` command.

- You can now configure the link detection level using the following command (PD2-86873002):

  `configure port <portlist> link-detection-level <link detection level>`

  ExtremeWare contains an interrupt service routine (ISR) that sends interrupts when links transition. The middle layer filter filters out continuous interrupt messages. You can use this command to enable or disable these two processes.

  The range of `link detection level` is 1 - 4, default is 2. Table 1 lists the behavior of the switch at each level.

  Table 1: Link detection level behavior

Level	ISR	Middle Layer Filter
1	off	off
2	on	off
3	off	on
4	on	on

- You can now configure the neutral state timeout value for an ESRP-enabled VLAN using the following command (PD2-104485403):

  `configure <vlan> esrp esrp-neutral-timeout <neutral-timer(0-512, 0 restores dflt)>`

  While in the neutral state, the VLAN does not send ESRP PDUs. When the timeout expires, the VLAN becomes the ESRP slave VLAN. The neutral state helps avoid dual master situations.

  Traffic is unaffected by the neutral state because the master ESRP VLAN continues to operate normally. The default `neutral-timer` is 2 x the ESRP hello timer (the default hello timer setting is 2 seconds). The `neutral-timer` range is 0 - 512. If you set `neutral-timer` to 0, ESRP uses the default. To see the `neutral-timer` settings, use the `show vlan esrp` command.

  CAUTION

  Configure the neutral state timeout only with guidance from Extreme Networks personnel. Misconfiguration can severely degrade the performance of ESRP and your switch.

- Reboot Loop Protection: If the system reboots due to a failure that remains after the reboot, it no longer continues to reboot (PD2-88926701). To configure reboot loop protection, use the following command:

  `configure reboot-loop-protection threshold <time-interval> <count>`

  The range of `time-interval` is 0 - 255 minutes. The range of `count` is 1 - 7. If you enter a `time-interval` but not a `count`, the default `count` is 3. If the switch reboots the specified number of times within the specified time interval, it stops rebooting and comes up in minimal mode. In minimal mode, only the CPU, NVRAM, management port, and minimal tasks are active. The following commands are supported in minimal mode:

  — Reboot

  — Unconfigure switch all

  — Unconfigure switch

— Use image
— Use configuration
— Download boootrom
— Download image
— Download configuration
— Configure iparp
— Configure vlan ipaddress
— Configure iproute add default
— Configure diagnostics
— Show iproute
— Show iparp
— Show vlan
— Show version
— Show log
— Ping
— Clear log
— Clear log diag-status

Specifying a threshold of 0 disables reboot loop protection. Specifying any other value enables it. To view the current settings, use the `show switch` or `show configuration` commands.

The reboot loop protection settings are stored in the switch memory, but are *not* saved in the switch configuration. The `synchronize` command does transfer the reboot loop protection settings to the synchronized MSM64i.

If you reboot the switch manually or use the `run msm-failover` or `run diagnostics` commands, the time interval and count are both reset to 0.

Features Added or Enhanced in ExtremeWare 6.2.2b27

- Dynamic Memory Scanning and Memory Mapping: These features now work on the following products, in addition to the BlackDiamond (1-B98W9):
  — Alpine 3808
  — Alpine 3804
  — Summit1i
  — Summit5i
  — Summit7i
  — Summit48i
  — Summit48si

NOTE

The `configure sys-health-check auto-recovery` *command does not support the* `number-of-tries` *option on Summit switches.*

- MSM64i Failover: Failover times for the MSM64i have been improved. Boot time is up to 37% faster, configuration saves are up to 35% faster, and software packet forwarding is up to 65% faster (1-B2G7X). The actual improvement is dependent upon the type of traffic, your specific configuration, and other issues.
- You can now force the master MSM64i to immediately fail over to the slave MSM64i with the `run msm-failover` command.
- Improved BlackDiamond 6816 POST and Diagnostics: The BlackDiamond 6816 POST speed, error output, and diagnostics now match those of the BlackDiamond 6808 (1-AJTM7).
- System Memory Dump: You can now download the entire contents of memory through the Ethernet management port (1-B98W1). This feature is for troubleshooting, and should not be used without assistance from TAC. The following command transfers the dump. If you do not specify an IP address, the configured system-dump server IP address is used:

  ```
  upload system-dump [<ip address>]
  ```

  This command specifies the IP address to which to transfer a dump if the `system-dump` option is specified in the configuration. This address is also used if no address is provided in the `upload system-dump` command. The default is 0 or "no IP".

  ```
  configure system-dump server <ip address>
  ```

  The following command sets an optional timeout for the dump transfer. The default is 0. The minimum non-zero value is 120 seconds. The minimum recommended value is 480 seconds.

  ```
  configure system-dump timeout <seconds>
  ```

  The following command returns the system-dump configuration to the defaults.

  ```
  unconfigure system-dump
  ```

  The following command displays the system-dump server IP and dump-timeout.

  ```
  show system-dump
  ```

  The sys-recovery-level command has a new option: `system-dump`. The `system-dump` option specifies a memory dump if a task generates a software exception. The four options specify the action taken when the dump transfer is complete. The actions occur whether or not the dump was successful. The `maintenance-mode` option leaves the switch in whatever state it was in before the dump.

  ```
  configure sys-recovery-level [all | critical] system-dump [maintenance-mode |
  msm-failover | reboot | shutdown]
  ```

  These commands are not documented in the *ExtremeWare 6.2.2 Command Reference Guide.*
- System Odometer Enhancement: The system odometer has been enhanced to record the date the unit was first installed (1-7KEEX).
- ARP response time is now faster (1-631SX).
- BGP Enhancements:
  - You can now limit the number of IP prefixes from a BGP neighbor (1-5LQI3).
  - The `show bgp neighbor detail` output was enhanced to provide information on the maximum prefix limit.
  - The Type of Service (TOS) field in the IP header is now set to "Internetwork Control" (1-9GPU2). This gives the IP packet preferential treatment at the intermediate nodes and at the destination.
  - The BGP task has been restricted to 75% utilization of the CPU.
  - TCP can now ignore the sequence number if it is lower than the expected receive sequence number, but process the rest of the fields in the ACK packet (1-8406T).

— If the reachability to a BGP next hop changes, only associated routes are reprocessed. If only the immediate gateway changes, no BGP updates are sent to the peers. Last, IGP next hop changes are processed before the BGP next hops (1-9GM22).

— BGP error processing is now delayed by 5 seconds, to allow IGP recalculation (1-AX8MX).

— The Input Policy can no longer be re-applied to an already-modified Path Attribute, thus protecting the Path Attributes (1-96X1V).

— The `configure debug trace bgp-neighbor` command is now supported and accepts IP addresses (1-9FBFL).

— The `clear bgp neighbor counters` command now clears FsmTransitions (1-BZC35).

- EAPS Enhancements:

  — You can no longer modify the configuration of a SuperBridge, Subbridge, or IP Range control VLAN (1-A7RPG).

  This limitation is not documented in the *ExtremeWare 6.2.2 Software User Guide.*

  — You can no longer modify the configuration of any control VLAN if the domain is active (1-A7RPG).

  This limitation is not documented in the *ExtremeWare 6.2.2 Software User Guide.*

  — You can no longer delete a domain if that domain is active (1-A7RPG).

  This limitation is not documented in the *ExtremeWare 6.2.2 Software User Guide.*

  — Enhanced `show eaps` command: This command now provides a `summary` option, as follows (1-8330Z):

  ```
  show eaps [detail | summary]
  ```

- Multicast Enhancements:

  — Configure PIM Register Interval: You can now configure the PIM register interval threshold and probe interval using the `configure pim register-suppress-interval <time> register-probe-interval <time>` command (1-8BB01, 1-885VT).

  — PIM Scalability: You can now configure the register interval for initial registers using the `configure register-rate-limit-interval` command (1-8BB01, 1-993WD).

  This command is not documented in the *ExtremeWare 6.2.2 Command Reference Guide.*

  — Configurable SPT Threshold: You can now configure the SPT threshold using the `configure pim spt-threshold <last hop router threshold>` command without configuring the RP threshold. In addition, a cache of the Source Specific Tree is created on the RP upon receipt of the register packet even though no cache of Shared Tree exists. Thus, new receivers need not wait for the next cycle of the null-register to receive the desired multicast stream (1-9157U).

- NAT Enhancement: NAT has been improved to increase performance by up to 25%.

- SNMP Enhancements:

  — You can now enable and disable traps by port, using the `enable/disable snmp traps {port-up-down ports [<portList> | all]}` command (1-6DDDC).

  — Enhanced `show management` output now includes trap information per port.

  — Trap receivers now support an enhanced mode, which accepts traps containing extra varbinds at the end. Only standard traps are sent to a standard mode trap receiver and only enhanced traps are sent to an enhanced mode trap receiver. In addition, a standard mode trap receiver is only sent standard traps from domain “s0”. For other domains, no traps are sent (1-61BMV, 1-BPZO1, 1-BP5AN).

  — The “ifDescr” and “ifAlias” varbinds were added to the proprietary EDP traps (1-60FXQ).

— You can now enable loopback mode on a VLAN using SNMP (13029).

— You can now configure the CPU transmit priority using SNMP (1-5E4YT).

— You can now manage multiple Spanning Tree domains using SNMP (1-60FXK).

— The BlackDiamond 6804 is now supported through SNMP (1-DDMYT).

— The show management command output was reorganized for better clarity (1-CZWD9).

- The number of OSPF Equal Cost Multiple Paths was increased from 8 to 12 (1-9G4OY).
- The syntax of the `configure ospf timer <transmit_delay>` command is now `configure ospf timer <transit delay>` (1-B1K6X).
- The VLAN name in the `show vlan` command output was expanded to display up to a maximum of 18 characters (1-99BX9).
- You can now overwrite 802.1p priority based on VLAN using the `create fdb any-mac vlan <name> dynamic ingress-qos <qosprofile>` command (1-968RZ).

  This command is not documented in the *ExtremeWare 6.2.2 Command Reference Guide*.
- The `show ports info` command output was enhances to include “enabled” and “disabled” flags for each port (1-8CEA7).
- You can now display the loadsharing groups using the `show ports sharing` command (1-8P8B9).
- You can now specify a default route as a blackhole using the `configure iproute add blackhole [default | ipaddress <ip address>]` and `configure iproute delete blackhole [default | ipaddress <ip address>]` commands (1-99CRT).
- Up to 1024 locked-down MAC addresses are now saved through reboots and downloaded configurations (1-ADCFL).
- Network Login users now have a Vendor-Specific Attribute to limit their access to the switch (1-98DW9).
- You can now configure a banner for Network Login users using the `configure banner netlogin` command (2-GQ1XR).
- You can now configure a domain suffix list up to six items long for the ExtremeWare DNS client (1-69RS9).
- ExtremeWare now supports protection against the “jolt,” “opentear,” “raped,” “boink,” and “winfreeze” DoS attacks (1-AY26W).
- If CLI paging is disabled, you can now press [q] and [Enter] to force the output to stop (1-90L0R, 1-7H2KP).
- You can now display the log in ascending chronological order using the `show log chronological` command (1-6AWX6).
- The maximum number of Access List entries is now 5120 (1-BPLJP).
- When ESRP restarts a port, it sends a message to the syslog (1-BK08Q).
- You can now configure the ESRP timeout using the `configure vlan esrp timer` command (1-BKEQP).
- Permanent FDB entry lookup is now faster (1-EB4IT).
- The software redundant port feature now fully supports IPX (1-A5EMP).
- The show iproute command output now includes a time stamp (1-60FYA).
- Spanning Tree now detects loopback ports, blocks the ports, and recalculates (1-D3TSX, 1-DWC1D).

- The auto-negotiation status of Gigabit Ethernet ports is now contained in the output of the `show configuration` command (1-962XM).
- The `mgmt` option was removed from the `restart port` command (1-9KMSI).
- The `show tech-support` command now captures the `show ipmc fdb` command output (1-A85H1).
- The `show vlan` command output now indicates active and inactive ports (1-E3MRP).

Supported Hardware

This release of ExtremeWare 6.2.2 is designed to support products using the "*i*" chipset *only.*

ExtremeWare 6.1.9 through ExtremeWare 6.2.1 requires version 7.2 BootROM. BootROM 7.2 is not backward compatible with previous versions of ExtremeWare 6.x.

ExtremeWare 6.1 or later requires that the BlackDiamond switch use only the MSM64i in slots marked "A", "B", "C", and "D". It is not possible to use MSM32 modules with ExtremeWare 6.x or higher.

This release supports the following hardware in addition to the hardware mentioned in the User Guides (support for hardware listed in *italics* is new for this release):

Table 2: Supported hardware

Extreme Switch Platform	ExtremeWare Filename/Version	BootROM Filename/Version
BlackDiamond 6804	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
BlackDiamond 6816	v622b108.Gxtr or v622b108.SGxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
BlackDiamond switch using MSM64i MSMs	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Alpine 3808	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Alpine 3804	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Summit 7i/7iT	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Summit 1i/1iT	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Summit 5i/5iT/5iLX	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Summit 48i	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6
Summit 48Si	v622b108.xtr or v622b108.Sxtr/v6.2.2b108	Ngboot7.6.bin/v7.6

NOTE

Please see the "Upgrading to ExtremeWare 6.2" chapter for special upgrade instructions when upgrading from 6.1.8b13 or earlier.

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 Module Support

BlackDiamond modules supported with ExtremeWare 6.1.5 and above and the MSM64i include:

Table 3: BlackDiamond module support

BlackDiamond Module	ExtremeWare 6.1.5 and above Support	Uses "*i*" Chipset
MSM64i	Yes	Yes
G12SXi	Yes	Yes
G8Xi	Yes	Yes
G8Ti	Yes	Yes
F48Ti	Yes	Yes
WDMi	Yes	Yes
F96Ti	Yes (ExtremeWare 6.1.8b12 or above)	Yes
F32Fi	Yes (ExtremeWare 6.1.8b13 or above)	Yes
F32T	Yes	No
F32F	Yes	No
G4SX - G4LX	Yes	No
G6SX - G6LX	Yes	No
DC Power Supply	Yes	N/A
220 VAC Power Supply	Yes	N/A
110 VAC Power Supply	Yes	N/A

NOTE

Mixed versions of the power supplies should not be installed in the same system. Both power supplies should be of the same type.

Alpine Module Support

Alpine modules supported with ExtremeWare 6.1.5 and above include:

Table 4: Alpine module support

Alpine Module	ExtremeWare 6.1.5 and above Support	Uses "*i*" Chipset
SMMi	Basic or Advanced license	N/A
GM-4Si/Xi/Ti	Yes	Yes
FM-32Ti	Yes	Yes
FM-24MFi	Yes	Yes
FM-24Ti	Yes (EW 6.1.7 or above)	Yes

Table 4: Alpine module support

Alpine Module	ExtremeWare 6.1.5 and above Support	Uses "*i*" Chipset
FM-24SFi	Yes (EW 6.1.7 or above)	Yes
GM-WDMi	Yes (EW 6.1.8 or above)	Yes
DC Power Supply	Yes	N/A

Summit Component Support

Summit components supported with ExtremeWare 6.1.5 and above include:

Table 5: Summit component support

Summit Module	ExtremeWare 6.1.5 and above Support	Uses "*i*" Chipset
Summit 7i DC Power Supply	Yes	N/A

GBIC Support

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 config` 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: GBIC support

Software Release	1000BaseSX Parallel ID	1000Base-LX Parallel ID	1000Base-SX Serial ID	1000Base-LX Serial ID	LX70 Serial ID
Release 1.X	SX	LX	Not Supported	Not Supported	Not Supported
Release 2.X	SX	LX	LX	LX	LX
Release 3.X	SX	LX	CX	CX	CX
Release 4.X	SX	LX	SX	LX	LX
Release 6.X	SX	LX	SX	LX	LX70 (6.1.6 and above)

Summit48si Mini-GBIC Support

The Summit48si supports the Extreme mini-GBIC only. For reliability and stability reasons, third-party mini-GBICs are not supported at this time.

Features Unique to the "*i*" Chipset

The following list summarizes the feature areas specific to the "*i*" chipset products. Unless noted otherwise, both I/O module and MSM must make use of the "*i*" chipset to make use of the features listed below.

- QoS and Access Policies — Complete use of IP Access Lists; support for IP DiffServ; support for eight QoS queues per port, instead of four; support for Random Early Detection.
- Bridging/Switching — Support for jumbo frames; support for address and round-robin-based load-sharing algorithms and non-contiguous load-sharing port groups.

- Routing — Wire-speed IPX routing (products without the "*i*" chipset support IPX routing, but not at wire-speed). Support for BGP4 (though it is not necessary to have "*i*"-based I/O modules to support BGP4 on the BlackDiamond). Policy-based Routing.
- Server Load Balancing — Support for all Server Load Balancing functions.
- Web Cache Redirection — Support for all WCR functions.
- QoS Bi-directional Rate Shaping — Ability to perform Policy-based QoS for a VLAN's traffic both into and out of the switch.
- Extreme Standby Router Protocol (ESRP) options — Support for ESRP Groups, ESRP Domains and ESRP Host Attach.
- Traffic statistics on a per VLAN basis.
- Subnet directed broadcast packet forwarding improvements.
- System health-checker on the BlackDiamond.
- Extreme Multiple Instance Spanning Tree Protocol (EMISTP) — An extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs.
- Extreme Automatic Protection Switching (EAPS) — Support for fast protection switching to layer 2 switches interconnected in an Ethernet ring topology.
- Virtual Redundant Router Protocol (VRRP) — Support for the proposed IETF standard protocol that allows multiple switches to provide redundant routing services to users.
- Network Address Translation (NAT) — Ability to convert a set of IP addresses, typically private IP addresses, to another set of IP addresses, typically public Internet IP addresses.
- Network login — Ability to control the admission of user packets into a network by giving addresses only to users that have been properly authenticated.

2 Upgrading to ExtremeWare 6.2

This chapter contains the following sections:

Staying Current

For support purposes, Extreme Networks recommends operating the most current General Deployment (GD) release of ExtremeWare. New releases of ExtremeWare are usually released first as General Availability (GA) releases. A GA release has undergone full regression testing and is supported by your local ExtremeWorks Technical Assistance Center, but should be deployed with the understanding that it is a not a GD release.

Extreme Networks does not recommend that customers perform a flash network-wide upgrade with any new GA release. As a precaution, you should start with lab testing and edge installations before moving a GA release to the core of networks with over 10,000 nodes.

If you are an Extreme Assist customer, the latest release and release notes are available through the support login portion of the Tech Support web site at http://www.extremenetworks.com/

Upgrading the BootROM

ExtremeWare 6.2.2 requires BootROM 7.6, but is compatible with BootROM 7.8. Upgrade the BootROM *before* upgrading ExtremeWare using the following command:

```
download bootrom [ <host_name> | <ip_addr> ] <ngboot.bin_name>
```

To downgrade to an earlier version of ExtremeWare, perform a BootROM downgrade *before* downgrading ExtremeWare. To downgrade BootROM, use the following command:

```
download bootrom [ <host_name> | <ip_addr> ] <ngboot.bin_name>
```

Once the BootROM downgrade is complete, you can reboot the system with the previously loaded ExtremeWare version.

Upgrading ExtremeWare

Below are instructions specific to upgrading to, and downgrading from, ExtremeWare 6.2.2 for Summit, Alpine, and BlackDiamond switches.

NOTE

You must upgrade to BootROM 7.2 to run ExtremeWare 6.1.9 through ExtremeWare 6.2.1. Also note that you must downgrade to BootROM 6.5 to run ExtremeWare 6.1.8 or earlier.

Follow these instructions carefully, especially if you switch between different versions and configurations multiple times. Improper upgrades can corrupt the FDB and otherwise damage the switch.

Upgrading Switches

ExtremeWare 6.2 can read a stored configuration saved by ExtremeWare 6.x. The procedures outlined below will preserve the ability to downgrade should it become necessary:

1. Ensure that the currently used configuration is stored in both the primary and secondary configuration spaces using the `save primary` and `save secondary` commands.
2. Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use config primary` commands.
3. Verify that all of the above procedures were completed successfully with the `show switch` command.
4. Upload the configuration of the switch to a TFTP server for safekeeping using the `upload config <ipaddress> <filename>` command.
5. If you are not already running BootROM 7.6, TFTP download BootROM 7.6 to the switch using the `download bootrom` command.
6. Reboot the switch using the `reboot` command.

Upgrading from ExtremeWare 6.1.8 or Earlier

If you are running a version of ExtremeWare prior to ExtremeWare 6.1.9b11:

1. TFTP download ExtremeWare 6.1.9b11 to the primary image space using the `download image primary` command.

   CAUTION

   If you do not upgrade to ExtremeWare 6.1.9b11 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. 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 `config red drop-probability` command.

6 Save the configuration to the primary space.

7 Follow the instructions for upgrading from ExtremeWare 6.1.9 in the next section.

Upgrading from ExtremeWare 6.1.9

If you are running ExtremeWare 6.1.9b11 through ExtremeWare 6.2.2b27:

1 TFTP download ExtremeWare 6.2.2b108 to the primary image space using the `download image primary` command.

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

NOTE

You must upgrade to either ExtremeWare 6.2.2b56, ExtremeWare 6.2.2b68, or ExtremeWare 6.2.2b108. These builds support the software signature feature. Interim builds might not.

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

3 Verify that the switch is operating as expected. After verification, configure features specific to the current version of ExtremeWare.

4 Save the 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.

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. To change the leave time-out value back to 10 seconds, use the following command:

```
configure igmp snooping leave-timeout 10000
```

5 Reboot the switch using the `reboot` command.

Downgrading Switches

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

1 Use the secondary configuration with the `use config secondary` command. If there is no previous configuration saved, re-configure or download the correct configuration file to the switch in Step 7.

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

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.

7 If you did not save the previous configuration, you can configure the switch sufficiently to TFTP download a configuration file. If you do not have a configuration file, re-configure the switch manually.

NOTE

When downgrading to a previous version of ExtremeWare, ensure that the switch configuration matches that version of ExtremeWare (or earlier). 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.

Installing ExtremeWare 6.2.2 on a BlackDiamond 6816

To install the BlackDiamond 6816 version of ExtremeWare 6.2.2 on a BlackDiamond 6816 for the first time, you must follow the procedure that follows. These steps must be followed even if you already have ExtremeWare 6816b6 installed.

1 Remove all modules (MSM64i and I/O) except the MSM64i in slot A.

NOTE

Make sure you have no configurations saved in primary or secondary.

2 Download BootROM 7.6 using the `download bootrom` command.

3 Enter `Y` to complete the upgrade.

4 Reboot the switch using the `reboot` command.

5 Download ExtremeWare 6.1.9b11 or 6.1.9b22 using the `download image` command.

NOTE

You only need to load into the primary image space.

6 Confirm the installation using the `show version` and `show switch` commands.

NOTE

Make sure you are booting to your primary image. Otherwise, configure the switch to boot from the primary image with the `use image primary` *command.*

7 Reboot the switch using the `reboot` command.

8 Download ExtremeWare 6.2.2b108_6816 using the `download image` command.

NOTE

Install code image into both primary and secondary.

9 Confirm the installation using the `show version` and `show switch` commands.

10 Clear the log using the `clear log static` command.

11 Copy the BootROM, configuration, and image to the other MSM64i modules using the `synchronize` command. This command reboots the synchronized modules.

12 Reboot the switch using the `reboot` command.

Repopulate the Chassis

To repopulate the chassis after you have installed the BlackDiamond 6816 version of ExtremeWare 6.2.2 on each MSM64i, perform the following steps:

1 Power down the chassis.

2 Install MSM64i modules in slots A - D.

3 Install all I/O modules.

4 Power up the chassis.

5 Confirm that each MSM64i is running the correct version of ExtremeWare using the `show switch` command.

6 Check the log using the `show log` command.

If you have critical or major errors, save them into a text file and contact Extreme Technical Support.

Error Message

If you install an MSM64i with a BlackDiamond 6816 image onto a BlackDiamond 6808 chassis, you might get an error message in the syslog indicating the image is not supported, as indicated by the MGMT LED. The message is part of the download protection. You still have minimal functionality available to download the proper image. To reset the LED, load the same image in both image spaces and synchronize the switch using the `synchronize` command.

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 7: Supported limits

Metric	Description	Limit
Access List rules	Maximum number of Access Lists (best case).	5120
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, BlackDiamond, Summit7i, and Alpine	Maximum number of routes contained in the BGP route table (best case).	400,000
BGP—routes, Summit1i, Summit5i, and Summit48i	Maximum number of routes contained in the BGP route table (best case).	200,000
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
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 entried per switch.	256

Table 7: Supported limits (continued)

Metric	Description	Limit
BGP—network statements	Maximum number of network statements 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.	3000
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
ESRP—Max instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—Max 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—Max VLANs in a single ESRP domain – Summit “*i*” series and 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
ESRP—Route-track entries, Summit “*i*” series and Alpine	Maximum number of routes that can be tracked by ESRP.	4
ESRP—Route-track entries, BlackDiamond	Maximum number of routes that can be tracked by ESRP.	4
ESRP—Max VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1
FDB—Max ports for permanent entries	Maximum number of ports supported for permanent FDB entries.	2,000
FDB—Max L2/L3 entries – MSM64i with “*i*” series I/O modules, Summit5i, Summit7i, Alpine	Maximum number of MAC addresses/IP host routes for the MSM64i, Alpine 3808, and Summit7i.	256,000
FDB—Max L2/L3 entries – Summit1i, Summit48i, and Summit48si	Maximum number of MAC addresses/IP host routes for the Summit1i, Summit5i, and Summit48i.	128,000
FDB—Max L2/L3 entries for non-“i” series BlackDiamond I/O modules.	Maximum number of MAC addresses/IP host routes for the G4X, G6X, F32T, and F32F.	32,000
Flow Redirection—Max 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—Max 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—Max subnet mode entries	Maximum number of active entries for subnet mode rules. Each mask can have 1 entry.	64

Table 7: Supported limits (continued)

Metric	Description	Limit
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	Maximum number of IP routes used in route sharing calculations. This includes static routes and OSPF ECMP.	12
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
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
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF external routes—BlackDiamond, Summit7i, and 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, and 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, and Summit48i	Recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	65,000

Table 7: Supported limits (continued)

Metric	Description	Limit
OSPF inter- or intra-area routes—Summit1i, Summit5i, and Summit48i	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.	40
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.	200
OSPF adjacencies—Summit7i, Alpine, BlackDiamond	Maximum number of OSPF adjacencies on a switch with 256 MB memory.	300
Policy Based Routing	Maximum number of policy based routes that can be stored on a switch.	64
Protocol-sensitive VLANs—active protocol filters	The number of simultaneously active protocol filters in the switch.	15 for "*i*" series switch products; 7 otherwise
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—Max number of simultaneous sessions	For Transparent and Translational and GoGo modes respectively.	500,000/500,000/ unlimited
SLB—Max number of VIPs	For Transparent and Translational and GoGo modes respectively.	1000/1000/unlimited
SLB—Max number of Pools	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—Max number of Nodes per Pool	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—Max 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
Spanning Tree—Max STPDs, Summit	Maximum number of Spanning Tree Domains.	128
Spanning Tree—Max STPDs, Alpine	Maximum number of Spanning Tree Domains.	256
Spanning Tree—Max STPDs, BlackDiamond	Maximum number of Spanning Tree Domains.	512
Spanning Tree—Minimum STPDs	Minimum number of Spanning Tree Domains.	1

Table 7: Supported limits (continued)

Metric	Description	Limit
Spanning Tree—Max 802.1d domains	Maximum number of 802.1d domains per port.	1
Spanning Tree—Max 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 port.	3
EMISTP & PVST+ — Max domains, Summit	Maximum number of EMISTP and PVST+ domains.	128
EMISTP & PVST+ — Max domains, Alpine	Maximum number of EMISTP and PVST+ domains.	256
EMISTP & PVST+ — Max domains, BlackDiamond	Maximum number of EMISTP and PVST+ domains.	512
EMISTP & PVST+ — Max ports	Maximum number of EMISTP and PVST+ ports.	4096
EMISTP & PVST+ — Max domains per port, Summit	Maximum number of EMISTP and PVST+ domains that can be configured per port.	128
EMISTP & PVST+ — Max domains per port, Alpine	Maximum number of EMISTP and PVST+ domains that can be configured per port.	256
EMISTP & PVST+ — Max domains per port, BlackDiamond	Maximum number of EMISTP and PVST+ domains that can be configured per port.	512
Static MAC FDB entries—Summit “i” series, Alpine, and 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 “i”-series and Alpine	Includes all VLANs plus sub VLANs, super VLANs, etc.	3000
VLANs—BlackDiamond 6816	Includes all VLANs plus sub VLANs, super VLANs, etc.	600
VLANs—BlackDiamond	Includes all VLANs plus sub VLANs, super VLANs, etc.	3000 in an all “i”-series system. 1024 in a mixed “i”-series/non “i”-series system
VRRP—Maximum VRIDs	Maximum numbers 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—Max VRIDs/switch	Maximum numbers of VRIDs per switch.	64

Table 7: Supported limits (continued)

Metric	Description	Limit
VRRP—Max VRIDs/VLAN	Maximum numbers of VRIDs per VLAN.	4
VRRP—Max ping tracks	Maximum numbers of ping tracks per VLAN.	4
VRRP—Max iproute tracks	Maximum numbers of iproute tracks per VLAN.	4
VRRP—Max VLAN tracks	Maximum numbers 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 appearing 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 6.2.2.

System Related – All Systems

Syslog Crashes and Rebooting

If the syslog task (tSyslogTask) crashes, you cannot reboot the system using the CLI; you must reboot by turning off power to the switch (PD2-116545563).

No Warning When Downloading Software Incompatible with Configuration

If you download software that is incompatible with the existing configuration, which can happen if you downgrade the software, the switch does not warn you of the incompatibility (13648).

Disconnected PSU Error Messages

If you disconnect the power from a PSU, an INFO error message is generated, instead of a WARNING message (PD2-85458386).

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).

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 configure ports auto-polarity Command

The `configure ports auto-polarity` command only works on the Summit48si, even though the command is available on other platforms. If you use this command on another platform, it has no effect (PD2-118503001).

The card-down Option

In a fully redundant configuration, if you configure the `card-down` option in the `configure sys-health-check` command and checksum errors are detected, the MSM is not taken offline as expected. To work around this, use the `configure sys-health-check auto recovery 3 offline` command (PD2-105991401).

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).

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).

UDP Echo Transmit Rate

The UDP Echo utility is designed to verify network connectivity. Transmit rates of 10 pps suffice for this function. UDP Echo rates of 20 pps should be sufficient. Do not set your UDP Echo rate higher than 100 pps, as the switch does not send replies faster than that rate (1-FAO89).

Downloading Incremental Configurations

Do not download an incremental configuration when you have time-critical applications running. When you download an incremental configuration, the switch immediately processes the changes, which can affect the processing of other tasks. We recommend that you either download small incremental configurations, or schedule downloads during maintenance windows (PD2-102929311).

ARP Entry Age

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

ARP Duplicate Address

An ARP request with 0 in the protocol address is reported as a duplicate address if the switch has the default VLAN with no IP address assigned (PD2-70889799).

Port Mirroring

If you mirror a port to an untagged port, you might get a "`Reached maximum otp index allocation`" message in the syslog. This can lead to incomplete FDB entries and unforwarded traffic (PD2-130140988).

When a multicast packet egresses from a port, two copies of the packet are sent to the mirror port. This does not affect network traffic in any way, as the duplicate packets are sent only to the mirror port. This does affect accounting and RMON statistics (1-DQK86).

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

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

Software Controlled Redundant Port

If you unconfigure a software redundant port, the redundant port remains down (PD2-105118423).

If the module containing the primary port is removed or taken offline, the redundant port remains down (1-C5DGW).

You can configure only one redundant port for each primary port.

You cannot configure hardware redundant ports (such as ports 49 and 50 on a Summit48i) as software controlled redundant ports.

Contrary to the information in the *ExtremeWare Software User Guide*, Software Controlled Redundant Port *is* supported on 1000-BaseT ports.

Setting Auto-negotiation Off on a Gigabit Port

When connecting to a device that does not support 802.3z auto-negotiation, it is necessary to turn off auto-negotiation for the switch port to which it is connecting. Although a gigabit port only runs at full duplex and at gigabit speed, the command to turn auto-negotiation off must still include specifying the duplex mode. For example the command:

```
config port 4 auto off duplex full
```

will turn auto-negotiation off if port 4 is a gigabit port.

Flow Control

Flow control is fully supported only on Gigabit Ethernet ports. Gigabit ports both advertise support and respond to pause frames. 10/100 Mbps Ethernet ports also respond to pause frames, but do not advertise support. Neither 10/100 Mbps or Gigabit Ethernet ports initiate pause frames.

Flow Control is enabled or disabled as part of auto-negotiation. If auto-negotiation is set to off, flow control is disabled. When auto-negotiation is turned on, flow control is enabled. (2815).

System Logging

By default, log entries of "warning" and "critical" levels are preserved in the log even after a reboot. The `clear log` command does not remove these static entries. The `clear log static` command removes all entries of all levels and clears the "ERR" LED on the master MSM module of the BlackDiamond switch (2840).

Enabled IdleTimeouts and Console Connections

If the IdleTimeout feature is enabled, and a telnet session becomes "timed-out", a subsequent telnet to the switch will be successful but will result in a pause or "hang" an existing direct serial console connection. If the subsequent telnet session is terminated, the console port will resume normal function and subsequent telnet sessions will work correctly (5094).

The Admin Account

For security reasons, you should not attempt to delete the default "admin" user account. If you delete the default account, it will be automatically restored, with no password, after you download a configuration. Therefore, to ensure security you should change the password on the admin account, but not delete it. The changed password will remain intact through configuration uploads and downloads (1-C5S7B).

If you *must* delete the default admin account, you must first create another administrator-level account before you delete the default admin account. You will need to remember to manually delete the default admin account again every time you download a configuration.

Show Memory Output

On some systems, the `show memory detail` command might show the cumulative memory allocation field as negative (9010).

TFTP Download of Configuration Files

When using TFTP to download a configuration file and selecting "no" for the switch reboot request, rebooting the switch at a later time will display a message that the configuration file has been corrupted. The user will be prompted to reboot the switch with factory default parameters. If an immediate reboot is performed after the download configuration command, the configuration file will be initiated correctly (12413).

Network Login and Saving the Configuration

If you save the configuration on a switch while there are open authenticated Network Login sessions, all those sessions will become unauthenticated. This occurs to prevent the authenticated ports from being permanently saved in the authenticated VLAN (1-981ML).

Network Login Design Guidelines and Limitations

Following are Network Login design guidelines and limitations:

- All client MACs on an authenticated port will have network access. You cannot authenticate on a per-MAC basis, only per-port.
- All client MACs on an unauthenticated port will see broadcast and multicast traffic.
- Network Login must be disabled on a port before that port can be deleted from a VLAN.
- Campus Mode login will not show the original VLAN to which the port was connected to once the port transition to destination VLAN takes place.
- A Network Login VLAN port should be an untagged Ethernet port and should not be a part of following protocols:
  - ESRP
  - STP
  - VLAN aggregation
  - Load-sharing
- Enabling any of these protocols on Network Login ports will take higher precedence. This may result in a port transitioning from a blocked state to a forwarding state.
- Network Login is not supported for ATM, PoS and MPLS TLS interfaces.
- MSM-failover will clear Network Login state information.

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:

- CPU-TRANSMIT-PRIORITY
- Summit-chipset module support
- Installed ATM, MPLS, ARM, and PoS modules
- Mirroring
- Dynamic 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).

System Related – BlackDiamond Switch

Hot-Swapping F48Ti Modules Generates Errors

If you hot-swap an F48Ti module, system health check errors are generated. You can safely ignore these error messages (PD2-93060119).

Broadcast Traffic on a VLAN with Two Ports

If you configure a VLAN with only two ports and send broadcast MAC traffic out those ports, the internal backplane ports of other modules also receive the broadcast traffic. To work around this, save the configuration and reboot the switch (PD2-128393646).

ESRP and IP forwarding Enabled on G1 Modules

If you enable IP forwarding on a G1 module and enable ESRP, the tNetTask utilization approaches 50%. This can affect other time-critical tasks (PD2-102537115).

The show ports utilization Command

On a switch with heavy traffic and slot 1 empty, if you execute the `show ports utilization` command and press [u] repeatedly, the MSM might fail over or be rebooted by the watchdog timer (PD2-110761007).

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).

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).

Limited Commands Mode and the reboot Command

In limited commands mode, the `reboot` command does not reboot the MSM64i; instead the command causes the 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.

The clear slot and unconfig slot Commands with 3,000 VLANs

If you have 3,000 VLANs configured, the clear slot and unconfig slot commands cause the switch to see the slot as mismatched and unconfigured (PD2-90223205). You must reconfigure the slot.

Dynamic Memory Scanning and Mapping Module Support

BlackDiamond I/O module memory scanning and mapping support is listed in Table 1.

Table 1: Memory scanning and mapping support in BlackDiamond modules

Module	Memory Scanning and Mapping
F32F	Yes
F32T	No
F48Ti	Yes
F96Ti	Yes
G12SXi	Yes
G4SX	No
G4LX	No
G6SX	No
G6LX	No
G8Ti	Yes
G8Xi	Yes
WDMi	Yes
MSM64i	Yes

Using Configurations on Different Chassis

Configurations created in a BlackDiamond chassis are not supported in a different model chassis. For example, a configuration from a BlackDiamond 6808 is not supported in a BlackDiamond 6804. Configurations for different models generate error messages for any line in the configuration that concerns unavailable slots.

If you load a configuration from a different model, you can safely write the correct configuration over the unsupported configuration.

BlackDiamond 6804 Module Support

The BlackDiamond 6804 does not support the MPLS, ATM, ARM, or PoS modules.

Reboot Slave MSM64i After Using synchronize Command

When you synchronize the MSM64i modules, reboot the slave MSM64i so that if it becomes the master MSM64i it uses the synchronized software and configuration (PD2-65213801, PD2-65071101, 1-5E9O9).

Enabled IdleTimeouts and Multiple BlackDiamond Console Connections

The idletimeouts feature should not be enabled if serial ports from both MSMs in a two MSM configuration are used for console connections. If the idletimeouts feature is enabled in this scenario, console sessions will not be re-established correctly (5093).

Hot Removal of an I/O Module with Traffic

If a BlackDiamond I/O module is removed during traffic flow to the module, several error messages may be written to the log immediately following. These messages should cease to occur after about 10 seconds. Under this circumstance, the error messages can be safely ignored. The error messages may contain one or more of the following (5160, 5082):

```
04/13/1999 17:18.46 <DBUG:KERN> killPacket: HW pqmWaitRx failed
```

```
04/13/1999 17:18.46 <DBUG:KERN> pqmWaitKill failed. Card 1 is removed.
```

Removal/Insertion of an I/O Module

The action of inserting or removing a BlackDiamond I/O module should be completed in a reasonable time frame. Be sure to remove or insert the module completely and to avoid partial insertion or connection of backplane connectors (7455).

Removal/Insertion of an MSM

The action of inserting or removing a BlackDiamond MSM will report the following message under certain circumstances. This message can be safely ignored (8547).

```
04/27/2000 12:39.37 <WARN:KERN> ngRxFirst failed WTX1 - (1, eeeeeeee, ffff)
```

Extended Diagnostics

The `run diags extended` command can cause the following messages to appear in the log. These messages are expected and indicate that the system is currently busy running the user initiated diagnostics (10800). This does not occur with the CLI `run diagnostics normal` command.

```
<CRIT:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8

<INFO:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8
```

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).

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).

Normal or Extended Diagnostics on BlackDiamond 6816

The BlackDiamond 6816 only supports the packet-memory option of the `run diagnostics` command. Users attempting to run either normal or extended diagnostics will receive the following message:

```
Warning: run-time diagnostics is not supported currently on the 6816.
```

Sync of Configurations

When you hot add a slave MSM, the slave will automatically do a sync to bring the master’s configurations over to the slave. However, if one of the configurations on the master MSM is empty, the sync process will not overwrite the corresponding configuration on the slave. If the configuration on the slave MSM is an older configuration, this can cause problems if the switch is rebooted using the outdated configuration (1-AJP7P).

Backplane Traffic

On the BlackDiamond switch, all backplane traffic is tagged. As a result, for cross-module traffic traversing the switch, dot1P QoS has the highest priority on egress (1-CPL8B).

QoS

If you configure QoS on an untagged ingress port, the dot1p bit of a packet leaving a tagged port on a different module is always replaced, even though dot1p replacement is disabled (1-E2UX2, 1-5I3VA).

System Related – Alpine Switches

Limited Commands Mode

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

Configuring Slots for the GM-4Xi and GM-4SXi

On the Alpine 3808 and Alpine 3804 switches, the only configurable option for The Alpine 1000BaseX I/O modules is the “GM-4Xi” option. When using EPICenter to manage the switch, EPICenter will display a slot mismatch for the GM-4SXi modules when configured as a GM-4Xi. The GM-4SXi will be fully operational and recognized as a “GM-4Xi” for the configured type (9884).

Using Configurations on Different Chassis

Configurations created in an Alpine chassis are not supported in a different model chassis. For example, a configuration from an Alpine 3808 is not supported in an Alpine 3804. Configurations for different models generate error messages for any line in the configuration that concerns unavailable slots.

If you load a configuration from a different model, you can safely write the correct configuration over the unsupported configuration.

System Related – Summit Switches

Summit48si Link Detection

If you configure the link detection level for a Summit48si as 3 or 4, ports 49 and 50 do not become active when the link goes down (PD2-117243907).

The sys-recovery-level shutdown Option

If you configure the `sys-recovery-level` for `shutdown`, Summit switches do not shut down links (PD2-111972310).

Autopolarity Automatically Enabled in Downloaded Configurations

If you download a configuration, autopolarity detection is automatically enabled on the Summit48si, even if you disabled it in the saved configuration. To work around this, disable autopolarity when you download the configuration (PD2-118279201).

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).

802.1Q and Odd Packet Sizes

When using 802.1Q tagged, odd size packets on 10/100 Mbps links cause the Summit48i to drop packets (1-EGCA8).

Memory Scanning and Memory Mapping

Memory scanning and memory mapping behavior differs based on the platform, the mode you configure (online or offline), and whether you configure auto-recovery or run the diagnostics manually.

Table 2 describes the behavior of the switch if you configure auto-recovery using the `config sys-health-check` command. The behavior differs based on the hardware configuration, the mode selected (online or offline), and the number of errors detected.

Table 2: Auto-recovery memory scanning and memory mapping behavior

Platform	Online	Offline	New Errors Detected	Behavior
Alpine	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch enters limited commands mode.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.

Table 2: Auto-recovery memory scanning and memory mapping behavior (continued)

Platform	Online	Offline	New Errors Detected	Behavior
Summit	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch enters limited commands mode.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.
BlackDiamond with one MSM64i (or slave MSM64i is offline)	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch enters limited commands mode.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.
BlackDiamond with two MSM64i's, errors on Master	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	Master MSM64i fails over.
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, Master MSM64i fails over.
BlackDiamond with two MSM64i's, errors on Slave	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	Slave MSM64i taken offline.
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, Slave MSM64i taken offline.
BlackDiamond with two MSM64i's, errors on both	✓		0	Both kept online.
	✓		1-7	Errors mapped, both kept online.
	✓		>7	Errors not mapped, both kept online.
		✓	0	Both enter limited commands mode.
		✓	1-7	Errors mapped, both kept online.
		✓	>7	Errors not mapped, both enter limited commands mode.
BlackDiamond 6816 MSM64i's in slots C and D	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	MSM64i taken offline
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, MSM64i taken offline.

Table 2: Auto-recovery memory scanning and memory mapping behavior (continued)

Platform	Online	Offline	New Errors Detected	Behavior
Alpine and BlackDiamond "*i*" series I/O modules	✓		0	Module kept online.
	✓		1-7	Errors mapped, module kept online.
	✓		>7	Errors not mapped, module kept online.
		✓	0	Module taken offline
		✓	1-7	Errors mapped, module kept online.
		✓	>7	Errors not mapped, module taken offline.

Table 3 describes the behavior of the switch if you run diagnostics manually using the `run diagnostics` command with the `normal` option. The behavior differs based on the hardware configuration, the mode selected (online or offline) using the `config sys-health-check` command, and the number of errors detected.

Table 3: Manual diagnostics memory scanning and memory mapping behavior, normal

Platform	Online	Offline	New Errors Detected	Behavior
Alpine	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch kept online.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.
Summit	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch kept online.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.
BlackDiamond with one MSM64i (or slave MSM64i is offline)	✓		0	Switch kept online.
	✓		1-7	Errors mapped, switch kept online.
	✓		>7	Errors not mapped, switch kept online.
		✓	0	Switch kept online.
		✓	1-7	Errors mapped, switch kept online.
		✓	>7	Errors not mapped, switch enters limited commands mode.
BlackDiamond with two MSM64i's, errors on Master	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	MSM64i kept online.
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, Master MSM64i fails over.

Table 3: Manual diagnostics memory scanning and memory mapping behavior, normal (continued)

Platform	Online	Offline	New Errors Detected	Behavior
BlackDiamond with two MSM64i's, errors on Slave	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	MSM64i kept online.
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, Slave MSM64i enters limited commands mode.
BlackDiamond 6816 MSM64i's in slots C and D	✓		0	MSM64i kept online.
	✓		1-7	Errors mapped, MSM64i kept online.
	✓		>7	Errors not mapped, MSM64i kept online.
		✓	0	MSM64i kept online.
		✓	1-7	Errors mapped, MSM64i kept online.
		✓	>7	Errors not mapped, MSM64i taken offline.
Alpine and BlackDiamond "*i*" series I/O modules	✓		0	Module kept online.
	✓		1-7	Errors mapped, module kept online.
	✓		>7	Errors not mapped, module kept online.
		✓	0	Module kept online.
		✓	1-7	Errors mapped, module kept online.
		✓	>7	Errors not mapped, module taken offline.

Table 4 describes the behavior of the switch if you run diagnostics manually using the `run diagnostics` command with the `extended` option. The behavior differs based on the hardware configuration and whether errors are detected (the mode selected has no effect).

Table 4: Manual diagnostics memory scanning and memory mapping behavior, extended

Platform	Errors Detected?	Behavior
Alpine	Y	Switch enters limited commands mode.
	N	Switch kept online.
Summit	Y	Switch enters limited commands mode.
	N	Switch kept online.
BlackDiamond with one MSM64i (or slave MSM64i is offline)	Y	Switch enters limited commands mode.
	N	Switch kept online.
BlackDiamond with two MSM64i's, errors on Master	Y	Master MSM64i fails over.
	N	MSM64i kept online.
BlackDiamond with two MSM64i's, errors on Slave	Y	MSM64i taken offline.
	N	MSM64i kept online.
BlackDiamond 6816 MSM64i's in slots C and D	Y	Module taken offline.
	N	Module kept online.
Alpine and BlackDiamond "*i*" series I/O modules	Y	Module taken offline.
	N	Module kept online.

Table 4: Manual diagnostics memory scanning and memory mapping behavior, extended (continued)

Platform	Errors Detected?	Behavior
BlackDiamond non-"*i*" series I/O modules	Y	Module taken offline.
	N	Module kept online.

Command Line Interface (CLI)

Do Not Use the Encrypted Option from the CLI

There is an option available in the CLI for encrypting a password in commands that specify access or authentication. This includes commands to create and configure accounts, to set the shared secret for RADIUS or TACACS+, for setting the SNMP community strings, for access to various services related to SLB, and others. *Do not use the encrypted option in these commands.* It is for use only by the switch when uploading and downloading an ASCII configuration file, so that passwords are not indicated in clear text within the configuration file (4229, 4719).

CLI Parser Limitation

The CLI parser is limited to 200 characters, including spaces and tabs. If the number of characters exceeds 200, the switch will return a "stack overflow" error. While the excess characters are clipped, the first 200 characters are correctly processed.

"show iproute" Command

The `show iproute` display has a special flag for routes that are active and in use, these routes are preceded by an "*" in the route table. If there are multiple routes to the same destination network, the "*" will indicate which route is the most preferable route.

The "Use" and "M-Use" fields in the route table indicate the number of times the software routing module is using the route table entry for packet forwarding decisions. The "Use" field indicates a count for unicast routing while the "M-Use" field indicates a count for multicast routing. If the use count is going up in an unexpected manner, this indicates that the software is making route decisions and can be something to investigate further.

Cosmetic PING Errors

When a ping is unsuccessful, the initially reported number of transmit frames is four, but in actuality the switch will continue to try beyond the four frames. Accurate statistics are reported after hitting a carriage return to terminate the ping function (5132).

When a ping is redirected, the statistics for the last packet received are reported as lost but in fact the ping was successful (5170).

Serial and Telnet Configuration

Be sure you have specified VT-100 terminal emulation within the application you are using (2125, 2126).

Be sure to maximize the telnet screen in order for automatically updating screens to display correctly (2380).

Displaying Management Port with show port config

The `show port config` command will only display the "mgmt" port configuration information if the "mgmt" port is explicitly defined in the command - i.e., `show port mgmt config` (8604).

Auto Negotiation and 1000BaseT Ports

Note that per specification, auto-negotiation cannot be disabled on 1000BaseT ports (8867).

Switching and VLANs

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).

Cannot Delete "mgmt-1" VLAN

A VLAN created with the name "mgmt-1" cannot be deleted (1-EEUPE).

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).

Management Port IP Address

Do not assign an in-band IP address to the management port VLAN. The management port VLAN is an out-of-band VLAN, so if it is assigned an in-band IP address (an address where the source and destination are in the same subnet), the switch will treat it as a normal VLAN and attempt to route traffic through it (14426).

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 6.2.0 switch. In v 6.2.1 the default value has been changed back to 300 seconds. However, when upgrading from 6.2.0 to 6.2.1, the default value will remain and 1800 seconds. For upgrades from earlier versions of 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).

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.

Modifying the Protocol “IP”

If you wish to modify filters associated with the pre-defined IP protocol, use the full syntax of the command. For example `config ip add` produces an error message but `config protocol ip add` works correctly (2296).

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).

GVRP/GARP

GVRP is currently not supported in ExtremeWare 6.1 and later.

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.

Maximum Number of VLANs Supported

The maximum number of VLANs supported on the BlackDiamond, Alpine, and Summit “*i*”-series switches is now 3000. To configure more than 1024 VLANs, the CPU-transmit-priority level must be set to “normal”. The CPU transmit priority is set to “high” by default to control the priority in which packets are transmitted from the switch in the event that lower priority queues are congested. This mechanism uses internal resources and limits the number of VLANs that can be configured on a switch. The following CLI command must be used to set the CPU-transmit priority:

```
config cpu-transmit-priority [high | normal]
```

To view the configured CPU-transmit priority, use the following command:

```
show switch
```

Note that the switch must be rebooted for this change to take effect. The default setting for the CPU-transmit priority is “high” (7120).

If non-“*i*” series I/O modules are installed in a BlackDiamond Chassis, the maximum number of VLANs supported will be 1024 (8908).

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).

MAC Security

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

Mirroring

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).

Load Sharing

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).

Enabling the Master Port.

Enabling the master load-sharing port can cause the redundant port to transition (PD2-105853230).

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 when the system is rebooted (8589).

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 Port Configuration

All the ports in a load sharing group must have the same exact configuration, including auto negotiation on/off, duplex half/full, ESRP host attach (don't-count), and so on.

Load Sharing and Software Controlled Redundant Port

When both Software Controlled Redundant Port and Load Sharing are configured, the following behaviors apply.

For fail-over to the redundant group of load shared ports:

- If the primary group of load shared ports is active, and one or more links in that group fail, the entire load shared group of ports will fail-over to their corresponding software controlled redundant ports configured as a redundant group of load shared ports (provided that enough links can be established on the redundant group of load shared ports to be greater than the number of active links remaining in the primary load shared group of ports).

For fail-back to the primary group of load shared ports:

- If one link in the redundant group of load shared ports fails, and its corresponding primary port is up, the entire group of load shared ports will fail-back to the primary load shared group of ports.
- If one link in the redundant group of load shared ports fails, and the corresponding primary port is down, there will be no fail-back to the primary group of load shared ports.
- It is possible for the primary group of load shared ports to be up when the number of active primary ports is less than that of the redundant group of load shared ports. For example, assume ports 4, 5, and 6 are configured as a redundant group of load shared ports for the primary group of load shared ports 1, 2, and 3. If primary port 1 fails, the primary group of load shared ports will fail-over to redundant group of load shared ports with ports 4, 5, and 6 up. Then, if primary port 2 fails, the redundant group of load shared ports (ports 4, 5, and 6) will remain up. However, if redundant port 6 fails, the redundant group of load shared ports will fail-back to the primary group of load shared ports because the corresponding primary port (port 3) for redundant port 6 is still up.

Spanning Tree

Do Not Configure All Ports in s0

With the system watchdog timer enabled, if you configure a switch with many ports, all in s0, the system reboots if you perform the following in quick succession:

1 Delete ports from a VLAN

2 Add them to another VLAN

3 Delete them from that VLAN

4 Add them back to the first VLAN

To avoid this, do not configure all ports in s0. If you must configure all ports in s0, execute the changes slowly, so the switch can process the changes without triggering the watchdog timer (PD2-118450167).

Ports Remain in Listening State

If you disable STP on untagged ports that are protected and then enable STP, the ports remain in the listening state until you reboot the switch (PD2-72369003).

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 6.2.2b66 (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 not Supported with ESRP

Spanning Tree is not supported and should not be attempted in conjunction with ESRP.

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 Default Domain Association

Newly created VLANs are no longer associated with STPD “s0” or any other domain by default.

EMISTP and Ingress Rate Shaping

If a loop exists in your network, but STP is not enabled but 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 will generate the “Stpd s0, Port 1:1 does not exist” error message because that VLAN does not belong to domain s0 by default (1-BMP5D).

QoS

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).

Access Lists on BlackDiamond I/O modules

Currently, access lists function only on i-series I/O modules and do not function on the G4X, G6X, F32T and F32F I/O modules.

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.

VLAN QoS Between I/O BlackDiamond Modules

When using VLAN QoS on a tagged VLAN between i-series I/O modules and non i-series I/O modules (G4X, G6X, F32T, and F32F), the "`show ports qosmonitor`" will display the active ports between the new and existing I/O modules as using different queues (7116).

MAC QoS

Broadcast MAC QoS does not take effect on non-"*i*" series I/O modules on a BlackDiamond. If an FDB entry is created with a broadcast MAC address assigned to a QoS Profile, the entry will be ignored against that QoS Profile on non-"*i*" series I/O modules (8841).

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).

Access List Precedence Intervals

Access lists with large intervals (greater than 10) between precedence values now perform better. Previously, configuring access lists using large intervals (greater than 10) between precedence values could result in several-minute delays for each add transaction. We still recommend that you configure ACL precedence with an interval value of less than 5 between each rule. This configuration avoids any adverse performance issues such as very long delays between add transactions and loss of access to configuration sessions (1-B6F48).

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).

QoS and dot1p

If you configure VLAN QoS to a higher precedence than dot1p QoS using QoStype priority, egress traffic will go out through Q0 (1-CH3MD).

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

When monitoring QoS, do not use the `show port qos` and `enable qosmonitor` commands on the same port at the same time (PD2-64202681).

Bi-Directional Rate Shaping

1000BaseT Ports as Loopback Ports

If the loopback port for bi-directional rate shaping configurations is configured on 1000BaseT 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.

Changing the Configuration of a Loopback Port

If you change the configuration (speed, duplex setting, etc.) of a loopback port, you must either save the configuration and reboot the switch, or delete the port from the VLAN and add it back (PD2-127582534).

EAPS

EAPS Performance Statistics

Table 5 lists the EAPS performance statistics for a single EAPS domain.

Table 5: EAPS performance statistics

Protected VLANs	Link Down Convergence (ms)	Link Up Convergence (ms)
1	173	106
500	194	135
1000	200	161
3000	257	236

EAPS Secondary Port Recovery

The EAPS secondary port does not recover if the following events occur in the following order (1-FY31X):

1. The EAPS ring fails, due to a Hello timeout or a link failure.
2. The EAPS master node secondary port fails or is disabled.
3. The EAPS master node secondary port recovers or is re-enabled. The port incorrectly blocks incoming traffic even though it is enabled.

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).

ESRP

Software Redundant Ports with Different Speeds

If you configure a software redundant port with a different port speed than the master port, the switch with the redundant port might not count the port as down, which will affect the ESRP port count and cause an incorrect slave/master election (PD2-109325845).

Load Sharing and Restart Port

If you configure restart ports, only the loadsharing master port is restarted, not the member ports (PD2-110113289).

Watchdog Timer and Load Sharing with ESRP

If the system watchdog timer is enabled and you delete and add a loadsharing port that is down, the system reboots. To avoid this, disable load sharing before you delete a loadsharing port that is down (PD2-110113235).

Multicast and Host-Attach Ports

If you use a multicast MAC address for IP packets and you configure host-attach ports, the packets are forwarded by the slave ESRP switch (PD2-116540017).

Disable ESRP Before Deleting a Domain Member

If you delete a domain-member VLAN that has multinet enabled, the slave VLAN transitions to master VLAN. To avoid this situation, disable ESRP, delete the domain member, and enable ESRP (PD2-110325044).

IP/IPX VLANs in the show esrp Output

If you configure an IP VLAN with an IPX net ID, the output of the `show esrp vlan` command does not display the IPX VLAN (PD2-102292601).

ESRP and Ingress Rate Shaping

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

Dual Master Recovery Not Logged

When two switches recover from a dual-master situation, in rare situations the new master might not log the state change (PD2-111406501).

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).

Failover Priority 0 is Invalid

Do not use an ESRP failover priority of 0 (PD2-68325201).

Port Restart not Supported on Member VLANs

Port restart is not supported on member VLANs; only the ESRP master VLAN (PD2-105118406).

IPX VLANs in the show esrp Command Output

The `show esrp` command output does not contain VLANs with both IPX and IP enabled (PD2-102292601).

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 Super-VLANs

The super-VLAN must contain all ports belonging to the sub-VLANs in order to operate properly as an ESRP VLAN (PD2-106782858). The ESRP active port counter counts the number of physical ports on the sub-VLANs.

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).

ESRP Hello Timer

If you have over 2,500 ESRP VLANs and 256,000 FDB entries, we recommend that you set the hello timer to more than 3 seconds to avoid spurious transitions (PD2-89481305).

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).

Neighbor Timeout in Large Configurations

In a large ESRP configuration, the slave ESRP VLAN might inadvertently become the master ESRP VLAN. This can occur when FDB entries are flushed during a master-slave transition. A large number

of VLAN and FDB entries can cause an ESRP neighbor timeout. To avoid this we recommend the general neighbor timeout guidelines listed in Table 6 (PD2-106782884).

Table 6: General neighbor timeout

Number of Domains	Number of VLANs	Number of Active ports	Suggested Neighbor Timeout (sec)
64	1000	6 or more	> 8
48 or more	1500	4 or more	> 10
48 or more	2000	4 or more	> 11

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.

EPD MAC Error

If you create, delete, or modify a VLAN tag when there are 256,000 MAC address, you might receive the following error message:

```
updateEdpFilter401: Unable to locate EDP MAC (VID=0xffd)
```

Clear some MAC addresses to restore ESRP functionality (PD2-90054207, PD2-90223201).

Multiple ESRP VLANs

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

ESRP Interoperability

We recommend that all switches participating directly in ESRP be running the same revision of ExtremeWare. If you must mix ExtremeWare revisions, do not use new ExtremeWare 6.1 ESRP features. These include route tracking and the ability to modify the election algorithm.

Mixing Clients and Routers on an ESRP-Enabled VLAN

Typically, ESRP is not be enabled on a VLAN that is also expected to exchange routes with other non-ESRP routers (e.g.: routers using RIP or OSPF). ESRP is intended and designed as a Layer 2 or Layer 3 redundancy method for clients with a single default route. ESRP's fail-over operation may interfere with normal routing protocol communication if an ESRP-enabled VLAN contains other routers not using ESRP (4874).

Ensure that EDP is Enabled

The Extreme Discovery Protocol must be enabled on the ports involved with ESRP in order to function correctly. By default EDP is enabled on all ports. To verify this, use the command "`show port <portlist> info`". To enable EDP on a port, use the command "`enable edp ports <portlist>`" (4072).

ESRP and Bi-Directional Rate Shaping

When a single ESRP VLAN is configured with bi-directional rate shaping ports and no direct physical connection to the 2nd ESRP router, the ESRP slave router flips back and forth to Master state. If a second rate-shaped VLAN or a direct link between the 2 ESRP routers exists, this will not occur (10739).

When ESRP and bi-directional rate shaping are configured simultaneously on the same switch, rate shaping traffic to the ESRP MAC address will not take effect until the switch is rebooted (13583).

ESRP Ping Tracking

The ESRP Ping Tracking option cannot be configured to ping an IP address within an ESRP VLAN subnet. It should be configured on some other normal VLAN (across the router boundary) (1-C5S6U).

VRRP

The show tech-support Command Through Telnet

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 transitions to master and back. To avoid this, use the `show tech-support` command only through a direct console connection (PD2-128764506).

IP Unicast Routing

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).

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).

VLAN Aggregation

Moving a sub-VLAN Client. When a client is moved from one sub-VLAN to another, the client may not be able to ping or communicate through the super-VLAN until the client has cleared its IP ARP cache for the default router or the switch has that IP ARP cache entry cleared (4977).

No Static ARP Entries. The use of Static ARP entries associated with superVLANs or sub-VLANs is not supported in this release (5106).

VLAN Aggregation and ESRP. A sub-VLAN should not be configured to run ESRP. The system will allow you to enable ESRP on a VLAN and then designate the VLAN as a sub-VLAN, but this is not a supported configuration (5193).

Multinetting

Multinetting and IP Multicast Routing. Combining any type of IP multicast routing on VLANs that are also part of an IP multinetted group is not supported (4418).

Multinetting and Client Default Gateways. It is critical that clients attached to multinetted segments have their default gateways correspond to the same subnet as their IP addresses and that subnet masks be configured correctly. Not doing so will result in slow performance of the switch (4938).

Multinetting and the Show VLAN Stats Command. The CLI "`show vlan stats <vlan_name>`" command is not supported on multinetted VLANs.

Multinetting and VRRP. Multinetting is not supported with VRRP.

RIP Routing

RIP V2 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.

IP Multicast Routing

Use the always Parameter to Guarantee Advertisement

The `enable rip originate-default` command does not always advertise the default RIP route to peers. To guarantee that the default RIP route is advertised, use the `always` parameter (PD2-124368763).

(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

NOTE

For proper Cisco interoperation, you must run 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).

IGMP & IGMP Snooping with IP Unicast and Multicast Routing

IGMP snooping and IGMP must be enabled when unicast IP routing, multicast routing, or VRRP are configured on the switch. By default, both IGMP and IGMP snooping are enabled. You can check this using the `show ipconfig` command (5112).

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).

OSPF

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).

A Large Number of FDB Entries and the disable ospf Command

If the SPF algorithm is being calculated on a switch with a large number of IP FDB entries and you use the `disable ospf` or `disable ospf export` commands (which purge OSPF LSAs), some routes that were installed based on these LSAs might remain in the IP routing table even after the LSAs are cleared from the OSPF database (PD2-103006530).

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).

BGP

Routes Advertised from a Route Reflector

The switch does not perform a next hop self-configuration when it receives a route advertised from a route reflector client (PD2-118471893).

Route Dropped if Switch's AS is First AS in Path

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 dropped as a loop. To avoid this, do not prepend the switch's AS number to the AS path (PD2-126767401).

Multi Exist Discriminator Not Compared

If a route is received from the same AS via EBGP and the IBGP peer, the switch does not compare the multi exist discriminator. To avoid this, use the `enable bgp always-compare-med` command (PD2-126767407).

Aggregate Routes After a BGP Soft Reset

When BGP is soft reset outbound, aggregated routes are not withdrawn or advertised when a corresponding blackhole route is present in the KRT (PD2-130524901).

IPX Routing

Tuning

In larger environments, it is helpful to increase the IPX SAP and IPX RIP update intervals to reduce CPU load (e.g. from default of 60 to 120 seconds).

To increase route stability, you may wish to increase the hold multiplier (default is 3 for 180 seconds), To modify these parameters use the following CLI commands: (4859).

```
config ipxrip <vlan name> update-interval <time> hold-multiplier <number>

config ipxsap <vlan name> update-interval <time> hold-multiplier <number>
```

IPX and Round-Robin Loadsharing

Due to packet sequencing problems, it is not recommended that IPX loadsharing run in conjunction with the round-robin loadsharing algorithm (8733, 9467).

IPX Performance Testing Using Traffic Generators

When using traffic generation equipment to test the wire-speed capability of IPX routing, if entries are allowed to age out with the ports remaining active, those entries cannot be re-learned on that port and will not be forwarded at wire-speed. Restarting the port or clearing the FDB will not address this issue. In a “real-world” IPX environment, clients and servers generally do not lose communication with the directly attached switch for the FDB entries to age out (9338).

IPX and Bi-Directional Rate Shaping

Bi-directional Rate Shaping is not supported in conjunction with IPX traffic (9226, 9153).

Security and Access Policies

RADIUS

When RADIUS authentication is configured on a BlackDiamond switch, upon reboot, the user 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.”
```

TACACS+ and RADIUS

If TACACS or RADIUS is enabled, but access to the TACACS/RADIUS primary and secondary server fails, the switch uses its local database for authentication.

SSH

When entering a pregenerated key using the `config ssh2 key pregenerated` command, separate groups of 99 characters (or less) with the ASCII newline character <LF> (PD2-82345223). To finish, enter a newline on a separate line.

Network Login

If you misconfigure your RADIUS server user accounts with the Extreme-Netlogin-VLAN attribute for a VLAN that does not exist on the switch, you cannot log in via Network Login with the misconfigured user account. After you correct the configuration, any previously attempted invalid session attempts must be cleared using the `clear session` command (PD2-101984392).

Server Load Balancing

Server Load Balancing and ESRP

Ping checking might count configured servers as active whether they are or not if ESRP transitions to the slave. To work around this, disable and enable SLB (PD2-116382046)

Default Ping Health Checking

For Transparent and Translational modes, the layer 3 PING is enabled for all members of a pool when it is defined. If a server is configured not to respond to ICMP Echo Requests, the server will be marked "down" after the first ping check interval of 30 seconds. The ping health checking can be disabled using the command:

```
disable slb node {all | <ipaddress>} ping-check
```

Server Load Balancing with 3DNS

3DNS is used as a global load balancing and site redundancy tool. Additional information concerning individual server health and performance can be gathered by 3DNS from the SLB services within the Extreme switch for more granular and accurate decision making by the 3DNS device. These additional functions apply when using Transparent or Translational modes. To enable responses to F5's 3DNS `i_query` requests from Extreme's SLB services, use the command:

```
enable slb 3dns iquery-client
```

To see what 3DNS devices are currently communicating with the SLB enabled switch, use the command:

```
show slb 3dns members
```

To disable responses to 3DNS queries, use the command:

```
disable slb 3dns iquery-client
```

The SLB enabled switch responds to directed queries from 3DNS. To direct 3DNS queries to the switch, you add a "Big/IP" device to the 3DNS configuration. Encrypted communications with 3DNS is currently not supported. These functions were tested with 3DNS v2.x and should function correctly with v3.x.

Web Cache Redirection/Policy Based Routing

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).

Health Checking

Under very high sustained loads a Web Cache Redirect may fail and a cache server is set to the "down" state and then brought 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 may 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
```

The FDB table will time out before the IPARP table on the ports connected to the cache servers. To work around this configure the switch to have a higher FDB time-out than the IPARP time-out.

An ICMP PING of the next hop address is turned on by default and cannot be disabled.

VLAN boundary

Web Cache Redirection traffic must come in on an "*i*"-series switch running version 6.1 or better software. Traffic that satisfies a flow redirection must otherwise have been forwarded at layer 3 (packets must cross a VLAN boundary). For example, in a Cache Redirection application the client traffic and the ultimate destination they wish to go to needs to cross a VLAN boundary within the switch, however the caches themselves may reside on the client VLAN or any VLAN on the switch. In instances where the clients and servers belong to the same subnet, the functionality can still utilized by using the proxy ARP functionality in the switch with minimal configuration changes to clients or servers.

WCR and SLB on the Same Switch

When configuring switches to use SLB and WCR simultaneously, ensure that no overlapping layer 4 IP ports exist in the configuration. TCP/UDP ports must be completely independent for WCR and SLB parameters. In this configuration, a request to a cache box cannot initiate a request for information from a SLB VIP as this would violate the overlap of L4 ports.

NOTE

Extreme Networks strongly recommends running SLB and WCR on separate switches.

Precedence of Flow Redirection Rules

Multiple flow redirection rules can overlap in making a redirection decision. In these cases, precedence is determined by "best match" where the most specific redirection rule that satisfies the criteria will win. The criteria for best match is determined in the following order:

- Destination IP address/mask
- Destination IP Port or Source IP port
- Source IP address/mask

In general, the following rules apply:

- If a flow with a comparatively better matching mask on an IP address satisfies the content of a packet, that flow will be observed.
- If one flow redirection rule contains 'any' as an L4 protocol and a second flow redirection rule contains explicit L4 port information, the second will be observed if the packet contains matching L4 information.

- If one flow has a comparatively better match on source information and a second flow has comparatively better match on destination information then the rule with the better match on the destination information will be selected.

For example, in the following 2 cases, the rule with the best match (using the above criteria) is the rule that is selected.

Table 7: Flow rule example 1

Rule #	Destination IP Address	Destination IP Port	Source IP Address	Priority Selection
1	192.0.0.0/8	80	ANY	1
2	192.168.0.0/16	ANY	ANY	2

In this case, Rule 1 is the rule with the best match as it contains an explicit Destination IP Port even though the mask for the Destination IP Address is less specific.

Table 8: Flow rule example 2

Rule #	Destination IP Address	Destination IP Port	Source IP Address	Priority Selection
1	192.168.2.0/24	80	ANY	2
2	192.168.0.0/16	ANY	10.10.10.0/24	4
3	192.168.2.0/24	ANY	10.10.0.0/16	3
4	192.168.2.0/24	80	10.10.0.0/16	1

In this case, Rule 4 is the rule with the best match as it again contains an explicit Destination IP Port.

NetFlow

If a flow record filter is configured on one port with type “match-all-flows” you cannot configure the same flow filter on any other port (1-7G1D8).

WEB Management - VISTA

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

Summit5i LX ifMauType MIB Object

The show ports statistics command output does not display statistics for ports 13 - 16. This affects the ifMauType MIB object, which does not contain a value for these ports (PD2-117277540).

Loopback Address Not Returned

If you send an SNMP request to the loopback IP address, the responses originate from the configured IP address, not the loopback address (1-7DBS0).

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).

Entries in the alarmTable

Entries in the alarmTable related to SMON, extremeRtStats, and extremeVlanL2Stats can create spurious corrupt entries after a save and reboot (PD2-91569801).

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).

Adding or Deleting a Trapreceiver

Adding or deleting a trapreceiver does not detect the correct community string (1-9I5LD).

Incrementing the intfIf Value

With a getnext or bulkget on a non-existent ifTable object ID, the intf returns next OID value instead of incrementing the intfIf (2-H1OOF).

WinSCP2 Not Supported

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

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

SNMP and the BGP MIB

When exercising the route table in the BGP MIB, high SNMP utilization messages will be printed to the system log (11718). This access to the MIB has no adverse effects to any protocol stability (i.e., ESRP, OSPF, BGP).

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).

Some of the counters for DHCP/BOOTP statistics do not display the correct value. As a result, DHCPRelay statistics are not correctly reported in the IPStats (PD2-73587422).

DLCS

DLCS is only supported on “i” series modules (8389).

Virtual Chassis

The Virtual Chassis is not supported in ExtremeWare 6.0 or higher.

Troubleshooting

System Watchdog with 1,000 Sub-VLANs

If you have the system watchdog enabled on a switch with a super-VLAN containing 1,000 or more sub-VLANs, each with four active tagged links, and you save the configuration and reboot the switch, the switch constantly reboots. To stop the switch from rebooting, remove active links until there are three remaining, and disable the system watchdog (PD2-106673778).

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).

Issues Resolved in ExtremeWare 6.2.2b108

The following issues were resolved in ExtremeWare 6.2.2b108. Numbers in parentheses are for internal use and can be ignored.

General

If 256,000 or more FDB entries are injected into the switch and then you create a new VLAN, that VLAN now correctly has an FDB entry (PD2-97137701).

The check for duplicate MAC addresses on switches from different manufacturers now works (PD2-110588018).

You can no longer enable mirroring on a port where mirroring is already configured (PD2-91960401).

The switch now correctly floods at layer 2 when a static IPARP entry exists (PD2-81903365).

The output of the `show configuration` command now correctly displays the quotation marks for the VLAN and access-profile name in a PIM candidate RP configuration (PD2-95046722).

BlackDiamond

If an MSM64i has 8 or more SRAM errors detected and is thus rebooted, it now passes the POST diagnostics.

The EPICenter save image primary / save image secondary / synch macro, or rapid execution of the same commands, no longer causes MSM B to reboot (PD2-108085984).

The MPLS MAC address is now correctly created in the FDB table when the FDB contains a large number of entries (PD2-88340101).

The F96Ti and G12SXi modules no longer lose the connection to the MSM64i (PD2-93060104, PD2-117966817).

Traffic through some slots in a BlackDiamond 6816 chassis is no longer blocked if you have multiple MSM master / slave transitions (PD2-126693691).

Hot-swapping a module no longer generates extraneous layer 2 broadcast packets (PD2-111329515).

Alpine

Messages are now correctly logged for system health check events (PD2-129795601, PD2-131405301).

Excessive transmission collision errors no longer occur on the FM-32Ti module in an Alpine 3808 switch (15772, PD2-109830730).

Summit

Traffic no longer leaks to another VLAN when cold booted in a Summit48si (PD2-109830701).

ESRP

ESRP traps are now sent for neutral state (PD2-107596623).

When host attach is enabled on the slave, traffic is now bridged to the master (PD2-109325856).

A WARNING log message is logged if the ESRP state changes to neutral when dual master is detected (PD2-110124001).

Restart port now works with an IP address on a VLAN or priority of 255 (PD2-108394424).

For the ESRP election algorithms that do not use MAC addresses, the ESRP master election state is now correct (PD2-108394414).

An ESRP PDU is required when ESRP state is transitioning from neutral to slave (PD2-110315703).

ESRP packets received on domain member VLANs are now passed on by ESRP enabled switches (1-5YTYA).

A flapping redundant link can no longer cause an incorrect ESRP port count (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 now immediately flushes the FDB table (PD2-124371801).

You can now configure the neighbor timeout to be higher than 30*hello timer (PD2-122556701).

Missed hello messages from a neighbor are now logged. To view the messages, use the `configure debug-trace esrp-message <level>` command and set the level to 1 (or greater) (PD2-121690560).

Using the `show tech-support` command on the ESRP slave through a telnet connection when 2,000 VLANs are configured on the switch no longer causes ESRP transitions on the slave switch (PD2-88733904).

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

VRRP

Adding or deleting a VLAN in VRRP now only affects the IP forwarding entries associated with that VLAN (PD2-106763439).

IPX

If you have the system watchdog enabled, sending a large number of routes no longer triggers a watchdog timer reboot (PD2-101489860).

Multicast

The Rendezvous Point (RP) now correctly initiates an (S,G) entry when it receives an (S,G) shared tree or Rendezvous Point Tree (RPT) entry (PD2-106763473).

Multicast packets with multicast source address are correctly discarded (PD2-123631150).

The intermediate switch no longer uses a pruned (S,G) shared tree or RPT entry (PD2-88707601).

BGP

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

When a BGP route attribute changes, the FDB entry is now correctly updated (PD2-65698301).

The output of the `show bgp neighbor <ip> transmitted-routes detail all` command no longer displays blank lines between route entries (PD2-118471834).

Under specific denial of service (DoS) attacks, a BGP session no longer becomes unstable and loses connectivity to peers (PD2-95046777).

If IGP is continuously flapping, the BGP peer no longer becomes unavailable (PD2-115331420).

Corruption in the AS Path attribute no longer results in a software exception of the BGP task (PD2-97150871).

A software exception no longer occurs in the SNMP task when a large number BGP routes are being removed while an SNMP process is polling the BGP AS Path attribute table (PD2-125728353, PD2-99109689).

The BGP Local Preference value no longer displays a negative number (1-DTLIG).

Configuring a password for BGP while the BGP neighbor is enabled no longer generates an error message (2-H2EUA).

Route reflector clients and non-clients now display route attribute originator ID and cluster ID (PD2-70653901).

The BGP neighbor can now be deleted if the VLAN IP address is changed to same as the BGP neighbor IP address (1-DF2QP).

Reflected routes now display all of the cluster ID's along the path (PD2-71508109).

The route reflector cluster ID is now added for both the route reflector client and non-client (PD2-70653911).

OSPF

Static OSPF external routes exported from an NSSA are no longer occasionally lost (PD2-116382017).

Security

If a soft-rate limited port is enabled and re-enabled while the switch is under the SQL Slammer DoS attack, the modified port is now added correctly (PD2-118292101 / PD2-119748085).

The switch is no longer vulnerable to the SSHredder DoS attack as described in CERT advisory CA-2002-36 (PD2-115337501).

Vista

Configuring Spanning Tree parameters using Vista no longer generates HTTP errors (1-DF3U7).

SNMP and Vista no longer display port utilization statistics greater than 100 percent of the traffic rate (PD2-107301980).

SNMP

You can now use SNMP to configure a QoS rule with a netmask other than the default (PD2-64784803).

Troubleshooting

A reboot-loop configuration with a time interval of 10 and a count of 1 now operates correctly when you intentionally reboot (PD2-106469614).

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

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

In minimum mode the timezone in the log message is now correct (PD2-110637205).

The time parameter in the reboot command now operates correctly if you have configured reboot loop protection (PD2-111222216, PD2-111201401).

SNMP and RMON2 now correctly reboot the switch without triggering minimal mode (PD2-111307101).

The Error Packet count in the show cpu diag command output now matches the errors reported in the system log (PD2-131210001).

Issues Resolved in ExtremeWare 6.2.2b68

The following issues were resolved in ExtremeWare 6.2.2b68. Numbers in parentheses are for internal use and can be ignored.

General

The `show version` command now displays the PCB suffix correctly (PD2-116226601).

The `show version` command now displays the QC and CLEI fields correctly (PD2-101476901).

As of ExtremeWare 6.2.0, you can use mirroring and the system health checker together (11222).

BlackDiamond

Fan tray status is now correctly checked and error messages are correctly logged (PD2-63609301, PD2-116415801).

With continuous traffic over 62,000 pps, FDB entries age out correctly (PD2-107596610).

Issues Resolved in ExtremeWare 6.2.2b56

The following issues were resolved in ExtremeWare 6.2.2b56. Numbers in parentheses are for internal use and can be ignored.

General

Upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.2 no longer corrupts permanent FDB entries (PD2-98730521).

False checksum error messages due to a software error when checking for a return code are no longer displayed to the system log (PD2-108354018).

When in limited commands mode, all links are now taken down (PD2-99107211).

Link transitions no longer generate additional checksum errors when checksum errors have already been recorded (PD2-104485401).

The `show diagnostics` output now correctly displays system health check status for Alpine and Summit switches, and the status LEDs now behave correctly (PD2-103356901).

Support added for a new OUI of 00-04-96-00-00-00 to 00-04-96-FF-FF-FF (base-16) (PD2-65050804).

BlackDiamond

The F96Ti and G12SXi modules no longer lose the connection to the MSM64i (PD2-93060104).

Multicast packets are now forwarded correctly after you disable IGMP snooping (1-EUCKP).

Alpine

If you download the default configuration and reboot the switch, erroneous health check messages are no longer recorded in the syslog after 4 minutes of operation (PD2-101622061).

When you enable sharing on an Alpine 3808 with slots 1 and 2 populated and slots 3 and 4 configured but not populated, the console no longer crashes (PD2-101622031).

When you configure load sharing for an unpopulated slot, save the configuration, and reboot the switch, the load sharing configuration is now implemented correctly (PD2-101622021).

Summit

The FDB now correctly recognizes ESRP-aware Summi48i redundant ports after a link transition, and the ESRP state is now also correctly recognized. In addition, connections to the redundant ports no longer show as simultaneously active after one of the redundant links transitions (PD2-89481383).

The LEDs on any ports connected to Summit48i ports 49R and 50R now operate correctly after a link transition within one second (PD2-97617503).

BGP

If you enable BGP and advertise 175,000 routes with RIP and OSPF already running, BGP no longer crashes (PD2-87756763).

If, when a BGP aggregate route becomes active, the advertised aggregate network is not available, ExtremeWare now adds a blackhole route to avoid a routing loop (PD2-80271343).

OSPF

OSPF now recalculates the cost of external routes correctly when a redistribution from static to OSPF is deleted and re-inserted (PD2-64596001).

In an environment with a large number of IPFDB entries associated with OSPF routes / default route, an OSPF change that caused an SPF calculation no longer consumes significant CPU cycles, which caused the system to become unresponsive for several minutes (PD2-99111708).

ESRP

The watchdog timer no longer reboots the switch after a large (100,000 entries) FDB table is cleared due to a link transition, the `clear fdb` command, an ESRP master / slave transition, etc. (PD2-86682761).

A link transition on a redundant switch no longer causes a momentary ESRP dual master situation (PD2-93199401, PD2-95068802).

If you remove a power supply or have an empty power supply bay, ESRP now changes the priority of the ESRP VLAN to the failover setting (PD2-86682767).

An ESRP transition with health checking enabled no longer causes a brief (10-20 msecs) broadcast storm on the network (1-9VHPA, 1-9VHOP).

When an ESRP master transitions to a slave, it now sends out a port restart on a gigabit port (1-9W4SH, 1-9W4R9).

You can now have an ESRP master VLANid of 1028 (PD2-86576752).

The slave ESRP VLAN no longer forwards traffic when the slave link transitions without an ESRP state change (PD2-89481303).

Spanning Tree

A large number of link transitions when there are a large number of VLANs in neighboring switches no longer causes the switch to run out of memory (PD2-89946701).

EAPS

A rapid link transition up, down, then up again on an EAPS transit switch no longer causes traffic disruption (PD2-102929324).

Issues Resolved in ExtremeWare 6.2.2b27

The following issues were resolved in ExtremeWare 6.2.2b27. Numbers in parentheses are for internal use and can be ignored.

General

The `enable web` and `disable web` commands no longer require a reboot to take effect (PD2-85458338).

A page break was added to the display format in the `show switch` command (PD2-70843722).

A software exception no longer occurs when using telnet to log in to switches. This occurrence was related to a system memory usage violation and would result in exceptions in tasks that appeared to be unrelated to the actual root cause [tNet, tOSPF, tpty0] (PD2-65438108).

The `config cpu-dos-protect` command no longer receives the wrong expiration counter (PD2-71951519).

On the Alpine and Summit switches, the `enable` or `disable sys-health-check` configuration parameter is now uploaded in the configuration file (PD2-64657201).

On the Summit48si and the F48Ti modules, adjustments were made to physical layer parameters to avoid the possibility of port level CRC errors when interoperating with various 10/100 connected devices (PD2-65114722).

Disconnected or failed Mini-GBICs on the Summit48si are now correctly recognized as inactive (PD2-80271359).

Modifications were made to PSU status checking on all platforms to avoid false PSU failure messages (PD2-63881218).

PSU input and output failure messages changed from INFO to CRIT in the system log (1-5IXTP).

BlackDiamond

The ACL hit counter now increments when a rule is applied to a port that is not on slot 1 (PD2-72319330).

Removal and insertion of an I/O module no longer causes log errors before the `synchronize` command is executed (PD2-64783016).

When running a high rate of multicast traffic, a BlackDiamond 6808 no longer stops forwarding packets and displaying "quake" error messages while connected to a BlackDiamond 6816 transmitting multicast and broadcast traffic across all 64 ports (PD 1-DCSSP).

Fan failure messages are no longer generated when upgrading to ExtremeWare 6.2.1 and ExtremeWare 6.2.2 (PD2-63609301).

Summit

A software exception no longer occurs in the tConsole task when using the `show igmp group` command on a Summit48si with IGMP messages flapping (PD2-64324233).

On the Summit48si, a chip initialization problem no longer causes CRC errors when the following are true:

- High traffic traversing ports 2, 10, 18, 26, 34, and 42
- Cables over 80 meters long

The problem was most acute when the switch was operated at cold temperatures (PD2-78758858).

Diagnostics

Alpine chassis no longer suffer intermittent failures in various slots when executing the `run extended diagnostics` command multiple consecutive times (PD2-65602092).

Failure modes are consistently reported between memory scanning and extended diagnostics (PD2-71316735).

Diagnostics failures and unrecoverable memory scanning failures on Summit and Alpine systems put the switches into limited command mode, making them consistent with behavior on BlackDiamond systems (PD2-82307201, PD2-82307203).

The `show diagnostics` command is now available when a system is in limited command mode (PD2-82953701).

The `clear log diag` command now clears the hardware error log on the system to allow you to bring the system back into operational mode (PD2-82816505).

Diagnostic results from a previous BlackDiamond module no longer exist after a hot removal/insertion of a different module (PD2-80411501).

If a single MSM64i in a BlackDiamond 6816 chassis fails diagnostics, the failed MSM64i now comes up in limited command mode for debugging purposes (PD2-80578751).

On Summit switches, normal diagnostics no longer displays text that includes the word “MSM” (PD2-83478305).

Load Sharing

When upgrading to ExtremeWare 6.2.x from ExtremeWare 6.1.9, configurations with address-based load sharing are now mapped to the new version of ExtremeWare (1-E5FS2/1-E5FR0).

Hot insertion of GM-4Xi, GM-4Si, and WDMi modules no longer causes Alpine systems to stop load sharing traffic (PD2-65287601). The following messages are no longer printed to the log:

```
Checksum Error on CPU received packet
health check packets are corrupted (type 3)
```

IP Routing

When the blackhole route becomes the best route, the ipfdb table is now dynamically updated (1-COWMJ).

IP Multicast

The Multicast Owner field in the `show ipmc cache` command no longer displays “0” in a large multicast topology, eliminating a connectivity issue where the join and prune messages would not be properly transmitted (PD2-64644201).

With 3 switches connected together in multi-access network, using the `clear igmp snooping` command on the intermediate switch no longer results in possible multicast packet loss (1-FOQ7O).

ACLs

On a BlackDiamond 6816, a configuration with 5,000 ACLs no longer causes an MSM64i reboot loop during an incremental configuration and subsequent reboot (PD2-64323672).

ESRP

In a large scale ESRP and STP environment, an ESRP failover while simultaneously transmitting broadcast packets no longer results in network flooding (PD2-63854015).

Hot removal and insertion of an F48Ti in slot 7 or 8 on a fully loaded BlackDiamond no longer results in an ESRP transition (PD2-64154928).

Using the `clear slot` command on a BlackDiamond module with many active ports no longer causes an ESRP transition (1-B6FYP).

ESRP now has the ability to have normal ports in a "don't count" mode. This is necessary for networks with asymmetrical counts of ports so that a port failure will not cause an undesired ESRP topology change (PD2-69799804).

EAPS

Based on certain combinations of EAPS+ ESRP design for layer 2 and layer 3 service protection, the EAPS Master node Secondary Port now always recovers upon certain downstream transit link failures. Such failures thus no longer result in the ESRP neighbor establishing 1 way connectivity only (1-FY31X).

VRRP

The load-sharing disable and enable commands now generate VRRP error messages correctly labeled "VRRP" (1-D3UFL).

A restriction was removed for VRRP configurations that used the same VRID for more than 4 VLANs (PD2-72590601).

STP

Injecting a high rate of broadcast traffic no longer causes STP 802.1d configurations to fail due to a CPU overload condition (PD2-64783002).

IPX

Duplicate internal VLAN IDs (intVLanId) are no longer assigned to multiple IPX VLANs, thus avoiding packet forwarding problems (PD2-72080203).

OSPF

An OSPF area can now be deleted after deleting a VLAN assigned to it (PD2-77020001).

The OSPF queue (QP6) no longer intermittently saturates with the cpu-dos-protect ACL rule (PD2-71270701).

DVMRP

A software exception no longer occurs in the tNetTask on a BlackDiamond running DVMRP with greater than 1000 streams after an I/O module hot-swap (PD2-65114401).

SNMP

A query of the extremeFdbMacFdbMacAddress MIB no longer returns the wrong output (.1.3.6.1.4.1.1916.1.16.1.1.3). (PD2-65602030).

Issues Resolved in ExtremeWare 6.2.2b18

The following issues were resolved in ExtremeWare 6.2.2b18. Numbers in parentheses are for internal use and can be ignored.

General

The `show diagnostics packet-memory slot` command now correctly records packet scanning and mapping defects (1-FHG21).

Exported OSPF, RIP, PIM, and route map configurations are now interpreted correctly when upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.1 (1-AHM25).

Software redundant 1000BASE-T ports now operate correctly with load sharing (1-AWZMN).

The show log command output no longer truncates the following error message (1-8EFVX):

```
<INFO:SYST> Checksum error (ffff in EEPROM vs 0 calculation) in card 1 memory defect
information, restore defau
```

Configurations that create large ACL or static FDB port lists now format the saved configuration so that a large list of ports no longer generates a “stack overflow when downloading” error (1-CND21).

If you disable smart redundancy, active backup links no longer fail over to the primary link (1-D3XCT).

Multiple simultaneous ARP entries are now handled correctly (1-DHY7W).

When you change the system time, ARP aging is computed properly (1-E3MRP).

Summit

The PSU status LEDs now operate as described in the *Consolidated Hardware Guide* (1-BMDGW, 12960).

Attempting to load BootROM 7.6 on a system with less than 128 MB of memory now generates an error message. In addition, attempting to run ExtremeWare 6.2.2 on system with less then 128 MB of memory now generates an error message and puts the system into limited mode (1-EIMNT).

Alpine

The `show diagnostics` command output now correctly displays information on the Alpine 3804 CPU (1-8TS79).

The `show slot` command output now correctly displays “FM32T” instead of “FM32” (1-AMDQP).

BlackDiamond

Enabling IGMP snooping on a BlackDiamond 6816 no longer generates an error message (1-BP5CD).

The power supply LEDs now consistently operate as described in the *Consolidated Hardware Guide* (1-9RC85).

The LEDs on the F48Ti now operate correctly when diagnostics take the card offline (1-9JX6Q).

Executing commands while the chassis is in “limited commands” mode no longer causes the MSM64i to crash (1-FAXIE).

The BlackDiamond 6816 does not power up using non iPower power supplies (1-FTW7L).

The `clear slot` command no longer causes the switch to reboot when a port on the I/O module belongs to 3,000 VLANs (1-FGFK5).

IPX

When a SAP entry was advertised with a network ID of zero, it was not added to the IPX services table. A value of zero indicates a local network and is now added with the local network number of the receiving interface (1-BTWKQ, 1-BTWK9).

VLANs

Two domains sharing a single VLAN now each have a unique VLAN tag (1-6EJM5).

If you create a VLAN with “mgmt” in the name, you can now delete that VLAN (1-EEUPY).

Mirroring

Enabling jumbo frames on mirroring ports without jumbo frames enabled on the monitor port now generates an error. To properly enable jumbo frames with mirroring, first enable jumbo frames on the monitor port and mirroring ports, then enable mirroring (1-8SJAL).

Load Sharing

If the master port is down, a restart now automatically restarts the next operational master (1-994B4).

If the master port is down, the FDB now correctly learns new MAC addresses (2-HAQAD, 2-H8KID, 2-H182X).

Spanning Tree

Do not configure a topology change time less than 15 seconds (PD2-64997595).

ESRP

On a Gigabit Ethernet port, port restart now correctly flushes the layer 2 ESRP-aware switch’s FDB (1-8S74I, 1-994AP, 11738).

EDP no longer floods packets when 3,000 or more VLANs are configured (1-6EH2H).

ESRP now correctly waits for the specified timeout before making state changes for a VLAN (1-E3TCC, 1-E3TE3).

VRRP

The performance of VRRP with large groups of VRIDs has been improved (1-5GS3X).

Attempting to configure two VLANs with the same port and VRID now generates an error message (1-F7C61, 1-DO0QD).

EMISTP

If you configure dot1d mode on tagged ports and delete the ports from the VLAN, the following error message is generated in the output for the `show stpd ports` command (1-81BID):

```
WARNING: s2 has dot1D port with no default vlan.
BPDU received on this port will not be flooded to other ports in the domain.
```

IP Multicast Routing

PIM is now correctly updated when the RP changes (1-CN8F8, 1-CN8FD).

Unconfiguring PIM now correctly sets the Register-Rate-Limit-Interval to the default (1-CMY1R).

BGP

The `show bgp neighbor <ip address> transmitted-routes all` command no longer crashes the system (1-AIDPH).

The `config debug trace bgp-misc` output now correctly displays a “Deleting Network” message (1-BZC4Z).

The transmitted route statistics for Aggregated Routes now displays the correct route statistics (1-CCDZT).

The output policy can no longer set the next hop while advertising the route to the IGP session (1-EP9V1).

The show bgp neighbor command output was modified to change “EBGP” and “IBGP” to “EGP” and IGP” (2-H09TL).

OSPF

OSPF SPF no longer make a directly attached network unreachable if that network moves multi-hops away (1-9D242, 1-9D23T).

The error message when VLAN deletion fails is more understandable (1-8SCKX).

OSPF now supports a minimum cost of 1, instead of 0 (1-8JFIL).

The `show ospf lsdb stat` command now operates correctly (1-81GWT).

Saving the configuration now correctly saves the OSPF filter (1-FQUPP).

EAPS

You now receive the following error message when attempting to add more than 64 EAPS domains (1-87LQ3):

```
<CRIT:EAPS> eaps.c 2639: Error! Reached maximum limit of EAPS instances
```

The EAPS Master Node now fails immediately when you disable a Primary or Secondary port (1-87LQI).

When the Primary port for an EAPS Master goes down, the secondary port comes up before the Primary port is deleted from the list of active ports, so that OSPF no longer re-converges (1-90L44).

You can no longer run EAPS without enabling EDP. Disabling EDP on an active EAPS Domain generates an error message and causes EAPS to be idle. You cannot configure a port that has EDP disabled as an EAPS ring port (1-9YM15).

NetFlow

You can now configure multiple ports with the `match-all-flows` type (1-7G1D8).

NAT

The NAT and UDP timeout values now work correctly (1-GAWX4, 1-5AJ9H).

SNMP

You can no longer use SNMP to rename or change the tag setting for the “default,” “Mgmt,” or “MacVlanDiscover” VLANs (1-ADUKD).

You can now create, configure, and delete a VLAN with a tag of 1 (16394).

You can now use SNMP to reset all QoS settings to the factory default (1-7YDFC).

The System ID now displays correctly (1-5AOFH, 14113).

The QoS profile priority is now displayed consistently in both the CLI and the SNMP MIB (1-7XD2X).

The extremeEdpPortIfIndex now records the correct value for port 4:1 (1-8SMO8).

You can now correctly configure WDMi modules in slots 4 and 8 using SNMP (1-CHMKY).

Flow Redirection

You can now enter any size netmask when creating a flow rule. If you configure subnet-based forwarding, all of the flow rules must use the same size netmask (1-64K4J, 11464, 16123).