



Release Notes for Ethernet Routing Switch 3600 Series

Release 6.4
9036471-00 Rev AC
May 2020

© 2017-2020, Extreme Networks, Inc.
All Rights Reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document	4
Purpose.....	4
Conventions.....	4
Text Conventions.....	4
Documentation and Training.....	6
Getting Help.....	6
Providing Feedback.....	7
Chapter 2: New in this Release	9
Chapter 3: Overview of Features by Release	11
Chapter 4: Important notices	18
File Names.....	18
Upgrading the Diag image using CLI.....	18
Updating the Diag image from the Boot menu.....	19
Supported software and hardware capabilities.....	20
Supported standards RFCs and MIBs.....	21
Standards.....	21
RFCs and MIBs.....	22
Software upgrade considerations.....	25
Tested Browsers.....	25
Chapter 5: Resolved issues	26
Chapter 6: Known issues and limitations	28

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document describes new features, hardware, and known issues and limitations for the Extreme Networks Ethernet Routing Switch 3600 in this software release.

The information in this document supersedes applicable information in other documents in the suite.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons







Icon	Alerts you to...
 Important:	A situation that can cause serious inconvenience.
 Note:	Important features or instructions.
 Tip:	Helpful tips and notices for using the product.
 Danger:	Situations that will result in severe bodily injury; up to and including death.
 Warning:	Risk of severe personal injury or critical loss of data.
 Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	<p>Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command.</p> <p>If the command syntax is <code>cfm maintenance-domain maintenance-level <0-7></code> , you can enter <code>cfm maintenance-domain maintenance-level 4</code>.</p>
Bold text	<p>Bold text indicates the GUI object name you must act upon.</p> <p>Examples:</p> <ul style="list-style-type: none"> • Click OK. • On the Tools menu, choose Options.
Braces ({ })	<p>Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command.</p> <p>For example, if the command syntax is <code>ip address {A.B.C.D}</code>, you must enter the IP address in dotted, decimal notation.</p>
Brackets ([])	<p>Brackets ([]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command.</p> <p>For example, if the command syntax is <code>show clock [detail]</code>, you can enter either <code>show clock</code> or <code>show clock detail</code>.</p>
Ellipses (...)	<p>An ellipsis (...) indicates that you repeat the last element of the command as needed.</p> <p>For example, if the command syntax is <code>ethernet/2/1 [<parameter> <value>]...</code>, you enter <code>ethernet/2/1</code> and as many parameter-value pairs as you need.</p>
<i>Italic Text</i>	<p>Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.</p>
Plain Courier Text	<p>Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages.</p>

Table continues...

Convention	Description
	<p>Examples:</p> <ul style="list-style-type: none"> • show ip route • Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]
Separator (>)	<p>A greater than sign (>) shows separation in menu paths.</p> <p>For example, in the Navigation tree, expand the Configuration > Edit folders.</p>
Vertical Line ()	<p>A vertical line () separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command.</p> <p>For example, if the command syntax is <code>access-policy by-mac action { allow deny }</code>, you enter either <code>access-policy by-mac action allow</code> or <code>access-policy by-mac action deny</code>, but not both.</p>

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware/software compatibility matrices](#) for Campus and Edge products

[Supported transceivers and cables](#) for Data Center products

[Other resources](#), like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

[Extreme Portal](#)

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

*** Note:**

You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.

About this Document

- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this Release

The following sections detail what is new in this release.

Pluggable Transceivers

This release introduces support for the following transceiver modules and direct-attach cables.

SFP+ direct-attach cables:

- SFP+ passive copper cable (PN: 10304), 1 meter
- SFP+ passive copper cable (PN: 10306), 5 meters

Transceiver modules:

- 10/100/1000BASE-T Copper SFP and Industrial Grade SFP Modules (PN: 10070H)
- 1 Gb SX and Industrial Grade SX SFP Modules (PN: 10051H)
- 1000BASE-BX Bidirectional 10 km SFP Modules (PN: 10056H and 10057H)
- 1 Gb LX and Industrial Grade LX SFP Modules (PN: 10052H)
- ZX SFP Module (PN: 10053H)
- LRM SFP+ Module (PN: 10303)
- SR SFP+ Module (PN: 10301)
- LR SFP+ Module (PN: 10302)
- ER SFP+ Module (PN: 10309)

The following table indicates where to find more information about optical transceivers and components.

Extreme Networks optical transceivers and components	Extreme Networks Pluggable Transceivers Installation Guide
Compatibility for Extreme Networks SFP, SFP+, SFP28, QSFP+, and QSFP28 transceiver modules with the VSP Series switches	Extreme Hardware/Software Compatibility and Recommendation Matrices

Zero Touch Provisioning Plus (ZTP+)

Note:

Note: ZTP+ is compatible with XMC version 8.4.0 or later.

Using ZTP+, switches communicate with the Extreme Management Center (XMC) as soon as they are connected to the network, allowing them to obtain firmware and configuration updates automatically. This auto-provisioning process significantly minimizes the amount of time required to configure a new switch and deploy it on the network.

For more information on ZTP+, see *Zero Touch Provisioning Plus (ZTP+)* in [Configuring Systems on Ethernet Routing Switch 3600 Series](#).

ZTP+ Considerations Before Software Upgrade

When you upgrade the software to the current release, ZTP+ is enabled by default, causing the auto-provisioning process to start as soon as the switch connects to an XMC server on the network. This can however result in unintentional provisioning, especially if a switch with existing configuration is upgraded. For information on how to prevent this before an upgrade, see [Software upgrade considerations](#) on page 25.

New Default IP Configuration

The default IP configuration mode is now BootP or DHCP or Default IP instead of BootP or Default IP. This change has been introduced to support ZTP+. This does not impact existing configurations during the upgrade process. The default mode will only take effect if the switch is returned to factory default settings.

For information on BootP or DHCP or Default IP, and other IP configuration modes, see *BootP automatic IP configuration and MAC address* in [Configuring Systems on Ethernet Routing Switch 3600 Series](#).

Software Image file Updates

The COM Plug in for the Enterprise Device Manager (EDM) is no longer generated. For more information on the software files for this release, see [File Names](#) on page 18.

Chapter 3: Overview of Features by Release

This section provides an overview of the ERS 3600 Series software features and the releases they were first introduced in.

This following table lists software features in [Using CLI and EDM on Ethernet Routing Switch 3600 Series](#).

Feature	Release Introduced
CLI pipe filter	6.0.x
ASCII Config File	6.0.x
HTTP web-based management	6.0.x
Show Running Config (verbose, non-verbose, module) enhancement	6.0.x
WEB HTTP download of ASCII — downloading of ASCII configuration files through HTTP	6.0.x

This following table lists software features in [Quick Start Configuration for Ethernet Routing Switch ERS 3600 Series](#).

Feature	Release Introduced
Username and password	6.0.x
SNTP & SNTP timezone enhancement	6.0.x
Static Routing with default route	6.0.x

This following table lists software features in [Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 3600 Series](#).

Feature	Release introduced
256 port-based VLANs with IVL	6.0.x
802.3ad- Link Aggregation Control Protocol (LACP)	6.0.x
802.1Q tagging	6.0.x
802.1w – rapid spanning tree	6.0.x
Autotopology	6.0.x
BPDU Filtering	6.0.x
Default settings for Spanning Tree mode	6.1
Distributed LAG (802.3ad LACP), up to 6 trunks with 4 links per trunk	6.0.x

Table continues...

Overview of Features by Release

Feature	Release introduced
Distributed MLT (DMLT), up to 6 trunks with 4 links per trunk	6.0.x
IPv6 VLANs (protocol based)	6.0.x
LAG (802.3ad LACP), up to 6 trunks with 4 links per trunk	6.0.x
MAC flush	6.0.x
MLT enable/disable whole trunk	6.0.x
MLT/DMLT/LAG dynamic add/delete	6.0.x
Multi-Link Trunking (MLT) with up to 6 trunks and 4 links per trunk	6.0.x
Show MAC Address enhancement	6.0.x
Single 802.1d Spanning Tree Protocol (STP) on all ports	6.0.x
SLPP Guard	6.0.x
Spanning Tree 802.1d compliance mode	6.0.x
Spanning Tree port mode	6.0.x
Static LACP key to trunk ID binding	6.0.x
Static STP Multicast Destination Configuration	6.0.x
VLACP	6.0.x
VLAN Tagging Enhancement	6.0.x
Voice VLAN Integration	6.0.x

This following table lists software features in [Configuring System Monitoring on Ethernet Routing Switch 3600 Series](#).

Feature	Release introduced
Auto Detection And Configuration (ADAC) with 802.1AB interaction	6.0.x
CPU & Memory Utilization	6.0.x
Cumulative system uptime	6.0.x
Dual Syslog servers	6.0.x
Identify Units (Blink LEDs)	6.0.x
Port mirroring (1-1, manytoOne)	6.0.x
Remote Logging - ability to log on remote servers	6.0.x
RMON (RFC1757): per port Statistics, History, Alarm and Events	6.0.x
Secure SLA Monitor agentserver communication	6.0.x
Service Level Agreement (SLA) Monitor	6.0.x
Show environmental	6.0.x
SLAMon	6.0.x
SLAMon phase 2 (including EDM)	6.0.x
SNMP MIB web page in EDM	6.0.x
SNMP Trap list web page in EDM	6.0.x

Table continues...

Feature	Release introduced
Software Exception Log	6.0.x
Stack Health Check	6.0.x
Syslog	6.0.x
Syslog enhancements	6.0.x
Unit Stack Uptime	6.0.x

This following table lists software features in [Configuring IP Routing and Multicast on Ethernet Routing Switch 3600 Series](#).

Feature	Release Introduced
DHCP Client	6.0.x
DHCP Option 82	6.0.x
DHCP Relay	6.0.x
DHCP Server	6.0.x
IGMP Selective Channel Block	6.1
IGMPv1/v2 snooping/proxy	6.0.x
IGMPv3 Snooping/proxy	6.0.x
IP Blocking	6.0.x
IP Local Static Routes	6.0.x
IP Non-Local Static Routes	6.0.x
L3 - RIPv1v2	6.0.x
MLD Proxy (MLDv1/MLDv2)	6.0.x
MLD snooping (MLDv1/ MLDv2)	6.0.x
Proxy ARP	6.0.x
RIP Policies	6.0.x
Static Routing with default route	6.0.x
UDP Forwarding	6.0.x

This following table lists software features in [Configuring Quality of Service on Ethernet Routing Switch 3600 Series](#).

Feature	Release Introduced
Advanced QoS	6.0.x
Automatic QoS	6.0.x
COS/DSCP — mapping the DSCP value	6.0.x
Traffic Profile	6.0.x
User Based Policies	6.2

This following table lists software features in [Configuring Security on Ethernet Routing Switch 3600 Series](#).

Overview of Features by Release

Feature	Release Introduced
802.1X EAP Accounting	6.0.x
802.1X EAP (MHSA, MHMV, Guest VLAN, Fail Open VLAN, Non-EAP, and RADIUS MAC)	6.0.x
802.1X EAP Separate enable/disable	6.0.x
802.1X Enhancement: Dynamic VLAN assignment for NEAP	6.0.x
802.1X Enhancement: Unicast request, Non-EAP IP Phone support	6.0.x
802.1X NEAP Accounting	6.0.x
802.1X NEAP and Guest VLAN on same port	6.0.x
802.1X NEAP Fail Open VLAN	6.0.x
802.1X NEAP Phone Support	6.0.x
802.1X NEAP re-authentication timer	6.0.x
802.1X NEAP with VLAN names	6.0.x
802.1X RFC2866/2869 RADIUS interim accounting updates	6.0.x
802.1X RFC3576 RADIUS auth extensions - CoA and DM	6.0.x
ARP Inspection	6.0.x
Configurable SNMP trap port (only SNMP v1 & v2)	6.0.x
DA Filtering	6.0.x
Default all EAP settings	6.0.x
DHCPv6 filtering	6.0.x
DHCP Snooping	6.0.x
Duplicate Address Detection (DAD) snooping and filtering	6.0.x
Dynamic "IPv6 Neighbor solicitation/ advertisement" inspection	6.0.x
EAP enhancements	6.1
EAPoL Fail Open VLAN (FOV) on a port	6.3
Enabling EAP and IP Source Guard simultaneously on a port	6.2
Extended IP Manager (IPv4 & IPv6)	6.0.x
HTTP port change	6.0.x
HTTPS/SSL secure web management	6.0.x
IPv6 Source Guard	6.0.x
IPv6 Enhancements - IPv6 Host Enhancement and IPv6 Loopback	6.0.x
IPV6 First Hop Security	6.0.x
Local password protection	6.0.x
MAC address based security with autolearn (BaySecure)	6.0.x
MIB enhancements — Entity MIB, Dot1Q MIB, P-Bridge	6.2
Multiple Host with Multiple VLANs (MHMV)	6.0.x

Table continues...

Feature	Release Introduced
Multiple Host with Single Authentication (MHSA) — No limit	6.0.x
NEAP Not Member of VLAN	6.0.x
NEAP password format	6.2
Neighbor Unreachability Detection (NUD) filtering	6.0.x
Password security	6.0.x
RADIUS-based security	6.0.x
RADIUS EAP / NEAP to different servers	6.0.x
RADIUS password fallback	6.0.x
RADIUS Server reachability	6.0.x
RADIUS use-management-ip	6.0.x
RFC 4675 — RADIUS Attributes: Egress-VLANID and Egress-VLANNAME	6.2
Router Advertisements (RA) filtering	6.0.x
Secure FTP (SFTP) – full support	6.0.x
SNMP-based network management	6.0.x
SNMP trap enhancements	6.0.x
SNMPv3 security	6.0.x
SSH enhancement to support RSA	6.0.x
SSHv2	6.0.x
Stack Monitor and Statistics	6.0.x
Sticky MAC	6.0.x
Storm Control	6.0.x
TACACS+	6.0.x
Unified Authentication	6.0.x
Viewing EAPOL Unauthenticated clients in EDM	6.2

This following table lists software features in [Configuring Fabric Attach on Ethernet Routing Switch 3600 Series](#).

Feature	Release Introduced
Edge Automation Enhancements	6.2
Fabric Attach	6.0.x
Fabric Attach Proxy	6.0.x
Fabric Attach Bindings Increase	6.2
Fabric Attach enhancements — Dynamic Trusted QoS interface updates, Tagging mode on FA Client port, Viewing authentication status related to FA and I-SID/VLAN Assignment TLV in CLI output for show fa elements command, FA statistics, Dual Key Authentication	6.1

Table continues...

Overview of Features by Release

Feature	Release Introduced
Fabric Attach enhancements — Management VLAN Advertisement Blocking and Automatic Management VLAN Assignment	6.2
Fabric Attach enhancements — Fabric Attach Client Trust and Fabric-Attach- Client-Trust-Binding	6.3

This following table lists software features in [Configuring Systems on Ethernet Routing Switch 3600 Series](#).

Feature	Release Introduced
802.1AB (LLDP) Standards Based Auto Topology	6.0.x
802.1AB and ADAC interoperability	6.0.x
802.1AB Customization features	6.0.x
802.1AB Integration features	6.0.x
802.1AB Location TL	6.0.x
802.1AB MED	6.0.x
Agent Auto Unit Replacement (AAUR)	6.0.x
Asset ID configuration	6.0.x
Autosave configuration	6.0.x
Auto Unit Replacement (AUR) per trunk	6.0.x
Autotopology	6.0.x
Autosensing and autonegotiation	6.0.x
Backup configuration	6.0.x
BootP or Default IP	6.0.x
BootP/TFTP for downloading software and config file	6.0.x
Configuring with IP Office Scrip	6.0.x
Custom Autonegotiation Advertisements (CANA)	6.0.x
Diagnostics Auto Unit Replacement (DAUR)	6.0.x
DNS – Domain Name Service capabilities	6.0.x
Download PoE firmware from SFTP	6.0.x
Extreme Networks Energy Saver	6.0.x
Factory-default command	6.0.x
No Banner & CTRL-Y Skip	6.0.x
Ping enhancement	6.0.x
Policy-enabled networking	6.0.x
Port mirroring	6.0.x
Power over Ethernet enhancements	6.1
PoE Module Firmware Version for a Stack Unit	6.3

Table continues...

Feature	Release Introduced
Rate Limiting	6.0.x
Show Flash History	6.0.x
Show UTC Timestamp	6.0.x
Shutdown, reload enhancement	6.0.x
SNTP and SNTP timezone enhancement	6.0.x
Stack Forced Mode	6.0.x
Stack IP Address	6.0.x
Telnet	6.0.x
Time Domain Reflectometer	6.1
Video Surveillance Script	6.0.x
Zero Touch Provisioning Plus (ZTP+)	6.4

Chapter 4: Important notices

This section provides important software and hardware related notices.

File Names

The following table describes the software files for ERS 3600 Series Software Release 6.4.

Module or file type	Description	File name	File size (bytes)
SSH runtime image	Software image for ERS 3600 Series	3600_640065s.img	16,400,828
Diagnostic software	Diagnostic software for ERS 3600 Series	3600_6100_diags.bin	7,096,948
MIB definition files	Management Information Base (MIB) definition files	Ethernet_Routing_Switch_36xx_MIBs_6.4.0.zip	1,660,031
EDM Help file zip	A downloadable zip file containing Help information for Enterprise Device Manager (EDM)	ers3600v630_HELP_EDM.zip	1,678,595

Upgrading the Diag image using CLI

Perform the following procedure to upgrade the Diag image using CLI.

Procedure

1. Connect a default switch to a TFTP server.
2. Set a valid IP address and subnet mask.
3. Configure the TFTP server address using the following command from Privileged EXEC mode:

```
tftp-server <A.B.C.D>
```
4. Verify the connection to the TFTP Server.

- At the command prompt, enter the `download` command with the following parameters.

```
download diag <WORD>
```

The Diag image is downloaded and then the switch is rebooted. To avoid rebooting the switch after the download, add the option `<no-reset>` to the `download` command.

Variable definitions

The following table describes the parameters for the `download` command.

Variable	Value
<A.B.C.D>	Enter the IP address of the TFTP server in the format XXX.XXX.XXX.XXX
<WORD>	The filename of the diagnostic image

Updating the Diag image from the Boot menu

Procedure

- Connect a default switch to a TFTP server.
- Reboot the switch (either a soft or hard reset).
- During the boot process, press `CTRL+C` until the following menu is displayed:

```
DIAGNOSTIC BREAK MENU

  1 - Launch Primary Agent-1
  2 - Download Agent/Diag
  3 - Reinitialize Agent Configuration Files
  4 - Display Error Log
  5 - Display System Information
  6 - Continue Boot Sequence
  7 - Reset
  8 - Toggle Do-POST Selection [ENABLED]
  9 - Run POST tests
```

- Press ``2'`.
- Choose option: 3 - Diagnostics.
- Choose option: 1 - Download via TFTP.
- Enter the filename, along with its extension; for example `_diag.bin`.
- Enter the TFTP server IP address.

9. Enter the switch IP address.
10. Enter the subnet mask.
11. Enter the port in which the cable is connected.

The download of the DIAG image begins.

Supported software and hardware capabilities

The following table summarizes the known capabilities for the ERS 3600 Series software.

Table 3: Supported capabilities for the ERS 3600 Series

Feature	Maximum number supported
QoS egress queues	4
QoS filters per precedence	256
QoS precedence	8
Total QoS filters	(4 x 256) = 1024
MAC addresses	16384
Layer 2	
VLANs	256
IGMP SCB filters	240
Multiple Spanning Tree Instances (MSTI) in MSTP mode	8
Multicast entries (IPv4 and IPv6)	248
IGMP Snoop VLANs	256
LLDP Neighbors (3626/3650)	416/800
LLDP Neighbors per port	16
MultiLink Trunking (MLT), Link Aggregation (LAG) groups	6
Links for each MLT or LAG	4
Layer 3	
ARP entries (local, static & dynamic)	512 (of which 32 are reserved for local ARPs)
Local ARP Entries (local IP interfaces)	32
Static ARP entries	256
Dynamic ARP entries	480
IPv4 route entries (local, static & dynamic)	32 local + 32 static + 256 dynamic
Static routes and Non-local Static routes	32
Local routes	32

Table continues...

Feature	Maximum number supported
Management routes	4
RIP routes	256
RIP Interfaces	16
UDP Forwarding entries	128
DHCP relay entries	256
DHCP relay forward paths	256
DHCP Server Pools	16 (one per VLAN)
DHCP Server clients per pool	256
DHCP Server clients per switch/stack	2000
IPv6 Interfaces	64
IPv6 Static Routes	128
Miscellaneous	
802.1X EAP scaling (clients for each port)	32
Jumbo frame support	9 K bytes
IGMP multicast groups	248
802.1X (EAP and NEAP) clients per stack	768
RMON alarms	400
RMON events	400
RMON Ethernet statistics	128 per unit
RMON Ethernet history	196 per unit
Fabric Attach operational mode	Proxy
Fabric Attach clients –proxy requests (proxy VLANs)	256

Supported standards RFCs and MIBs

Standards

The standards in the following list are supported on the switch:

- IEEE 802.1AB (Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discover (LLDP-MED))
- IEEE 802.1Q (VLANs)
- IEEE 802.1p (Priority Queues)
- IEEE 802.1D (Spanning Tree)

- IEEE 802.1w (Rapid Spanning Tree)
- IEEE 802.1s (Multiple Spanning Tree Groups)
- IEEE 802.1X (Extensible Authentication Protocol (EAP))
- IEEE 802.3 (10BASE-T/100BASE-TX)
- IEEE 802.3u (100BASE-T (ANSI) Auto-Negotiation)
- IEEE 802.3x (Pause Frames / Flow Control)
- IEEE 802.3z (1000BASE-X)
- IEEE 802.3ab (1000BASE-T)
- IEEE 802.3ad (Link Aggregation Control Protocol (LACP))
- IEEE 802.3af (PoE) – 15.4W max
- IEEE 802.3aq (10GBASE-LRM 10 Gbit/s Ethernet over fiber)
- IEEE 802.3at (Power over Ethernet plus— PoE+ (32W))
- IEEE 802.3az Energy Efficient Ethernet (EEE)

RFCs and MIBs

For more information about networking concepts, protocols, and topologies, consult the following RFCs and MIBs:

- RFC 783 Trivial File Transfer Protocol (TFTP)
- RFC 791/ 950 Internet Protocol (IP)
- RFC 792 Internet Control Message Protocol (ICMP)
- RFC 826 Address Resolution Protocol (ARP)
- RFC 854 Telnet Server and Client
- RFC 951/ 1542 (BOOTP)
- RFC 1058 RIPv1
- RFC 1112 Internet Group Management Protocol v1 (IGMPv1)
- RFC 1213 MIB-II
- RFC 1215 SNMP Traps Definition
- RFC 1271 / 1757 / 2819 RMON
- RFC 1361 / 1769 Simple Network Time Protocol (SNTP)
- RFC 1493 (Bridge MIB)
- RFC 1573 / 2863 Interface MIB
- RFC 1643 / 2665 Ethernet MIB

- RFC 1905 / 3416 SNMP
- RFC 1906 / 3417 SNMP Transport Mappings
- RFC 1907 / 3418 SNMP MIB
- RFC 1945 HTTP v1.0
- RFC 1981 Path MTU Discovery for IPv6
- RFC 2011 SNMP v2 MIB for IP
- RFC 2012 SNMP v2 MIB for TCP
- RFC 2013 SNMP v2 MIB for UDP
- RFC 2131 DHCP Client
- RFC 2132 DHCP Options 6, 43 & 60
- RFC 2138 RADIUS
- RFC 2236 Internet Group Management Protocol v2 (IGMPv2)
- RFC 2453 RIPv2
- RFC 2460 Internet Protocol v6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IPv6
- RFC 2462 Auto-configuration of link local addresses
- RFC 2464 IPv6 over Ethernet
- RFC 2474 Differentiated Services Support
- RFC 2570 / 3410 SNMPv3
- RFC 2571 / 3411 SNMP Frameworks
- RFC 2572 / 3412 SNMP Message Processing
- RFC 2573 / 3413 SNMPv3 Applications
- RFC 2574 / 3414 SNMPv3 USM
- RFC 2575 / 3415 SNMPv3 VACM
- RFC 2576 / 3584 Co-existence of SNMP v1/v2/v3
- RFC 2616 HTTP
- RFC 2660 HTTPS (Secure Web)
- RFC 2665 Ethernet MIB
- RFC 2674 Q-Bridge MIB
- RFC 2710 MLDv1 for IPv6
- RFC 2737 Entity MIBv2
- RFC 2819 RMON MIB

Important notices

- RFC 2863 Interfaces Group MIB
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions (interim updates)
- RFC 3046 (& 5010) DHCP option 82, Relay Agent Information Option
- RFC 3058 RADIUS Authentication
- RFC 3361 DHCP option 120 SIP Servers
- RFC 3376 Internet Group Management Protocol v3 (IGMPv3)
- RFC 3484 Default Address Selection for IPv6
- RFC 3596 DNS Extensions for IPv6
- RFC 3810 MLDv2 for IPv6
- RFC 3879 Deprecating Site Local Addresses
- RFC 4007 Scoped Address Architecture
- RFC 4022 MIB for TCP
- RFC 4113 MIB for UDP
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4252 SSH
- RFC 4291 IPv6 Addressing Architecture
- RFC 4293 MIB for IP
- RFC 4301 Security Architecture for the Internet Protocol
- RFC 4432 SSHv2 RSA
- RFC 4443 Internet Control Message Protocol (ICMPv6) Update to RFC 2463
- RFC 4541 IGMP and MLD Snooping Switches Considerations
- RFC 4675 RADIUS Attributes for VLAN and Priority Support
- RFC 4861 Neighbor Discovery for IPv6
- RFC 4862 IPv6 Stateless Address Autoconfig
- RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
- RFC 5176 RADIUS Change of Authorization
- RFC 5859 TFTP Server DHCP option

Software upgrade considerations

Zero Touch Provisioning Plus (ZTP+)

When you upgrade to Release 6.4, ZTP+ auto-provisioning is enabled on the switch by default, and automatically begins as soon as the switch connects to the XMC server on the network.

However, ZTP+ auto-provisioning must only be used on new switch deployments.

To prevent unintentional auto-provisioning of a switch that is upgraded to Release 6.4, ensure that the switch does not connect to the XMC server by resolving its *extremecontrol* address using DNS.

Tested Browsers

EDM has been tested with the following web browsers:

Browser	Version
Microsoft Internet Explorer, Windows 10	11.973.17763.0
Mozilla Firefox, Windows 10	72.0.2
Google Chrome	79.0.3945.130
Microsoft Edge, Windows 10	44.17763.831.0
Opera, Windows 10	66.0.3515.44

Chapter 5: Resolved issues

The following table lists the issues resolved in the current software release.

Reference number	Description
ERS3600-613	Logs are seen on the FA server stating that the maximum number of bindings has been reached.
ERS3600-719	Add the IfName varbind to link and interface traps so that the XMC properly interprets the SNMP packet and displays the trap information correctly.
ERS3600-729	When authenticating two EAP clients simultaneously, one on the base unit (BU) and the other on a non-base unit (NBU), in the same RADIUS assigned FA binding, the NBU client gets authenticated but at first all RADIUS-assigned VLANs (RAV) are considered invalid.
ERS3600-736	Automation of EAP port mode configuration using the FA Zero Touch auto-trusted-mode-fa-client option does not work if the matching FA Client is discovered on an access port that has EAPoL enabled with the auto status. This causes all traffic arriving from the FA Client to not honor QoS markings and reset it to 0.
ERS3600-738	In an FA setup, if an ERS 3600 switch acting as the FA Proxy is deployed with Network Admission Control (NAC) to force authentication on clients, all ISID-VLAN assignments from the FA clients continue to remain in the pending state and do not move to the active state.
ERS3600-739	EDM: The FailOpenVlanUBP tab is duplicated. There is no operational or functional impact.
ERS3600-742	The switch drops MC packets if they arrive with an interval more than twice the IGMP sender expiration timer, that is, 2x106 seconds.
ERS3600-744	The system does not accept the pipe symbol () as one of the two required special characters when setting the password for telnet access.
ERS3600-747	The switch displays the VSP 8404C as <code>unknownDataType</code> in the EDM Topology Table.
ERS3600-749	The switch incorrectly displays the MTU size for jumbo frames as 1514 instead of 9216.
ERS3600-753	The XMC server loses inter-switch links in the topology.
ERS3600-755	The admin status of an FA-enabled MLT uplink port changes from disable to enable after the stack unit is rebooted.
ERS3600-758	Very rarely, after an upgrade you can no longer login using the RADIUS credentials.

Table continues...

Reference number	Description
ERS3600-762	For better password security, the system must not allow the creation of passwords longer than 15 characters. Valid passwords are between 10 and 15 characters in length.
ERS3600-763	Include support for the Extreme 10GBASE-LRM 1310nm (220m) LC GBIC with Part number: 10303, on the switch.
ERS3600-764	The switch continues to allow MAC addresses to be added to the port, even though the maximum limit is reached.
ERS3600-765	Disabling the ADAC feature deletes all configuration and restores the pre-ADAC port configuration saved in NVRAM on all ADAC-enabled ports (Telephony, Call Server, and uplink).
ERS3600-767	<p>Urgent/11 VxWorks Vulnerabilities Details</p> <ul style="list-style-type: none"> • Fixed CVEs: 12255, 12261, 12262, 12258 • Non-vulnerable CVEs: 12256, 12260, 12263, 12257, 12264, 12259, 12265 <p>For more information, see: Vulnerabilities in Wind River VxWorks (URGENT/11)</p>
ERS3600-768	The EDM interface of the switch not accessible, following a TDR test run using the EDM.
ERS3600-770	The switch applies configuration from an ASCII file only partially.
ERS3600-771	The VID and VLAN values do not appear in the output of the show running config command when the Fail Open VLAN is enabled with a specific VLAN on the interface.
ERS3600-772	SNMP users are not restored after swapping out the base unit of a two-unit stack.
ERS3600-773	ERS 5900: A client connecting to a port on the stack is able to ping other hosts within the same subnet but is unable to reach the default gateway and beyond.
ERS3600-774	After the switch receives an LLDP/FA PDU, if it receives another LLDP/FA PDU from the same device and this PDU has a change in the FA Element TLV state (specifically, the tagging mode), the switch deletes the FA element associated with that port and partially returns it to its default setting. For example, the VLAN returns to the configured PVID.
ERS3600-778	In the MHMV mode, a port is removed from the initial VLAN after client authentication. This only occurs when non-EAP clients are connected to ports that are not initially assigned to a VLAN. If however, the port is initially assigned to a VLAN, this VLAN is retained after client authentication.
ERS3600-794	The switch displays the following FA binding conflict alarm: <code>EAP: FA bind conflict between [vlan-id Z : i-sid A] and [vlan-id Z : i-sid B] on port x/y, if the switch is configured with RADIUS EAPoL or non-EAP re-authentication.</code>
ERS3600-795	The byte order is reversed on the DHCP relay agent IP address, when two agents are configured.

Chapter 6: Known issues and limitations

The following table lists and describes known issues and limitations. Where available and appropriate, workarounds are provided.



Reference number	Description
ERS3600-69	Inconsistency between CLI and EDM: In EDM it should exist a tab in the folder RUN script for RUN VS.
ERS3600-310	EAP: Auto-configured VLAN should be deleted when NEAP clients are disconnected  Note: Removing all authenticated clients on a dynamically autocreated VLAN by EAP, may cause that auto-created VLANs to not be deleted under some circumstances.
ERS3600-345	EDM offbox: After creating vlan from EDM offbox with assigned IP address, the vlan created in EDM offbox are displayed in ACG in incorrect order in module I3-protocols.
ERS3600-404	COM: Error "CommitFailed" when configuring DHCPv6 Guard ServerAccessListName and ReplyPrefixListName with invalid values in EDMOffBox.
ERS3600-426	EDM: Port status is not updated instantly when link state changes.
ERS3600-432	EDM: Refresh button in EDM does not function. Workaround: Use the F5 function key.
ERS3600-435	Disabled SFP Ports do not flash when disabled.
ERS3600-450	Cannot upload ASCII config when vlans dynamically created are present (FA, EAP). The VLANs created dynamically are not automatically re-created after a device reboot. When executing a ASCII config file (after a reboot) the CLI commands that are using these VLANs will fail. Manual re-creation of the missing VLANs is recommended before executing the ASCII script.
ERS3600-485	FA ZT EDM: Should not accept auto-port-mode-fa-client and auto-pvid-mode-fa-client enabled at the same time  Note: When both policies are configured, only the one that was configured first is applied.

Table continues...

Reference number	Description
ERS3600-486	<p>FA ZT EDM: Should not accept auto-port-mode-fa-client and auto-client-attach enabled at the same time.</p> <p>* Note:</p> <p>When both policies are configured, only the one that was configured first is applied.</p>
ERS3600-505	<p>FA transition from stack to standalone: FA ZT policy is not applied on AP after transition</p> <p>Workaround: In case that the FA ZT policy is not applied on a AP after transition from stack to standalone, do the following:</p> <ul style="list-style-type: none"> • Make sure there is only a single connection to the server. • Eliminate the other proxy connections (proxy to proxy is not supported). • Delete the binding data configured on the AP so that the only configuration being installed is the ZTC data.
ERS3600-519	<p>Autosave won't re-enable after reload is canceled without reboot when ASCII config not available.</p> <p>The autosave is not re-enabled when a reload is activated then canceled. A device reboot is required for the autosave activation.</p>
ERS3600-523	<p>EDM does not display any link info about stacking ports in stack mode in device physical view.</p> <p>In the stacking mode the number of available ports is 26/50 (the stacking ports are not counted); therefore, there are no instances of the SNMP objects for the stacking ports.</p>
ERS3600-630	<p>FA: VLAN pushed by AP authenticated by RADIUS is not removed from device after stack standalone transition and it is not seen as auto-created.</p> <p>To recover from this state, reboot the entire stack and the FA server to remove the VLANs.</p>
ERS3600-638	<p>FA: Port tagging is reverted from tagall to untagall on uplink port to an FA Server after BU failover.</p> <p>To recover from this state, disable FA on uplink ports, configure tagging back to untagall and then re-enable FA afterwards.</p> <p>Workaround: Enable tagging tagall on all trunk ports to FA server before FA Server is discovered initially.</p>
ERS3600-639	<p>FA: Port tagging is not reverted for uplink ports to an FA Server when disabling FA on the FA Proxy side.</p> <p>To recover from this state, reconfigure tagging.</p> <p>Workaround: Do not disable FA on the uplink trunk on the FA Proxy side.</p>
ERS3600-686	<p>There is an inter-connectivity problem and the link does not get established when you connect the ERS 3600 switch with another switch using a breakout cable (BOC).</p>

Table continues...

Known issues and limitations

Reference number	Description
	Workaround: Replace the cable with a single 10 Gbps link.
ERS3600-725	<p>Egress mode port mirroring (xtx mode) does not work on ports that have Wireless Access Points (WAP) connected to them. The transmitted traffic is not captured.</p> <p>Workaround: Use a network hub or capture the traffic from the WAP if possible.</p>
ERS3600-812	<p>After a cold reboot, the switch fans run with a lot of noise, although the low-power-budget PoE mode is enabled. This does not however have a functional impact on those fans.</p> <p>Workaround: If the problem occurs immediately after a cold reboot, reboot the switch again. This causes the switch to boot up with the fans running at the correct speed, thereby reducing the noise.</p>
ERS3600-816	<p>After a hard reset of the switch, the PoE power budget mode changes from low to high. This causes the fans to spin faster, generating a lot of noise. This does not however have a functional impact on the fans.</p> <p>Workaround: Manually change the PoE power budget mode back to low.</p>
ERS3600-838	<p>The NBU FA uplink in redundant LACP configuration stays disabled after a reboot or rejoin of the NBU to the stack.</p> <p>Workaround: Use MLT instead of LACP for FA uplinks.</p>