



ExtremeWare IPv6 1.2 Release Note

This release note contains information about features and issues specific to ExtremeWare IPv6 1.2b19 (ExtremeWare 7.0.0b61_ipv6_1.2b19). The information in this release note is not covered in the *ExtremeWare Software User Guide* or the *ExtremeWare IPv6 1.2 User Guide*.

ExtremeWare IPv6 1.2b19 is the only supported version of ExtremeWare IPv6 software.

You can install ExtremeWare IPv6 on certain “i” series switches for software forwarding, or on a BlackDiamond 6808 or BlackDiamond 6804 with an MPLS module for module-based forwarding. This note describes all upgrade procedures.

Requirements

ExtremeWare IPv6 requires a full layer 3 license.

For software forwarding, ExtremeWare IPv6 1.2b19 requires BootROM 7.8.

For module-based forwarding, ExtremeWare IPv6 1.2b19 requires a BlackDiamond 6808 or BlackDiamond 6804, an MSM64i with BootROM 7.8 and ExtremeWare 7.0.0b61_ipv6_1.2b19.xtr (or later), and an MPLS module with BootROM 1.18 and ExtremeWare 7.0.0b61_ipv6_1.2b09.ipv6 (or later).

Get the Images

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

Installation Procedures

To install ExtremeWare IPv6 1.2, perform the following steps, in the following order:

- 1 Upgrade the switch BootROM.
- 2 Upgrade to ExtremeWare 6.2.2b56 if you are *not* using ExtremeWare IPv6 1.2.b11 (or later)
- 3 Install ExtremeWare IPv6 1.2 on the switch.

To enable module-based forwarding, perform the following additional steps:

- 4 Change the module type.
- 5 Upgrade the IPv6 module BootROM.
- 6 Install ExtremeWare IPv6 1.2 on the IPv6 module.



You must repeat steps 4 - 6 for each module.

Upgrade the Switch BootROM

To upgrade the switch BootROM:

- 1 Download BootROM 7.8 using the `download bootrom` command.
- 2 Reboot the switch using the `reboot` command.

Upgrade the Switch Software

If you are not using ExtremeWare IPv6 1.2b11 (or later), you must upgrade to ExtremeWare 6.2.2b56 before installing ExtremeWare IPv6 1.2.

Upgrade to ExtremeWare 6.1.9

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

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



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

ERROR: File too large

- 2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved going from the previous version of ExtremeWare to ExtremeWare 6.1.9.
- 3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.
- 4 Check the log for configuration errors. Manually enter configurations that did not load.
- 5 Save the configuration.



If you have configured Random Early Drop Probability in the ExtremeWare 6.1.8 or earlier configuration, re-configure the Random Early Drop Probability to the desired value using the `config red drop-probability` command and save the configuration to the desired location prior to upgrading to ExtremeWare 6.2.2.

Upgrade to ExtremeWare 6.2.2b56

If you are running ExtremeWare 6.1.9 to ExtremeWare 6.2.2b43 or ExtremeWare IPv6 1.2b10 (or earlier), upgrade to ExtremeWare 6.2.2b56:

- 1 TFTP download ExtremeWare 6.2.2b56 to the primary image space using the `download image primary` command.
- 2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.
- 3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.
- 4 TFTP download the saved configuration, and answer `y` at the prompt to reboot the switch.
- 5 Check the log for configuration errors. Manually enter configurations that did not load.
- 6 Save the configuration.

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



NOTE

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

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

Install ExtremeWare IPv6 on the switch

If you are running ExtremeWare 6.2.2b56 or ExtremeWare IPv6 1.2b11 (or later), install ExtremeWare IPv6 1.2:

- 1 Download ExtremeWare 7.0.0b61_ipv6_1.2b**.xtr into the primary image space using the `download image primary` command.
- 2 Configure the switch to use the primary image using the `use image primary` command.
- 3 Unconfigure the switch using the `unconfig switch all` command (if you did not save your configuration in the preceding procedures, do so before you unconfigure the switch).
- 4 Answer `yes` at the prompt to reboot the switch.
- 5 Restore IP connectivity to your TFTP server.
- 6 Download the saved configuration from the TFTP server using the `download config` command.



NOTE

Not all IPv4 features are supported in this release. The unsupported features are listed on page 5.

- 7 Reboot the switch using the `reboot` command.

Change the Module Type

To change the module type to IPv6:

- 1 Change the module type using the `config slot <slot number> set network-processor ipv6` command.
- 2 Reboot the IPv6 module using the `reboot slot` command.

Upgrade the IPv6 Module BootROM

To upgrade the IPv6 module BootROM:

- 1 Download BootROM 1.18 using the `download bootrom [<ipaddress> | <hostname>] <filename> slot <slot>` command.
- 2 Reboot the IPv6 module using the `reboot slot` command.

Install ExtremeWare IPv6 on the MPLS Module

To upgrade the IPv6 software to IPv6:

- 1 Download ExtremeWare 7.0.0b61_ipv6_1.2b**.ipv6 using the `download image [<ipaddress> | <hostname>] <filename> {primary | secondary} slot <slot>` command.
- 2 Reboot the IPv6 module using the `reboot slot` command.

Switch Support

ExtremeWare IPv6 1.2b19 supports only the following switches:

- BlackDiamond 6808
- BlackDiamond 6804
- Alpine 3804
- Alpine 3808
- Summit “i” series

The MPLS module is only available on the BlackDiamond family.

Module Support

ExtremeWare IPv6 1.2b19 supports only the following modules:

- MSM64i
- SMMi
- G8Xi
- G8Ti
- F48Ti
- FM-32Ti
- GM-4Xi
- GM-4Si
- GM-4Ti

- MPLS (with module-based IPv6 forwarding)

Limitations

Following are the tested limitations of ExtremeWare IPv6 1.2:

- 500 VLANs per switch
- 1,000 routes per switch
- 100 IPv6 in IPv4 tunnel interfaces per switch
- 2,000 IPv4/IPv6 hosts per switch
- 10 routers per network for OSPFv3

Unsupported Features

ExtremeWare IPv6 1.2 does not support the following IPv4 features:

- IPX RIP*
- IPX SAP*
- IS-IS*
- DVMRP*
- ESRP*
- EMISTP
- EAPS*
- BGP*
- VRRP*
- NAT*
- SLB*
- Flow redirection
- Vista
- Jumbo frames
- DHCP Server
- Path MTU discovery
- Mirroring*
- IPv4 Traps
- IPv4 MIBs
- RMON/RMON II
- NMS ACLs
- EPICenter support
- ISM support
- NetFlow*

- TACACS+
- DLCS
- Network Login*
- MAC security
- ACLs
- 4,000 VLANs
- PIM DM
- Ingress rate shaping
- QoS
- DiffServ
- MPLS
- ATM
- PoS
- ARM

The “*” indicates features that cannot be enabled from the CLI. Even though you can enable a feature, the features in this list are *not* supported.

New Features

Following are the new ExtremeWare IPv6 1.2 features:

- IPv6 Forwarding via MPLS Module—ExtremeWare IPv6 1.2 supports IPv6 forwarding on the BlackDiamond 6808 or BlackDiamond 6804 via the MPLS module. IPv6 packets in configured and automated (6to4) tunnels are also forwarded by the MPLS module.
- IPv6 MIB Support—ExtremeWare IPv6 1.2 supports the IPv6 General MIB (RFC 2465) and the ICMPv6 MIB (RFC 2466).
- OSPFv3—ExtremeWare IPv6 1.2 supports basic OSPFv3 with the following limitations:
 - No equal cost multipath
 - No ABR, NSSA BR functions
 - No Opaque LSA / traffic engineering functions
 - No MPLS related functions
 - No route filtering

Known Issues

Following are the known issues with ExtremeWare IPv6 1.2b19:

- 1 Output from the traceroute command shows the incoming interface for the switch rather than the outgoing interface.
- 2 Static routes are not removed from the FDB when next hops become unreachable. You must manually update static routes when their next hops are unreachable.

- 3 When using 6to4 automated tunneling with multiple 6to4 addresses on a single 6to4 tunnel interface, ensure that the 6to4 addresses all embed the same IPv4 address.
- 4 When an IPv4 switch receives both 6to4 tunnel traffic and configured IPv6 in IPv4 tunnel traffic from another IPv4 switch, the receiving switch cannot determine the correct tunnel interface. Both traffic flows have the same IPv4 source and destination addresses and protocol type. The switch uses the configured tunnel interface by default. Thus, to ensure that 6to4 tunnel traffic is forwarded, enable IPv6 forwarding on the configured tunnel interfaces.
- 5 Dynamic changes to the OSPFv3 configuration are blocked by the CLI. To work around this limitation, disable OSPFv3 before modifying its configuration. After making changes, enable OSPFv3 for the changes to take effect.
- 6 When an IPv4 static route or default route is created (manually or dynamically), an incomplete IPARP entry is created (PD2-117558117).
- 7 Configuring the IPARP timeout causes existing IPARP entries to be marked as incomplete (PD2-117558120).

Resolved Issues

Following are the issues resolved with ExtremeWare IPv6 1.2b19. You can ignore numbers in parenthesis.

- 1 ICMP Echo Replies are now consistently sent out the correct interface (PD2-120949401).
- 2 You can now have up to 500 VLANs in RIP (PD2-120361798).
- 3 A tConsole exception is no longer received when showing the OSPFv3 LSDB when the LSDB is updated (PD2-111403119).
- 4 The switch no longer hangs when the show memory command is issued from a telnet session (PD2-120361786).
- 5 RIP routes exported into OSPF as AS External Type 5 or 7 no longer flap every 30 seconds (PD2-122249601).

Following are the issues resolved with ExtremeWare IPv6 1.2b17.

- 1 FDB memory test no longer fails during reboot on a BlackDiamond chassis (PD2-102432013).
- 2 The correct metric is now sent in OSPFv3 intra-area-prefix LSA (PD2-103451318).
- 3 The CLI session no longer locks up after disable/enable of OSPFv3 (PD2-106305919).
- 4 The IPv6 routing table is now updated after an interface goes down (PD2-106556301).
- 5 IPv4 Multicast with PIM-SM now forwards data through (*,*,RP) entry (PD2-110389652).
- 6 When an IPv4 route is removed from the routing table, traffic is no longer forwarded (PD2-110421685).
- 7 An OSPFv3 Designated Router log error is no longer received after modifying the routerid (PD2-102785101).
- 8 The maximum upload configuration file size is now correct (PD2-110775579).
- 9 Adding a port after a default or other static route is configured no longer generates a get rtfree() message (PD2-117205501).
- 10 PIM SM and multicast traffic no longer generates abnormal messages on the console followed by an tIRDP task suspension (PD2-117247007).

- 11** Routes exported into OSPFv3 now appear on Juniper and Hitachi products (PD2-116202241).
- 12** The OSPFv3 neighbor is no longer stuck in exstart state (PD2-116202247).
- 13** When upgrading to IPv6 from ExtremeWare 6.2.2b58, the syslog no longer contains messages from rtinit() indicating that the source address length was not set in a data structure (PD2-109103413).
- 14** When you delete the IPv4 default route, you no longer get console panic and a “no such buffer allocated” message (PD2-117205531).
- 15** Performing the OSPFv3 DR election after modifying the router ID no longer generates an internal error.
- 16** The LSA is now received at a DRO after adding or removing a prefix on another DRO and this image is acting as the DR (OSPFv3).
- 17** RIP now correctly exports OSPFv2 external type 1/2 RTEs after enabling or disabling OSPFv2.
- 18** The tag value is now displayed in the OSPFv3 show LSDB output.

Following are the issues resolved with ExtremeWare IPv6 1.2b12:

- 1** Route redistribution into OSPFv3 is now supported.
- 2** Modifying the OSPFv3 priority now produces the desired results (such as promotion from DROTHER to BDR).
- 3** OSPFv3 now correctly calculates SPF after an ospf-intra route is removed.
- 4** The show iproute command now displays the correct counts.
- 5** The show iproute command no longer displays neighbor information.
- 6** The maximum uploaded configuration file size with RIPng and OSPFv3 is increased.
- 7** 250 VLANs configured on a port no longer cause a crash when the link is restarted.
- 8** Typing “q” while displaying routes now has the desired effect.

Following are the issues resolved with ExtremeWare IPv6 1.2b9:

- 1** OSPFv3 is now supported.

Following are the issues resolved with ExtremeWare IPv6 1.2b5:

- 1** When downloading a configuration, all ports are no longer put into the default VLAN.
- 2** OSPFv2 is now supported.
- 3** RIPng is now supported over a configured tunnel on a BlackDiamond containing an MPLS module.

Following are the issues resolved with ExtremeWare IPv6 1.2b4:

- 1** ExtremeWare IPv6 1.2 now supports multicast forwarding and routing.
- 2** After downloading a configuration you are no longer required to reboot the switch for the configuration to take effect.

Following are the issues resolved with ExtremeWare IPv6 1.2b3:

- 1** IPv4 echo requests larger than one packet no longer result in an incorrect IP header checksum on the first echo reply sent back to the source.
- 2** The Summit48si is now supported.
- 3** SNMP is now supported.

Following are the issues resolved with ExtremeWare IPv6 1.2b2:

- 1** Fixed an IPv4 UDP broadcast forwarding problem that prevented DHCP from working in some networks.