ExtremeWare Release Note Summit24e3 Switch

Software Version 6.2e.1b17

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

Published: November 2002
Part Number: 120125-00 Rev 06

©2002 Extreme Networks, Inc. All rights reserved. Extreme Networks and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. ExtremeWare, ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Alpine, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrive logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

NetWare and Novell are registered trademarks of Novell, Inc. Merit is a registered trademark of Merit Network, Inc. Solaris is a trademark of Sun Microsystems, Inc. F5, BIG/ip, and 3DNS are registered trademarks of F5 Networks, Inc. see/IT is a trademark of F5 Networks, Inc.

All other registered trademarks, trademarks and service marks are property of their respective owners.

Author: Hugh Bussell, Megan Mahar

Editor:

Production:

Special Thanks:

Contents

Chapter 1 Overview

Supported Hardware **7**
- Summit24e3 GBIC Support 8
- Mini-GBIC Types and Specifications 8
  - *LX Mini-GBIC* *8*
  - *SX Mini-GBIC* *8*
- Safety Information 9

Supported Features **10**
- New Features in ExtremeWare v6.2e.1 10
- Features in ExtremeWare v6.2e.0 10

Chapter 2 Upgrading to ExtremeWare 6.2

Staying Current **13**

Upgrading the BootROM **13**

Upgrading ExtremeWare **13**
- Upgrading Switches 14
- Downgrading Switches 14

Chapter 3 Supported Limits

Supported Limits **15**

Chapter 4 Clarifications, Known Behaviors, and Resolved Issues

Clarifications and Known Behaviors **19**
- System Related 19
  - *Rate-Limiting Access List Rates* *19*
  - *Setting Auto-negotiation Off on a Gigabit Port* *20*
  - *Recovery Mode* *20*
  - *System Logging* *21*
  - *Enabled IdleTimeouts and Console Connections* *21*
  - *Xmodem Downloads* *21*

EDP Packet Length 21
TFTP Download of Configuration Files 21
Command Line Interface (CLI) 21
CLI Output for Power 21
Don't Use the Encrypted Option from the CLI 22
"show iproute" Command 22
Cosmetic PING Errors 22
Cosmetic Configuration Download Warnings 22
Console Appears Locked after Telnet Attempt 22
Serial and Telnet Configuration 22
Incorrect Counters 23
Switching and VLANs 23
Renaming System VLANs 23
Adding/Deleting a Port to an IP VLAN 23
Default Routes or Static Routes 23
Port Learning/Static FDB Entries 23
Port Learning 23
RIP Routing 23
RIP V2 Authentication 23
Spanning Tree Protocol 24
Reconnecting STP Link Causes Problems 24
WEB Management - VISTA 24
EAPS 24
Clearing FDB 24
SNMP 24
Port Mirroring 24
SMON dataSourceCaps 24
traceRouteCtlTable 24
lookupCtlTable 24
RMON Alarms not Generated 24
Trap Receivers as Broadcast Entry 24
Control of UDP Port Used in Sending Traps 25
SNMP Time-out Setting 25
Network Login 25
ISP Mode with RADIUS 25
DHCP Server 25
Documentation Errata and Addenda 25
Documentation Errata 25
Enable License Command is not Documented in User Guide 25
Configuring Switch Load Sharing Limits 26
IP Multicast Routing Section Should Be Ignored 26
Documentation Addenda 27
MAC-Based VLANs 27
MAC-Based VLAN Guidelines 27
MAC-Based VLAN Limitations 28
MAC-Based VLAN Example 28
Timed Configuration Download for MAC-Based VLANs 28
Issues Resolved in Current and Previous Releases 30

Issues Resolved in v6.2e.1b17 **30**
Switching and VLANs 30
Number of VLANs Supported *30*
Non-IP Multicast Forwarding *30*
Spanning Tree Protocol 30
BPDU Forwarding *30*
GVRP/GMRP 30
GVRP/GMRP Forwarding *30*
EAPS 30
EAPS Over Load-Sharing Links *30*
Load Sharing 31
Load Sharing Groups *31*
IP Multicast Routing 31
Enabling IPMC Forwarding *31*
Command Line Interface (CLI) 31
Packet Statistics *31*
CLEI/QC Information Display *31*
Issues Resolved in v6.2e.1b15 **31**
System Related 31
CRC Errors with Long Ethernet Cables *31*
Command Line Interface (CLI) 32
CLI Output for Temperature *32*
Redundant Ports (PHY) *32*
Issues Resolved in v6.2e.1b14 **32**
ESRP-Aware 32
ESRP-Aware Display and Operation *32*
SNMP 32
SNMP CERT Advisory 2002-03 *32*
Issues Resolved in v6.2e.0b10 **32**
General 32
Show Version String *32*
Issues Resolved in v6.2e.0b9 **33**
General 33
Switching and VLANs 33
IGMP 33
Load Sharing 33

1 Overview

These release notes contain information on features and issues specific to this release of ExtremeWare v6.2e not covered in the *Summit24e3 Switch Installation and User Guide*. Numbers that appear in parenthesis are used for internal reference and can be ignored

This chapter contains the following sections:

- "Supported Hardware" on page 7
- "Supported Features" on page 10

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.

Supported Hardware

This release supports the following hardware (support for hardware listed in *italics* is new for this release):

Table 1: Supported hardware

Extreme Switch Platform	ExtremeWare Filename/Version	BootRom Filename/Version
Summit 24e3	v62e1b17.xtr or v62e1b17_ssh.xtr / ExtremeWare v6.2e.1b17	S24e3_boot1_3.bin/v1.3

NOTE

This release of ExtremeWare is compatible with the Summit24e3 switch only.

Summit24e3 GBIC Support

The Summit24e3 switch supports the SFP GBIC, also known as the mini-GBIC. The system uses identifier bits to determine the media type of the mini-GBIC that is installed. The Summit24e3 supports only the Extreme Networks mini-GBIC.

Mini-GBIC Types and Specifications

This section describes the mini-GBIC types and specifications.

LX Mini-GBIC

Table 2 describes the LX mini-GBIC specification.

Table 2: LX Mini-GBIC Specifications

Parameter	Minimum	Typical	Maximum
Transceiver			
Optical output power	-9.5 dBm		-3 dBm
Center wavelength	1275 nm	1310 nm	1355 nm
Receiver			
Optical input power sensitivity	-23 dBm		
Optical input power maximum			-3 dBm
Operating wavelength	1270 nm		1355nm
General			
Total system budget			13.5 dBm

Total optical system budget for the LX mini-GBIC is 13.5 dBm. Measure cable plant losses with a 1310 nm light source and verify this to be within budget. When calculating the maximum distance attainable using optical cable with a specified loss per kilometer (for example 0.25 dB/km) Extreme Networks recommends that 3 dBm of the total budget be reserved for losses induced by cable splices/connectors and operating margin. Thus, 10.5 dBm remains available for cable induced attenuation. There is no minimum attenuation or minimum cable length restriction.

SX Mini-GBIC

Table 3 describes the SX mini-GBIC type and distances for the Summit24e3 switch.

Table 3: SX Mini-GBIC Types and Distances

Standard	Media Type	Mhz•Km Rating	Maximum Distance (Meters)
1000BASE-SX (850 nm optical window)	50/125 µm multimode fiber	400	500
	50/125 µm multimode fiber	500	550
	62.5/125 µm multimode fiber	160	220
	62.5/125 µm multimode fiber	200	275

Table 4 describes the specifications for the SX Mini-GBIC.

Table 4: SX Mini-GBIC Specifications

Parameter	Minimum	Typical	Maximum
Transceiver			
Optical output power	-9.5 dBm		-4 dBm
Center wavelength	830 nm	850 nm	860 nm
Receiver			
Optical input power sensitivity	-21 dBm		
Optical input power maximum			-4 dBm
Operating wavelength	830 nm		860 nm
General			
Total system budget			11.5 dBm

Total optical system budget for the SX mini-GBIC is 11.5 dBm. Extreme Networks recommends that 3 dBm of the total budget be reserved for losses induced by cable splices/connectors and operating margin. While 8.5 dBm remains available for cable induced attenuation, the 1000Base-SX standard specifies supported distances of 275 meters over 62.5 micron multimode fiber and 550 meters over 50 micron multimode fiber. There is no minimum attenuation or minimum cable length restriction.

Safety Information

Before you begin the process of installing or replacing a mini-GBIC, read the safety information in this section.

CAUTION

Mini-GBICs can emit invisible laser radiation. Avoid direct eye exposure to beam.

Mini-GBICs are a class 1 laser device. Use only Extreme-approved devices.

NOTE

If you see an amber blinking mini-GBIC port status LED on your Summit24e3 switch, you do not have an Extreme-supported mini-GBIC installed in your switch. To correct this problem, make sure you install an Extreme-supported mini-GBIC into the port on the switch.

Remove the LC fiber-optic connector from the mini-GBIC prior to removing the mini-GBIC from the switch.

Supported Features

The following sections list the features supported for the Summit24e3.

New Features in ExtremeWare v6.2e.1

The following list summarizes the features added and improved in v6.2e.1, the second major release for the Summit24e3.

- Network Address Translation (NAT)
- Ethernet Automated Protection Switching (EAPS) support
- Open Shortest Path First (OSPF) routing protocol
- Diffserv support
- Access list support for packet filtering and prioritization
- Access list support for rate-limiting
- Network Login
- Improved IP forwarding table update performance
- ICMP, IGMP, ARP reply, RIP, and OSPF packets to the CPU are prioritized for better performance
- IP packets addressed to the switch are prioritized to make remote administration of the switch more reliable

Some software features may require a license key. See the section “Software Licensing” in the *Summit24e3 Switch Installation and User Guide* for information on which features require a license. See the table “Enable License Advanced-Edge Command” on page 26 of this document for information on enabling software licenses.

Features in ExtremeWare v6.2e.0

The following list summarizes the features in ExtremeWare v6.2e.0, the first release of ExtremeWare for the Summit24e3.

- Access-policy support for routing protocols
- Virtual local area networks (VLANs) including support for IEEE 802.1Q and IEEE 802.1p
- Spanning Tree Protocol (STP) (IEEE 802.1D)
- Quality of Service (QoS) including support for IEEE 802.1p, MAC QoS, and four hardware queues
- Wire-speed Internet Protocol (IP) routing
- BOOTP client
- DHCP/BOOTP Relay
- Extreme Standby Router Protocol (ESRP) - Aware support
- Routing Information Protocol (RIP) version 1 and RIP version 2
- Wire-speed IP multicast routing support
- IGMP snooping to control IP multicast traffic
- TACACS+ support
- RADIUS client and per-command authentication support

- Console command-line interface (CLI) connection
- Telnet CLI connection
- SSH2 connection
- Simple Network Management Protocol (SNMP) support
- Remote Monitoring (RMON)
- Static Routes
- Standard MIBs
- Load sharing on multiple ports
- Port based mirroring for tagged and untagged packets
- Syslog support
- TFTP support for software/configuration updates

2 Upgrading to ExtremeWare 6.2

This chapter contains the following sections:

- "Staying Current" on page 13
- "Upgrading the BootROM" on page 13
- "Upgrading ExtremeWare" on page 13

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

The BootROM image comes preinstalled on the Summit24e3 from the factory. In the event that a new BootROM image is needed, use the following command:

```
download bootrom [ <host_name> | <ip_addr> ] <s24e3_boot.bin_name>
```

Upgrading ExtremeWare

This section describes how to upgrade to ExtremeWare v6.2e.1 and downgrade from ExtremeWare v6.2e.1 for Summit24e3 switches.

Upgrading Switches

ExtremeWare v6.2e can read a stored configuration saved by an earlier version of ExtremeWare v6.2e. 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. Use the `save primary` and `save secondary` commands to save the currently used configuration.
2. Configure the switch to use the primary image and the primary configuration. Use the `use image primary` and `use config primary` commands to configure the switch image and configuration.
3. Verify that all of the above procedures were completed successfully with the command `show switch`.
4. Upload the configuration of the switch to a TFTP server for safekeeping. Use the `upload config <ipaddress> <filename>` command to upload the switch configuration.
5. If not already running BootROM v1.3, TFTP download BootROM v1.3 to the switch. An example command is `download bootrom <ipaddress> S24e3_boot1_3.bin`. Reboot the switch to come up with BootROM v1.3.
6. TFTP download desired version of ExtremeWare v6.2e to the primary image space. An example command is `download image <ipaddress> v62e.xby.xtr primary`.
7. Reboot the switch. The previous configuration of the switch will be preserved going from the previous version of ExtremeWare to the desired version of ExtremeWare v6.2e. Verify that the switch is operating as expected. After verification, you may configure features specific to the current version of ExtremeWare. Save the configuration to the primary space, and do NOT save to the secondary configuration space unless until you are certain a downgrade to the previous image is not required.

Downgrading Switches

It is assumed that you have followed the upgrade instructions correctly and that the desired previous configuration has been preserved in the secondary configuration space.

1. If, per upgrade instructions, the secondary configuration was saved while using a previous ExtremeWare v6.2e or previous ExtremeWare v6.2e image, configure the switch to use the secondary configuration. Use the `use config secondary` command to use the secondary configuration. If there is no stored configuration saved for that version of ExtremeWare, you will need to re-configure or download the correct configuration file to the switch when running the desired image.
2. Use the image in the secondary image space by using the `use image secondary` command.
3. Verify that the above procedures were completed successfully with the `show switch` command.
4. Reboot the switch. If you have followed the upgrade instructions, your original configuration should be in place. If you do not have the correct configuration downloaded, you may provide minimal configuration for the switch through the CLI sufficient to TFTP download the configuration file generated during the upgrade procedure. If you do not have the configuration file, reconfigure the switch manually.

NOTE

When downgrading to a previous version of ExtremeWare, you must ensure that the switch configuration matches that version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported.

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 5: Supported limits

Metric	Description	Limit
Access Masks	Maximum number of access masks that can be configured by user	13
Access Lists/Rate Limits	Maximum number of access list rules, including rate limit rules	1014
Rate Limits	Maximum number of rate limit rules	315
Access Profiles	Used by SNMP, Telnet, SSH2, and Routing Access Policies	128
Access Profile entries	Used by SNMP, Telnet, SSH2, and Routing Access Policies	256
EAPS—Domains/switch	Maximum number of EAPS domains.	1
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	1
EAPS—VLAN links	Recommended maximum number of Control or Protected VLANs per switch.	128
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit
Load Sharing	Maximum number of ports per group Maximum number of groups	8 6
NAT—Maximum connections	Maximum number of simultaneous connections per switch.	4096
NAT—Maximum rules	Maximum number of rules per switch.	256
NAT—Maximum VLANs	Recommended maximum number of inside or outside VLANs per switch.	128

Table 5: Supported limits (continued)

Metric	Description	Limit
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF routes	Recommended maximum number of routes contained in an OSPF LSDB for a “real” network.	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	Maximum number of OSPF routed interfaces on a switch. Maximum number of passive OSPF interfaces	2 Unlimited
OSPF virtual links	Maximum number of OSPF virtual links supported.	2
OSPF adjacencies	Maximum number of OSPF adjacencies on a switch.	4
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
VLANs	Maximum number of VLANs (includes all VLANs).	255
IP Router interfaces	Maximum number of VLANs performing IP routing.	32
Spanning Tree—Maximum STPDs	Maximum number of Spanning Tree Domains.	64
Spanning Tree—Maximum number of ports	Maximum number of ports that can participate in a single Spanning Tree Domain.	Same as the number of available physical ports on the switch
IP Static Routes	Maximum number of permanent IP routes.	1024
IP Route Sharing Entries	Maximum number of IP routes used in route sharing calculations. This includes static routes and OSPF ECMP.	8
IP Static ARP entries	Maximum number of permanent IP static ARP entries supported.	512
Static IP ARP Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
Static MAC FDB entries	Maximum number of permanent MAC entries configured into the FDB.	128
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
FDB—Maximum number of L2 entries	Maximum number of MAC addresses for the Summit24e3.	8191
FDB—Maximum number of L3 entries	Maximum number of IP addresses for the Summit24e3	2047
Mirroring—Mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8 (however, more than 3 may affect performance)
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000

Table 5: Supported limits (continued)

Metric	Description	Limit
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	32

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 on page 19
- Issues Resolved in Current and Previous Releases on page 30

Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 6.2e.1.

System Related

CAUTION

In order for configuration changes to be retained through a switch power cycle or reboot, you must issue a 'save' command. For more information on the 'save' command, refer to the Summit24e3 Switch Installation and User Guide*.*

Rate-Limiting Access List Rates

The rate limit specified in the command line does not precisely match the actual rate limit imposed by the hardware, due to hardware constraints. The actual rate is in fact .94 times the CLI-specified rate. For example, if you specify a rate limit of 10 Mbps, the hardware imposes a rate of 9.4 Mbps. The same is true for the Gigabit ports; a CLI-rate of 128 Mbps equates to a hardware rate of 120.32 Mbps.

Table 6: Selected CLI Rate-Limits Compared to Actual Rate-Limit (Mbps)

100 Mbps Ports		1000 Mbps Ports (Gigabit Ports)	
CLI Rate	**Hardware Rate**	**CLI Rate**	**Hardware Rate**
1	.94	8	7.52
2	1.88	16	15.04

Table 6: Selected CLI Rate-Limits Compared to Actual Rate-Limit (Mbps) (continued)

100 Mbps Ports		1000 Mbps Ports (Gigabit Ports)	
CLI Rate	**Hardware Rate**	**CLI Rate**	**Hardware Rate**
10	9.4	80	75.2
20	18.8	160	150.4
30	28.2	240	225.6
40	37.6	320	300.8
50	47	400	376
60	56.4	480	451.2
70	65.8	560	526.4
80	75.2	640	601.6
90	84.6	720	676.8
100	94	800	752
		880	827.2
		960	902.4
		1000	940

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 25 auto off duplex full speed 1000
```

will turn auto-negotiation off if port 25 is a gigabit port.

Recovery Mode

The switch checks the switching device periodically. If there are any hardware faults, the switch will attempt to recover by clearing the error or resetting the device. Normally, this is enough for the switch to recover from the faults. If the switch is unable to recover from the faults by resetting the device, the next level of possible recovery is a switch reboot. The automatic reboot will occur only if the Recovery Mode is set to “critical” or “all”. By default, the Recovery Mode is “none”. To change the Recovery Mode, use the following command:

```
config sys-recovery-level [none | critical | all]
```

and indicate either the “critical” or “all” parameter for an automatic switch reboot. Setting the value to “critical”, causes the switch to monitor certain critical software tasks for exceptions. The tasks monitored are tBGTask and tNetTask.

NOTE

Extreme Networks recommends that you set the sys-recovery-level to critical. For more information on the ’sys-recovery- level’ command, refer to the Summit24e3 Switch Installation and User Guide.

System Logging

By default, log entries of "warning" and "critical" levels are preserved in the log even after a reboot. Issuing a "`clear log`" command will not remove these static entries. Issuing a "`clear log static`" command will remove all entries of all levels.

Enabled IdleTimeouts and Console Connections

If the IdleTimeout feature is enabled, and a telnet session that becomes "timed-out", a subsequent telnet to the box 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).

Xmodem Downloads

This feature is not supported in bootrom version 1.3.

EDP Packet Length

The length field in the Ethernet MAC Header of an EDP frame indicates that the length is 316 bytes even though the length of an EDP frame is 338 bytes. Some hosts and network equipment report an error when receiving an EDP frame and may correct the packet (truncate it) before forwarding the packet. In the case where the MAC Header is modified, Extreme switches may report an EDP "`PDU length>packet length`" message to the log (7830).

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).

Uploaded configuration files containing the command `enable subvlan-proxy-arp <vlan>` for each VLAN configured, a supported feature, will result in a syntax error when you download a configuration file via TFTP. This does not affect functionality of the switch (15750).

Uploaded configuration files incorrectly set the command `disable rip exportstatic` as `disable rip export static` and this causes a syntax error and reverts the rip export static state back to default when the config is downloaded via TFTP (15752).

Uploaded configuration files containing the command `configure igmp snooping timer 260 260`, an unsupported feature, will result in a syntax error when you download a configuration file via TFTP. This does not affect functionality of the switch (15735).

Command Line Interface (CLI)

CLI Output for Power

Power supply status is not displayed in the CLI `show switch` command.

Don't Use the Encrypted Option from the CLI

There is an option available in the CLI for encrypting a password when creating a user account. Do not use this option. It is for use only in conjunction when uploading and downloading an ASCII configuration file to the switch so passwords are not indicated in clear text within the configuration file (4229, 4719).

"show iproute" Command

The "show iproute" display has a special flag for routes that are active and in use, these routes are preceded by a "*" 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 is reported as lost but in fact the ping was successful (5170).

If during the execution of a PING command, the switch receives any ICMP messages that are not an echo reply (e.g. IDRP, Time to Live expired, destination unreachable); an error message is displayed on the console. The error message can be safely ignored (2082).

Cosmetic Configuration Download Warnings

During the execution of the ASCII configuration file during the download configuration process, warning messages may appear when attached to the console port. If you scroll back to review these warnings, the indications are harmless and the desired configuration should have taken place (4931).

Console Appears Locked after Telnet Attempt

If you telnet to an unresponsive device from the CLI, the console may appear to be locked or frozen. Pressing the <ctrl>] (control and right bracket) keys simultaneously will close the frozen telnet session (4557).

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).

Incorrect Counters

Oversized frames greater than 1524 bytes will be counted as jabber frames instead of oversized frames (15168).

Switching and VLANs

This section describes issues associated directly with Layer 2 switching and VLANs.

Renaming System VLANs

Do not rename the system created VLANs, Default and MacVlanDiscover (PD2-75774602).

Adding/Deleting a Port to an IP VLAN

Adding or deleting a port to an IP VLAN will clear all the IP forwarding entries associated with that VLAN (1-81DE0).

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.

Port Learning/Static FDB Entries

Traffic forwarding to static FDB entries will not work after a reboot, if port learning is disabled.

A workaround is to toggle port learning (enable then disable port learning) after rebooting. Traffic forwarding to static FDB entries will then work (PD2-74885718).

Port Learning

The command `conf vlan add ports mac-limit` is not supported (PD2-72521401).

The command `disable learning port` has been removed from the CLI since it is not supported due to hardware limitations (1-5BEGB).

RIP Routing

RIP V2 Authentication

The authentication feature of RIPv2 is not supported.

Spanning Tree Protocol

Reconnecting STP Link Causes Problems

When a link on a spanning tree, not directly connected to the Summit24e3, is pulled and then reconnected, the forwarding databases (fdb) on the Summit24e3 does not flush on reconnecting. This may cause connectivity problems. However, flushing the fdb manually will clear the problem (1-CHM0S).

WEB Management - VISTA

Vista is not currently supported in this build, however web pages for Network Login are supported.

EAPS

Clearing FDB

When EAPS is operating in Master Mode, clearing the FDB with more than 3000 entries may cause EAPS to log state changes. However, as these state changes are not caused by real failures, they can be ignored safely. A workaround is to increase the EAPS failtime (PD2-70896155).

SNMP

Port Mirroring

Port mirroring cannot be displayed or configured using SNMP (PD2-69772213).

SMON dataSourceCaps

The SMON dataSourceCapsPort group of SMON-MIB is not supported (PD2-69772201).

traceRouteCtlTable

The set operation for traceRouteCtlTable is not supported (PD2-68759116).

lookupCtlTable

The set operation for lookupCtlTable is not supported (PD2-68759133).

RMON Alarms not Generated

RMON rising/falling alarms are not generated (PD2-68759101).

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).

Control of UDP Port Used in Sending Traps

The control of what UDP port number to be used when sending SNMP traps can be done through the appropriate attributes in RFC 2021. It cannot be currently controlled through CLI and is not stored as part of a configuration (4914).

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).

Network Login

ISP Mode with RADIUS

In ISP Mode, Extreme specific attributes should not be configured for the user entries when RADIUS server is used for authentication. Specifically, the presence of the Extreme-Netlogin-Vlan attribute in ISP Mode may cause the display of the authenticated user names as `Unknown` with `show netlogin info` (PD2-73637801).

DHCP Server

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

Documentation Errata and Addenda

Documentation Errata are errors found in the documentation after final production. Addenda are additional information released between production updates. Please update any copies that you may have. These errata and addenda refer to the *Summit24e3 Switch Installation and User Guide, Software Version 2.0,* part number 100102-00 Rev. 02, published August, 2002.

Documentation Errata

Enable License Command is not Documented in User Guide

The command `enable license advanced-edge` is not documented in the *Summit24e3 Switch Installation and User Guide.* The syntax and description are provided in Table 7.

Table 7: Enable License Advanced-Edge Command

Command	Description
enable license advanced-edge <license_key>	Enables the advanced edge software feature license. Specify `<license_key>` as an integer. The command `unconfig switch all` does not clear licensing information. This license cannot be disabled once it is enabled on the switch.

Configuring Switch Load Sharing Limits

On page 74, the last bullet item should read:

- Ports on the switch are divided into a maximum of six groups.

See the entry for *Load Sharing* in Table 5, “Supported limits” on page 15 in this document for load sharing limits.

IP Multicast Routing Section Should Be Ignored

The section on page 206, “Configuring IP Multicast Routing”, should be ignored. The Summit24e3 does not support multicast routing. The section was inadvertantly included when the information about IGMP snooping, which is supported, was included in the document.

Documentation Addenda

The following pages of the release notes, up to the section “Issues Resolved in Current and Previous Releases” on page 30, are provided for your convenience in configuring the Summit24e3. The information is taken from the *ExtremeWare Softeware User Guide, Software Version 6.2.2.*

MAC-based VLANs became officially supported on the Summit24e3 with the release of ExtremeWare 6.2e.1b17.

MAC-Based VLANs

MAC-Based VLANs allow physical ports to be mapped to a VLAN based on the source MAC address learned in the FDB. This feature allows you to designate a set of ports that have their VLAN membership dynamically determined by the MAC address of the end station that plugs into the physical port. You can configure the source MAC address-to-VLAN mapping either offline or dynamically on the switch. For example, you could use this application for a roaming user who wants to connect to a network from a conference room. In each room, the user plugs into one of the designated ports on the switch and is mapped to the appropriate VLAN. Connectivity is maintained to the network with all of the benefits of the configured VLAN in terms of QoS, routing, and protocol support.

MAC-Based VLAN Guidelines

When using the MAC-to-VLAN mapping, consider the following guidelines:

- A port can only accept connections from an endstation/host and should not be connected to a layer-2 repeater device. Connecting to a layer-2 repeater device can cause certain addresses to not be mapped to their respective VLAN if they are not correctly configured in the MAC-VLAN configuration database. If a repeater device is connected to a MAC-Based VLAN port, and the configured MAC-to-VLAN mapped station enters on the repeater, any endstation that is attached to the repeater can be mapped to that VLAN while the configured endstation is active in that VLAN. Upon removal of the configured MAC-to-VLAN endstation, all other endstations lose connectivity.
- Groups are used as a security measure to allow a MAC address to enter into a VLAN only when the group mapping matches the port mapping.

  As an example, the following configuration allows MAC 00:00:00:00:00:aa to enter into the VLAN only on ports 10 and 11 because of membership in group 100:

```
* Summit48:50 # show mac
Port    Vlan                Group         State
10      MacVlanDiscover     100           Discover
11      MacVlanDiscover     100           Discover
12      MacVlanDiscover     any           Discover
13      MacVlanDiscover     any           Discover
14      MacVlanDiscover     any           Discover
Total Entries in Database:2
 Mac                Vlan     Group
00:00:00:00:00:aa   sales    100
00:00:00:00:00:01   sales    any
2 matching entries
```

- The group “any” is equivalent to the group “0”. Ports that are configured as “any” allow any MAC address to be assigned to a VLAN, regardless of group association.
- Partial configurations of the MAC to VLAN database can be downloaded to the switch using the timed download configuration feature.

MAC-Based VLAN Limitations

The following list contains the limitations of MAC-based VLANs:

- Ports participating in MAC VLANs must first be removed from any static VLANs.
- The MAC- to-VLAN mapping can only be associated with VLANs that exist on the switch.
- A MAC address cannot be configured to associate with more than 1 VLAN. If this is attempted, the MAC address is associated with the most recent VLAN entry in the MAC-to-VLAN database.
- The feature is intended to support one client per physical port. Once a client MAC address has successfully registered, the VLAN association remains until the port connection is dropped or the FDB entry ages out.

MAC-Based VLAN Example

In this following example, three VLANs are created: *engineering*, *marketing*, and *sales*. A single MAC address is associated with each VLAN. The MAC address 00:00:00:00:00:02 has a group number of "any" or "0" associated with it, allowing it to be plugged into any port that is in MacVlanDiscover mode (ports 10-15 in this case). The MAC address 00:00:00:00:00:01 has a group number of 10 associated with it, and can only be assigned to a VLAN if inserted into ports 16 or 17. The MAC address 00:00:00:00:00:03 has a group number of 200 associated with it and can only be inserted into ports 18 through 20.

```
enable mac-vlan mac-group any ports 10-15
enable mac-vlan mac-group 10 ports 16-17
enable mac-vlan mac-group 200 ports 18-20
config mac-vlan add mac-address 00:00:00:00:00:01 mac-group 10 engineering
config mac-vlan add mac-address 00:00:00:00:00:02 mac-group any marketing
config mac-vlan add mac-address 00:00:00:00:00:03 mac-group 200 sales
```

Timed Configuration Download for MAC-Based VLANs

To allow centralized control of MAC-based VLANs over multiple switches, a timed TFTP configuration download allows you to download incremental configuration files from a primary or secondary server at specified time intervals. The timed downloads are configurable in 24 hour intervals. When a switch reboots, the configuration is automatically downloaded immediately after booting, per the configured primary and secondary servers.

To configure the primary and/or secondary server and file name, use the following command:

```
config download server [primary | secondary] [<host_name> | <ip_address>] <filename>
```

To enable timed interval downloads, use the following command:

```
download configuration every <hour:minute>
```

To display timed download information, use the following command:

```
show switch
```

Example. In relation to MAC-based VLANs, the downloaded file is an ASCII file that consists of CLI commands used to configure the most recent MAC-to-VLAN database. This feature is different from the normal download configuration command in that it allows incremental configuration without the automatic rebooting of the switch.

The following example shows an incremental configuration file for MAC-based VLAN information that updates the database and saves changes:

```
config mac-vlan add mac-address 00:00:00:00:00:01 mac-group any engineering
config mac-vlan add mac-address 00:00:00:00:ab:02 mac-group any engineering
config mac-vlan add mac-address 00:00:00:00:cd:04 mac-group any sales
.
.
config mac-vlan add mac-address 00:00:00:00:ab:50 mac-group any sales
config mac-vlan add mac-address 00:00:00:00:cd:60 mac-group any sales
save
```

Issues Resolved in Current and Previous Releases

Below is a historical listing of issues resolved by release. 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/techsupport.asp.

Issues Resolved in v6.2e.1b17

The following issues were present in ExtremeWare v6.2e.1b15, and possibly in earlier versions, and were resolved in the current release (ExtremeWare v6.2e.1b17).

Switching and VLANs

Number of VLANs Supported

Issues associated with downloading a configuration containing more than 220 VLANs have been fixed. The Summit24e3 now supports up to 255 VLANs (PD2-56888315, PD2-76185301).

Non-IP Multicast Forwarding

Support for simultaneous operation of IGMP snooping and non-IP multicast packet forwarding (AppleTalk, DEC multicast) has been added.

Spanning Tree Protocol

BPDU Forwarding

BPDUs are now forwarded by the Summit24e3 on STP domains that are disabled (1-5BEG5, PD2-86143393, PD2-78758583).

GVRP/GMRP

GVRP/GMRP Forwarding

GVRP and GMRP frames are now forwarded by the Summit24e3.

EAPS

EAPS Over Load-Sharing Links

EAPS over load-sharing links now operates correctly.

Load Sharing

Load Sharing Groups

The CLI now checks for the maximum number of load sharing groups supported (six). Also, a problem has been fixed in the “disable sharing” processing that allowed creation of more than the maximum number of groups (PD2-96352601).

IP Multicast Routing

Enabling IPMC Forwarding

The command `enable ipmcforwarding {vlan <name>}` was removed from the CLI. The Summit24e3 does not support any IP Multicast Routing Protocols, so the command has no effect. However, the command `disable ipmcforwarding` was left in the CLI in order that users who inadvertantly added IP multicast forwarding to their configurations can remove it (PD2-102203201).

Command Line Interface (CLI)

Packet Statistics

The title of the `show port packet` command display has been corrected to reflect the fact that the packet counts displayed include both received packets and transmitted packets on the Summit24e3 (PD2-81582901).

CLEI/QC Information Display

The `show version` command was enhanced to display the Common Language Equipment Identifier (CLEI) and Quality Control (QC) information (PD2-101490152).

Issues Resolved in v6.2e.1b15

The following issues were present in ExtremeWare v6.2e.1b14, and possibly in earlier versions, and were resolved in the current release (ExtremeWare v6.2e.1b15).

System Related

CRC Errors with Long Ethernet Cables

CRC errors would sometimes occur with Ethernet cables longer than 70 meters on some of the ports (PD2-76080701, PD2-80117511).

Command Line Interface (CLI)

CLI Output for Temperature

Switch temperature status was not displayed in the CLI `show switch` command and the temperature value was incorrectly displayed as 0 degrees by EPICenter (PD2-80224930, PD2-77015649).

Redundant Ports (PHY)

The CLI incorrectly allowed you to configure and unconfigure redundant ports. Although they were present in the CLI, the Summit24e3 does not support the command `config ports <portlist> redundant` or the command `unconfig ports <portlist> redundant`. The commands have been removed from the CLI (PD2-79637801).

Issues Resolved in v6.2e.1b14

The following issues were present in ExtremeWare v6.2e.0b10, and possibly in earlier versions, and were resolved in ExtremeWare v6.2e.1b14.

ESRP-Aware

ESRP-Aware Display and Operation

The ESRP-Aware feature and its display did not operate reliably (1-CHM0A).

SNMP

SNMP CERT Advisory 2002-03

The SNMP vulnerabilities detailed in CERT Advisory 2002-03 have been fixed (1-9I8DD, 1-9KMBI).

Issues Resolved in v6.2e.0b10

The following issues were present in ExtremeWare v6.2e.0b9, and possibly in earlier versions, and were resolved in ExtremeWare v6.2e.0b10.

General

Show Version String

The `show version` string has been modified to reflect the application of this software version to the manufacturing flow (2-H7VFO).

Issues Resolved in v6.2e.0b9

The following issues were present in ExtremeWare v6.2e.0b6, and possibly in earlier versions, and were resolved in ExtremeWare v6.2e.0b9.

General

- Due to a problem in internal allocation of entries within software, switches would stop forwarding packets even though entries in the FDB and ARP tables were correctly populated. A reboot appeared to solve the problem until the next event leading to this condition (1-BP8QX).
- A software exception would occur due to a sequencing problem during memory access. The following information would be printed to the system log during this event (1-CHLYO):

```
<CRIT:KERN> inFlags=8 eType=800 offset=12 gMbuf=0
<CRIT:KERN> Line=0 card=0 chsub=2 len=82e
<CRIT:KERN> Crash Dump Information for tBGTask
<CRIT:SYST> Task: 0x81714220 "tBGTask"
```

Switching and VLANs

- Traffic with source macs that are configured destination blackhole were not forwarded at line rate (1-5B5KD).

IGMP

- The CLI disable IGMP snooping command would not take effect (1-CGZ4A).
- Multicast control packets were not being forwarded when IGMP snooping was enabled on a switch resulting in all connected Layer 3 devices to be unable to communicate even though the “All group” snooping entries were created and the multicast control packets were registered (1-CT22L).

Load Sharing

- When load sharing was configured and enabled between an Extreme device and a Summit24e3, packets being transmitted through the load share group to the Summit24e3 would be transmitted from the Summit24e3 to the respective destinations with a VLAN ID of “1” regardless of the configured VLAN ID of the destination/switch (1-994C0).