ExtremeWare Installation and Release Notes

Software Version 7.8.4b1-patch1-4

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: February 2012
Part Number:120396-00 Rev 30

Contents

1 CHAPTER Overview

NOTE

These Release Notes document ExtremeWare® 7.8.4b1-patch1-4. ExtremeWare 7.8 enables new hardware products and software features.

NOTE

You can only load ExtremeWare 7.8 on a switch running ExtremeWare 7.0 or later.

This chapter contains the following sections:

Feature Enhancements in ExtremeWare 7.8

Following are the new software features supported in ExtremeWare 7.8. These features are documented in the *ExtremeWare User Guide* or the *ExtremeWare Command Reference Guide*.

- Wireless configuration is no longer supported through web interface (Vista) after ExtremeWare 7.7 (PD3-56805293).
- A Message Authenticator attribute has been added to ExtremeWare software for RADIUS client access to ensure interoperability with other third party security appliances (PD3-131187593, PD3-168662236).
- A new option has been added to enable replacing stacking switches with another type of switch. For example, you can now replace a Summit® 400-24 with a Summit 400-48 in a stack (PD3-108698145).
- SNMPv1v2c and SNMPv3 can now be enabled and disabled individually using the enable `snmp access` {`snmp-v1v2c` | `snmpv3`} and `disable snmp access` {`snmp-v1v2c` | `snmpv3`} commands (PD3-143288531).

- Management or default VLAN IP addresses and IP route information is now saved when running the `unconfigure switch` command, no longer requiring configuring management IP addresses and IP route information for each `unconfigure switch` command (PD3-129938061).
- BlackDiamond® series and Summit 400 series switches now support 1000Base-BX-U and 1000Base-BX-D mini-GBICs (PD3-140205532).
- SNMP private MIB variables for system memory (total, free, allocated) are now available to remotely monitor free memory on a switch (PD2-91657034, PD3-115547398).
- Log messages for OSPF neighbor state changes can now be shown without enabling log debug-mode (PD3-97246261).
- SNMPv3 default-users and default-groups can now be disabled to prevent MIB access (PD3-188395462).
- Ports and VLANs can now be configured at the same time for limit-learning or lock-down for all untagged edge ports (PD3-96945710).
- A send MAC identifier has been added to the EDP EAPS PDU that enables discarding of looped L2 PDU link down messages for increased EAPS resiliency (PD3-123447826).
- DHCP now provides the ability to add a secondary DNS server. The secondary DNS server helps hosts resolve IP address issues in case of a primary DNS failure (PD3-93756551).
- UDP syslog and UDP TFTP ports can now be disabled and re-enabled as necessary, eliminating a potential security threat (PD3-76207333).
- SNMP now provides MIB support for retrieving FDB table counts through SNMP monitoring (PD3-154455113).
- SNMP now provides MIB support for retrieving per VLAN IP statistics and task names (PD3-14163261).
- Web-based network login now works with proxy server configurations (PD3-93442589).
- *ForceAuthorized* and *forceUnauthorized* modes are now included in 802.1x authentication for standard compliance (PD3-49511592).
- Command output for the `show ipfdb` command now includes flag descriptions (PD3-154717991).

Supported Hardware

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

ExtremeWare 7.3 (and later) supports "*i*" series and "e" series products.

Following is a list of the "i" series switches:

- BlackDiamond 6816
- BlackDiamond 6808
- BlackDiamond 6804
- Alpine® 3808
- Alpine 3804
- Alpine 3802
- Summit7i/7iT
- Summit1i/1iT
- Summit5i/5iT/5iLX

- Summit48i
- Summit48si

Following is a list of the "e" series switches:

- Summit 400-48t
- Summit 400-24p
- Summit 400-24t
- Summit 200-24/48
- Summit 200-24fx
- Summit 300-24
- Summit 300-48

Table 1 lists software filenames for the hardware that requires software. Summit 400-24 switches require ExtremeWare 7.4 or later. Summit 200-24fx switches require ExtremeWare 7.5 or later.

Table 1: Software for Supported Hardware

Extreme Hardware	ExtremeWare Filename	BootROM Filename/ Version
BlackDiamond 6816	v784b1-patch1-3.Gxtr or v784b1-patch1-3.SGxtr	ngboot8.2.bin/8.2
BlackDiamond 6808	v784b1-patch1-3.xtr or v784b1-patch1-3.Sxtr	ngboot8.2.bin/8.2
BlackDiamond 6804	v784b1-patch1-3.xtr or v784b1-patch1-3.Sxtr	ngboot8.2.bin/8.2
Alpine 3808	v784b1-patch1-3.xtr or v784b1-patch1-3.Sxtr	ngboot8.2.bin/8.2
Alpine 3804	v784b1-patch1-3.xtr or v784b1-patch1-3.Sxtr	ngboot8.2.bin/8.2
Alpine 3802	v784b1-patch1-3.xtr or v784b1-patch1-3.Sxtr	ngboot8.2.bin/8.2
Summit 400-48t	v784b1-patch1-3.Cxtr or v784b1-patch1-3.SCxtr	s400_boot51.bin
Summit 400-24p	v784b1-patch1-3.Cxtr or v784b1-patch1-3.SCxtr	s405_boot51.bin
Summit 400-24t	v784b1-patch1-3.Cxtr or v784b1-patch1-3.SCxtr	s405_boot51.bin
Summit 200-24/48 (see note)	v784b1-patch1-3.Fxtr or v784b1-patch1-3.SFxtr	s200_boot51.bin
Summit 200-24fx	*v784b1-patch1-3.Fxtr or v784b1-patch1-3.SFxtr*	*s200_boot51.bin*
Summit 300-24	v784b1-patch1-3.Fxtr or v784b1-patch1-3.SFxtr	s200_boot51.bin
Summit 300-48	v784b1-patch1-3.Lxtr or v784b1-patch1-3.SLxtr	s300_bs.1.1.1.b2.bin s300_bl.1.2.0.b3.bin
Altitude 300[1]	ART-7_7_3.bin	ABS-1_8_0.bin ABL-2_13_7.bin
Summit7i/7iT	v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr	ngboot8.2.bin/8.2
Summit1i/1iT	v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr	ngboot8.2.bin/8.2
Summit5i/5iT/5iLX	v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr	ngboot8.2.bin/8.2
Summit48i	v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr	ngboot8.2.bin/8.2
Summit48si	v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr	ngboot8.2.bin/8.2
ARM module	v784b1-patch1-3.arm	v784b1-patch1-3.nprom/1.18
OC3 PoS module	v784b1-patch1-3.oc3	v784b1-patch1-3.nprom/1.18
OC12 PoS module	v784b1-patch1-3.oc12	v784b1-patch1-3.nprom/1.18
OC3 ATM module	v784b1-patch1-3.atm3	v784b1-patch1-3.nprom/1.18
MPLS module	v784b1-patch1-3.mpls	v784b1-patch1-3.nprom/1.18

Table 1: Software for Supported Hardware (Continued)

Extreme Hardware	ExtremeWare Filename	BootROM Filename/ Version
T1 module	v784b1-patch1-3.t1	t1boot28.wr/2.8
E1 module	v784b1-patch1-3.e1	e1boot28.wr/2.8
T3 module	v784b1-patch1-3.t3	t3boot28.wr/2.8

1. For an Altitude 300 to work in SummitWM mode, you will need SummitWM-compatible AP image A300-1.1.x.yy.zz.img (released with SummitWM 1.1 or later software for the Altitude 300 platform). Refer to the SummitWM Software Version 1.1 Release Notes (or later) for details.

NOTE

In addition to the filenameLs listed in Table 1, v784b1-patch1-3.Wxtr and v784b1-patch1-3.SWxtr are used for upgrading Summit 200 switches from ExtremeWare 7.1e.

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.

NOTE

Systems with 128 MB memory should use the v784b1-patch1-3.Bxtr or v784b1-patch1-3.SBxtr image. To determine how much memory is available, use the `show memory` command.

BlackDiamond Component Support

BlackDiamond components supported with ExtremeWare 7.8, and the minimum ExtremeWare version required by the chassis to support each component, include:

Table 2: BlackDiamond Component Support

BlackDiamond Component	ExtremeWare Required
BlackDiamond 6804	6.2.2b56[1]
BlackDiamond 6808	6.2.2b56[1]
BlackDiamond 6816	6.2.2b56[1]
MSM-3	7.1.1
MSM64i	6.2.2b56[1]
G8Xi	6.1.3
G8Ti	6.1.3
G12SXi	6.1.4
G16X[3]	7.0.1
G24T[3]	7.0.1
F32Fi	6.1.8

Table 2: BlackDiamond Component Support (Continued)

BlackDiamond Component	ExtremeWare Required
F48Ti	6.1.2
F96Ti	6.1.8
WDMi	6.1.5
10GLRi	7.0
10GX3	7.2.0b20
MPLS	7.0
ARM	7.0
P3cMi	7.0
P3cSi	7.0
P12cMi	7.0
P12cSi	7.0
A3cMi	7.0
A3cSi	7.0
DC Power Supply	6.1.5
110 V AC Power Supply	6.1.5
220 V AC Power Supply	6.1.5

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

NOTE

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

Alpine Component Support

Alpine components supported with ExtremeWare 7.8, and the minimum ExtremeWare version required, include:

Table 3: Alpine Component Support

Alpine Component	ExtremeWare Required
Alpine 3802	6.2.2b56[1]
Alpine 3804	6.2.2b56[1]
Alpine 3808	6.2.2b56[1]
SMMi	6.2.2b56[1]
GM-4Si/Xi/Ti	6.1.5
GM-16X[3]	7.0.1
GM-16T[3]	7.0.1

Table 3: Alpine Component Support (Continued)

Alpine Component	ExtremeWare Required
FM-32Ti	6.1.5
FM-24MFi	6.1.5
FM-24Ti	6.1.7
FM-24SFi	6.1.7
FM-32Pi	7.2.0b20
GM-WDMi	6.1.8
WM-4T1i	7.0.1
WM-4E1i	7.0.1
WM-1T3i	7.0.1
FM-8Vi	7.0.1
AC Power Supply	6.1
DC Power Supply	6.1.5

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

Summit "i" and Summit "e" Series Platforms

Table 4 and Table 5 list the "i" series and "e" series switches and the required ExtremeWare.

Table 4: "i" Series Platforms

"i" Series Platform	ExtremeWare Required
Summit7i/7iT	6.2.2b56[1]
Summit1i/1iT	6.2.2b56[1]
Summit5i/5iT/5iLX	6.2.2b56[1]
Summit48i	6.2.2b56[1]
Summit48si	6.2.2b56[1]

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

Table 5: "e" Series Platforms

"e" Series Platform	ExtremeWare Required
Summit 400-48t	7.4.1
Summit 400-24p	7.4.1
Summit 400-24t	7.4.1
Summit 200-24/48	7.4.1
Summit 200-24fx	7.4.1
Summit 300-24	7.4.1
Summit 300-48	7.4.1

GBIC Support

NOTE

Extreme Networks optics are tested and work in all supported Extreme switches. It is recommend customers use these GBIC optics in their Extreme Networks gear. Extreme Networks assumes no liability for third party optics that do not function in our switches. Extreme does not block third party optics and can investigate issues involving interoperability of our switches with standards based on third party optics, provided the customer has a valid service contract for the third party equipment and the third party optics are made available to Extreme support staff for testing. Extreme Networks cannot ensure ALL third party optics will work across all our products.

GBICs supported with ExtremeWare 7.8, and the minimum ExtremeWare version required, include:

Table 6: GBIC Support

GBIC	ExtremeWare Required
SX parallel ID	1.0
SX serial ID	2.0
LX parallel ID	1.0
LX serial ID	2.0
ZX	6.2.2
ZX Rev 03	6.2.2
LX70	2.0
LX100	6.1.9
UTP	6.1.9
BX Mini	7.8.0b8
SX Mini	7.0.1b11
LX Mini	7.0.1b11
ZX Mini	7.0.1b11

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

Table 7: ExtremeWare Recognition of GBIC Type

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

Mini-GBIC Support

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

XENPAK Module Support

XENPAK modules supported with ExtremeWare 7.8, the minimum ExtremeWare version required, and the manufacturers supported include:

Table 8: XENPAK Support

XENPAK Module	ExtremeWare Required	Manufacturers Supported
LR	7.2.0b20	Intel, Opnext
ER	7.2.0b20	Intel, Opnext
SR	7.4.0b42	Intel
LX4	7.7.1b1	EMCORE
CX4	7.7.1b1	Opnext
ZR	7.7.1b1	Opnext

Channel Mapping

Table 9 lists the channel mapping for Altitude 300-2i wireless ports connected to a Summit 300-48 using ExtremeWare 7.8. The UAA features contained in this table apply to the Summit 300-48 switch only.

Table 9: Altitude 300-2i Channel Mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	34/38/42/46	1-13	1-14
Argentina	AR	52/56/60/64/149/153/157/161	1-13	1-13
Australia	AU	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	36/40/44/48	1-13	1-13
Belgium	BE	36/40/44/48/52/56/60/64	1-13	1-13
Brazil	BR	36/40/44/48/149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	None	1-13
China	CN	149/153/157/161/165	1-13	1-13
Colombia	CO	36/40/44/46/52/56/60/64/149/153/157/161/165	1-11	1-11
Costa Rica	CR	None	1-13	1-13
Cyprus	CY	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Czech Republic	CZ	36/40/44/48/52/56/60/64	1-13	1-13

Table 9: Altitude 300-2i Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Denmark	DK	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Finland	FI	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
France	FR	36/40/44/48/52/56/60/64	1-13	1-13
Germany	DE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Greece	GR	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Hungary	HU	36/40/44/48	1-13	1-13
Iceland	IS	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Israel	IL	None	1-13	1-13
Italy	IT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Jordan	JO	36/40/44/48	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	36/40/44/48/52/56/60/64	1-13	1-13
Lithuania	LT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Luxembourg	LU	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	36/40/44/48/52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
New Zealand	NZ	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Poland	PL	36/40/44/48/52/56/60/64100/104/108/112/116/120/124/ 128/132/136/140	1-13	1-13
Portugal	PT	36/40/44/48/52/56/60/64100/104/108/112/116/120/124/ 128/132/136/140	1-13	1-13
Puerto Rico	PR	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11

Table 9: Altitude 300-2i Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	36/40/44/48/52/56/60/64	1-13	1-13
Slovenia		36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
South Africa	ZA	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Spain	SP	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Sweden	SE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13
Switzerland	CH	36/40/44/48/52/56/60/64	1-13	1-13
Taiwan	TW	56/60/64/149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	36/40/44/48/52/56/60/64	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13

Table 10 lists the channel mapping for indoor Altitude 300-2d wireless ports connected to a Summit 300-48 switch using ExtremeWare 7.8.

Table 10: Altitude 300-2d Indoor Channel Mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	34/38/42/46	1-13	1-14
Argentina	AR	52//56/60/64/149/153/157/161	1-13	1-13
Australia	AU	52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	36/40/44/48	1-13	1-13
Belgium	BE	36/40/44/48/52/56/60/64	1-13	1-13
Brazil	BR	149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	1-13	1-13
China	CN	149/153/157/161/165	None	1-13
Colombia	CO	52/56/60/64/149/153/157/161/165	1-11	1-11
Costa Rica	CR	None	1-13	1-13
Cyprus	CY	36/40/44/48/52/56/60/64/100/104/108/112/116/120/ 124/128/132/136/140	1-13	1-13

Table 10: Altitude 300-2d Indoor Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Czech Republic	CZ	36/40/44/48/52/56/60/64	1-13	1-13
Denmark	DK	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Finland	FI	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
France	FR	36/40/44/48/52/56/60/64	1-13	1-13
Germany	DE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Greece	GR	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Hungary	HU	36/40/44/48	1-13	1-13
Iceland	IS	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Israel	IL	None	1-13	1-13
Italy	IT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Jordan	JO	36/40/44/48	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	36/40/44/48/52/56/60/64	1-13	1-13
Lithuania	LT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Luxembourg	LU	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
New Zealand	NZ	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Poland	PL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Portugal	PT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 10: Altitude 300-2d Indoor Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Puerto Rico	PR	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	36/40/44/48/52/56/60/64	1-13	1-13
Slovenia		36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
South Africa	ZA	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Spain	SP	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Sweden	SE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Switzerland	CH	36/40/44/48/52/56/60/64	1-13	1-13
Taiwan	TW	56/60/64/149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	36/40/44/48/52/56/60/64	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 11 lists the channel mapping for outdoor Altitude 300-2d wireless ports connected to a Summit 300-48 switch using ExtremeWare 7.8.

Table 11: Altitude 300-2d Outdoor Channel Mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	None	1-13	1-14
Argentina	AR	52//56/60/64/149/153/157/161	1-13	1-13
Australia	AU	52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	None	1-13	1-13
Belgium	BE	None	1-13	1-13
Brazil	BR	149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	None	1-13
China	CN	149/153/157/161/165	1-13	1-13
Colombia	CO	52/56/60/64/149/153/157/161/165	1-11	1-11
Costa Rica	CR	None	1-13	1-13
Cyprus	CY	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 11: Altitude 300-2d Outdoor Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Czech Republic	CZ	None	1-13	1-13
Denmark	DK	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Finland	FI	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
France	FR	None	1-7	1-7
Germany	DE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Greece	GR	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Hungary	HU	None	1-13	1-13
Iceland	IS	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Israel	IL	None	5-7	5-7
Italy	IT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Jordan	JO	None	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	None	1-13	1-13
Lithuania	LT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Luxembourg	LU	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
New Zealand	NZ	52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Poland	PL	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Portugal	PT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Puerto Rico	PR	52/56/60/64/149/153/157/161/165	1-11	1-11
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	None	1-13	1-13
Slovenia	SI	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
South Africa	ZA	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Spain	SP	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Sweden	SE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 11: Altitude 300-2d Outdoor Channel Mapping (Continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Switzerland	CH	None	1-13	1-13
Taiwan	TW	149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	None	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Tested Third-Party Products

This section lists the third-party products tested for the Summit 300-48 switch. The UAA features contained in this section apply to the Summit 300-48 switch only.

Tested NICs

The wireless NICs in Table 12 through Table 16 are tested with the listed software (or later) and authentication method.

Table 12: 802.11 a/b/g Wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Proxim A/B/G Gold	2.4.2.1.7 2.3.0.75	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
D-link DWL-AG650 Air-Expert	1.2.0.1	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-link DWL-AG660 Air Premier	2.1.3.1	WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS
3Com 3CRWE154A72	3.0.0.46	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS
Linksys AG WPC55AG	2.3.2.4	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS PEAP/TLS
Cisco Air-CB21AG	3.0.0.111	W2K SP4 WinXP SP1/SP2	Card Utility	PEAP/TLS

Table 13: 802.11 a/b Wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Linksys WPC51AB	2.0.1.254	W2K SP4 WinXP SP/ SP21	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Orinoco Gold A/B	7.64.1.316	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-Link DWL-650 AB Air Pro	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS

Table 14: 802.11b Wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Cisco Aironet350 b	8.1.6.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
Netgear MA401 b-only	2.0.2.0	W2K SP4	Odyssey 2.2/Card Utility	PEAP/TLS PEAP/TLS
Microsoft b card MN520	D-link 2.0.1.254	W2K SP4 WinXP SP1	Odyssey 2.2	PEAP/TLS PEAP/TLS
3Com 11b-only 3CRWE60292B	2.1.1.3005	W2K SP4 WinXP SP1	Odyssey 2.2/Card Utility	PEAP/TLS PEAP/TLS/TTLS

Table 15: 802.11g Wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WG511	2.1.25.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
Buffalo WLI-CB-G54	3.50.21.10	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Linksys WPC54G	3.20.21.0	WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-Link DWL G650Airplus	2.2.2.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.23.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-Link DWL-G650-B2	2.21.4.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Microsoft MN-720	3.20.26.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS

Table 16: 802.11g Mini PCI Wireless NIC

NIC	Driver	OS	Third-Party Software	Authentication Method
Broadcom 54G MaxPerformance	3.20.23.0	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
Dell True Mobile 1300	3.20.23.0	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

The wireless PCI cards in Table 17 are tested with the listed software (or later) and authentication method.

Table 17: Wireless PCI Cards

NIC	Driver	OS	Third-Party Software	Authentication Method
Linksys WMP54G	3.30.15.0	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WAG311 Tri-mode	3.0.0.43	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WG311	2.4.0.71	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

WPA-Compliant Wireless NICs

The wireless NICs in Table 18 through Table 21 are WPA-compliant.

NOTE

WPA compliant wireless NICs support TKIP and AES with pre-shared and dynamic keys.

Table 18: Wireless Tri-Mode NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/ SP21	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-link DWL-AG650 AirExpert	1.2.0.1	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
3Com 3CRWE154A72	3.0.0.46	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 18: Wireless Tri-Mode NICs (Continued)

NIC	Driver	OS	Third-Party Software	Authentication Method
3Com 3CRPAG175	1.0.0.25	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Proxim A/B/G	2.4.2.1.7	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.02	PEAP/TLS/TTLS
D-Link AG660	2.1.3.1	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Linksys AG WPC55AG	3.0.0.111	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Cisco Air-CB21AG	3.0.0.111	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS

Table 19: Wireless 802.11g NICs (WPA Compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
Buffalo WLI-CB-G54	3.50.21.10	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
NetGear WG511T	3.3.0.156	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	WPA-PSK
Linksys WPC54G	3.20.21.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-Link DWL-G650-B2	2.2.4.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Microsoft MN-720	3.20.21.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 20: Wireless 802.11 a/b NICs (WPA Compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
D-link AirPro AB650	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 20: Wireless 802.11 a/b NICs (WPA Compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WAB501	2.4.0.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Avaya Platinum A/B	2.4.1.21	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 21: Wireless 802.11 a/b/g PCI-NICs (WPA Compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
Dell True Mobile 1450	3.40.65.0	W2K SP4 WinXP SP1/ SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

Tested RADIUS Servers

These RADIUS servers are fully tested:

- Microsoft Internet Authentication Server
- Funk Steel Belted RADIUS Enterprise Edition 4.5
- Meeting House
- Free Radius
- InfoBlox RadiusONE
- Roving Planet
- Cisco ACS

Tested Third-Party Clients

These third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.00.0.937

Tested Laptops

These laptops are fully tested:

- IBM Thinkpad T40 (Intel Centrino-based 802.11b)
- IBM Thinkpad T41 (Intel Centrino-based 802.11b)
- Dell Latitude D800 (Intel Centrino-based 802.11b)
- HP/Compaq nx9010 (Broadcom 54G MaxPerformance MiniPCI)

- Fujitsu Lifebook N series (Broadcom 54G MaxPerformance MiniPCI)
- Sony PCG-K15
- Dell Latitude D600

Tested PDAs

These PDAs are fully tested:

- iPAQ H5550
- Dell Axim x3i
- HP Pocket PC 4155

Tested Tablets

These tablets are fully tested:

- NEC Tablet

Tested Scanner

The following scanner is fully tested:

- Intermec Scanner Model 700 Color-Pocket PC - 802.11b CF: Open Authentication/No encryption, Shared/WEP, and Open/WEP

Tested Embedded WNIC Modules

- Dell Truemobile 1200, 1300, 1350, 1450
- IBM Thinkpad T40p Trimode (Centrino card)

Tested Spectralink Supported Handsets

- Avaya 3606
- Spectralink Netlink 1640

Tested Spectralink Gateway

- Netlink SVP Avaya Voice Priority Processor
- Netlink SVP100 Gateway

Legacy IP Phones

These wired IP phones have been verified for PoE power up only:

- Avaya 4610SW IP
- Avaya 4620 IP New 03-016A/B

- Avaya 4620SW IP
- Super tex PD1 v1
- Super PD+PS
- TI PTB48540 CL003ENG
- 3COM NJ105
- 3COM NJ220
- 3COM NJ200 Old
- 3COM NJ200 New
- 3COM NJ100 New
- 3COM NJ100 Old
- 3COM 3C10248B with 3CNJVOIPMOD-NBX
- 3COM 3C10248PE IP Phone
- 3COM 3C10226PE IP Phone
- Avaya 4602SW IP Phone
- Avaya 4620 IP Phone
- Avaya 4630SW IP Phone
- Polycom IP 300 With 2457-11077-002 Rev.X1
- Polycom IP 500 With 2457-11077-002 Rev.X1
- Polycom IP 600
- Polycom Speaker IP 3500 with Cisco PIM
- Polycom Speaker IP 3500 with IEEE
- Linear CD671
- 3COM 655003403 PD with 3CNJVOIPMOD-NBX
- Avaya 4602 IP Phone
- Linear LTC4257IS8 with 4257
- Linear Edge PD
- TPS2375 Eval Chip #22
- TPS2375 Eval Chip #20
- Siemens Optipoint 410 Standard FV
- Siemens Optipoint 410 Entry FV
- Polycom SoundPoint IP LAN/Power Cable

Legacy Phones with Dongle

- Cisco 7910
- Cisco 7940
- Cisco 7960
- Cisco 7970

2 CHAPTER Upgrading to ExtremeWare 7.8

This chapter contains the following sections:

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site:

http://www.extremenetworks.com/go/esupport.htm.

ExtremeWare Software Images for Summit 200/300/400 Series Switches

Table 22 lists the software images for the ExtremeWare Summit 200/300/400 Series switches and describes the purpose of each image.

Table 22: ExtremeWare 7.8 Software Images

Filename	Description and Usage
s200_boot51.bin	This is the BootROM file version 5.1 for Summit 200-24, Summit 200-48, and Summit 300-24 Series switches. The Summit 300-24 switch is architecturally the same as the Summit 200-24 except it offers PoE functionality. When upgrading to ExtremeWare 7.4 or later from ExtremeWare 7.1e, it is likely those switches will have older BootROM versions. The wrapper image (files that end with .Wxtr) will automatically upgrade the BootROM to the required version of 5.1, if necessary.

Table 22: ExtremeWare 7.8 Software Images

Filename	Description and Usage
s300_bl.1.2.0.b3.bin	This is the Bootloader file version 1.2.0 for the Summit 300-48 (build 3). Generally, most Summit 300-48 switches will be running at least this version. If this is not the case, download the BootLoader as stated in the upgrade steps.
s300_bs.1.1.1.b1.bin	This is the BootStrap file version 1.1.1 for the Summit 300-48 (build 1). Generally, most Summit 300-48 switches will be running at least this version. If this is not the case, download the BootStrap as stated in the upgrade steps.
ABS-1_8_0.bin	This is the BootStrap image for an Altitude 300.
ABL-2_13_7.bin	This is the Bootloader image for an Altitude 300.
ART-7_7_3.bin	This is the runtime image for an Altitude 300.
s400_boot51.bin	This is the BootROM file version 5.1 for the Summit 400-48. When upgrading to ExtremeWare 7.8, ensure that the BootROM in your Summit 400 is at least version 5.1. If this is not the case, follow the upgrade procedures to update the BootROM version 5.1.
s405_boot51.bin	This is the BootROM file version 5.1 for the Summit 400-24t and Summit 400-24p.
v783b5.Wxtr	This is the wrapper image for the Summit 200 series switches, also known as the intermediate image. ExtremeWare 7.3e is a much larger image compared to ExtremeWare 7.1e, this image is needed to repartition the flash to store the ExtremeWare 7.3e image and the configuration. It should be used only when upgrading Summit 200-24 and Summit 200-48 switches running a version earlier than release ExtremeWare 7.3e.
v783b5.SWxtr	This is the same as v783b5.Wxtr except this file supports SSH functions.
v783b5.Fxtr	This is the actual ExtremeWare 7.8 image for Summit 200-24, Summit 200-48, and Summit 300-24 series switches.
v783b5.SFxtr	This is the same as v783b5.Fxtr except this file supports SSH functions.
v783b5.Lxtr	This is the actual ExtremeWare 7.8 image for the Summit 300-48 series switch.
v783b5.SLxtr	This is the same as v783b5.Lxtr except this file supports SSH functions.
v783b5.Cxtr	This is the actual ExtremeWare 7.8 image for the Summit 400-48t, Summit 400-24t, and Summit 400-24p series switch
v783b5.SCxtr	This is the same as v783b5.Cxtr except this file supports SSH functions.
v783b5.mib	This is the MIB file associated with this release.

Upgrading ExtremeWare “i” Series Switches

Table 23 lists the BootROM required for each version of ExtremeWare.

Table 23: Required BootROM Versions

ExtremeWare Version	BootROM Version
ExtremeWare 7.3 and later	BootROM 8.2 (or later)
ExtremeWare 7.1.1 through ExtremeWare 7.2.0	BootROM 8.1 (or later)
ExtremeWare 7.0.0 through ExtremeWare 7.1.0	BootROM 7.8 (or later)

Following are specific instructions on upgrading to, and downgrading from, ExtremeWare 7.3 for Summit, Alpine, and BlackDiamond switches.

Upgrading the BootROM to Version 8.2

Before you upgrade ExtremeWare, upgrade to BootROM 8.2 (BootROM 8.2 is compatible with all ExtremeWare versions back to ExtremeWare 7.0).

1 Download the BootROM using the download bootrom `[<host_name> | <ip_addr>] <ngboot82.bin_name>` command.

NOTE

Reboot the switch using the `reboot` command.

NOTE

The BootROM upgrade can be incorporated into firmware upgrade procedure. If you are upgrading the BootROM only, follow this procedure.

PoE Firmware Upgrade

NOTE

ExtremeWare 7.4 contains a PoE firmware upgrade for the Alpine FM-32Pi module. PoE firmware changes are **not** automatically performed by the software. You must manually download the new firmware using the `download firmware` CLI command. If you are upgrading from a version earlier than ExtremeWare 7.4, you must manually download the new firmware. Until this firmware update is completed, the PoE ports are not powered up. The PoE firmware download may take up to 5 minutes per Alpine FM-32Pi module. It is also subject to failure. Check switch log messages to ensure the firmware change was successful. If unsuccessful repeat the firmware download.

Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until the firmware update is completed, the PoE ports are not powered up. Refer to “Upgrading PoE Firmware on an Alpine Switch with a PoE Module” on page 32.

Upgrading “i” Series Switches to ExtremeWare 7.8

To install ExtremeWare 7.8 on an “i” series switch, you must:

1 Save the configuration to a TFTP server.

2 Upgrade the BootROM to Version 8.2, if required.

3 Upgrade to ExtremeWare 7.8 as described on page 30.

4 Upgrade T1, E1, or T3 Modules from ExtremeWare 7.0 or Later as described on page 31.

5 Upgrade ATM, MPLS, ARM, or PoS modules as described on page 31.

6 Upgrade the PoE firmware, if required, on the Alpine switch as described on page 32.

NOTE

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

Saving the Current Configuration

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

1 If you are using the network login campus mode:

   a Disable network login using the `disable netlogin` command to prevent users from re-authenticating during the backup process.

   b Use the `clear netlogin state port` command on all network login user ports, causing all network login users to be unauthenticated and all client ports to move back to their respective unauthenticated VLAN configuration.

   c Use the `show netlogin` and `show vlan` commands to verify that all network login ports are in the unauthenticated state and the client ports are members of their respective unauthenticated VLANs.

2 If you are using ACLs and the CPU DoS protect feature, ensure that the CPU DoS protect filter precedence follows the rules described in "CPU DoS Protect and ACL Precedence" on page 59. If there is a precedence conflict, CPU DoS protect is not enabled.

3 Save the current configuration in both the primary and secondary configuration spaces using the `save configuration primary` and `save configuration secondary` commands.

4 Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use configuration primary` commands.

5 Verify that all of the above procedures were completed successfully with the `show switch` command.

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

Upgrading to ExtremeWare 7.8

If you are running any software image from ExtremeWare 7.0 to ExtremeWare 7.3, upgrade to ExtremeWare 7.8:

NOTE

If you are running ExtremeWare 7.4 or later, save your configuration, follow steps 3 and 4 in the following procedure, and reboot the switch.

NOTE

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

1 Upload the configuration to your TFTP server using the `upload configuration` command.
2 Download the BootROM using the `download bootrom [<host_name> | <ip_addr>] <ngboot82.bin_name>` command, if required.
3 TFTP download ExtremeWare 7.8 to the non-active partition image space using the `download image <partition>` command.
4 Select the downloaded image partition using the `use image secondary/primary` command.
5 TFTP download the configuration you saved in Step 1, and enter `y` at the prompt to reboot the switch.
6 Check the log for configuration errors. Manually enter configurations that did not load.
7 Save the new configuration to the active configuration space. Do **not** save to the non-active configuration space until you are certain a downgrade to the previous image is not required.
8 If you are upgrading a BlackDiamond switch, synchronize the BootROM, image, and configuration across all installed MSM modules using the `synchronize` command. This command reboots the synchronized modules. You can ignore any diagnostics failure messages generated by the synchronization.
9 If you are using network login campus mode:
   a Manually enable network login using the `enable netlogin [web-based | dot1x]` command.
   b Verify that users are able to authenticate and successfully access network resources.

Upgrading T1, E1, or T3 Modules

If you are using a T1, E1, or T3 module with BootROM 2.8 (or later), upgrade the module to ExtremeWare 7.8:

1 TFTP download the latest ExtremeWare for the module using the `download image slot primary` command.
2 Configure the module to use the primary image with the `use image primary slot` command.
3 Reboot the module using the `reboot slot` command.

Upgrading ATM, MPLS, ARM, or PoS Modules

If you are using an ATM, MPLS, ARM, or PoS module, upgrade the module to ExtremeWare 7.8:

1 Upgrade your switch to ExtremeWare 7.8 by following the upgrade instructions “Upgrading “i” Series Switches to ExtremeWare 7.8” on page 29. When your switch is successfully booted on ExtremeWare 7.8 continue with step #2.
2 TFTP download ExtremeWare 7.8 for the module using the `download image slot primary` command.
3 Configure the module to use the primary image with the `use image primary slot` command.
4 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 4 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

5 Verify that the correct ExtremeWare is loaded using the show version command.
6 Download the BootROM using the `download bootrom slot` command.

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

8 Verify the slot is operational using the `show slot <#>` command.

Upgrading PoE Firmware on an Alpine Switch with a PoE Module

If you are using an Alpine switch with a PoE module, upgrade the PoE firmware. A version of PoE firmware is built into ExtremeWare to allow easy replacement if necessary. If the current micro controller firmware becomes corrupted, or requires an upgrade, ExtremeWare logs a message in the syslog prompting for a firmware upgrade.

NOTE

Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until this firmware update is completed, the PoE ports are not powered up.

1 Use the following command to download the firmware to the selected slot:

```
download firmware slot <slot_number>
```

2 Verify that the PoE firmware loaded correctly using the `show inline-power stats <slot number>` command.

If the upgrade is not successful, perform the upgrade procedure again.

Downgrading “i” Series Switches

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

1 If you saved a previous configuration during the upgrade process, configure the switch to use that configuration with the `use configuration secondary` command.

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

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

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

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

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

6 Reboot the switch.

NOTE

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

Upgrading ExtremeWare on the Summit “e” Series Switches Using the CLI

This section describes how to upgrade to ExtremeWare 7.8 on the Summit “e” series switches.

NOTE

Because of the drastic change in the functionality between ExtremeWare 7.8 and ExtremeWare 7.1e, not all configuration databases are automatically converted during the initial boot of ExtremeWare 7.8. Failure to download the saved configuration will leave the switch with a minimal default configuration.

NOTE

If you are using ExtremeWare 7.1e and stacking is enabled, the stacking functionality has changed drastically since ExtremeWare 7.4. As a result, some CLI commands are not compatible. Refer to the ExtremeWare 7.4 (or later) User Guide or Command Reference Guide for configuration differences.

NOTE

If you need SSH functionality, and if you are upgrading from ExtremeWare 7.4 or earlier, you must first download the non-SSH image followed by downloading the SSH image. If you are upgrading to ExtremeWare 7.4 or later, use the following procedure. To request SSH code, contact Extreme Networks Technical Support.

Upgrading a Summit 200 or Summit 300-24 to ExtremeWare 7.8

Upgrade a Summit 200 or Summit 300-24 switch to ExtremeWare 7.8 as follows:

1. Upload the current configuration to a TFTP server using the `upload configuration` command.
2. Download ExtremeWare 7.8 image v783b5.Wxtr to the primary image space using the `download image primary` command.
3. Download the configuration you saved in step 1.
4. When the switch asks `Would you like to reboot the system?`, enter `y`.
5. When the switch comes back up, save the configuration by running the `save configuration` command.
6. Run the `show version` or `show switch` command to display the ExtremeWare version running on your switch.

Upgrading a Summit 300-48 to ExtremeWare 7.8

Upgrade a Summit 300-48 switch to ExtremeWare 7.8 as follows:

1. Upload the current configuration to a TFTP server using the `upload configuration` command.
2. Download ExtremeWare 7.8 image v783b5.Lxtr to the primary image space using the `download image primary` command.
3. Download the configuration you saved in step 1.

Upgrading a Summit 400 to ExtremeWare 7.8

Upgrade a Summit 400 to ExtremeWare 7.8 as follows:

1. Upload the current configuration to a TFTP server.
2. If the current software version is ExtremeWare 7.3 or ExtremeWare 7.4 and BootROM version is 5.1, download v783b5.Cxtr to the primary image space using `download image primary` command then go to step 6.
3. Download BootROM S400_boot51.bin for Summit 400-48t or S405_boot51.bin for Summit 400-24 and reboot the switch using the `reboot` command.
4. If the current software version is earlier than ExtremeWare 7.3, first download v73e0b43.Cxtr to the primary image space using the `download image primary` command and reboot the switch using the `reboot` command.
5. Download ExtremeWare 7.8 image v783b5.Cxtr to the primary image space using the `download image primary` command.
6. Download the configuration you saved in step 1.

Upgrading a Summit “e” Series Stack to ExtremeWare 7.8

Upgrade a Summit “e” series stack to ExtremeWare 7.8 as follows:

1. Upload the current configuration to a TFTP server using the `upload configuration` command.
2. Download ExtremeWare 7.8 image to the stack master primary image space (v783b5.Cxtr for Summit 400 switches and v783b5.Fxtr for Summit 200/300 switches) using the `download image <tftp server ip> <imagelocation/imagename> primary` command.
3. Download ExtremeWare 7.8 image to the stack`s slave slot primary image space (v783b5.Cxtr for Summit 400 switches and v783b5.Fxtr for 200/300 switches) using the `download image <tftp server ip> <imagelocation/imagename> primary slot <slot no>` command.
4. Repeat step 2 for each slave slot in the stack.
5. Download the configuration you saved in step 1.

NOTE

Ensure the secondary image on the switch is the current working image.

Downgrading ExtremeWare

These instructions assume that you followed the upgrade instructions correctly and that the desired previous configuration has been preserved in the secondary configuration space.

1. If the secondary configuration was saved while using a previous image, configure the switch to use the secondary configuration using the `use configuration secondary` command.
2. If there is no stored configuration saved for that version of ExtremeWare, you must either reconfigure, or unconfigure, the configuration file chosen (using the `unconfig switch all` command) or download the correct configuration file to the switch while running the desired image.
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 Reboot the switch.

6 If you do not have the appropriate configuration downloaded, reconfigure the switch or download the appropriate configuration.

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.

Upgrading ExtremeWare on Summit Series Switches Using EPICenter 5.0

If you have multiple switches you plan to upgrade to ExtremeWare 7.8, you can use Extreme's EPICenter Management Suite 5.0 software to do a bulk upgrade of these devices. EPICenter's Firmware Manager enables you to do a bulk upgrade of devices of the same type, which greatly speeds and simplifies the upgrade process, and avoids the need to upgrade your switches one by one.

For information on upgrading Summit 200, 300, and 400 series switches to ExtremeWare 7.8 using EPICenter, see the EPICenter 5.0 Service Pack 3 Release Note. For general information on EPICenter 5.0, and on using the EPICenter Firmware Manager, see the *EPICenter Reference Guide* available on the Extreme Networks website.

Upgrading Wireless Port Images

The following procedure describes how to upgrade the software images (Boostrap, Bootloader, and runtime) on Altitude 300 Access Points connected to any of the following switches:

- Summit 300-48
- Summit 300-24
- Summit 400-24p
- Alpine

The procedure for upgrading Direct Connect or Remote Connect APs remains the same.

NOTE

Upgrading to ExtremeWare 7.8 requires network downtime for wireless networks.

AP Image Names

AP image files are named as follows:

- Bootstrap Image—ABS-X_Y_Z.bin
- Bootloader—ABL-X_Y_Z.bin
- Runtime—ART-X_Y_Z.bin

where

X = Major version number

Y = Minor version number

Z = SR or build number

For example:

ABS-1_8_0.bin is an AP Bootstrap image.

ABL-2_13_7.bin is an AP Bootloader image.

ART-7_7_3.bin is an AP runtime image.

When you specify filenames in the image configuration commands, the names must match the AP image type indicated in the command line.

Before the Upgrade

Before you perform this or any other upgrade, make the following preparations:

- You should back up the current configuration to an external TFTP server using the `upload configuration` command. You should also download the current switch runtime image to the secondary image location on the switch before you download a new image to the primary location on the switch.
- It is strongly recommended that you document the current bootcode versions of all APs to be upgraded. This information may be important to have if any troubleshooting is required in the event of specific AP upgrade failures. In most cases, you will be running one of the following code versions:
  - 1.5.2 BootROM—older APs running only in Direct Connect mode. This is the single bootcode version of the AP.
  - 1.8.0 Bootstrap, and 2.10.x/2.11.x/2.12x/2.13x Bootloader code versions—the split bootcode version of the AP that is required for anyone operating an AP in Remote Connect mode. This split code version of the AP may also be used to operate APs in Direct Connect mode.
  - If an AP already has 1.8.0 Bootstrap, you do not need to upgrade the AP Bootstrap.

  To retrieve this information, use the following command while the AP is up and running:

  ```
  show wireless ports <x:y> detail
  ```

Quick Summary

To upgrade the image software on Altitude 300 Access Points, you will be following these steps:

1. Back up the current configuration to an external TFTP server.
2. Upgrade the switch image to ExtremeWare 7.8.
3. Load the AP Bootstrap, Bootloader, and runtime images onto a TFTP server on your switch.
4. Configure the Bootstrap, Bootloader, and runtime images.
5. Reset the wireless port.
6. When the upgrade is complete for all APs, you can remove the TFTP server from the network. Unconfigure the Bootstrap and Bootloader images for the port.

Upgrade Procedure

NOTE

Before performing any upgrade, you should back up the current configuration to an external TFTP server. You should also download the current switch runtime image to the secondary image location on the switch before you download a new image to the primary location on the switch.

CAUTION

Do not disconnect Altitude 300 APs during the upgrade process; unplugging them during the upgrade can cause file corruption.

To download a new image for the APs, perform the following steps:

1. Upgrade the switch image to ExtremeWare 7.8.
2. Load the AP Bootstrap, Bootloader, and runtime images onto a TFTP server on your network. Ensure the TFTP server is reachable from the switch and AP by proper Layer 2 or Layer 3 configuration.
3. Configure the Bootstrap, Bootloader, and runtime images using the following commands:

   ```
   configure wireless image-configuration bootstrap [<host name> | <ip address>] <filename>
   ```

   ```
   configure wireless image-configuration bootloader [<host name> | <ip address>] <filename>
   ```

   configure wireless ports [<portlist> | all] image-configuration runtime [<host name> | <ip address>] <filename>

   Reset the wireless ports using the `reset wireless ports` command. The AP now starts upgrading the bootstrap, bootloader, and runtime image as configured. You can upgrade all the APs on a switch at one time or as a group of APs, as required. However, you should upgrade all the APs using the ExtremeWare 7.8 AP images before putting them in operation. Older AP image versions may not be compatible with ExtremeWare 7.8.
4. When the upgrade is complete for all APs, you can remove the TFTP server from the network. Unconfigure the bootstrap and boot loader images for the ports using the following commands:

   - `unconfigure wireless image-configuration bootstrap`
   - `unconfigure wireless image-configuration bootloader`

   This prevents subsequent unnecessary attempts to upgrade the Bootstrap and Bootloader files if the APs are reset.

During the AP upgrade, you can monitor progress using the `show log` and `show wireless ports [all | <portlist>] {detail}` commands.

Notes on the Upgrade Procedure

The two most common causes of failure for this procedure are:

- Lack of connectivity between the AP and the TFTP source of the AP image being downloaded to the AP.
- Misconfiguration of the IP address and/or filename location for the image being downloaded to the AP.

Error Messages

In case of a failure, the switch log shows the cause for the failure. Following are the different causes of failures that can occur:

TFTP Related Failures

Following is the error message

```
Wireless port <port number>. <image type> image transfer failed. Reason : <fail
reason>
```

Resetting the wireless port.

For example, if the runtime image is not found in the TFTP server, the following error message is displayed:

```
Wireless port 1:3. Runtime image transfer failed. Reason : File not found. Resetting
the wireless port.
```

Reasons for Failure

Server not reachable.
AP is not able to reach the TFTP server.

Unknown host
AP is unable to resolve the TFTP server name.

File not found
Requested file is not available in the TFTP server.

Version Mismatch
Switch version does not match with the transferred file.

Checksum failed
TFTP failed due to checksum error.

General Error
This is due to some general TFTP protocol error such as malformed packets.

Version Conflict

In the case of Bootstrap and Bootloader, the AP checks for version of the file transferred. If the AP already has the same image as the one sent from TFTP server, the file is ignored with the log of the following type:

```
Wireless port <port> Version conflict found in transferred Bootstrap. Proceeding to
next file type.
```

```
Wireless port <port> Version conflict found in transferred Bootloader. Proceeding to
next file type.
```

In the case of a runtime error, the AP verifies the version number sent by the switch to ensure it matches the transferred file. If it does not match, the AP ignores the runtime image.

Successive Failures

Any time an AP encounters five successive TFTP failures, the AP/wireless port is moved into an error state and a trap is generated.

The following error message is generated:

```
Too many TFTP tries made for port=<port>. Sending out trap and moving port to ERR."
```

To retry the AP image upgrade or boot-up, you must disable the port and then enable it.

Flash Write Failure

The following error message is generated when the AP fails to write a runtime image onto flash:

```
Failed writing AP runtime onto FLASH
```

If the AP fails to write a runtime image on flash, it can still come up by downloading the runtime image from the network.

3 CHAPTER Supported Limits

This chapter summarizes the supported limits in ExtremeWare 7.8 and contains the following sections:

- Supported Limits for ExtremeWare "i" Series Switches on page 41.
- Supported Limits for ExtremeWare "e" Series Switches on page 48.
- Stacking Limits for Summit Series Switches on page 52.

Supported Limits for ExtremeWare "i" Series Switches

Table 24 lists the supported limits for the "i" series switches. The contents of this table supersede any values mentioned in the *ExtremeWare 7.8 User Guide.*

Table 24: Supported Limits for "i" Series Switches

Metric	Description	Limit
Access list rules	Maximum number of Access Lists (best case).	5,120
Access list rules—BlackDiamond 6816	Maximum number of BlackDiamond 6816 Access Lists (best case).	3,500
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 list rules—IGMP	Maximum number of IGMP access lists that can be present in the system.	512
Access profiles	Maximum number of access profiles per switch.	128
Access profile entries	Maximum number of access profile entries per switch.	256
Application examination rules	Maximum number of Application Examination rules.	1,000
Application examination rules/port	Maximum number of Application Examination rules per port.	60
BGP—peer groups	Maximum number of BGP peer groups per switch.	16

Table 24: Supported Limits for "i" Series Switches (Continued)

Metric	Description	Limit
BGP—peers	Maximum number of BGP peers per switch.	200
BGP—routes, MSM-3	Maximum number of routes received and contained in the BGP route table (best case).	810,000
BGP—routes, MSM64i	Maximum number of routes received and contained in the BGP route table (best case).	280,000
BGP—routes, Alpine	Maximum number of routes received and contained in the BGP route table (best case).	315,000
BGP—routes, Summit7i	Maximum number of routes received and contained in the BGP route table (best case).	385,000
BGP—routes, Summit48i	Maximum number of routes received and contained in the BGP route table (best case).	80,000
BGP—routes, Summit5i	Maximum number of routes received and contained in the BGP route table (best case).	59,000
BGP—routes, Summit1i	Maximum number of routes received and contained in the BGP route table (best case).	85,000
BGP—routes, Summit48si	Maximum number of routes received and contained in the BGP route table (best case).	85,000
BGP—NLRI filters	Maximum number of NLRI filters per switch.	127
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.	127
BGP—AS-Path filter add entries	Maximum number of AS-Path filter add entries per switch.	256
BGP—network statements	Maximum number of network statements per switch.	256
BGP—aggregate addresses	Maximum number of aggregate routes that can be originated per switch.	256
DNS—maximum simultaneous servers	Maximum number of simultaneous domain name servers.	8
DNS—maximum suffixes	Maximum number of simultaneous domain suffixes.	6
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.	4,093
EAPS—bridge links	Maximum number of EAPS bridge links per switch.	8,192
EAPS—bridge links	Maximum number of EAPS bridge links on switches with 256MB memory.	8,192
EAPS—bridge links	Maximum number of EAPS bridge links on switches with 128MB memory.	4,096
EAPS—master nodes	Number of Master nodes per EAPS domain.	1
EAPS—switches	Maximum number of EAPS switches per ring.	No limit
EMISTP & PVST+ — maximum domains, Summit	Maximum number of EMISTP and PVST+ domains.	128
EMISTP & PVST+ — maximum domains, Alpine	Maximum number of EMISTP and PVST+ domains.	256

Table 24: Supported Limits for “i” Series Switches (Continued)

Metric	Description	Limit
EMISTP & PVST+ — maximum domains, BlackDiamond	Maximum number of EMISTP and PVST+ domains.	512
EMISTP & PVST+ — maximum ports	Maximum number of EMISTP and PVST+ ports.	3,840
EMISTP & PVST+ — maximum domains per port, Summit	Maximum number of EMISTP and PVST+ domains that can be configured per port.	127
EMISTP & PVST+ — maximum domains per port, Alpine	Maximum number of EMISTP and PVST+ domains that can be configured per port.	255
EMISTP & PVST+ — maximum domains per port, BlackDiamond	Maximum number of EMISTP and PVST+ domains that can be configured per port.	512
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum ESRP groups with bi-directional rate shaping	Maximum number of ESRP groups within a broadcast domain when bi-directional rate shaping is enabled.	3
ESRP—maximum VLANs in a single ESRP domain – Summit, Alpine	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	256 recommended; 3000 maximum
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.	1,024 recommended; 3,000 maximum
ESRP—route-track entries, Summit, Alpine, BlackDiamond	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1
FDB—maximum ports for permanent entries	Maximum number of ports supported for permanent FDB entries.	2,000
FDB—maximum L2/L3 entries – BlackDiamond, Summit5i, Summit7i, Alpine 3804, Alpine 3808	Maximum number of MAC addresses/IP host routes for the MSM64i, Summit5i, Summit7i, Alpine 3804, and Alpine 3808.	262,144
FDB—maximum L2/L3 entries – Summit1i, Summit48i, Summit48si, Alpine 3802	Maximum number of MAC addresses/IP host routes for the Summit1i, Summit48i, Summit48si, and Alpine 3802.	131,072
Flow redirection—maximum redirection rules	Maximum number of rules that can point to the same or separate groups of web cache servers.	64 (8 servers is the maximum)
Flow redirection—maximum enumeration mode entries	Maximum number of active entries for enumeration mode rules. For example, one /16 rule can take all of the available entries.	32,764
Flow redirection—maximum subnet mode entries	Maximum number of active entries for subnet mode rules. Each mask can have 1 entry.	64
IP ARP entries	Maximum number of IP ARP entries.	20,480
IP ARP static entries	Maximum number of permanent IP static ARP entries supported.	4,096
IP ARP static proxy entries	Maximum number of permanent IP ARP proxy entries.	512

Table 24: Supported Limits for "i" Series Switches (Continued)

Metric	Description	Limit
IP route sharing entries (ECMP)—OSPF	Maximum number of OSPF routes used in route sharing calculations.	12
IP route sharing entries (ECMP)—static	Maximum number of static routes used in route sharing calculations.	1,024
IP route sharing entries (ECMP)—IS-IS	Maximum number of IS-IS routes used in route sharing calculations.	8
IP router interfaces	Maximum number of VLANs performing IP routing - excludes SubVLANs.	512
IP static routes	Maximum number of permanent IP routes.	1,024
IP subnet FDB entries	Maximum number of IP subnet FDB entries.	Alpine 3804, Alpine 3808, BlackDiamond, Summit5i,Summit7i, — 262,144
IP subnet FDB entries	Maximum number of IP subnet FDB entries.	Alpine 3802, Summit1i, Summit48i, Summit48si—131,072
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.	2,000 for each
IPX router interfaces	Maximum number of IPX router interfaces.	256
IPX access control lists	Maximum number of Access Lists in which all rules utilize all available options.	worst case: 255
IS-IS—maximum routing interfaces	Maximum IS-IS routing interfaces.	255
IS-IS—maximum routes	Maximum IS-IS routes.	25,000
IS-IS—maximum adjacencies	Maximum IS-IS adjacencies per routing interface.	64
IS-IS—maximum domain summary addresses	Maximum IS-IS domain summary addresses.	32
IS-IS—maximum redistributed routes, regular metric	Maximum IS-IS redistributed routes using the regular metric.	20,000
IS-IS—maximum redistributed routes, wide metric	Maximum IS-IS redistributed routes using the wide metric.	30,000
IS-IS—maximum redistributed routes, both metrics	Maximum IS-IS redistributed routes using both metrics.	10,000
Jumbo frame size	Maximum size supported for Jumbo frames, including the CRC.	9,216
Load sharing groups	Maximum number of groups.	Depends on physical ports available.
Load sharing ports/group	Maximum number of ports per group.	8
Logged messages	Maximum number of messages logged locally on the system.	20,000
MAC-based VLANs—MAC addresses	Maximum number of MAC addresses that can be downloaded to the switch when using MAC-based VLANs.	7,000
MAC-based security	Maximum number of MAC-based security policies.	1,024

Table 24: Supported Limits for “i” Series Switches (Continued)

Metric	Description	Limit
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 NAT connections per switch.	BlackDiamond, Alpine, Summit 7i—256,000
NAT—maximum connections	Maximum number of simultaneous NAT connections per switch.	Summit 1i, Summit 48i, Summit 48si—200,000 Summit 5i—150,000
NAT—maximum rules	Maximum number of rules per switch.	2,048
NAT—maximum VLANs	Maximum number of inside or outside VLANs per switch.	The switch’s limit
NetFlow—filters	Maximum number of NetFlow filters in a switch.	128
NetFlow—groups	Maximum number of NetFlow groups.	32
NetFlow—hosts	Maximum number of NetFlow hosts.	8/group
Network login—MAC-based RADIUS authentication	Maximum number of MAC password entries.	48
Network login—maximum clients	Maximum number of network login clients per switch.	1,024
Network login—802.1x	Maximum recommended Session-Timeout value returned by RADIUS server.	7,200 seconds
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF external routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain.	Alpine—115,000 BlackDiamond—100,000 Summit7i—130,000
OSPF intra-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	Alpine—9,000 BlackDiamond—9,000 Summit7i—11,500
OSPF inter-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	16,000
OSPF external routes—Summit1i, Summit48i, Summit48si	Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain.	27,000
OSPF external routes— Summit5i	Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain.	21,990
OSPF intra-area routes	Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	Summit1i, Summit48i, Summit48si—2,000 Summit 5i—1,700
OSPF inter-area routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	8,000
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	200
OSPF interfaces on a single router	Recommended maximum number of OSPF routed interfaces on a switch.	384

Table 24: Supported Limits for "i" Series Switches (Continued)

Metric	Description	Limit
OSPF virtual links	Maximum number of OSPF virtual links supported.	32
OSPF adjacencies—Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of OSPF adjacencies on a switch with 128 MB memory.	150
OSPF adjacencies—Summit7i, Alpine, BlackDiamond	Maximum number of OSPF adjacencies on a switch with 256 MB memory.	225
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8,000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	384
Route maps	Maximum number of route maps supported on a switch.	128
Route map entries	Maximum number of route map entries supported on a switch.	256
Route map statements	Maximum number of route map statements supported on a switch.	512
SLB—maximum number of simultaneous sessions	For Transparent and Translational and GoGo modes respectively.	500,000/500,000/ unlimited
SLB—maximum number of VIPs	For Transparent and Translational and GoGo modes respectively.	1,000/1,000/unlimited
SLB—maximum number of pools	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of nodes per pool	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of physical servers per group	Applies to GoGo mode only; a group shares any number of common VIPs.	8
SNMP—trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—users	Maximum number of SNMPv3 users.	32
SNMPv3—groups	Maximum number of SNMPv3 groups.	64
SNMPv3—accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—communities	Maximum number of SNMPv3 communities.	64
SNMPv3—target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—filters	Maximum number of SNMPv3 notify filters.	400
Spanning Tree—maximum number of common instances spanning tree (CIST) domains	Maximum number of CIST domains.	1

Table 24: Supported Limits for “i” Series Switches (Continued)

Metric	Description	Limit
Spanning Tree—maximum number of recommended multiple spanning tree instances (MSTI) domains and VLANs	Maximum number of MSTI domains and VLANs.	64/4,000
Spanning Tree—maximum number of multiple spanning tree protocol (MSTP) regions	Maximum number of MSTP regions.	1
Spanning Tree—maximum STPDs, Summit	Maximum number of spanning tree domains.	128
Spanning Tree—maximum STPDs, Alpine	Maximum number of Spanning Tree Domains.	256
Spanning Tree—maximum STPDs, BlackDiamond	Maximum number of Spanning Tree Domains.	512
Spanning Tree—minimum STPDs	Minimum number of Spanning Tree Domains.	1
Spanning Tree—802.1d domains	Maximum number of 802.1d domains per port.	1
Spanning Tree—minimum number of ports	Minimum number of ports that can participate in a single Spanning Tree Domain.	1
Spanning Tree—minimum number of domains/port	Minimum number of Spanning Tree Domains that can be configured per port.	1 for default VLAN, 0 for others
Spanning Tree—spanning tree modes	Maximum number of Spanning Tree modes per switch.	2 (dot1d and dot1w)
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
Standard Multinetting—maximum secondary IP addresses per switch	Maximum secondary IP addresses that can be configured per switch.	64
Standard Multinetting—maximum secondary IP addresses per VLAN	Maximum secondary IP addresses that can be configured per VLAN.	64
Static MAC FDB entries—Summit, Alpine, BlackDiamond	Maximum number of permanent MAC entries configured into the FDB.	4,096
Super-VLAN—number of ports & sub-VLANs	Maximum number of ports and sub-VLANs associated with each super-VLAN.	2,550
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
Trusted MAC entries	Maximum number of simultaneous trusted MAC entries.	48
UDP profiles	Number of profiles that can be created for UDP forwarding.	10
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs—Summit, Alpine	Includes all VLANs plus sub VLANs, super VLANs, etc.	4,095
VLANs—BlackDiamond 6816 fully populated	Includes all VLANs plus sub VLANs, super VLANs, etc.	681
VLANs—BlackDiamond 6816 with up to 7 I/O modules	Includes all VLANs plus sub VLANs, super VLANs, etc.	1776

Table 24: Supported Limits for "i" Series Switches (Continued)

Metric	Description	Limit
VLANs—BlackDiamond	Includes all VLANs plus sub VLANs, super VLANs, etc.	4,095
VLANs—maximum active protocol-sensitive filters	The number of simultaneously active protocol filters in the switch.	15
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4
VRRP—maximum VRIDs with bi-directional rate shaping	Maximum number of unique VRID numbers per switch when bi-directional rate shaping is enabled.	3
VRRP—maximum VLANs/switch	Maximum number of VLANs per switch.	128
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

Supported Limits for ExtremeWare "e" Series Switches

Table 25 summarizes tested metrics for a variety of features in the ExtremeWare 7.8 "e" series switches. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *Summit 400 Series Switch Installation and User Guide*.

Table 25: Supported Limits for "e" Series Switches

Metric	Description	Limit
Access lists/rate limits	Maximum number of access list rules, including rate limit rules.	Summit 200-24—990 Summit 200-48—1,740 Summit 300-24—990 Summit 300-48—1,980 Summit 400-24—1,536 Summit 400-48—5,800
Access list rules—IGMP	Maximum number of IGMP access lists that can be present in the system.	256
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.	4
EAPS—domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	4
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

Table 25: Supported Limits for “e” Series Switches (Continued)

Metric	Description	Limit
EMISTP — maximum domains/ VLANs	Maximum number of EMISTP domains and VLANs.	Summit 200—20/80 Summit 300—20/80 Summit 400—40/150
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum VLANs in a single ESRP domain	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	Summit 200—252 Summit 300—252 Summit 400—256 recommended
ESRP—route-track entries	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1
FDB—maximum multicast entries	Maximum number of multicast entries for the switch.	Summit 200—252 Summit 300—252 Summit 400-24—128 Summit 400-48—256
FDB—maximum number of L2 entries	Maximum number of MAC addresses.	Summit 200—8,000 Summit 300—8,000 Summit 400—16,000
FDB—maximum number of L3 entries	Maximum number of IP addresses.	Summit 200—2,000 Summit 300—2,000 Summit 400-24—2,000 Summit 400-48—4,000
IP router interfaces	Maximum number of VLANs performing IP routing.	Summit 200—32 Summit 300—32 Summit 400-24—128 Summit 400-48—512
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
IP static routes	Maximum number of permanent IP routes.	1024
IP subnet FDB entries	Maximum number of IP subnet FDB entries.	Summit 200—16 Summit 300-24—16 Summit 300-48—16 Summit 400-24—1,024 Summit 400-48—4,096
Load sharing groups	Maximum number of groups.	Summit 200—6 Summit 300-24—6 Summit 300-48—5 Summit 400—25
Load sharing ports/group	Maximum number of ports per group.	8
Mirroring—mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8 (however, more than 3 may affect performance)

Table 25: Supported Limits for "e" Series Switches (Continued)

Metric	Description	Limit
Multicast groups	Maximum number of multicast groups.	Summit 200—252 Summit 300—252 Summit 400-24—127 Summit 400-48—255
NAT—maximum connections	Maximum number of simultaneous NAT connections per switch.	256,000
Network login—802.1x	Maximum recommended session timeout value returned by RADIUS server.	7200
Network login—MAC-based RADIUS authentication	Maximum number of MAC entries.	48
Network login—maximum clients	Network login maximum clients.	1024
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF intra-area routes	Recommended maximum number of intra-area routes contained in an OSPF LSDB.	Summit 200—3,000 Summit 300—2,500 Summit 400—5,000
OSPF inter-area routes	Recommended maximum number of inter-area routes contained in an OSPF LSDB.	5000
OSPF external type 1 or 2 routes	Recommended maximum number of external type 1 or 2 routes contained in an OSPF LSDB.	Summit 200—37,000 Summit 300—35,000 Summit 400—100,000
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.	2
OSPF interfaces, passive	Maximum number of passive OSPF interfaces.	Same as the number of routing interfaces.
OSPF virtual links	Maximum number of OSPF virtual links supported.	2
OSPF adjacencies	Maximum number of OSPF adjacencies on a switch.	4
PVST+ — maximum domains/ VLANs	Maximum number of recommended PVST+ domains and simultaneous VLANs.	Summit 200—40/40 Summit 300—40/40 Summit 400—50/50
Rate limits	Maximum number of rate limit rules.	3,024
Packet buffer—10/100/1000 port	Size of the packet buffer on each 10/100/1000 port.	80 KB
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8,000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	32
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—users	Maximum number of SNMPv3 users.	32
SNMPv3—groups	Maximum number of SNMPv3 groups.	64
SNMPv3—accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128

Table 25: Supported Limits for “e” Series Switches (Continued)

Metric	Description	Limit
SNMPv3—communities	Maximum number of SNMPv3 communities.	64
SNMPv3—target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—filters	Maximum number of SNMPv3 notify filters.	400
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Spanning tree—maximum number of common instances spanning tree (CIST) domains	Maximum number of CIST domains.	1
Spanning tree—maximum number of Multiple spanning tree instances (MSTI) domains and VLANs	Maximum number of MSTI domains and VLANs.	Summit 200—15/252 Summit 300—15/252 Summit 400—32/1,000
Spanning tree—maximum number of multiple spanning tree protocol (MSTP) regions	Maximum number of MSTP regions.	1
Spanning tree—maximum STPDs	Maximum number of Spanning Tree domains.	Summit 200—20 Summit 300—20 Summit 400—40
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
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
Trusted MAC entries	Maximum number of simultaneous trusted MAC entries.	48
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	Maximum number of VLANs (includes all VLANs).	Summit 200—254 Summit 300—254 Summit 400—4,094
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4
VRRP—maximum VLANs/switch	Maximum number of VLANs per switch.	Summit 200—32 Summit 300—32 Summit 400—64
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

Stacking Limits for Summit Series Switches

When creating a stack of Summit 200 and Summit 300-24 switches for powering Power over Ethernet (PoE) devices, the maximum number of PoE capable switches can be eight. However, if creating a stack with Summit 300-24 switches that is expected to process a high volume of data traffic at line rates of 100 Mbps, Extreme Networks recommends limiting the number of Summit 300-24 switches to three. This limitation does not apply to stack configurations that only have IP phones and wireless APs that operate at speeds much lower than 100 Mbps.

When stacking Summit 400 switches, up to eight PoE capable switches can be stacked. The time it takes to make all PoE ports operational increases with the number of PoE capable switches in the stack.

Table 26: Supported Limits for Stacking Summit Series Switches

Metric	Description	Stacking Limits
Access lists/rate limits	Maximum number of access list rules, including rate limit rules	It is the sum of all individual switch limitations in the stack.
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.	4
EAPS—domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	4
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
EMISTP — maximum number of domains/VLANs	Maximum number of EMISTP domains and VLAN.	Summit 200—20/20 Summit 300—20/20 Summit 400—10/30
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum VLANs in a single ESRP domain	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	Summit 200—252 Summit 300—252 Summit 400—256 recommended
ESRP—route-track entries	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1

Table 26: Supported Limits for Stacking Summit Series Switches (Continued)

Metric	Description	Stacking Limits
FDB—maximum multicast entries	Maximum number of multicast entries for the switch.	Master switch limitations apply to the entire stack if the master is: Summit 200—252 Summit 300—252 Summit 400—255
FDB—maximum number of L2 entries	Maximum number of MAC addresses.	Master switch limitations apply to the entire stack if the master is Summit 400—16,000 Summit 200 and Summit 300—8,000
FDB—maximum number of L3 entries	Maximum number of IP addresses.	Master switch limitations apply to the entire stack if the master is: Summit 200—2,000 Summit 300—2,000 Summit 400-24—2,000 Summit 400-48—4,000
IP router interfaces	Maximum number of VLANs performing IP routing.	Master switch limitations apply to the entire stack if the master is: Summit 200—32 Summit 300—32 Summit 400-24—128 Summit 400-48—512
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
IP static routes	Maximum number of permanent IP routes.	1,024
IP subnet FDB entries	Maximum number of IP subnet FDB entries.	Master switch limitations apply to the entire stack if the master is: Summit 200—16 Summit 300-24—16 Summit 400-24—1,024 Summit 400-48—4,096
Load sharing groups	Maximum number of groups.	Master switch limitations apply to the entire stack if the master is: Summit 200—6 Summit 300-24—6 Summit 400—25
Load sharing ports/group	Maximum number of ports per group.	8
Mirroring—mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8 (however, more than 3 may affect performance).

Table 26: Supported Limits for Stacking Summit Series Switches (Continued)

Metric	Description	Stacking Limits
Multicast groups	Maximum number of multicast groups.	Master switch limitations apply to the entire stack if the master is Summit 200—252 Summit 300—252 Summit 400-24—127 Summit 400-48—255
NAT—maximum connections	Maximum number of simultaneous NAT connections per switch.	Summit 200—100,000 Summit 300—100,000 Summit 400—256,000
Network login—802.1x	Maximum recommended session timeout value returned by RADIUS server.	7,200
Network login—MAC-based RADIUS authentication	Maximum number of MAC entries.	48
Network login—maximum Clients	Network login maximum clients.	1,024
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF intra-area routes	Recommended maximum number of intra-area routes contained in an OSPF LSDB.	Summit 200—1,500 Summit 400—5,000
OSPF inter-area routes	Recommended maximum number of inter-area routes contained in an OSPF LSDB.	5,000
OSPF external type 1 or 2 routes	Recommended maximum number of external type 1 or 2 routes contained in an OSPF LSDB.	Summit 200—19,000 Summit 400—100,000
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.	2
OSPF interfaces, passive	Maximum number of passive OSPF interfaces.	512
OSPF virtual links	Maximum number of OSPF virtual links supported.	2
OSPF adjacencies	Maximum number of OSPF adjacencies on a switch.	4
PVST+ — maximum domains/ VLANs	Maximum number of recommended PVST+ domains and simultaneous VLANs.	Summit 200—40/40 Summit 300—40/40 Summit 400—50/50
Rate limits	Maximum number of rate limit rules.	3,024
Packet buffer—10/100/1000 port	Size of the packet buffer on each 10/100/ 1000 port.	80 KB
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8,000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	32
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—users	Maximum number of SNMPv3 users.	32

Table 26: Supported Limits for Stacking Summit Series Switches (Continued)

Metric	Description	Stacking Limits
SNMPv3—groups	Maximum number of SNMPv3 groups.	64
SNMPv3—accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—communities	Maximum number of SNMPv3 communities.	64
SNMPv3—target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—filters	Maximum number of SNMPv3 notify filters.	400
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Spanning Tree—maximum number of common instances spanning tree (CIST) domains	Maximum number of CIST domains.	1
Spanning tree—maximum number of multiple spanning tree instances (MSTI) domains and VLANs	Maximum number of MSTI domains and VLANs.	Summit 200—15/252 Summit 300—15/252 Summit 400—32/1,000
Spanning tree—maximum number of multiple spanning tree protocol (MSTP) regions	Maximum number of MSTP regions.	1
Spanning tree—maximum STPDs	Maximum number of Spanning Tree domains.	Summit 200—10 Summit 300—10 Summit 400—20
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
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
Trusted MAC entries	Maximum number of simultaneous trusted MAC entries.	48
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	Maximum number of VLANs (includes all VLANs).	Master switch limitations apply to the entire stack if the master is: Summit 200—253 Summit 300—253 Summit 400—4,094
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4

Table 26: Supported Limits for Stacking Summit Series Switches (Continued)

Metric	Description	Stacking Limits
VRRP—maximum VLANs/switch	Maximum number of VLANs per switch.	Summit 200—32 Summit 300—32 Summit 400—64
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

4 CHAPTER 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.

Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 7.8. For changes made in previous releases, see the release notes specific to the release.

General

Link-Down Detection Takes Random Amounts of Time on ExtremeWare “i” Series Switches

Link-down detection on ExtremeWare "i" series switches takes random amounts of time, even when link-detection filters are applied (PD3-77462461).

Retransmitted TCP Packets Show Real Server IP Address

Retransmitted TCP packets from a server are forwarded with the real IP address of the server instead of the virtual IP address (PD3-206704231).

Link Becomes Active After Inserting a GBIC in a Combination Port

A link becomes active after inserting a GBIC in a combination port. The link may not stay in the Active state and link flapping may occur (PD3-206577066).

Traffic is Still Sent With Auto-Polarity Off

When two Summit 400-48 switches are connected using a straight-through cable, traffic is still sent when auto-polarity is off (PD3-194767924).

Rebooting Switch Generates an Error Message

The following message is displayed after a system reboot:

```
CRITICAL ERROR: Backplane EEPROM has invalid MAC Address. System halted.
```

This occurs when both MSM A and MSM B are trying to read the backplane EEPROM without first determining which MSM is master/slave (PD3-123573391).

Hot Swapping with Mirroring

Disable mirroring before hot swapping the mirroring slot (PD3-48619436).

Traffic in Mirror to Port is Twice the Actual Traffic in Mirror From Port

When sending unknown traffic, the traffic in the mirror to port (mirroring port) is double the traffic in the mirror from port (mirrored port) (PD3-46218041).

Diffserv Not Supported on Summit 400-24 Platforms

Diffserv examination cannot be enabled on Summit 400-24p and Summit 400-24t platforms. This is a system limitation and will not be resolved (PD3-45617861).

Some APs Reboot in Heavy Traffic and High RF Interference

A switch with 20 plus APs and a high level of RF interference may experience up to three AP reboots in a 24-hour period (PD3-36148261).

Enabling HTTP on a Non-SSH ExtremeWare 7.4 or Later Image

In ExtremeWare 7.3, the CLI command syntax used to enable HTTP is `enable web http` even when upgrading a non-ssh image. In ExtremeWare 7.4, the `enable web` command is use with the option `http/https`. This command option is only available with the ssh image. Therefore, when upgrading an ExtremeWare 7.3 non-ssh configuration to an ExtremeWare 7.4 non-ssh configuration, the `enable web http` command will fail.

```
# enable web http
Syntax error at token http
Next possible completions:
<cr> access-profile
```

Load Sharing Group Cannot be Rate Shaped with Loopback Port

You cannot configure a load sharing group for rate shaping with a loopback port, nor can you tag a rate shaped port, even though the CLI is allowing you to do so (PD2-243742672).

CPU DoS Protect and ACL Precedence

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

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

Alpine

Deleting a Port Causes a Set of Unrelated Ports to Stop Receiving Traffic

When deleting a port from a protocol VLAN on an Alpine3800 switch with five or more FM32Ti I/O modules, a set of unrelated ports is unable to receive traffic (PD3-157524611).

EPICenter/SNMP Does Not Show Port Display String

When configuring a port string using an Alpine switch and viewing the port information from EPICenter, the configured port string is not shown in the port information (PD3-40520509).

BlackDiamond 6800

Running “show eaps” Command May Cause Task Crash

Running the `show eaps` command on a BlackDiamond 6808 switch after making configuration changes results in a task crash (PD4-870070501).

Summit Family of Switches

Packet Information is Not Shown for 1,024–1,518 Size Packets

In a Summit 400 stack master node, the CLI command `show port <port no>` packet does not show packet information for 1,024-1,518 size packets for a slave node port (PD3-205108795).

Loopback Detect Does Not Work on ExtremeWare 7.4e.1b5

On a Summit 300-48 switch running ExtremeWare 7.4e.1b5, if you connect loopback on a specific port and then enable loopback detect, loopback is detected and the port is brought down after 3 or 4 hours. The port is then bought up and down continuously (PD3-39424321).

Bridging

Hot Swapping an I/O Module with Load-Share Group, Can Display Incremented Port Count

In an EAPS ring with load-share ports, if the load-share ports on any of the nodes are hot-swapped, the port count on the master node is incremented (PD3-48242106).

Deleting Member VLANs Flushes FDB Entries

Deleting a member VLAN flushes all FDB entries in the translation and member VLANs (PD3-24824553).

CLI

CLI Syntax for "configure ports auto off" Command is Not Complete

The `configure ports auto off` command as shown in the E*xtremeWare Command Reference Guide, Software Version 7.7*, should include the keyword `speed`. This has been corrected in the E*xtremeWare Command Reference Guide, Software Version 7.8* (PD3-204810096).

Control Protocols

Memory Allocation Errors are Generated when LLDP is Enabled on all Ports

The following memory allocation errors are generated when LLDP is enabled on all ports in an eight slot Summit 200or Summit 300 stack.

```
memPartAlloc: block too big - LLDP enabl81372ed on both Rx a in partition nd Tx
0xfor Port 8132336c8.:230x
82c8ce50LLDP (enabled on both RtConsolex and Tx for):  Port memPartAlloc: block too
big - 881372:24 in partition
0x* D-Lc08-33:18 8132336c# .
0x82c8ce50 (tConsole): memPartAlloc: block too big - 81372 in partition 0x8132336c

<Crit:ELSM> lldpEnable: lldpInfo structure allocation failure, Port 8:24
<Crit:ELSM> lldpEnable: lldpInfo structure allocation failure, Port 8:23
```

(PD3-61417001)

Mirroring Does Not Work on MSTP Enabled Tagged Ports

When configuring MSTP, mirroring does not work on the MSTP enabled tagged port (PD3-53171654).

OSPF Adjacency Lost when an MSTI Root Port is Disabled and Re-enabled

OSPF adjacency is lost when an MSTI root port is disabled and re-enabled in an STP domain (PD3-59194524).

Documentation

"enable/disable bgp advertise-inactive-route" Commands Missing From ExtremeWare Command Reference Guide

The following BGP commands were not included in Chapter 22, "BGP Commands—"i" Series Switches Only" in the *ExtremeWare 7.8 Command Reference Guide*:

If you enable the `advertise-inactive-route` parameter, all the best routes in the local RIB are advertised whether those routes are best routes in the kernel routing table or not. Use the following command to enable inactive route advertisement:

enable bgp advertise-inactive-route

Use the following command to disable inactive route advertisement:

disable bgp advertise-inactive-route

Inactive route advertisement is disabled by default.

(PD2-121338901, PD4-614723231)

ESRP

Rate-Shaped ESRP Slave Interface Loses Some of the ESRP Hello Packets

A rate-shaped ESRP slave interface loses some of the ESRP hello packets from the master and flips between the slave and pre-master state when the election parameters suit the slave to win the ESRP election (PD3-26798641).

IS-IS

Secondary IP Addresses are Not Processed by IS-IS

Secondary IP addresses are not processed by IS-IS when the secondary IP is configured using standard multinetting (PD3-158994569).

NAT

NAT Rules are Not Deleted from Configuration

NAT rules are not deleted from a configuration after a VLAN is deleted (PD3-50714371, PD3-42469211).

Network Login

Web-Based Network Login Using HTTP Proxy is Not Working Correctly

Web-based network login using HTTP proxy configurations does not work on the BlackDiamond series switch, Alpine, or Summit48 switch (PD3-208178593).

DUT Drops Broadcast Frames to the Trusted MAC Client

DUT drops broadcast frames to the trusted MAC client connected to a network login port. Use proxy ARP to forward ARP requests to the trusted MAC client connected to the network login enabled port (PD3-63692861).

extremeNetloginStationAddr is Sent as 0.0.0.0 for Wireless Network Login Traps

Wireless network login and logout traps send the extremeNetloginStationAddr MIB as 0.0.0.0 (PD3-53931118, PD3-43138750).

Mirroring

Egress Layer 3 Traffic Mirroring Across Units is Not Working

Layer 3 traffic mirroring across units in egress direction is not working properly (PD3-92929451).

Multicast

Multicast Traffic Not Switched Across Ports on User VLAN when MVR is Enabled

In an MVR setup, when a sender is part of a user VLAN, traffic is not switched to receivers within a VLAN using IGMP snooping. An IP multicast FDB flush is required to switch traffic (PD3-208833311).

Routing

Exported Static Route in IS-IS is Advertised After Removing the VLAN and Static Route

If a VLAN is removed prior to removing a static route, the exported static route is not removed, even after removing the static route configuration.

Workaround: Remove the static route before deleting the VLAN with the gateway IP address.

(PD3-31673591)

SNMP

MIB Table Becomes Empty When Adding Policy Rules through EPICenter

When adding multiple IP policy rules through EPICenter's Policy Manager, frequently the MIB table will become empty or partially cleared (only some of the rules will remain), even though no error message has occurred, and the policy rules are still in place on the switch. When this happens it is no longer possible to create policies on the switch through EPICenter (PD3-36028540).

LLDP Enabled Port in LldpLocManAddrTable Object

One entry should be created for each LLDP enabled port in the LldpLocManAddrTable object. When the MIB table is queried, it returns only the management address of the first enabled LLDP port (PD3-35774621).

SNMP Response Time From the Switch is Slow

SNMP response time from the switch is slow when the number of APs configured for the switch is more than seven. EPICenter polling may result in a SNMP failure since the default setting for SNMP is 5s timeout and 1 retry.

Workaround. Increase the timeout value in SNMP Client Tool. Suggested values for more than seven APs: timeout: 7 seconds; retry = 2.

(PD3-36087851)

SSH

Timed Configuration Downloads Fail

Timed configuration downloads fail when used with an SSH connection to the switch (PD3-208318211).

Stacking

Slave Port Returns Incorrect Values for IF-MIB Counters

In a Summit 400 stack, when transmitting unicast traffic through a slave port and performing an SNMP Get, the slave port statistics are inconsistently shown (PD3-208402041).

Save and Download Commands Generate a Send Failure

Running the `save` and `download` commands generates the following error:

```
"Request send failed"
```

Workaround. Repeat the `save` and `download` commands.

(PD3-98175399)

Vista Login is Displayed for Web-based Network Login

In a stack of Summit 200-24 switches, web-based network login may show the Vista login instead of the web-based network login page (PD3-57652255).

With 3000 or More Entries in Host Table, "Table Full" Error Appears in Log

In Summit 400-48 platforms, the IP FDB table may become full before reaching 4,000 entries when there are a large number of entries in the ip-subnet-fdb table (PD3-42986309).

When Configuring Large Number of ACLs in the Stack, NVRAM May Run Out of Space

When configuring a very large number of ACLs (more than 5000), there may not be enough space in the NVRAM to save the ACLs. You may see the following message when saving the configuration:

```
Do you want to save to the primary configuration database? y

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>ERROR: ACL: too many rules to save in NVRAM
(requires 6566568 bytes available 6144000 bytes).

>>>>>>>>>>!.!.!Saved to primary configuration database.
```

(PD3-47170526)

PoE Configurations are only Applied to Operational Slots

In a stack, PoE configurations are not applied to slots that are not yet operational. Ensure that the slot is operational before applying the PoE configuration for that slot through the CLI (PD3-46295816).

Bootup Time May Take up to Two Minutes to Bootup

A full stack consisting of eight Summit 200 or Summit 300-24 switches may take slightly over two minutes to bootup. However, a full stack of Summit 400 switches would take just under two minutes on the average to bootup.

Configuring the Mirrored-to Port

Once you configure the mirrored-to port to be either tagged or untagged, if you change it from tagged to untagged, or from untagged to tagged, the change will only take affect after a reboot (PD3-29054741).

VLAN Tagged 2 Cannot be Used When Stacking is Enabled

If stacking is enabled on the switch, the switch will not allow you to create a user VLAN with a tag of 2 (PD3-30253861).

Wrong Number of Ports Displayed in Default VLAN

The default VLAN shows the incorrect number of active ports after all ports are deleted from the VLAN if the following procedure is followed:

1. Save the configuration using the ExtremeWare 7.4 image.
2. Reboot the switch and save the configuration using the ExtremeWare 7.3 image.
3. Reboot the switch to the ExtremeWare 7.4 image using the saved ExtremeWare 7.3 configuration.
4. If all ports are deleted from the default VLAN, the incorrect number of active ports is shown.

(PD3-28261405)

Mix Mode Stacking is Not Supported

Mixed mode stacking, that is, stacking between Summit 200/300/400 series switches, is not supported in this release (PD3-25989591).

Wireless

Upgrading AP Bootloader through AP Runtime May Generate an Error

The `upgrade wireless ports x:xx bootloader` command may generate the following error:

```
downloadFile: Cannot upgrade. TFTP task spawn failed
```

(PD3-85756744)

Remote Connect AP with DHCP server

When a DHCP server is used for assigning IP addresses to a remote connect AP, the AP reboots every few minutes and requests a different IP address each time.

Workaround: Configure a fixed IP address for each remote connect AP in the DHCP server.

(PD3-39416246)

No Error Generated When Adding Channel 0 to an AP Scan

No error is generated when adding channel 0 to an AP scan list. Channel 0 is equivalent to no channel configured, so `enable wireless ports interface ap-scan off-channel` command will fail (PD3-45607200, PD3-38741731).

IAPP Does Not Support WPA and WPA2

IAPP roaming works with the following authentication methods:

- Open WEP
- Shared WEP
- Open MacRadius
- Shared MacRadius
- dot1x

IAPP is not supported for WPA and WPA2 (PD3-45607119, PD3-29602669).

Request Error Running show wireless ap-scan result Command with Two APs

The following request error is generated when running the `show wireless ap-scan result` command on two APs in continuous off-channel scan:

```
<Erro:SYST> No rows retrieved from AP
<Erro:SYST> Error message: Unknown error while getting varbind.
<Erro:SYST> Failed request for port v:2 interface 2 member
(name) WI_STATISTICS_BLOB
```

Workaround. Run the `show wireless port x:y int z ap-scan result` command to show the results for individual ports.

(PD3-45606949, PD3-38959831)

Wireless Network Login is Not Supported in Remote Connect AP

Wireless network login is not supported in remote connect. Therefore, do not assign a wireless network login security profile to a virtual port (PD3-45607276, PD3-38588890).

TCP/IP Connection is Lost if Internal DHCP is Enabled

The TCP/IP connection between the switch and the AP is lost if internal DHCP is enabled and wireless network login is not configured on the wireless port.

Workaround. Enable DHCP on a wireless port only when wireless network login is used.

(PD3-45606873, PD3-35311601)

SNMP Error Messages are Generated When Wireless Port is Reset

When you reset a wireless port that is online, the following SNMP error messages are logged:

```
<Erro:WLANSYST> <WLAN> Port 1 SNMP failed to parse the packet with 7a198
<Info:WLANSYST> <WLAN> Port 1 Wireless Port Down
<Info:SYST> 10.255.52.7 admin: reset wireless ports 1
```

(PD3-36028901)

Stacking and UAA Functionality

UAA functionality is stated to be available on a master slot of a stack in the *ExtremeWare 7.4 User Guide*. This is incorrect. UAA is not supported on any stacking. This will be corrected in future updates of the *ExtremeWare 7.4 User Guide* (PD3-36334122).

Wireless Client Sees Wrong Log Message

Wireless clients on A radio show 11930 hours of logged on time when the `show wireless ports 1:X interface 1 clients` command is executed.

```
00:20:A6:4C:FE:C1 1:44:1 FORWARD   WEP128   DOT1X      11930:25:41
```

This is usually a cosmetic problem. The logged on time shows the correct value after the next RADIUS timer refresh (PD3-28788118).

Logout Window Moves to “Cannot Find Server”

The logout pop-up window moves to the "cannot find server" state after x minutes in network login (PD3-28788428).

A300 Cannot Boot

The A300 cannot boot if the wireless management VLAN is not configured (PD3-28462210, PD3-23854771).

Some IAPP Debug Messages Are Not Logged

If you configure debug-trace for wireless ports to debug-level 5 and set the syslogd priority to debug, when you roam from one AP to another AP, the `show log` command does not display all of the IAPP debug messages, whereas the `show wireless ports x:y log` command displays all IAPP debug messages correctly (PD3-28462355, PD3-6273069).

Do Not Enable AP_Scan on More than Two Interfaces at a Time

If you enable the AP scan on more than two interfaces simultaneously, the scan will run for a few minutes but once you issue the `show wireless ap-scan results` command, the switch reboots (PD3-28764622, PD3-3868131).

Issues Resolved in Extremeware 7.8.4b1-patch1-4

The following issues were resolved in ExtremeWare 7.8.4b1-patch1-4. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

STP blocks LAG master port if member links flap often. This results in traffic loss across LAG. (PD4-1946108425)

A VRRP task crash occurs if a switch receives a VRRP packet from a different IP and VRID when multinetting is enabled. (PD4-2515132229)

Issues Resolved in Extremeware 7.8.4b1-patch1-3

The following issues were resolved in ExtremeWare 7.8.4b1-patch1-3. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

When port sharing is enabled across modules, disabling sharing results in "tConsole" task crash (PD4-2266033860).

EAPS

ExtremeWare switches drop unknown EAPSv2 PDUs in slowpath, which results in traffic loss for approximately 30 seconds in the EAPS network containing ExtremeXOS switches (PD4-1508094351).

Issues Resolved in ExtremeWare 7.8.4b1

The following issues were resolved in ExtremeWare 7.8.4b1. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

Alpine 3800

PIM-SM shadow entries may be corrupted when multiple sources are present for the same multicast group (PD4-1855227631).

Summit 400

When a LAG member port is in the down state, after executing the disable sharing command, broadcast packets are not forwarded to the previous LAG member ports (PD4-1865984441).

Issues Resolved in ExtremeWare 7.8.3-patch1-6

The following issues were resolved in ExtremeWare 7.8.3b5-patch1-6. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

Alpine 3800

Running ELRP on an EAPS protected VLAN generates the following error message:

Callback function is NULL (PD4-1737549356).

Summit 200

Even with STP enabled, a short loop is generated when untagged ports in the same VLAN but on a different stack are connected (PD4-1679158821).

Summit 400

After running the `disable sharing` command, broadcast packets may not be forwarded to the previous LAG member ports (PD4-1008588924).

Issues Resolved in ExtremeWare 7.8.3-patch1-5

The following issues were resolved in ExtremeWare 7.8.3b5-patch1-5. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

The thttpd process may crash during network login authentication (PD4-1686813762).

BlackDiamond 6800

The number of reboots for a backup MSM to enter minimal mode is not equivalent to the configured reboot-loop-protection value (PD4-1687904846).

Summit 200

The command output for the `show netlogin` command does not display the authenticated netlogin client. (PD4-1121217505).

Issues Resolved in ExtremeWare 7.8.3b5-patch1-4

The following issues were resolved in ExtremeWare 7.8.3b5-patch1-4. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

When a host name begins with a number, the system is unable to resolve the IP address (PD4-1419915040).

BlackDiamond 6800

The number of system reboots needed to enter minimal mode is not equivalent to the configured reboot-loop-protection value (PD4-1465735503).

Summit 200

An authenticated web-based netlogin client cannot access network resources using the DHCP behavior of a Summit 200 switch (PD4-1458363875).

When a Summit 200 or Summit 400 switch receives LACP packets, FDB entries are learned on blocked ports (PD4-1597840529).

DHCP

When a DHCP server on a Summit 400 switch allocates DHCP bindings, the bindings time out after five minutes (PD4-1516494312).

Issues Resolved in ExtremeWare 7.8.3b5-patch1-3

The following issues were resolved in ExtremeWare 7.8.3b5-patch1-3. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

Flow-redirect next-hop goes down and up when an STP state changes while flow-redirect next-hop is not in that STP VLAN (PD4-504431596).

IGMP

IGMPv2 join and membership requests do not have a `router alert` option in the IP header set of the packets. If the `router alert` option is not set, network routers may experience problems processing the IGMP joins (PD4-1318478153).

Issues Resolved in ExtremeWare 7.8.3b5-patch1-1

The following issues were resolved in ExtremeWare 7.8.3b5-patch1-1. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

BlackDiamond 6800

In a customer specific EAPS topology, rebooting a BlackDiamond 6800 switch causes the system to crash (PD4-1212726321).

Issues Resolved in ExtremeWare 7.8.3b5

The following issues were resolved in ExtremeWare 7.8.3b5. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

The MSTP region setting is not shown in the output of the `show configuration detail` command (PD4-498662057).

GVRP related commands and configurations are no longer supported in ExtremeWare (PD4-629151986, PD3-64731521).

Retransmitted TCP packets from a server are forwarded with the real IP address of the server instead of the virtual IP address (PD3-206704231).

Ports on a Summit7i switch move to Ready state after a soft reboot because of the hardware watchdog (PD4-912140316).

A Summit5i switch experiences memory depletion when running 1,000 or more multicast streams (PD4-909055989).

When a soft rate-limit is configured on a port, if CPU DoS protect is enabled, messages are logged for no reason (PD4-750703317).

Alpine 3800

Alpine switches running ExtremeWare software drop traffic sent to a CPU when the slot with the master port of a cross module load-share group is removed (PD4-365209879).

G16X fiber ports on an Alpine 3804 switch stay in the Speed Cfg=AUTO state and do not forward packets if the ports were previously configured as loopback ports (PD4-1082073161).

BlackDiamond 6800

A port is showing as half-duplex when configured for full-duplex in certain configurations (PD4-1132842302).

Loop-back mode cannot be disabled on a "default" VLAN (PD4-803184113).

Hidden MPLS commands such as `disableOamDiscovery` should not be generated in the `show` and `upload configuration` command output (PD4-1005796025).

PIM packets loopback and create IGMP snooping using the L3 interface IP address as the router port (PD4-968386356).

Summit 1i

After removing a rate-limiting configuration from a Summit 1i switch, forwarding fails (PD4-950712851).

Summit 200

In Summit 200-48 stack, loop occurs even when STP edge mode is configured (PD4-963320633).

Summit 400

In a Summit 400 stack, when transmitting unicast traffic through a slave port and performing an SNMP Get, the slave port statistics are inconsistently shown (PD3-208402041).

DHCP

A switch does not respond to a DHCP request message with a source address of 0.0.0.0 and a destination address of 255.255.255.255 from a client PC. The switch should reply with a DHCP NACK message (PD3-206956821).

IGMP

With IGMP snooping proxy enabled, IGMP leave is forwarded when multiple IGMP receivers are connected through a single port (PD4-1087700970).

Multicast

Multicast packets are egressing on sender source ports when the transmitting port is not the first active port in a slot (PD4-808656341).

Network Login

Using dot1x authentication, if the mode is forceAuthorize, SNMP traps are not generated when a user logs in to the system (PD4-579141865).

Alpine switches fill with RADIUS error messages when receiving a large number of requests simultaneously (PD4-817691609).

Security

The HTTP server name is not masked in packet headers (PD4-811849681).

SNMP

An SNMP trap is not generated when running the `disable slot msm-b` command (PD4-735701386).

The SNMP task crashes when executing an SNMP get/getnext for the OID ipNetToMediaIfIndex (PD4-721845962).

VRRP

A watchdog timer expires when `ip-subnet-lookup` is enabled and a switch learns 500 IP ARP entries (PD4-908676603, PD4-487662171).

Issues Resolved in ExtremeWare 7.8.2b1

The following issues were resolved in ExtremeWare 7.8.2b1. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

ICMP configurations are not uploaded to a TFTP server (PD4-556821963).

The message "Task 0x84e3abe0 has exceeded its own stack boundary (mportTask)" is logged frequently, therefore, the mportTask stack size has been increased from 8,000 to 9,000 (PD4-597789884).

When a route to a source is lost, PIM DM does not install a kill entry for the (S,G) (PD4-328276448, PD3-1986563).

Do not upload "create ospf area 0.0.0.0" in a switch configuration as the default value (PD4-556822022).

A QoS profile configuration that is not applicable to a management port displays incorrectly in the output of the show vlan mgmt command (PD4-554109343).

A RIP import-filter does not filter the default route in permit or none modes (PD3-206390241).

RIPv1 routes are learned with different netmasks in ExtremeWare 7.3.0b44, ExtremeWare 7.3.0b49, and ExtremeWare 7.7.3b5 (PD3-207946788).

After running the `configure configuration-mode enhanced` command, the configuration is changed to enhanced mode. However, the output for the `show switch` command remains "Default configuration-mode is standard." The switch requires a reboot to correct the display (PD3-198480450).

After issuing the disable slot x command and replacing the I/O module, the system does not recognize the serial number of the swapped module. This issue does not occur if you are running ExtremeWare 7.3 or earlier (PD3-171240201).

ESRP

An ESRP-aware switch does not flush FDBs belonging to a domain member VLAN (PD4-573244753).

IGMP

When adding a static Internet Group Management Protocol (IGMP) group to a port not belonging to the assigned VLAN, the switch silently drops the configuration without displaying an error or warning message (PD4-409050501).

An IGMP membership query is sent out when running the `clear igmp snooping` command even though IGMP is disabled (PD3-202676751).

OSPF

OSPF inter- and inter-area routes are not filtered when using access-profiles or route-maps (PD4-360116037).

SNMP

SNMP stops responding if the SNMP response size is between 2,044-2,048 bytes (PD4-554108760).

A link up or link down trap for a management port is not sent after resetting an ExtremeWare configuration to factory defaults (PD4-248373901).

After uploading and downloading a configuration and then running the show snmpv3 access command, the read-view keyword is enabled for the configured SNMPv3 access group (PD3-208733461).

Issues Resolved in ExtremeWare 7.8.1b1-patch1-9

The following issues were resolved in ExtremeWare 7.8.1b1-patch1-9. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

When all connected hosts come online, a RADIUS failure occurs when sending out bulk requests (PD4-536048620).

On Summit 300 and 400 platforms, auto polarity does not work after rebooting or upgrading a switch to ExtremeWare 7.7.3b5-patch1-10 (PD4-484315416).

Network Login

A network login authentication window will not open if a user is already authenticated. However, if a user opens more than one netlogin session before authentication and tries to login from each session, it is allowed. Network login authentication should not be allowed if the user is already authenticated (PD4-310106562).

Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) interoperability issues occur between ExtremeWare and other third party software vendors (PD4-487580225).

Issues Resolved in ExtremeWare 7.8.1b1-patch1-8

The following issues were resolved in ExtremeWare 7.8.1b1-patch1-8. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.4b1. For information on those fixes, see the appropriate release notes.

General

Link Aggregation Control Protocol (LACP) stops working after running continuously for 497 days (PD4-477516360).

After upgrading to ExtremeWare 7.8.1b1, SSH and Telnet access to the switch stops working (PD4-499856017).

EDP

After disabling Extreme Discovery Protocol (EDP) between an ExtremeWare and an ExtremeXOS switch, the ExtremeWare switch continuously sends an EdpNeighborRemoved Simple Network Management Protocol (SNMP) trap (PD4-476783070).

Network Login

When authenticating a user using web-based network login, a thttpd task crash occurs if the user name is more than 256 bytes (PD4-426950899).

When executing the `show netlogin port <port no> <vlan name>` command, the tConsole task crashes.

Workaround: Run the `show netlogin port <port no> <vlan name>` command after running the `disable clipaging` command.

(PD4-368976553)

SNMP

During system bootup, the SNMPv3 engine boot value is read from NVRAM. In rare cases, the memory is corrupted and returns a value of -1. When this occurs, a warning or error message should be logged (PD4-457250653).

Wireless

Wireless Access Point information cannot be displayed on a Summit 300-48 switch after running the `clear iparp` command if an AP is disconnected and connected to a disabled port (PD3-208369639).

Issues Resolved in ExtremeWare 7.8.1b1-patch1-1

The following issues were resolved in ExtremeWare 7.8.1b1-patch1-1. ExtremeWare 7.8 includes all fixes up to and including ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, ExtremeWare 7.3e.3b4, ExtremeWare 7.4.4b9, ExtremeWare 7.5.4b3, ExtremeWare 7.6.4b4, and ExtremeWare 7.7.3b5 though patch 1-14. All patches currently available for ExtremeWare 7.7.3 will be included in the next sustaining release of ExtremeWare 7.8 (ExtremeWare 7.8.2). For information on those fixes, see the appropriate release notes.

Summit Family of Switches

A Summit 400-24, when configured with an SNTP update interval of 7,200, displays inconsistent time intervals between the `syslog` and `show switch` commands (PD3-204998748).

IS-IS

If an IS-IS router uses an overload bit, it should not be used as a transit router. However, it should route direct attached networks. With ExtremeWare, when an LSP is received with an overload bit set, all routes to that IS-IS router are deleted. Only the routes that are routed through the IS-IS router should be deleted, not directly attached routes (PD3-206354100).

Multicast

In PIM multicast border router (PMBR), even after Internet Group Management Protocol (IGMP) RX is deleted from the dense mode (DM) domain, multicast packets are sent to the CPU in the PMBR (PD4-270936257).

In a Protocol Independent Multicast (PIM) scenario, when you run the `clear ipmc cache` command, the *, *, and rp entries are removed, stopping further traffic to PIM-DM subscribers (PD4-270936748).