Release Notes for Ethernet Routing Switch 4900 and 5900 Series

Contents

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 and important information about the latest release. Release notes include a list of known issues (including workarounds where appropriate), known limitations and expected behaviors that may first appear to be issues.

This document describes new features, hardware, and known issues and limitations for the following products:

- Ethernet Routing Switch 4900 Series
- Ethernet Routing Switch 5900 Series

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.

Table continues…

Icon	Alerts you to...
⊕ **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 (< >)	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.
	If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon.
	Examples:
	• Click **OK**.
	• On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command.
	For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command.
	For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed.
	For example, if the command syntax is `ethernet/2/1 [ <parameter>`

Table continues…

Convention	Description
	`<value> ]...,` you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	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.
`Plain Courier Text`	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. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	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. For example, if the command syntax is `access-policy by-mac action { allow	deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and software compatibility for Extreme Networks products
Extreme Optics Compatibility
Other resources such as 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.
- 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 section details what is new in this release.

Fabric Attach Zero Touch

This release supports updates to the operation of Fabric Attach Zero Touch.

Single Link Link Aggregation Groups

Release 7.8.1 introduces Single Link LAG functionality.

The primary reason for enabling a Single Link LAG on the ERS 4900 and 5900 Series is the LACP interaction with Fabric Attach (FA) in a distributed LACP in a stack. Enabling a single link minimum LAG means that even if one of two LACP links fails, the remaining link will be kept as part of a trunk.

Prior to Release 7.8.1, having a distributed two link LAG with FA means that if one of the units fails; or if one of the LACP links fail for any reason; the LACP will be left with only one link and the trunk will become disabled. The FA process would then have to restart on this link. Single link LAG functionality keeps the LAG enabled when at least one link of the aggregator remains up, except for a scenario that involves transitioning from a stack to a standalone.

MultiLink Trunks

This release introduces support for a maximum of 64 MultiLink Trunks.

Pluggable Transceivers

This release introduces support for the following transceiver modules.

Transceiver modules

Part Number	Description	Vendor Number
10GB-LR271-SFPP	10GB CWDM LR SFP+, 1271NM	RCPX0SLR-S27
10GB-LR291-SFPP	10GB CWDM LR SFP+, 1291NM	FTLX2471DC029
10GB-LR331-SFPP	10GB CWDM LR SFP+, 1331NM	FTLX2471DC033
MGBIC-BX40-U	1000BASE-BX40-U BIDIRECTIONAL SFP	RBT12SEX-IT3
MGBIC-BX40-D	1000BASE-BX40-D SFP	RBT12SEX-IT4
MGBIC-BX120-U	1000BASE-BX120-U SFP	RBT12SVX-IT4
MGBIC-BX120-D	1000BASE-BX120-D SFP	RBT12SVX-IT5
10GB-BX10-D	10 GB, SINGLE FIBER SM, -D 10 KM	RBTX0SLR-S27
10GB-BX10-U	10 GB, SINGLE FIBER SM, -U 10 KM	RBTX0SLR-S33
10GB-ER23-SFPP	10GB-ER, DWDM CH23 SFP+	RDPX0SER-S23

Table continues…

Part Number	Description	Vendor Number
10GB-ER29-SFPP	10GB-ER, DWDM CH29 SFP+	RDPX0SER-S29
10GB-LR271-SFPP	10GB CWDM LR SFP+, 1271NM	FTLX2471DC027
10GB-LR331-SFPP	10GB CWDM LR SFP+, 1331NM	RCPX0SLR-S33

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+)

This release introduces support for Zero Touch Provisioning Plus (ZTP+).

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.

Overview of Features by Release

This section provides an overview of which release introduced feature support for a particular platform. Each new release for a platform includes all the features from previous releases unless specifically stated otherwise.

This following table lists software features in Using CLI and EDM on Ethernet Routing Switch 4900 and 5900 Series.

Features	Release by platform series	
	ERS 5900	**ERS 4900**
Ability to set password, username and type of security for any switch in stack	7.0	7.1
Ability to query USB file information	7.2	7.2
Command Line Interface (CLI)	7.0	7.1
CLI list command	7.0	7.1
Enterprise Device Manager	7.0	7.1
Global Regular Expression Print (GREP) with show commands	7.2	7.2
SFTP License and DHCP external support	7.0	7.1
Write memory and save config command	7.0	7.1

This following table lists software features in [Quick Start Configuration for Ethernet Routing Switch ERS 4900 and 5900 Series](#).

Features	Release by platform series	
	ERS 5900	**ERS 4900**
Out-of-band management	7.0	7.1

This following table lists software features in [Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 4900 and 5900 Series](#).

Features	Release by platform series	
	ERS 5900	**ERS 4900**
802.1D Compliancy Support	7.0	7.1
ADAC Uplink over SPBM	7.0	7.1
BPDU filter	7.0	7.1
BPDU filtering on trunks	7.2	7.2
Disable MAC Learning	7.0	7.1
Distributed MultiLink Trunking (DMLT)	7.0	7.1
Independent VLAN Learning (IVL) support	7.0	7.1
MLT enable/disable whole trunk (MLT shutdown ports on disable)	7.0	7.1
Multi-Link Trunking	7.0	7.1
Non-unicast hashing over MLT/DMLT/LAG	7.0	7.1
Private VLANs	7.3	7.3
Port-based VLAN support	7.0	7.1
Protocol-based VLAN support (including IPv6 protocol VLANs)	7.0	7.1
Rapid Spanning Tree Protocol (802.1w)	7.0	7.1
RSTP SNMP traps	7.0	7.1
show VLAN interface verbose command	7.0	7.1
Simple Loop Prevention Protocol (SLPP)	7.5	7.5
SLPP Guard	7.0	7.1
SLPP Guard on trunk	7.0	7.1
SNMP Trap enhancements	7.0	7.1
Spanning Tree Protocol Group (802.1D, 802.1t)	7.0	7.1
Static FDB MAC Entry	7.0	7.1
STP BPDU filtering ignore-self	7.0	7.1
Virtual LACP	7.0	7.1
Voice VLAN Integration	7.0	7.1

This following table lists software features in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.

Features	Release by platform series	
	ERS 5900	ERS 4900
802.1AB (Link Layer Discovery Protocol)	7.0	7.1
802.1AB PoE Conservation Level Request TLV	7.0	7.1
802.1AB Call server TLV	7.0	7.1
802.1AB File server TLV	7.0	7.1
802.1AB 802.1Q Framing TLV	7.0	7.1
802.1AB IP Phone TLV	7.0	7.1
802.1AB customization	7.0	7.1
802.1AB integration	7.0	7.1
802.1AB (LLDP) MED Network Policy CLI	7.0	7.1
802.1AB MED support	7.0	7.1
802.1AB location TLV	7.0	7.1
802.3at LLDP based discovery	7.0	7.1
ADAC (including 802.1ab support)	7.0	7.1
ASCII configuration file generator	7.0	7.1
ASCII Download Enhancements	7.0	7.1
Automatic Unit Replacement	7.0	7.1
Autosave configuration enhancement	7.0	7.1
Autotopology (802.1ab, SONMP)	7.0	7.1
Backup CONFIG file	7.0	7.1
boot partial-default command	7.0	7.1
Booting with an ASCII configuration file from the local file system	7.1	7.1
Change RADIUS Password	7.0	7.1
Configure asset ID	7.0	7.1
Custom Autonegotiation Advertisement (CANA)	7.0	7.1
Default IP	7.0	7.1
DHCP Client	7.0	7.1
Diagnostic Auto Unit Replacement (DAUR) enhancement	7.2	7.2
Downloading PoE firmware from SFTP	7.6	7.6
Energy Saver	7.0	7.1
EDM improved download support	7.0	7.1
Flow Control on gigabit Ethernet ports (802.3x)	7.0	7.1
Half duplex mode	7.2	7.2

Table continues…

Inactivity time out	7.0	7.1
Increase PoE power	7.0	7.1
IPFix	7.0	7.1
IPv4 Automatic Address Assignment	7.0	7.1
IPv6 management	7.0	7.1
IPv6 static routes	7.0	7.1
Jumbo frames	7.0	7.1
Link Aggregation (802.3ad)	7.0	7.1
Link Layer Discovery Protocol (802.1AB)	7.0	7.1
Link-state tracking	7.0	7.1
MLT/DMLT/LAG Dynamic VLAN Changes	7.0	7.1
MLT and LAG Scaling	7.0	7.1
Network Time Protocol (NTP)	7.0	7.1
Network Time Protocol version 4 (NTPv4)	7.5	7.5
New unit quick to config	7.0	7.1
Ping command	7.0	7.1
Ping source address	7.0	7.1
PoE enhancements: PoE high inrush mode	7.3	7.3
Port-based VLAN support	7.0	7.1
Port mirroring (including ingress and egress)	7.0	7.1
Quick start command and Web interface	7.0	7.1
Reload command	7.0	7.1
RO user access to telnet and SSH	7.0	7.1
Run IP Office Script	7.0	7.1
Run Scripts	7.0	7.1
Secure File Transfer Protocol (SFTP)	7.0	7.1
SFTP server mode enhancements (ramdisk)	7.6	7.6
show flash function	7.0	7.1
show ip netstat	7.0	7.1
show port enhancement	7.0	7.1
show software status	7.0	7.1
shutdown command	7.0	7.1
TACACS+	7.0	7.1
TACACS support for EDM — authentication and authorization of a user	7.6	7.6
Time Domain Reflectometer	7.0	7.1

Table continues…

Trivial File Transfer Protocol (TFTP)	7.0	7.1
Username password enhancement	7.0	7.1
Write memory and save config command	7.0	7.1
Zero Touch Provisioning Plus (ZTP+)	7.8.1	7.8.1

This following table lists software features in Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Features	Release by platform series	
	ERS 5900	ERS 4900
Application Telemetry	7.7	7.7
CPU utilization	7.0	7.1
Dual Syslog Server Support	7.0	7.1
Improved syslog capabilities	7.0	7.1
Many to Many Port Mirroring	7.0	7.1
Port mirroring (including ingress and egress)	7.0	7.1
Port operational status enhancements	7.0	7.1
Port VLAN based mirroring	7.2	7.2
Remote Monitoring (RMON)	7.0	7.1
Remote Monitoring (RMON) scaling	7.0	7.1
Remote Switch Port Analyzer	7.0	7.1
RSPAN over MLT/LACP	7.2	7.2
sFlow	7.2	7.2
show environmental	7.0	7.1
show port enhancement	7.0	7.1
SLA Monitor	7.0	7.1
SLAMon Agent	7.0	7.1
SNMP support for additional PSU information	7.8	7.8
Stack counters	7.0	7.1
Stack Forced Mode	7.0	7.1
Stack health check	7.0	7.1
Stack health monitoring and recovery	7.0	7.1
Stack loopback tests	7.0	7.1
Stack monitor	7.0	7.1
Stack	7.0	7.1
Trace functions	7.0	7.1

This following table lists software features in Configuring Quality of Service on Ethernet Routing Switch 4900 and 5900 Series .

Features	Release by platform series	
	ERS 5900	**ERS 4900**
Automatic QoS and 802.1AB MED Interoperability	7.0	7.1
QoS - Diffserv Code Points (DSCP RFC2998) marking and classification	7.0	7.1
Quality of Service (QoS) - 802.1q	7.0	7.1
QoS Double Wide	7.1	7.1
Quality of Service (QoS) - Layer 2 to Layer 4 filtering and policies	7.0	7.1
Quality of Service (QoS) - Offset filtering (first 80 bytes)	7.0	7.1
QoS traffic profiles enhancement for egress filtering	7.5	7.5
QoS IP/L2 Filter Options	7.0	7.1
QoS Queue Set Support	7.0	7.1
QoS queue statistics	7.0	7.1
RADIUS Dynamic UBP ACL	7.8	7.8
Traffic Profile Filter Set Support	7.0	7.1
User Based Policies	7.0	7.1

This following table lists software features in [Configuring Security on Ethernet Routing Switch 4900 and 5900 Series](#).

Features	Release by platform series	
	ERS 5900	**ERS 4900**
802.1AB new default parameters	7.0	7.1
802.1X-2004 support	7.0	7.1
802.1X non-EAP Accounting	7.0	7.1
802.1X non-EAP re-authentication	7.0	7.1
802.1X or Non-EAP and Guest VLAN on same port	7.0	7.1
802.1X or Non-EAP with Fail Open VLAN	7.0	7.1
802.1X or Non-EAP with VLAN name	7.0	7.1
802.1X or Non-EAP use with Wake on LAN	7.0	7.1
802.1X RFC3576	7.0	7.1
802.1x multiple host single authentication	7.0	7.1
802.1x NEAP support (MAC authentication)	7.0	7.1
Ability to disable outbound SSH and Telnet clients	7.3	7.3
Ability to set password, username and type of security for any switch in stack	7.0	7.1
Accounting Session ID enhancement	7.0	7.1

Table continues…

Configurable SNMP trap port	7.0	7.1
Default all EAP settings	7.0	7.1
DHCP Option 82 Support	7.0	7.1
DHCP Snooping	7.0	7.1
DHCP snooping external save	7.0	7.1
Digital certificates	7.5	7.5
Disable CLI audit log command	7.0	7.1
Disable USB and console	7.0	7.1
Dynamic ARP inspection	7.0	7.1
EAP enhancements: CLI command to verify RADIUS server reachability, RADIUS authentication fallback to secondary server, Fail Open VLAN Recovery Improvement, RADIUS authentication delay, Track all MACs per port, RFC 4675 RADIUS attributes: Egress-VLANID and Egress-VLAN-NA	7.3	7.3
EAP Fail Open with multi-VLAN	7.0	7.1
EAPOL and IP Source Guard simultaneously on a port	7.6	7.6
EAP and NEAP separation	7.0	7.1
EAP and non-EAP MultiVLAN capability	7.0	7.1
EAP-MD5 authentication	7.0	7.1
EAPoL Multihost MAC-max	7.0	7.1
EAPoL (802.1x) MHSA/MHMV and Guest VLAN	7.0	7.1
EDM support for TACACS	7.6	7.6
Enhanced Secure Mode	7.2	7.2
Extreme Networks Identity Engines Ignition Server	7.0	7.1
Extended IP Manager	7.0	7.1
Fabric Attach Client discovery and disconnect traps	7.5	7.5
Fail Open VLAN Continuity mode	7.0	7.1
Fail Open UBP	7.1	7.1
FIPS 201-2 Standard	7.6	7.6
IP Source Guard	7.0	7.1
IPv6 First Hop Security	7.0	7.1
IPv6 Source Guard	7.1	7.1
Lockout for failed logon attempts	7.0	7.1
MACsec	7.5	N/A
MAC security port lockout	7.0	7.1
MIB enhancements — Entity MIB, Dot1Q MIB, P-Bridge MIB	7.6	7.6

Table continues…

Multiple Hosts with Multiple VLANs for EAP-enabled ports (MHMV) auto configuration	7.1	7.1
Multiple local RW and RO user accounts	7.0	7.1
NEAP not member of VLAN	7.0	7.1
Password change using EDM	7.0	7.1
Password complexity and password aging and lockout policy	7.2	7.2
RADIUS Accounting Enhancements (RFC2866)	7.0	7.1
RADIUS Assigned VLAN update for 802.1x - use most recent RADIUS VLAN enhancement	7.0	7.1
RADIUS attributes for EAP and NEAP authentications: Called- Station-Id and Calling-Station-Id	7.0	7.1
RADIUS Dynamic UBP ACL	7.8	7.8
RADIUS EAP or non-EAP requests from different servers	7.0	7.1
RADIUS Management Accounting with TACACS+ support	7.0	7.1
RADIUS NEAP password configurable key	7.0	7.1
RADIUS Request use Management IP	7.0	7.1
Remote Authentication Dial-In User Server (RADIUS)	7.0	7.1
RFC 5176 Disconnect and CoA support for NEAP clients	7.1	7.1
RO user access to telnet and SSH	7.0	7.1
Secure AAA Server Communication (IPsec protocol for IPv4 and IPv6 and IKE protocol for IPv4)	7.5	7.5
Secure File Transfer Protocol (SFTP)	7.0	7.1
Secure Shell (SSH, SSHv2)	7.0	7.1
SFTP License and DHCP external support	7.0	7.1
SNMP support for additional PSU information	7.8	7.8
SNMP Trap enhancements	7.0	7.1
SSH banner	7.0	7.1
SSH client	7.0	7.1
SSH retries	7.0	7.1
Sticky MAC Address	7.0	7.1
Storm control	7.0	7.1
Syslog support for 802.1X/EAP/NEAP/UBP	7.0	7.1
Trace functions	7.0	7.1
Trace support for 802.1X	7.0	7.1
User Based Policies	7.0	7.1
Username password enhancement	7.0	7.1

This following table lists software features in Configuring IP Routing and Multicast on Ethernet Routing Switch 4900 and 5900 Series.

Features	Release by platform series	
	ERS 5900	**ERS 4900**
BOOTP and DHCP RELAY	7.0	7.1
Circuitless IP	7.0	7.1
Circuit-less IPv6 (CLIP)	7.1	7.1
Configurable route preference	7.2	7.2
Dynamic Route Table Allocation	7.0	7.1
Equal Cost MultiPath (ECMP)	7.0	7.1
Equal Cost MultiPath (ECMP) support for IP Shortcuts	7.3	7.3
Internet Group Management Protocol version 2 (IGMPv2, RFC 2236)	7.0	7.1
Internet Group Management Protocol (IGMP) Querier	7.0	7.1
Internet Group Management Protocol (IGMP v1/v2) Snooping and Proxy	7.0	7.1
Internet Group Management Protocol (IGMP) version 3	7.1	7.1
IP local and static routes	7.0	7.1
IPv6 over IPv4 Data Tunneling	7.1	7.1
IPv6 tunneling	7.0	7.1
Layer 3 Brouter Port	7.0	7.1
Layer 3 Virtual Router Redundancy Protocol	7.0	7.1
Multicast Listener Discovery (MLD) snooping	7.0	7.1
Multicast Listener Discovery (MLD) Proxy	7.1	7.1
Multicast VLAN Registration	7.2	7.2
Non local Static Routes	7.0	7.1
Non local static routes for IPv6	7.2	7.2
Open Shortest Path First	7.0	7.1
Protocol Independent Multicast-Sparse Mode (PIM-SM)	7.0	7.1
Protocol Independent Multicast-Source Specific Multicast (PIM-SSM)	7.1	7.1
Routing Information Protocol	7.0	7.1
Routing Information Protocol next generation (RIPng)	7.2	7.2
Routing policies	7.0	7.1

This following table lists software features in Configuring Fabric Connect on Ethernet Routing Switch 4900 and 5900 Series.

Features	Release by platform series	
	ERS 5900	**ERS 4900**

Table continues…

Ability to manage device using IPv6 over SPB network	7.1	7.1
CFM Integration with IP Shortcut	7.1	7.1
EAP enhancements: Delayed MAC authentication, Support for FA bindings in CoA requests, FA Client Dual-Key Authentication	7.3	7.3
Edge Automation Enhancements	7.6	7.6
E-Tree	7.3	7.3
Fabric Attach	7.0	7.1
Fabric Attach Bindings Increase	7.6	7.6
Fabric Attach Client discovery and disconnect traps	7.5	7.5
Fabric Attach enhancements — Management VLAN Advertisement Blocking and Automatic Management VLAN Assignment	7.6	7.6
Fabric Attach updates: FA Server and FA Proxy functionality, FA Auto Provision	7.0.1	7.1
Fabric Attach Tagging mode on FA Client port updated based on client specific state, Change of Authorization (COA) in FA Mode, Zero Touch Client, Trusted FA Client	7.3	7.3
IPv4 shortcuts	7.1	7.1
Multicast over SPB	7.0	7.1
NNI to NNI forwarding	7.2	7.2
Removal of partial-default requirement when enabling SPBM	7.2	7.2

This following table lists software features in [Troubleshooting Ethernet Routing Switch 4900 and 5900 Series](#).

Features	Release by platform series	
	ERS 5900	**ERS 4900**
AUR enhancement	7.0	7.1
RSTP traps	7.0	7.1
RSTP SNMP traps	7.0	7.1
Stack Forced Mode	7.0	7.1

Overview of Hardware Models by Release

The following tables provides list of hardware models in ERS 4900 and ERS 5900 Series.

Table 3: Ethernet Routing Switch 5900 Series

Switch model	Part number	Description	Initial Release
ERS 5928MTS-uPWR	AL590009A-E6GS	No fans, no PSU, no power cord	7.4
	AL5900A9B-E6GS	Two fan tray modules, back to front 1400 Watt PSU, no power cord	7.4
	AL5900A9F-E6GS	Two fan tray modules, front to back 1400 Watt PSU, no power cord	7.4
ERS 59100GTS	AL5900A5A-E6	No fans, no PSU, no power cord	7.2
	AL5900A5B-E6	Two fan tray modules, back to front 450 Watt PSU, no power cord	7.2
	AL5900A5F-E6	Two fan tray modules, front to back 450 Watt PSU, no power cord	7.2
ERS 59100GTS-PWR+	AL5900A6A-E6	No fans, no PSU, no power cord	7.2
	AL5900A6B-E6	Two fan tray modules, back to front 1400 Watt PSU, no power cord	7.2
	AL59006FA-E6	Two fan tray modules, front to back 1400 Watt PSU, no power cord	7.2
ERS 5928GTS-uPWR	AL590007A-E6	No fans, no power supply unit (PSU), no power cord	7.1
	AL5900A7B-E6	Base software license, two fan tray modules, back to front 1400 Watt PSU, no power cord	7.1
	AL5900A7F-E6	Two fan tray modules, front to back 1400 Watt PSU, no power cord	7.1
ERS 5928GTS	AL590001A-E6	No fans, no power supply unit (PSU), no power cord	7.0
	AL5900A1B-E6	Two fan tray modules, back to front 450 Watt PSU, no power cord	7.0
	AL5900A1F-E6	Base software license, two fan tray modules, front to back 450 Watt PSU, no power cord	7.0
ERS 5928GTS-PWR+	AL590002A-E6	No fans, no PSU, no power cord	7.0
	AL5900A2B-E6	Two fan tray modules, back to front 1400 Watt PSU, no power cord	7.0
	AL5900A2F-E6	Two fan tray modules, front to back 1400 Watt PSU, no power cord	7.0
ERS 5952GTS	AL590003A-E6	No fans, no PSU, no power cord	7.0
	AL5900A3B-E6	Two fan tray modules, back to front 450 Watt PSU, no power cord	7.0

Table continues…

Switch model	Part number	Description	Initial Release
	AL5900A3F-E6	Two fan tray modules, front to back 450 Watt PSU, no power cord	7.0
ERS 5952GTS-PWR+	AL590004A-E6	No fans, no PSU, no power cord	7.0
	AL5900A4B-E6	Two fan tray modules, back to front 1400 Watt PSU, no power cord	7.0
	AL5900A4F-E6	Two fan tray modules, front to back 1400 Watt PSU, no power cord	7.0

Power cords must be ordered separately for the ERS 5900 Series. For more information, see [Installing Ethernet Routing Switch 5900 Series](#).

Table 4: Ethernet Routing Switch 4900 Series

Switch model	Part number	Description	Initial Release
ERS 4926GTS	AL4900A01-E6	One 250 Watt PSU, .5 M stack cable, no power cord	7.1
ERS 4926GTS-PWR+	AL4900A02-E6	One 250 Watt PSU, .5 M stack cable, no power cord	7.1
ERS 4950GTS	AL4900A03-E61	One 1025 Watt PSU, .5 M stack cable, no power cord	7.1
ERS 4950GTS-PWR+	AL4900A04-E6	One 1025 Watt PSU, .5 M stack cable, no power cord	7.1

Power cords must be ordered separately for the ERS 4900 Series. For more information, see [Installing Ethernet Routing Switch 4900 Series](#).

Chapter 3: Important notices and new features

This section describes important software and hardware related notices.

The warranty includes access to software updates for features and maintenance releases.

Release file names

This section lists the software files.

Table 5: Software components

File Type	ERS 4900		ERS 5900	
	File Name	**File Size (bytes)**	**File Name**	**File Size (bytes)**
Secure runtime image	4900_781055s.img	20,534,292	5900_781055s.img	21,152,724
Diagnostic software versions	Diag_7504.zip	7,470,411	Diag_7504.zip	7,470,411
Enterprise Device Manager Help Files	ers5000v780_HELP_EDM.zip	2,090,545	ers5000v780_HELP_EDM.zip	2,090,545
MIB Definition File Archive	Ethernet_Routing_Switch_4900_MIBs_7.8.0.zip	1,719,625	Ethernet_Routing_Switch_5900_MIBs_7.8.0.zip	1,887,126
PoE firmware	5900_poe_v15011.bin	40,960	5900_poe_v15011.bin	40,960

ZTP+ in Fabric Attach environments

Use the following guidelines when configuring ZTP+ in Fabric Attach environments:

- A single link uplink should be used with onboarding using In-Band management. Trunk usage is not suitable for this scenario.
- Trunks can be used with onboarding using Out-of-Band management when a tailored workflow is configured in Extreme Management Center™.

MultiLink Trunks

Dynamic protocols, such as Fabric Attach and ADAC, that change VLAN attributes over trunk members require that the trunk be enabled first and the dynamic protocol second.

Starting in Release 7.8.1, a combination of static and dynamic VLAN settings is not permitted over MLT/LACP members. For example, a port taking its VLAN settings dynamically from a Fabric Attach Server cannot be a member of the same trunk with a port having the same VLAN settings configured statically.

For Fabric Attach, this happens primarily because the trunk is created after one of the ports is already an FA Element. Normally, the trunk should be enabled first and FA afterwards so that the Server is discovered over a trunk and not over a single link. Recovering from this situation implies shutting down the ports, removing FA (and consequently the dynamic VLAN attributes), enabling the trunk and re-enabling FA and the ports.

The same principle is applied for any protocol which changes dynamic VLAN settings for trunk members; the trunk must be enabled first and the dynamic protocol enabled after the trunk is formed.

Downgrading to a previous release

Switch configuration will be defaulted after downgrading from 7.8.1 or other 7.8.x releases, to 7.8.0. Releases 7.8.1, and other future 7.8.x releases, contain enhancements not supported by 7.8.0. After downgrading to 7.8.0, the switch or stack must be reconfigured based on a previous configuration file.

Software Upgrade

This section provides procedures to upgrade the software — diagnostic and agent software.

Upgrade considerations for Enhanced Secure Mode

Upgrading from a previous version not supporting Enhanced Secure Mode maintains the existing non Enhanced Secure configuration. If you switch to Enhanced Secure Mode after upgrade, the configuration is defaulted.

Upgrading to a newer release supporting Enhanced Secure Mode maintains the existing configuration parameters including the following:

- Users and passwords
- Network configuration
- Settings for TFTP, TELNET, SSH protocols

Downgrading the switch to an earlier release restores the default settings. The IP management address does not change.

Upgrade consideration for password security

If you upgrade from Release 7.0 or Release 7.1 to Release 7.2, 7.3, or 7.4, there is an impact on the password security default values; therefore, you must configure password security options to the default values.

⊛ **Note:**

> You cannot configure password security options to default values for Release 7.0 or 7.1.

If you upgrade from Release 7.2 or 7.3 to Release 7.4 and Release 7.0 or 7.1 was not installed on your system, then configuring the password security options to the default values is optional. You can configure the default values for the password security feature before or after you upgrade.

Perform the following procedure when you upgrade from Release 7.0 or 7.1 to Release 7.2, 7.3, 7.4.

1. Verify the software release version.

2. If the software release version is 7.0 or 7.1, you must configure password security options to the default values when you upgrade, as follows:

   a. upgrade from Release 7.0 or 7.1 to Release 7.2 or 7.3

   b. successive upgrade from Release 7.0 or 7.1 to Release 7.2, 7.3

   c. successive upgrade from Release 7.0 or 7.1 to Release 7.2, 7.3, 7.4

   d. upgrade from Release 7.0 or 7.1 to Release 7.4

The following table details the default password security options.

Table 6: Default password security options

Password security option	Default
default username lockout-retries	Default value is 0. When configured to default value, an incorrect password can be entered multiple times and the account does not lock.
default username lockout-time	Default value is 1 minute. When configured to the default value, the threshold on the number of incorrect passwords is exceeded, the account locks for 1 minute.
default password aging-time	Default value is 0. When configured to the default value, the password remains valid and does not expire.
username <usernames> inactive-period 0	Default is 0 days. When configured to the default value, the user account is not disabled if the account is inactive.
default password aging-time username <usernames>	Default username configures the aging time.
password unlock-timer 1	Default is 7 days.

Table continues…

Password security option	Default
	When configured to the value of 1, the disabled account due to inactivity timeout is reenabled in 1 day.
default password complexity	Password complexity does not require a specific value of upper case, lower case, numeric, or special characters for a password.
password check-repeated disable	Default is disable. When configured to the default, account passwords can be repeated.
password check-sequential disable	Default is disable. When configured to the default, account passwords can be sequential.
password password-change-on-first-login disable	Default is disable. When configured to the default, the password accepts the default username and password at first login.

Before you Upgrade

This section provides important considerations and precautions *before* you upgrade.

Zero Touch Provisioning Plus (ZTP+)

✳ **Note:**

When you upgrade to this release, 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 this release, ensure that the switch does not connect to the XMC server by resolving its *extremecontrol* address using DNS.

VLAN ID 4060 should not be used

✳ **Note:**

VLAN ID 4060 is used internally by SPBM with IP Shortcuts Multicast and should not be used on ERS 5900 and ERS 4900.

Before upgrading, if VLAN ID 4060 exists, migrate it to a different VLAN ID.

Upgrade SLAMon Server

As of Release 7.5, only TLS 1.1 and TLS 1.2 are supported; TLS 1.0 is no longer supported. Older versions of SLAMon servers using TLS 1.0 no longer operate after deploying Release 7.5. Upgrade to SLAMon Server version 2.5 SP3.

Upgrading Diagnostic Software

Use the following procedure to upgrade the diagnostic software image.

Before you begin

Extract the diagnostic image `radiag_xxxx.bin` file from the `Diag_xxxx.zip` archive.

About this task

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the `no-reset` parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

Procedure

1. Access the CLI through a Telnet or Console connection.

2. Enter Privileged EXEC mode using the `enable` command.

3. Enter `download address [usb] <ip_address> diag <image_name> [no reset]` to transfer the diagnostic image to the device.

Variable Definitions

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

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the diagnostic image is hosted.
diag <image_name>	The name of the diagnostic image file on the TFTP server.
no-reset	This parameter specifies that the device will not reset after the upgrade is complete.
usb	This parameter specifies that the software download will occur from a USB device instead of the network.

Upgrading agent software

Use this procedure to upgrade agent software.

1. Access the CLI through a Telnet or Console connection.
2. Enter Privileged EXEC mode using the `enable` command.
3. Use the command `download address [usb] <ip_address> {primary | secondary} {image <image_name> | image-if-newer <image_name> |`

      `poe_module_image <image_name>} [no-reset]` to transfer the agent image to the device.

The following table describes the parameters for this command.

Parameter	Description
address <ip_address>	The IPv4 or IPv6 address of the TFTP server on which the agent image is hosted.
primary | secondary	Designates whether the image is stored in the primary or secondary image location. The default is primary.
image <image_name> | image-if-newer <image_name> | poe_module_image <image_name>	The name of the agent image file on the TFTP server. Each option is mutually exclusive. Use the option described with the following situation: • To load the agent image under normal circumstances, use the image option. • To load the agent image only if it is newer than the current image, use the image-if-newer option. • To load the agent image if it is a PoE module image, use the poe_module_image option.
no-reset	Specifies that the device will not reset after the upgrade is complete.
usb	Specifies that the software download will occur from a USB device instead of the network.

The upgrade process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process.

When the process is complete, the device automatically resets unless the `no-reset` parameter was used. The software image initiates a self-test and returns a message when the process is complete.

During the download process the switch is not operational.

Upgrading the PoE+ firmware

About this task

Upgrade the PoE+ firmware to the latest version on all PoE+ units.

Before you begin

Verify the PoE+ firmware version using command `show sys-info`. In the command output, check `PoE Module FW`. In a stack, to view this information for a specific unit, connect to the serial console of that unit.

Procedure

1. Do any one of the following to upgrade the POE+ firmware:

   • To upgrade the PoE+ firmware from TFTP, enter the following command:

   ```
   download [ address <TFTP server address> ] poe_module_image
   5900_poe_v15011.bin
   ```

   OR

   • To upgrade the PoE+ firmware from an USB storage device, enter the following command:

   ```
   download usb poe_module_image 5900_poe_v15011.bin [ unit <unit
   number> ]
   ```

2. The switch or stack reboots after the firmware is successfully downloaded and saved to the PoE+ board.

Upgrading the PHY Firmware for ERS 5928MTS-uPWR

🛈 **Important:**

The latest firmware is shipped with the MTS unit and it is not available online. Only in the case of finding a bug in this firmware version will a new version be made available online.

About this task

Use the following procedure to upgrade the PHY firmware on the ERS 5928MTS-uPWR switch.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. To upgrade the PHY firmware, enter the following command:

   ```
   download phy_firmware "copper_ports_module.cld"
   ```

Example

```
5928MTS-uPWR#download phy_firmware "copper_ports_module.cld"
```

Using TLS1.2 Certificate and Resetting SSL Server

About this task

The RSA key size is increased from 1024 bit to 2048 bit in Release 7.2. After upgrading, use the following procedure to use TLS 1.2 certificate and reset the SSL server.

✳ **Note:**

If you are upgrading from Release 7.2, you do not need to perform this procedure again.

Procedure

1. Enter the following command to replace the SSL certificate:

   `ssl certificate`

2. Enter `y` to create the certificate.

3. Enter the following command to reset the SSL server:

   `ssl reset`

Example

```
Switch(config)#ssl certificate
Certificate already exists. Create it anyway (y/n) ? y
Switch(config)#ssl reset
```

How to get EDM Online Help Files for Embedded EDM

Help files are not included with the embedded EDM software files on the switch. A network administrator must copy the software-release-specific help files onto a TFTP server. After the help files are downloaded to the TFTP server, the network administrator must configure the switch with the path to the help files on the TFTP server. You can use CLI or EDM to configure a path from your switch to the help files. After the path to the help file is configured, whenever an EDM user clicks the help button on the toolbar, the switch downloads and displays help information in the Web browser.

If you are using Configuration and Orchestration Manager (COM) to manage your switch, help resides with COM and you do not need to use these procedures.

For more information about EDM, see Using CLI and EDM on Ethernet Routing Switch 4900 and 5900 Series.

How to configure the path to the embedded EDM help files

If you are using embedded EDM, use the procedures in this section to configure the path to the help files. You can configure the help file path with CLI or EDM.

Configuring the path to the help files using CLI

About this task

Use the following procedure to configure the path to the help files using CLI.

Procedure

In CLI, go to the Global Configuration mode and use the following command:

`edm help-file-path <path name> tftp address <tftp address>`

The following table describes the parameters for the edm-help-file-path command.

Parameter	Description
path name	Specifies the path name you created for EDM help files. The path name is stored in NVRAM.
TFTP address	Specifies EDM TFTP server IP address. Use this address only for EDM help files. If you do not specify a TFTP server address, the system uses the address specified most recently. WARNING: Because the TFTP server address is stored in NVRAM, each time the system returns to the default configuration, you must reconfigure the path to EDM online help.

Example

Following is an example of a CLI EDM help file path:

```
edm help-file-path ERS5900_xx_Help tftp address 100.100.100.15
```

In the preceding example, xx is the software release version and ERS5900_xx_Help is a folder that contains help files. The folder is located on a TFTP server at the 100.100.100.15 address.

Configuring the path to the help files using EDM

Use the following procedure to configure the path to the help files.

Procedure steps

1. From the navigation tree, click **Edit**.

2. From the Edit tree, click **File System**.

3. Select the **Help File Path** tab.

4. In the Path dialog box, enter the path to the help file storage location.

   Example

   tftp://xxx.xxx.xxx.xxx/file_name

Tested browsers

EDM has been tested with the following web browsers:

Browser	Version
Microsoft Internet Explorer, Windows 10	11.0.9600.19724
Mozilla Firefox, Windows 10	77.0.1 (64-bit)
Google Chrome, Windows 10	83.0.4103.116 (64-bit)
Microsoft Edge, Windows 10	83.0.478.54 (64-bit)
Opera, Windows 10	68.0.3618.173 (64-bit)

> **Note:**
>
> EDM supports HTTPS connections using Google Chrome starting in Release 7.8.0. An SSL reset is required after upgrading to a 7.8.x or later release from a release earlier than 7.8.0 for HTTPS to work.

Supported Software and Hardware Capabilities

This section lists software scaling capabilities.

Table 7: Supported software and hardware scaling capabilities

Unless stated otherwise, the capabilities are listed per stack, where a stack consists of one to eight units.

Feature	ERS 5900 Series	ERS 4900 Series
SPB:		
SPB nodes for each region	1000	750
IS-IS adjacencies	4	4
BEBs for each region	512[1]	512[1]
CVLANs	1000	500
SPB Switched UNI	500	500
SPB ISIDs (Maximum L2 VSN)	1000	500
Maximum Multicast Streams	512	512
Max L2 VSN with Multicast enabled	256	256
Operational modes	Standalone or stacked 8 high [2]	Standalone or stacked 8 high
B-VLANs	2	2
IS-IS interfaces	4	4
IPv6:		
Maximum IPv6 in IPv4 data tunnels	16	16
IPv6 DHCP relay forwarding paths for each unit or stack	256	256
IPv6 Static Routes	512	512
IPv6 interfaces	256	256
IPv6 Routes total (includes learned routes, static and local routes	2048	2048
IPv6 Dynamic routing interfaces	64	64
QoS:		

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
Per port egress queues	8	8
QoS precedence for each ASIC	16	16
QoS rules for each precedence	256	256
Total QoS rules	4096	4096
Performance:		
MAC address capacity	32768	32768
Stacking port bandwidth, FDX	42 Gbps	26 Gbps
Maximum ports for each stack	416	416
Miscellaneous:		
Maximum port mirroring instances	4	4
Maximum admin accounts	10	10
RSPAN VLANs	4	4
RSPAN destinations for each unit or stack	4	4
802.1X (EAP) clients for each port, MHMV	32	32
802.1X (EAP) clients for each MHSA	1 authenticated / balance unlimited	1 authenticated / balance unlimited
802.1x (EAP and NEAP) clients for each switch or stack	768	768
Maximum RADIUS servers	2	2
Maximum 802.1X EAP servers	2	2
Maximum 802.1X NEAP servers	2	2
Maximum RADIUS/EAP/NEAP servers	6	6
IPFix number of sampled flows	100000	100000
RMON alarms	800	800
RMON events	800	800
RMON Ethernet history	249	249
RMON Ethernet statistics	110	110
Link State Tracking instances	2	2
sFlow maximum number of collectors	4	4
sFlow minimum packet sampling rate	1 out of 4096	1 out of 4096
Layer 2:		
Concurrent VLANs	1024	1024

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
Supported VLAN IDs	1 – 4094 (0 and 4095 reserved. 4001 reserved by STP. 4002-4008 reserved by multiple STP)	1 – 4094 (0 and 4095 reserved. 4001 reserved by STP. 4002-4008 reserved by multiple STP)
	✳ **Note:** VLAN ID 4060 should not be used on ERS 5900 and ERS 4900. Before upgrading ERS 5900 from Release 7.0 to later release, if VLAN ID 4060 exists, then migrate it to a different VLAN ID.	
Protocol VLAN types	16	16
Multi-Link Trunking (MLT), Distributed Multi-Link Trunking (DMLT), and Link Aggregation (LAG) groups	32	32
Links or ports for MLT, DMLT or LAG	8	8
Static MAC addresses	1024	1024
Spanning Tree Group instances (802.1s)	8	8
Spanning Tree Groups	8	8
DHCP Snooping table entries for each unit	1024	1024
LLDP Neighbors for each port	16	16
LLDP Neighbors for each switch or stack	800	800
Private VLANs	200	200
Layer 3:		
IP Interfaces (VLANs or Brouter ports)	256	256
ARP Entries total (local, static and dynamic)	4096	1792
ARP Entries — local (IP interfaces for each switch or stack)	256	256
ARP Entries — static	256	256
ARP Entries — dynamic	3584	1280
IPv4 Routes total (local, static and dynamic)	4096	2048
IPv4 Static routes	512	512
IPv4 Local routes	256	256

Table continues…

Feature	ERS 5900 Series	ERS 4900 Series
IPv4 Dynamic routes (RIP and OSPF)	4096	2048
Dynamic Routing interfaces (RIP and OSPF)	64	64
OSPF areas	4	4
OSPF adjacencies (devices for each OSPF areas)	32	32
OSPF Link State Advertisements (LSA)	10000	10000
OSPF virtual links	4	4
OSPF host routes	32	32
ECMP (Maximum concurrent equal cost paths)	4	4
ECMP (Max next hop entries)	256	128
VRRP instances	256	256
Management routes	4	4
UDP forwarding entries	128	128
DHCP relay entries	256	256
DHCP relay forward paths	512	512
Multicast:		
IGMP v1, v2 and v3 multicast groups	1024	1024
IGMP enabled VLANs	256	256
MLD snooping enabled VLANs	512 MLDv1 entries 256 MLDv2 entries	512 MLDv1 entries 256 MLDv2 entries
PIM-SM forward entries for each stack	1024	512
PIM-SM interfaces (active and passive)	64 (4 active and 60 passive)	32 (4 active and 28 passive)
[1] Maximum number of BEBs for each region can be reduced when SPB Multicast is enabled or when connecting to IST switches.		
[2] ERS 59100GTS and ERS 59100GTS support only four units high stack.		

Licensing Support

Only one software license is required for each ERS 4900 Series or ERS 5900 Series switch or stack.

To obtain a new license, go to the Extreme Networks Support Portal at https://extremeportal.force.com/ExtrLicenseLanding.

✱ **Note:**

Release 7.5 or later is required to support licenses generated through the Extreme Networks Support Portal.

❶ **Important:**

The software continues to support .xml licenses generated by Avaya.

If you require a change or regeneration of Avaya-provided licenses, send your email request to:datalicensing@extremenetworks.com.

The following sections detail the different categories of licenses.

Base License

A Base license gives customers the right to use Base software features on the switch.

ERS 4900 Series and ERS 5900 Series Advanced Software License

You can obtain a trial license to try out advanced license features for 60 days. After the trial period expires, the licensed feature is disabled.

The Advanced trial license is generated using the system MAC address of a switch and can only be generated and used once for a given MAC address. After the expiry of the 60 day trial period, you will see messages on the console and in the alarms database that the license has expired. If you restart the system after the license expiration, the Advanced features will not be loaded even if they are in the saved configuration. If you purchase an Advanced license, you must obtain and install a license file.

You must obtain the Advanced Software License for the following features:

- Open Shortest Path First (OSPF)
- Virtual Router Redundancy Protocol (VRRP)
- Equal Cost Multi Path (ECMP)
- Protocol Independent Multicast-Sparse mode (PIM-SM)
- IPv6 Forwarding
- IP Shortcuts
- Routing Information Protocol next generation (RIPng)
- MACsec

ERS 4900 Series Advanced License part numbers

Part Number / Order Code	Description
383772	ERS 4900 Series Advanced Software License
383773	ERS 4900 Series Advanced Software Trial License

ERS 5900 Series Series Advanced License part numbers

Part Number / Order Code	Description
380221	ERS 5900 Series Advanced Software License
383168	ERS 5900 Series Base License with MACsec
383770	ERS 5900 Series Advanced License with MACsec

Supported standards, MIBs, and RFCs

This section lists the supported standards, MIBs, and RFCs.

Standards

The following IEEE Standards contain information that applies to this switch:

IEEE 802.1D	Spanning Tree Protocol
IEEE 802.1w	Rapid Spanning Tree
IEEE 802.1s	Multiple Spanning Tree
IEEE 802.1t 802.1D	Maintenance
IEEE 802.1p	Prioritizing
IEEE 802.1Q	VLAN Tagging
IEEE 802.1X	Ethernet Authentication Protocol
IEEE 802.1AB	Link Layer Discovery Protocol
IEEE 802.1AX	Link Aggregation Control Protocol (LACP)
IEEE 802.1ag	Connectivity and Fault Management
IEEE 802.1aq	Shortest Path Bridging MAC
IEEE 802.3	Ethernet
IEEE 802.3af	Power over Ethernet
IEEE 802.3at	Power over Ethernet Plus
IEEE 802.3ad / 802.1AX	Link Aggregation Control Protocol
IEEE 802.3ab-1999	1000Mbps operation, 1000base-T copper
IEEE 802.3ae-2002	10Gbps operation implemented as 10GBase-SFP+
IEEE 802.3ak	10GBase-CX4
IEEE 802.3bz	2.5GBase-T
IEEE 802.3i	10Base-T
IEEE 802.3u	Fast Ethernet

Table continues…

IEEE 802.3x	Flow Control
IEEE 802.3z-1998	1000Mbps Operation implemented as 1000BaseX

RFCs

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

Table 8: Supported RFCs

RFC	Release by platform Series	
	ERS 5900	ERS 4900
FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors	7.6	7.6
RFC 768 UDP	7.0	7.1
RFC 783 TFTP	7.0	7.1
RFC 792 ICMP	7.0	7.1
RFC 793 TCP	7.0	7.1
RFC 826 ARP	7.0	7.1
RFC 854 Telnet	7.0	7.1
RFC 894 IP over Ethernet	7.0	7.1
RFC 903 Reverse ARP	7.0	7.1
RFC 950 / RFC 791 IP	7.0	7.1
RFC 951 BootP	7.0	7.1
RFC 1058 RIPv1	7.0	7.1
RFC 1112 IGMPv1	7.0	7.1
RFC 1122 Requirements for Internet hosts	7.0	7.1
RFC 1155 SMI	7.0	7.1
RFC 1156 MIB for management of TCP/IP	7.0	7.1
RFC 1157 SNMP	7.0	7.1
RFC 1212 Concise MIB definitions	7.0	7.1
RFC 1213 MIB-II	7.0	7.1
RFC 1215 SNMP Traps Definition	7.0	7.1
RFC 1305 NTP version3	7.0	7.1
RFC 1340 Assigned Numbers	7.0	7.1
RFC 1350 TFTP	7.0	7.1
RFC 1354 IP Forwarding Table MIB	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 1398 Ethernet MIB	7.0	7.1
RFC 1442 SMI for SNMPv2	7.0	7.1
RFC 1450 MIB for SNMPv2	7.0	7.1
RFC 1493 Bridge MIB	7.0	7.1
RFC 1591 DNS Client	7.0	7.1
RFC 1650 Definitions of Managed Objects for Ethernet-like Interfaces	7.0	7.1
RFC 1724 / RFC 1389 RIPv2 MIB extensions	7.0	7.1
RFC 1769 / RFC 1361 SNTP	7.0	7.1
RFC 1886 DNS extensions to support IPv6	7.0	7.1
RFC 1908 Coexistence between SNMPv1 & v2	7.0	7.1
RFC 1945 HTTP v1.0	7.0	7.1
RFC 1981 Path MTU Discovery for IPv6	7.0	7.1
RFC 2011 SNMP v2 MIB for IP	7.0	7.1
RFC 2012 SNMP v2 MIB for TDP	7.0	7.1
RFC 2013 SNMP v2 MIB for UDP	7.0	7.1
RFC 2080 Routing Information Protocol next generation (RIPng)	7.2	7.2
RFC 2096 IP Forwarding Table MIB	7.0	7.1
RFC 2131 / RFC 1541 Dynamic Host Configuration Protocol (DHCP)	7.0	7.1
RFC 2138 RADIUS Authentication	7.0	7.1
RFC 2139 RADIUS Accounting	7.0	7.1
RFC 2236 IGMPv2	7.0	7.1
RFC 2328 / RFC 2178 / RFC 1583 OSPFv2	7.0	7.1
RFC 2453 RIPv2	7.0	7.1
RFC 2454 IPv6 UDP MIB	7.0	7.1
RFC 2460 IPv6 Specification	7.0	7.1
RFC 2461 IPv6 Neighbor Discovery	7.0	7.1
RFC 2464 Transmission of IPv6 packets over Ethernet	7.0	7.1
RFC 2474 Differentiated Services (DiffServ)	7.0	7.1
RFC 2541 Secure Shell protocol architecture	7.0	7.1
RFC 2597 Assured Forwarding PHB Group	7.0	7.1
RFC 2598 Expedited Forwarding PHB Group	7.0	7.1
RFC 2616 / RFC 2068 HTTP 1.1	7.0	7.1
RFC 2660 HTTPS - Secure Web	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 2665 / RFC 1643 Ethernet MIB	7.0	7.1
RFC 2674 Q-BRIDGE-MIB	7.0	7.1
RFC 2710 Multicast Listener Discovery version 1 (MLDv1)	7.0	7.1
RFC 2715 Interoperability Rules for Multicast Routing Protocols	7.0	7.1
RFC 2787 Definitions of Managed Objects for VRRP	7.0	7.1
RFC 2819 / RFC 1757 / RFC 1271 RMON	7.0	7.1
RFC 2851 Textual Conventions for Internet network addresses	7.0	7.1
RFC 2863 / RFC 2233 / RFC 1573 Interfaces Group MIB	7.0	7.1
RFC 2865 RADIUS	7.0	7.1
RFC 2866 / RFC 2138 RADIUS Accounting	7.0	7.1
RFC 2869 RADIUS Extensions - Interim updates	7.0	7.1
RFC 2933 IGMP MIB	7.0	7.1
RFC 3058 RADIUS Authentication	7.0	7.1
RFC 3140 / RFC 2836 Per-Hop Behavior Identification codes	7.0	7.1
RFC 3162 RADIUS and IPv6	7.0	7.1
RFC 3195 Reliable delivery Syslog (only in Enhanced Secure Mode)	7.2	7.2
RFC 3246 Expedited Forwarding Per-Hop Behavior	7.0	7.1
RFC 3260 / RFC 2475 Architecture for Differentiated Services	7.0	7.1
RFC 3289 DiffServ MIBs	7.0	7.1
RFC 3315 DHCPv6	7.0	7.1
RFC 3410 / RFC 2570 SNMPv3	7.0	7.1
RFC 3411 / RFC 2571 SNMP Frameworks	7.0	7.1
RFC 3412 / RFC 2572 SNMP Message Processing	7.0	7.1
RFC 3413 / RFC 2573 SNMPv3 Applications	7.0	7.1
RFC 3414 / RFC 2574 SNMPv3 USM	7.0	7.1
RFC 3415 / RFC 2575 SNMPv3 VACM	7.0	7.1
RFC 3416 / RFC 1905 SNMP	7.0	7.1
RFC 3417 / RFC 1906 SNMP Transport Mappings	7.0	7.1
RFC 3418 / RFC 1907 SNMPv2 MIB	7.0	7.1
RFC 3484 Default Address Selection for IPv6	7.0	7.1
RFC 3513 IPv6 Addressing Architecture	7.0	7.1
RFC 3569 Overview of Source Specific Multicast (SSM)	7.0	7.1
RFC 3579 RADIUS support for EAP	7.0	7.1
RFC 3584 / RFC 2576 Co-existence of SNMP v1/v2/v3	7.0	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 3587 IPv6 Global Unicast Format	7.0	7.1
RFC 3596 DNS extensions to support IPv6	7.0	7.1
RFC 3621 Power over Ethernet MIB	7.0	7.1
RFC 3635 Definitions of Managed Objects for the Ethernet-like Interface Types	7.0	7.1
RFC 3768 / RFC 2338 VRRP	7.0	7.1
RFC 3810 MLDv2 for IPv6	7.0	7.1
RFC 3826 AES for the SNMP User-based Security Model	7.0	7.1
RFC 3917 Requirements for IPFIX	7.0	7.1
RFC 3954 Netflow Services Export v9	7.0	7.1
RFC 3993 DHCP Subscriber-ID sub-option	7.0	7.1
RFC 4007 Scoped Address Architecture	7.0	7.1
RFC 4022 / RFC 2452 TCP MIB	7.0	7.1
RFC 4113 UDP MIB	7.0	7.1
RFC 4133 / RFC 2737 / RFC 2037 Entity MIB	7.0	7.1
RFC 4193 Unique Local IPv6 Unicast Addresses	7.0	7.1
RFC 4213 Transition Mechanisms for IPv6 Hosts & Routers	7.0	7.1
RFC 4250 SSH Protocol Assigned Numbers	7.0	7.1
RFC 4251 SSH Protocol Architecture	7.0	7.1
RFC 4252 SSH Authentication Protocol	7.0	7.1
RFC 4253 SSH Transport Layer Protocol	7.0	7.1
RFC 4254 SSH Connection Protocol	7.0	7.1
RFC 4291 IPv6 Addressing Architecture	7.0	7.1
RFC 4292 IP Forwarding Table MIB	7.1	7.1
RFC 4293 IPv6 MIB	7.0	7.1
RFC 4344 SSH Transport layer Encryption Modes	7.0	7.1
RFC 4345 Improved Arcfour Modes for SSH	7.0	7.1
RFC 4429 Optimistic Duplicate Address Detection (DAD) for IPv6	7.0	7.1
RFC 4432 SSHv2 RSA	7.0	7.1
RFC 4443 / RFC 2463 ICMPv6 for IPv6	7.0	7.1
RFC 4541 Considerations for IGMP and MLD snooping switches	7.0	7.1
RFC 4601 Protocol Independent Multicast – Sparse Mode (PIM-SM) Protocol Specification	7.0	7.1
RFC 4604 / RFC 3376 IGMPv3	7.0	7.1
RFC 4632 Classless Inter-domain Routing (CIDR)	7.1	7.1

Table continues…

RFC	Release by platform Series	
	ERS 5900	ERS 4900
RFC 4673 RADIUS Dynamic Authorization Server MIB	7.0	7.1
RFC 4675 Egress-VLAN-Name and Egress-VLANID attributes (partial support)	7.3	7.3
RFC 4716 SSH Public Key File Format	7.0	7.1
RFC 4750 / RFC 1850 / RFC 1253 OSPF v2 MIB	7.0	7.1
RFC 4789 SNMP over IEEE 802 Networks	7.0	7.1
RFC 4861 Neighbor Discovery for IPv6	7.0	7.1
RFC 4862 / RFC 2462 IPv6 Stateless Address Auto-Configuration	7.0	7.1
RFC 5010 / RFC 3046 DHCP Relay Agent Information Option 82	7.0	7.1
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6	7.0	7.1
RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for Exchange of IP Traffic	7.0	7.1
RFC 5176 / RFC 3576 Dynamic Authorization Extensions to RADIUS	7.0	7.1
RFC 5186 IGMPv3/MLDv2 and Multicast Routing Interaction	7.0	7.1
RFC 5246 TLS Protocol Version 1.2	7.1	7.1
RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	7.6	7.6
RFC 5905	7.4.1	7.4.1
RFC 6187 X.509v3 Certificates for Secure Shell Authentication x509v3-ssh-rsa publickey algorithm only)	7.6	7.6
RFC 6329 IS-IS Extensions Supporting Shortest Path Bridging	7.0	7.1
RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	7.6	7.6
SP 800-78-4 Cryptographic Algorithms and Key Sizes for Personal Identity Verification	7.6	7.6

Table 9: Obsolete RFCs

RFC	Obsolete Release
RFC 1519 Classless Inter-Domain Routing (CIDR)	7.1

The following table lists IPv6 specific RFCs.

Table 10: IPv6 specific RFCs

Standard	Description	Compliance
RFC 1886	DNS Extensions to support IPv6	Supported
RFC 1981	Path MTU Discovery for IPv6	Supported

Table continues…

Standard	Description	Compliance
RFC 2080	Routing Information Protocol next generation (RIPng)	Supported
RFC 2460	Internet Protocol v6 (IPv6) Specification	Supported
RFC 2461	Neighbor Discovery for IPv6	Supported
RFC 2462	IPv6 Stateless Address Auto-configuration	Auto-configuration of link local addresses only
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Supported
RFC 3162	RADIUS and IPv6	Supported
RFC 3315	DHCPv6	Support for IPv6 DHCP Relay
RFC 3587	IPv6 Global Unicast Format	Supported
RFC 3596	DNS extensions to support IPv6	Supported
RFC 3810	MLDv2 for IPv6	Supported
RFC 4007	Scoped Address Architecture	Supported
RFC 4022	Management Information Base for TCP	Mostly supported
RFC 4113	Management Information Base for UDP	Mostly supported
RFC 4193	Unique Local IPv6 Unicast Addresses	Supported
RFC 4213	Transition Mechanisms for IPv6 Hosts and Routers	Supports dual stack and configured tunnels
RFC 4291	IPv6 Addressing Architecture	Support earlier version of RFC (3513)
RFC 4292	IP Forwarding Table MIB	Supported
RFC 4293	Management Information Base for IP	Mostly supported
RFC 4429	Optimistic Duplicate Address Detection (DAD) for IPv6	Supported
RFC 4443	Internet Control Message Protocol (ICMPv6)	Support earlier version of RFC (2463)
RFC 4541	Considerations for IGMP and MLD snooping switches	Supported
RFC 4861	Neighbor Discovery for IPv6	Supported
RFC 4862 / RFC 2462	IPv6 Stateless Address Auto-Configuration	Supported
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	Supported

Chapter 4: Resolved issues

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

Issue Number	Description
ERS495900-5617, ERS495900-5692	Fabric Attach uplink on a Non-Base Unit in a redundant LACP configuration remains disabled after the unit rejoins the Stack.
ERS495900-5627	Delay in convergence of traffic with Fabric Attach uplinks when a unit in the Stack is powered off.
ERS495900-5701	System unresponsiveness due to bcmRx task not releasing memory.
ERS495900-5724	SSH and Console access failure.
ERS495900-5736	Adding new units to SPBM stack caused some configuration loss on the initial units.
ERS495900-5794	The memory allocated for the SLPP BPDUs that were looped between two ports was never released.
ERS495900-5830	An SNMP crash may be encountered when a high number of traps are sent continuously to a trap receiver.

Chapter 5: Known issues and limitations

Use the information in this section to learn more about known issues and limitations. Where appropriate, use the workarounds provided.

Known issues

This section identifies the known issues.

Table 11: Known issues for Release 7.8.1

Issue number	Description
ERS495900-5728	An incorrect port number is specified in the MSTP General Log when a port participating in an MLT goes down and comes back up again and STP is enabled on the port. WORKAROUND: Disable STP on trunk ports.
ERS495900-5744	When a stack receives a BPDU belonging to the stack on a trunk port, only the trunk ports local to the unit receiving it are shut down. WORKAROUND: Disable STP on trunk ports.
ERS495900-5745	BPDU filtering with ignore self activated on MLT shuts down the trunk port on which the self BPDU is received.
ERS495900-5769	Dynamic Management IP settings should be displayed under the `Last BootP/ DHCP` column in the output of the `show ip` and `show ip mgmt` commands. They are displayed under the `Configured` column instead.
ERS495900-5823	Downloading the primary or secondary image using SNMP and the **no-reset** option blocks the stack in the software download process. This issue increases the time of an upgrade from 5 to 10 minutes to 30 minutes. ✱ **Note:** This issue is present in Release 7.8.0 only. RECOMMENDATION: Do not download images using SNMP and the **no-reset** option when upgrading from Release 7.8.0. Alternatively, Telnet/SSH or the console can be used for upgrades as well.
ERS495900-5835	Octets are not aging out properly in IPFIX reporting.

Table continues…

Issue number	Description
ERS495900-5842	A RADIUS authenticated NEAP client with no RAV does not have the client MAC address learned on the target VLAN.
ERS495900-5848	Dynamic IP addresses requested by standalone units before the stack is formed are present in ACG after the units join the stack.
ERS495900-5849	Static Management IP settings will be overwritten on the Out of Band Management port if they are configured after the DHCP process starts. The device will continue to send DHCP requests until settings are obtained and overwrite the statically configured settings. WORKAROUND: Configure the static Management IP settings again. Use the `ip mgmt address source configured-address` command to disable Dynamic Management IP settings.
ERS495900-5851	The password expiry notification is displaying an incorrect amount of days.

Table 12: Known issues for Release 7.8 and earlier

Issue number	Description
wi01187211/ ERS495900-18	If IS-IS adjacency is established over an MLT/LACP trunk, the information about IS-IS interfaces is displayed for both the trunk and its members in EDM and only for the trunk itself in CLI.
wi01206409/ ERS495900-82	SNMP users cannot be created from the EDM Offbox. **Workaround**: Create SNMP users from EDM or CLI.
wi01208072/ ERS495900-99	When a non-SPBM switch is connected to an SPBM switch and the Multiple Spanning Tree Protocol (MSTP) instances do not match, the in-band port from management VLAN is set to discarding mode instead of forwarding mode. WORKAROUND: Ensure all VLANs are in the Common and Internal Spanning Tree (CIST) for this scenario. See Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 4900 and 5900 Series for more information regarding MSTP.
wi01222464/ ERS495900-172	SSHC DSA/RSA key cannot be uploaded to USB from the non-base unit using NetSNMP. **Workaround**: Set each MIB separately to ensure key file uploads successfully.
wi01223662/ ERS495900-194	EDM: In the Ascii Config Script Files screen in EDM, not all applications are available for selection for entries at the bottom of the screen due to the size of the pop-up window. **Workaround**: Scroll the screen so that the entry is in the upper part of the EDM screen, or use CLI to configure.
wi01223817/ ERS495900-197	In an SPBM environment, remote MAC addresses are not learned on the destination device after NNI ports are bounced on the source device. **Workaround**: Bounce IS-IS on the source SPBM switch.
wi01224130/ ERS495900-204	When enabling link aggregation on a group of ports with inconsistent settings, an error is issued ('% Ports have different IPSG configurations') as expected. However,

Table continues…

Issue number	Description
	link aggregation is enabled partially on the list of ports, up to the first port with different settings.
wi01224917/ ERS495900-219	In a stack in TBU mode, when using the serial console on the former base unit which left and rejoined the stack, some QoS UBP statistics (**show qos ubp statistics**) may be displayed as 0. **Workaround**: Use the serial console on the temporary base unit or use telnet/SSH to view the correct QoS UBP statistics.
ERS495900-44	SPBM L2VSN Stacking: SPBM MAC addresses on an MLT are not correctly displayed after disabling/enabling the MLT. The traffic is not affected.
ERS495900-64	SLA Mon: DSCP is reset to zero while performing NTR tests on CVLAN.
ERS495900-89	EDM: Option to map VLANs in MSTP to MSTIs is not available.
ERS495900-301	Issuing a **show interface config** command from an SSH session does not display proper output and the cursor blocks when the terminal length is set to 0.
ERS495900-265	Adding classifier with meter to an existing set is not allowed even if resources are available.
ERS495900-628	CFM Integration with IP Shortcut: EDM does not support L2 Ping IP and L2 Traceroute IP.
ERS495900-672	EDM: Changing QoS if-group on all ports is not possible (action is done only partially on some ports and errors are displayed.
ERS495900-832	CPU stays at 100% and traffic fluctuates for 125 to 150 seconds after the second NNI added on the DUT where the MC source is connected (MC traffic for 1024 groups in 256 VLANs).
ERS495900-1061	UBP GRIP 15329 and re-architecture: When UBP clients with 128 classifiers are added or removed, the following log message is generated even if the filter is removed from the port. "Unable to delete UBP filter set on interface."
ERS495900–1285	TDR test was not able to detect polarity when cross over cables are used.
ERS495900-1300	When setting a port as NNI, the switch does not display a warning message stating that it is recommended to remove the NNI ports from non-SPB VLANs or automatically remove the NNI interfaces from non-SPB VLANs
ERS495900-1359	SPBM EAP: When SPBM is enabled, EAP clients will not get authenticated if an invalid RADIUS Assigned VLAN is received from RADIUS Server.
ERS495900-1440	EDM: In the Globals tab (path: Configuration ->IS-IS -> IS-IS), when only IpSourceAddressType is set, IpSourceAddress is set to a random IP address. This can be avoided by setting IpSourceAddressType and IpSourceAddress together.
ERS495900-1460	EDM: There is inconsistency between CLI and EDM output for **show flash history** command.
ERS495900-1853	EDM: Option to default the port FA Message authentication key is not available in the ports tab (path: **Configuration** > **Edit** > **Fabric Attach**). **Workaround**: Use CLI to default the Authentication Key.

Table continues…

Issue number	Description
ERS495900-2142	SNMP trap is not sent when Link State Tracking upstream port is down and the unit is in power off state. SNMP trap is sent when LST upstream port is up after the unit is powered on and bsLstInterfaceStatusChanged log message is added to the log list.
ERS495900-2202	Port mirroring VLAN: Control packets are mirrored on NNI interface even when the VLAN parameter from the configured instance is different.
ERS495900-2391	EDM: Option to select Multicast VLAN Registration (MVR) application does not appear in the path **Configuration-** > **Edit** > **File System** > **Ascii Config Script Files**.

Workaround: Leave the Application field empty rather than using Select All in the dialog box. This is to ensure ASCII configuration contains MVR settings. |
| ERS495900-2455 | Incorrect log message appears while moving NEAP clients to another VLAN. |
| ERS495900-2527 | Storm Control: Sampling works poorly with minimum poll interval (default value), ports are blocked or unblocked even if the rate is constant and always under the high watermark.

Workaround: If high accuracy is required it is recommended to increase the "Poll interval" value. If small "Poll interval" is needed the values for High/Low watermarks should be adjusted to compensate for an error of +- 10 to 20 percent. |
| ERS495900-2538 | When using PuTTY as an SSH client configured with 1 minute rekeying, SSH secured TCP remote Syslog session is unstable after running SNMP walk. The secured tunnels do not re-open and SSH session rekey does not happen every minute.

Workaround: Configure SSH client's session rekey parameter to an interval of at least 5 minutes. |
| ERS495900-2711 | SFP Port Led: EDM shows green when actual front panel light is amber for a 1 GB SFP module in 10 GB SFP+ port. |
| ERS495900-2713 | If both In-band and Out-of-band management addresses are configured with RADIUS use-management-ip enabled, the source IP address in RADIUS packets sent by the switch are associated with the interface through which the packets are sent. If the RADIUS server is reachable through both interfaces, it is not always predictable which one will be selected for the source IP. If the source IP address is not known in the RADIUS server configuration, request packets are dropped.

Workaround: Configure the RADIUS server to allow both addresses. Both addresses must be added as RADIUS clients. |
| ERS495900-2772 | EDM: Error returned when viewing USB file list from EDM and the USB contains a big number of files.

If a query of USB device using EDM or AFO returns error "The request timed out! The connection with the device may be lost or the device may be down".

EDM/AFO utilize SNMP to retrieve the USB file structure, if the USB device is very full or has a complex file structure the SNMP response may timeout. A USB memory device with fewer files or less complex file structure will respond quicker, preventing the timeout condition. |

Table continues…

Issue number	Description
ERS495900-2889	Console: bcmLINK.0 appears on console after closing all the interfaces.
	This error might be seen intermittently. It can be safely ignored.
ERS495900-2933	EAP track all MACs :eap users in Held state not tracked after failing authentication because of UBP with high security.
	show eap summary command counts only authenticated EAP clients. For EAP clients in other states, double check with **show eap sessions eap** command.
ERS495900-2983 ERS495900-2982	Support COA in FA Mode: VLANs created by CoA Request are not deleted when stack transitions to standalone or when BU failover occurs with the FA client connected on BU.
	Failover scenarios, such as removing a unit from the stack, stack transition to standalone or vice-versa may result in not removing autocreated VLANs even if it has no members.
ERS495900-2987	EDM: If the next hop displayed in EDM for routes learned through IP Shortcuts is 127.x.x.x, it means it is an IP Shortcut next hop over the SPBM cloud.
	Workaround: Use CLI to display next hops.
ERS495900-3052	Many error messages are displayed when trying to enable storm control on ports with rate limiting settings. This is only a display issue.
ERS495900–3059	SPBM Multicast: not all multicast traffic recovers after flushing igmp on source in a scenario with non-spbm device connected to BEB
	This is reproducible only after the groups are flushed multiple times. The traffic recovers after a period of time.
ERS495900–3097	UBP: Unable to correctly install UBP if DHCP Snooping and ARP Inspection are enabled (SPB environment).
	Workaround: The dhcp-snooping should be enabled on the initial vlan, before trying to authenticate the clients.
ERS495900-3177	PVLAN: Inconsistency with legacy VLAN, if configcontrol is Automatic user is not permitted to move isolated port from one PVLAN to another without removing it from the first PVLAN.
ERS495900-3212	EDM: Inconsistency between EDM and EDM Offbox regarding Radius or TACACS authentication for serial or Web/Telnet.
ERS495900–3234	When using OpenSSL to sign subject certificates, the policy should be set to policy_loose in openssl.cnf file.
ERS495900–3239	Serious logging displayed: "Used stack size of task <taskname> is (2147483647%)".
	This is only a display issue and can be ignored.
ERS495900-3256	IPSC with route-maps: Set-metric option does not work when redistributing routes into ISIS.
ERS495900-3299	Static Mroute for PIM: Direct route between devices do not take precedence over the static-mroute configured between devices.

Table continues…

Issue number	Description
	`show port statistics` on a port does not increment filtered packets on the ERS 59100 Series.
ERS495900-3353	Radius: Inconsistency between Global Radius and Radius used by EAP/Neap concerning the mgmt ip address used to send Radius messages while authenticating eap/neap clients. When only the global Radius server is used for authenticating eap or neap users both out-of-band and in-band management addresses are used as source for sending Radius messages by the switch. The address that is used depends on the routing table. If the route to reach Radius server uses out-of-band configuration than the out-of-band address is used; otherwise, the in-band management address is used. When different servers are configured for eap and neap authentication only the in-band address is used as source for the radius messages sent to the server.
ERS495900-3540	QoS blocks or individual policies having system-elements combined with other system elements or l2/ip elements may not work on even stacks (in full ring). **Workaround:** Combine the elements information into one system-element, or use l2/ip elements to create qos blocks and policies.
ERS495900-3514	IGMP with Roaming Multicast Source with SPB enabled currently does not work.
ERS495900-3262	Device does not send as expected the second ESP packet when AES-CTR encryption is used. To recover from this state, select 3DES or AES-CBC encryption. **Workaround**: Use 3DES or AES-CBC encryption instead of AES-CTR. If AES-CTR is required, set a very short lifetime for the IPsec SAs. For example: Lifetime-Sec: 2 / Lifetime-Byte: 100.
ERS495900-3978	MLD Snooping: traffic not received after the base unit rejoins stack as a non-base unit. **Workaround:** To recover from this state, issue the following command: `(config)#ipv6 mld flush stream`.
ERS495900-4104	When more than 4 multicast clients are interested in the same multicast stream, PIM-SM might display only the first 4 output interfaces (OIFs) in the multicast routing table. This is only a display issue.
ERS495900-4119	MLD groups are not erased on querier side when Done is sent. On a setup where the Querier is connected to a remote device B, with the same MLD v1 enabled VLAN and MLD proxy as the device A where the client is attached, when the ipv6 multicast Client sends Done, the group is not flushed on the device B the querier is connected to. It is flushed on device A where the client is connected.
ERS495900-4125	IP Shortcuts Multicast: The switch does not forward the first packet from a multicast stream when IP Shortcuts is enabled on switch.
ERS495900-4131	MLT/DMLT/LAG Dyn VLAN Changes: Trying to change VLAN membership of a single (tagged) LAG port from EDM or EDM Offbox has no effect on the initial port or the other LAG ports. **Workaround:** Use CLI interface instead.

Table continues…

Issue number	Description
ERS495900-4139	Port Driver: After disable Toggle Do-POST tests, some connected interfaces are down. **Workaround:** Do not disable POST tests. ✱ **Note:** This issue exists for the ERS5928MTS-UPWR device only.
ERS495900-4438	EDM: Users can't connect on switch via secure EDM using Chrome version 59 or newer. Problem description: Starting with version 59, Chrome reports the self-signed certificate issued by ERS family as having bad format and will fail to connect via secure EDM. **Workaround 1:** Use Digital Certificates signed by an external Certificate Authority. **Workaround 2:** Use Firefox (v54 or older), IE (v11 or older), Edge (v20 or older) or Chrome (v58 or older).
ERS495900-4501	QoS traffic profile sets using IPv6 egress filters cannot be applied if IPv4 egress filter set is created before IPv6 egress filter set. **Workaround 1:** Create only one traffic profile set using IPv4 and IPv6 egress filters in different blocks.
ERS495900-4542	802.1p field is not updated for an SPBM enabled VLAN when tagged traffic is sent on that port.
ERS495900-4833	SPB traffic over MLT might be affected on a stack when running in TBU mode, if all the MLT links are configured on the former BaseUnit.
ERS495900-4866	CLI commands using `lldp vendor-specific avaya` will fail using ASCII or manual configuration. The commands are changed to `lldp vendor-specific`. Old ASCII configs must be changed removing "avaya" from the CLI commands.
ERS495900-5031	COM+ : Configuration Backup and Restore cannot be performed from COM+/EFO using SSH due to a "Session negotiation failure". The SSH session failure is occurring because SSH server on switch side does not accept negotiation with diffie-hellman-group1-sha1 key exchange algorithm used by COM+. This algorithm is considered weak and was removed starting with Release 7.5. This is a known COM+ limitation and COMNG-237 will track this issue on the COM+ side. To recover from this state, use CLI commands from switch. **Workaround**: Keep telnet access enabled on the switch so COM+ can use a telnet session for configuration backup/restore or use CLI commands from switch.
ERS495900-5248	With IP routing enabled and no configured mgmt routes the switch will forward packets with the SA of OOB interface out IB interface (mgmt VLAN). **Workaround**: Add an OOB management route and packets will egress on the OOB interface correctly.

Table continues…

Issue number	Description
ERS495900-5273	UBP re-architecture: Filter appears to be installed when it should not be and the system log displays the error wrongly as "Unable to apply pre-defined UBP filter set to new user". This applies to user based policy classifiers that cannot be placed in the same precedence without being declared as double-wide. **Workaround**: Specify double-wide parameter from the beginning.
ERS495900-5288	UBP re-architecture: Best effort mode (default mode) does not work for double-wide classifiers. The policy fails to install with the error message "Unable to apply pre-defined UBP filter set to new user". This applies to user based policy classifiers that cannot be placed in the same precedence without being declared as double-wide. **Workaround**: Specify the extra double-wide parameter explicitly (do not rely on default) and avoid the issue altogether.
ERS495900-5376	When NTP is used for the system clock source, CLI timestamp on a stack unit is not synchronized with the device clock if that unit is rebooted. **Workaround**: On the impacted unit, use the `clock sync-rtc-with-ntp enable` command then bounce NTP with `no ntp`/ `ntp`.
ERS495900-5413	STP port learning is changed to disabled on non-default MSTI on BU after stack to standalone transition. **Workaround**: Reintegrate that unit back in the original stack.
ERS495900-5472	Intermittent: LLDP neighbors are not consistent between the units of the stack after stack reboot. **Workaround**: Bounce the link with LLDP neighbor not seen on BU.
ERS495900-5507	FA WAP connection authentication status is not correctly displayed in the output of the command: `show fa elements`, for EAP enabled ports. **Workaround**: Use `show fa assignment` and `show vlan dynamic` to verify that the assignments are properly created for the port.
ERS495900-5594	When you use BOOTP to automatically assign an IP address or DNS, the switch does not configure the DNS and the domain name. **Workaround**: Use DHCP instead.

Limitations and considerations

The following table lists known limitations and considerations for ERS 4900 and 5900 Series.

Item	Description
1	Some terminal programs can cause the Console Interface to crash if you enter a RADIUS secret containing the character "k". The issue has been reproduced using Tera Term Pro (version 2.3), as well as Minicom (version 2.1) on a Linux system.
2	Avoid using MAC security on a trunk (MLT).

Table continues…

Item	Description
3	Failed attempts to log in (using TACACS+ authentication and accounting) are not stored in the accounting file.
4	When switches are in Multiple Spanning Tree Protocol (MSTP) mode and connected using a trunk (MLT), and at least one MSTI is configured, the switch can return an incorrect STPG root if you change the mode to STPG and reset the switches.
	MSTP is the default spanning tree mode. When using the switch with SPB enabled, MSTP will not converge if used in the same MSTP region with switches that are not running SPB. This is not an issue if all VLANs are in the common and internal spanning tree (CIST).
5	While downloading the image file, you may receive the following error message: "Error reading image file."
	WORKAROUND: Typically, this issue can be resolved by simply restarting the image download. If this does not resolve the issue, you should try an alternate method to download the image to the switch (that is, the Web Interface).
6	The IPFIX sampling data rate cannot be changed because of a related hardware limitation.
7	Demo License to enable OSPF, ECMP, VRRP, and IPFIX is for a period of 60 days. The trial license expires at the end of the 60 day period and the features are disabled. The system sends traps advising of license expiration.
	Demo license expiry traps:
	• Five days prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 5 day(s).
	• One day prior to demo license expiry: bsnTrialLicenseExpiration: Trial license 1 will expire in 1 day(s).
	• At termination of demo license: bsnTrialLicenseExpiration: Trial license 1 has expired.
8	Do not enable IP Source Guard on trunk ports.
9	Non-existent VLAN Mapping for MSTI: EDM/SNMP support for VLAN Mapping for MSTI is not available.

10	You cannot enable MAC Security on LACP enabled ports. The following message displays:
	 `%Cannot modify settings`
	 `%MAC Security status cannot be modified. Disable LACP first.`

11	Rate Limiting: When you have the following scenario: 1. rate-limiting is performed at 10% (or by setting any percent value threshold) 2. the speed ratio between the inbound port and the client port is 10:1 (for example 10Gbps inbound link and 1Gbps client port link) 3. inbound broadcast or multicast traffic throughput on the inbound link is more than 10% link-rate speed

Table continues…

Item	Description
	then the client port will receive 0.1 * [inbound traffic rate] and not the expected 1Gbps broadcast or multicast traffic.
	Example:
	• inbound port link rate = 10Gbps , client outbound link rate = 1Gbps , rate limiting set to both at 10%
	• inbound traffic rate = 3Gbps broadcast traffic
	The actual client traffic received rate = 333Mbps and not the expected 1Gbps
12	In a stack configuration, SSHC configuration options are only available from the base unit
13	When you manually create an LLDP MED network policy, LLDP checks that the specified VLAN ID corresponds to a voice VLAN created inside the VLAN application. If the VLAN is not a voice VLAN or the VLAN does not exist, the switch displays a warning message. The switch creates the policy even if the VLAN is not voice enabled or does not exist. The switch may display one of the following messages:
	`% Policy will be set on port x with vlan-id of a non-existent vlan y`
	`% Policy will be set on port x member of the non-voice vlan y`
14	If you configure a stack of three or more units in Both Directions, (the stack is cabled in a non-ring configuration and the missing cable is between two non-base units) there will be no temporary base unit election in case the base unit fails. In this scenario, the stack will break and the base unit cannot be replaced and its CFG image will not be mirrored. In addition, the base unit is not present in the AUR cache, so the base unit will not be ready for replacement, and its MAC address cannot be displayed or removed.
15	In a ring stack, of four or more units, if rebooting or powering off a unit that is not directly connected to the base unit, the stack will be configured in Both Directions configuration (the stack is cabled in a non-ring configuration and the missing cable is between two non base units). In this scenario there will be no temporary base unit election in case the base unit fails. If the base unit fails, the stack will break, so the base unit cannot be replaced, and its CFG image will not be mirrored. In this case the base unit is not present in the AUR cache, so the base unit will not be ready for replacement, and its MAC address cannot be displayed or removed, as long as the stack remains in this state.
16	The area ID 0.0.0.0 is created by default and it is reserved for the backbone area.
	Error message is displayed when you create area ID 0.0.0.0 on the switch using CLI or EDM. For example, the following error message is displayed on CLI when the command area 0.0.0.0 is entered:
	`% Cannot modify settings% Can't delete or modify backbone area`
17	In order for EAP to work with SPBM configurations, all VLANs used by EAP should be SPB VLANs (C-VLANs), including initial VLANs, Guest VLAN, Fail Open VLAN, VoIP VLANs, RADIUS Assigned VLANs, and ADAC Voice VLANs (in the case where ADAC authentication is used).

Table continues…

Item	Description
18	The CLI command, `show stack-cable-info` is not available in ERS 4900 Series. Information about the stack cables cannot be viewed.
19	Starting with Release 7.2, DHCP relay is disabled by default.
20	Stack Monitor: Because the Syslog task uses UDP sockets for remote logging, the message may not reach the remote logging server.

VLACP issue

In some situations, when you use VLACP the switches remove a link from service due to variations in the arrival time of VLACP messages (VLACP PDUs) from the far end. The issue can exist between the ERS 5900 Series or ERS 4900 Series models and ERS 8300 and ERS 8600 Series models when the system runs short timers with a default timeout interval of 3 time-outs or less. The switches maintain a rolling history of the last 3 received VLACP PDUs (by default) and calculate the time variance across and between these VLACP messages.

SOLUTION: Increase the VLACP timeout-scale value to 3 or more.

Filter Resource Consumption

Applications consume filter resources, which are a combination of masks and filters, also known as rules.

A filter specifies the bit pattern to match.

A mask specifies the bit position to match and the evaluation precedence of the filters.

To enable some applications, for example Port Mirroring and IGMP, a set number of masks and filters are required.

The following table summarizes the applications that require mask and filter resources.

Table 13: Application mask and filter resource requirements

Application	Category	Masks required	Filters required
Broadcast ARP and ARP Inspection	Non QoS	1	1[a]
DHCP Relay or DHCP Snooping	Non QoS	1	4[a]
QoS (default untrusted policy)	QoS	2	2[a]

Table continues…

Application	Category	Masks required	Filters required
QoS (DAPP with status tracking)	QoS	1	1[a]
QoS (Auto QoS)	QoS	1	4[a]
Port Mirroring (MAC based, xrxytx)	Non QoS	1	2[a]
EAP Authetication (EAPoL packet filter)	Non QoS	1	2[a]
IPFIX	Non QoS	1	1[a]
ADAC	Non QoS	1	1[a]
RIP	Non QoS	1	1[a]
UDP Broadcast	Non QoS	1	1[a]
VRRP	Non QoS	1	1[a]
OSPF	Non QoS	1	1[a]
Content Based Forwarding	Non QoS	1	up to 16[a]
IP Source Guard	Non QoS	1	11[a]
PIM	Non QoS	1	2[a]
SPB	Non QoS	1	1[a]
SPB - DHCP	Non QoS	1	6[b]
SPB - CFM	Non QoS	2	2[a]
IGMP	Non QoS	up to 2	1[c]
MLD	Non QoS	up to 2	1[c]
FHS	Non QoS	1	24[b]
IPv6	Non QoS	1	1[a]
IPv6 over SPBM (when IPv6 Forwarding is enabled)	Non QoS	up to 3	1[a]
Private VLAN	Non QoS	1	1[b]
Notes: **a**: number of filters required per port **b**: number of total filters **c**: number of filters required per VLAN enabled plus one common filter per mask (i.e. 256 VLANs enabled require two masks with 256 filters on first mask and two filters on second mask)			

On the switch, the resources are shared across groups of ports. For each group of ports, 16 masks are available, with 256 filters available for each mask. By default, the system consumes one mask with one filter per port for ARP. This leaves 15 masks available, each with 256 filters for QoS and other non QoS applications to configure dynamically. In SPBM mode one more mask is used by default leaving 14 masks available.

You can use the `show qos diag` command to assess the current filter resource usage for each port on the switches.

The `show qos diag` command displays the number of QoS masks and filters and non QoS masks and filters consumed on each port. You can determine whether an application that requires filter resources can be enabled on a port by verifying that the number of available masks and filters meets the mask and filter requirements of the application.

On the switch, you can count the unused masks to determine the number of available masks for a port by using the output of the `show qos diag` command. The switches share resources across a group of ports. The filters used by QoS or non QoS applications on a port for a specific mask determine the available filters for that mask for all ports from that group.

On the switch, you can determine the number of filters available for a mask from a group of ports by adding the total number of QoS and non QoS filters in use and subtracting that number from 256. If the number of filters in use for a mask equals 256, you cannot use that mask on other ports from the same group.

★ **Note:**

Maximum eight precedences can be used with meter for QoS policies or Non-QoS applications. Using `show qos diag` command, you can view total number of precedences (from 16 to 1) and check the QoS and Non-QoS meters used. By default, ARP uses meters on precedence 16. If the other seven precedences are using meters (QoS and Non-QoS) then no other precedence can be used with meter (QoS and Non-QoS) .

Example - IP Source Guard on an switch port

On the switch, you need 1 mask and 11 filters to enable IP Source Guard on a port. When you view the `show qos diag` command output you see that port 5 is currently using a total of 4 masks. IP Source Guard uses the next available mask and, from the command output, you can see that there are 256 filters available for mask 14. So you can enable IP Source Guard.

Flow Control

The default value for flow control is asymmetric/asymm-pause-frame (forced settings / auto-negotiation advertisement).

Example

Disabling flow control when auto-negotiation is enabled:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface ethernet 7-8
Switch(config-if)#auto-negotiation-advertisements port 7 1000-full
Switch(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- -----------------------------------------------------------
7                               1000Full
8    10Full        100Full       1000Full          AsymmPause
```

```
Switch(config-if)#show interfaces 7-8
              Status                       Auto                          Flow
Port Trunk  Admin   Oper  Link  LinkTrap  Negotiation  Speed    Duplex  Control
---- -----  ------- ----  ----  --------  -----------  -------- ------  -------
7           Enable  Down  Down  Enabled   Custom
8           Enable  Down  Down  Enabled   Enabled
```

Enabling asymmetric flow control when auto-negotiation is enabled:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface ethernet 7-8
Switch(config-if)#$iation-advertisements port 7 1000-full asymm-pause-frame
Switch(config-if)#show auto-negotiation-advertisements port 7-8
Port Autonegotiation Advertised Capabilities
---- ------------------------------------------------------------------
7                                   1000Full          AsymmPause
8    10Full          100Full        1000Full          AsymmPause
Switch(config-if)#show interfaces 7-8
              Status                       Auto                          Flow
Port Trunk  Admin   Oper  Link  LinkTrap  Negotiation  Speed    Duplex  Control
---- -----  ------- ----  ----  --------  -----------  -------- ------  -------
7           Enable  Down  Down  Enabled   Custom
8           Enable  Down  Down  Enabled   Enabled
```

Disabling flow control when auto-negotiation is disabled:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 7-8
Switch(config-if)#duplex port 7-8 full
Switch(config-if)#flowcontrol port 7-8 disable
Switch(config-if)#show interfaces 7-8
              Status           Auto                     Flow
Port Trunk Admin  Oper  Link  Negotiation  Speed  Duplex Control
---- ----- ------ ----  ----  -----------  -----  ------ -------
7          Enable Up    Up    Disabled     1000Mbps Full Disable
8          Enable Up    Up    Disabled     1000Mbps Full Disable
```

Enabling asymmetric flow control when auto-negotiation is disabled:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface ethernet 7-8
Switch(config-if)#flowcontrol port 7-8 asymmetric
Switch(config-if)#show interfaces 7-8
              Status           Auto                     Flow
Port Trunk Admin  Oper  Link  Negotiation  Speed  Duplex Control
---- ----- ------ ----  ----  -----------  -----  ------ -------
7          Enable Up    Up    Disabled     1000Mbps Full Asymm
8          Enable Up    Up    Disabled     1000Mbps Full Asymm
```