6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

ADVANCE WITH US

Customer Release Notes

Ethernet Routing Switch 4900 and 5900 Series

Software Release 7.9.0
June 2021

INTRODUCTION:

This document provides specific information for version 7.9.0 of agent software for the Ethernet Routing Switch 4900 and 5900 Series (All models).

The purpose of this version is to address customer feature requests and internally found software issues.

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE

If diagnostic upgrade is needed, extract the diagnostic image `radiag_xxxx.bin` file from the `Diag_xxxx.zip` archive.

PLATFORMS SUPPORTED

Ethernet Routing Switch 4900 and 5900 Series (All models)

NOTES FOR UPGRADE

Please see "Release Notes for Ethernet Routing Switch 4900 and 5900 Series, Release 7.8", available at https://www.extremenetworks.com/documentation for details on how to upgrade your Switch.

FILE NAMES FOR THIS RELEASE

Ethernet Routing Switch 4900 Series

File Name	Module or File Type	File Size (bytes)
4900_790003s.img	Secure runtime image	20546484
Diag_7504.zip	Diagnostic software	7470411
Ethernet_Routing_Switch_Ranger_MIBs_7.9.0.zip	MIB Definition File archive	1737318
ers5000v780_HELP_EDM.zip	EDM Help file zip	2090545
5900_poe_v15011.bin	POE firmware	40960

Ethernet Routing Switch 5900 Series

File Name	Module or File Type	File Size (bytes)
5900_790003s.img	Secure runtime image	21164548
Diag_7504.zip	Diagnostic software	7470411
Ethernet_Routing_Switch_Ranger_MIBs_7.9.0.zip	MIB Definition File archive	1905924
ers5000v780_HELP_EDM.zip	EDM Help file zip	2090545
5900_poe_v15011.bin	POE firmware	40960

COMPATIBILITY

This software release is managed with Enterprise Device Manager (EDM), which is integrated into the agent software.

CHANGES IN THIS RELEASE

New Features in This Release

RFC 5997 RADIUS Status-Server reachability method

- Prior to this release, ERS RADIUS reachability methods are either periodic pings or dummy access requests
- This release introduced support for a dedicated RADIUS request, Status-Server, with code 12 and a Message-Authenticator field, which is defined in RFC 5997
- The Server checks the message authenticator hash and if correct, replies with Access-Accept and possibly extra information about the server

CLI commands

New CLI option was added for existing command:

```
ERS(config)#radius reachability mode use-status-server
```

```
            ERS(config)#radius reachability mode ?
            use-icmp Enable RADIUS server reachability using ICMP
            use-radius Enable RADIUS server reachability using RADIUS requests
            use-status-server Enable RADIUS server reachability using RADIUS
            Status-Server requests
```

- The existing logic for RADIUS reachability (retries, timeout etc) is kept, only the packets/transaction are different
- “`show radius-server`” will print the current timers until next check and reachability status:

```
            ERS(config)#show radius-server
            RADIUS Global Server
            -------------------------------------------------------------
            Primary Host : 10.3.38.43
            Secondary Host : 0.0.0.0
            Port : 1812
            Time-out : 10
            Key : ***************
            Radius Accounting : Disabled
            Radius Accounting Port : 1813
            Radius Retry Limit : 3
            Current Status : Reachable via Primary
            Time Until Next Check : 50

            (config)#show radius reachability
            **********************************************************************
            Command Execution Time: 1970-01-01 00:51:23 GMT+00:00
            **********************************************************************
            RADIUS reachability: USE STATUS-SERVER
            RADIUS reachability timeout: 10
            RADIUS reachability retry: 3
            RADIUS reachability bad timer: 60
            RADIUS reachability good timer: 180
```

New Features in This Release

RFC 5746 SSL Secure Renegotiation for EDM

- Interleaved handshake used with certificate authentication
- Legacy SSL Renegotiation as per RFC 5246 is not secure
- RFC 5746 adds an extension to the Client/Server Hello called “renegotiation_info”. TLS maintains new state values to validate the previously finished handshake
- Can be enabled from the browser (in Firefox for example, set *security.ssl.require_safe_negotiation*” to True)
- Mitigates against current man-in-the-middle attacks
- No new CLI commands are included, it’s just just the Mocana capability that is activated

New Features in This Release

Management session IP TCP Keepalive

This mechanism checks the connected TCP sockets (Telnet/SSH sessions) and determine whether the connection is still up and running or if it has broken. TCP keepalive probes (sent every second) provide a method to detect unresponsive peers and remove dead sockets. By default, the feature is Disabled.

TCP Keepalive parameters, like “interval” and “retries” are configurable via CLI and their role is to determine when the invalid TCP connection is closed. The connection is considered not valid after “retries” probes were sent, at “interval” seconds between them and there is no answer from the other peer.

CLI commands:

#ip tcp-keepalive {enable|interval|retries}

```
ERS(config)#ip tcp-keepalive ?
enable Enable tcp keepalive
interval TCP keepalive interval timer in seconds.
retries TCP keepalive retries number.

ERS(config)#ip tcp-keepalive enable

ERS(config)#ip tcp-keepalive retries ?
  <1-50>  Number of unack probes.
ERS(config)#ip tcp-keepalive retries 10

ERS(config)#ip tcp-keepalive interval ?
  <1-600>  Seconds
ERS(config)#ip tcp-keepalive interval 8
```

#show ip tcp-keepalive

```
ERS(config)#show ip tcp-keepalive
****************************************************************************
Command Execution Time: 1970-01-01 04:23:19 GMT+00:00
****************************************************************************
IP TCP Keepalive parameters
------ --------- ----------
Enable: Yes
Interval timer: 8 sec
Retries number: 10
```

New Features in This Release

TLS-min-version configurable

This feature allows to configure the minimum TLS version for web-server as either TLS version 1.1 or TLS version 1.2.

Configuring TLS-min-version using CLI
Use the following procedure to set the TLS-min-version as either TLS version 1.1 or TLS version 1.2.
The default TLS-min-version is TLS version 1.2.

1. Enter Global Configuration mode:
   enable
   configure terminal
2. At the command prompt, enter the following command:
   web-server {tls-min-ver tlsv11|tlsv12}
3. Verify the configuration:
   show web-server

Example

```
#web-server {tls-min-version tlsv11|tlsv12}
```

```
      (config)#web-server tls-min-version ?
      tlsv11 Set the TLS version to 1.1
      tlsv12 Set the TLS version to 1.2

      (config)#web-server tls-min-version tlsv12

      (config)#show web-server
      *****************************************************************************
      Command Execution Time: 1970-01-01 04:45:55 GMT+00:00
      *****************************************************************************
      WEB Access: Enabled
      TLS-minimum-version : TLSv12
      WEB IP List Access Control: Enabled
      Allowed Source IP Address Allowed Source Mask
      ------------------------- -------------------
      1 0.0.0.0 0.0.0.0
      2 255.255.255.255 255.255.255.255
```

Old Features Removed from This Release
None.

Problems Resolved in This Release	
ERS495900-5962	Reboot of stack leads to port disabled in MLT on boot because ports have different settings
ERS495900-5971	STP_NVCFG_VLAN_STPGID parameter error, vIdx = 4094 Message Continuously Scrolls On Console
ERS495900-5972	Fan speed changes result in higher temperatures in some environments
ERS495900-5977	Logging sort-reverse does not show the current log on unit 1

Problems Resolved in This Release	
ERS495900-5983	ZTP+: Continuos memory leak when device is left in ZTP+ Pending Edit state
ERS495900-5987	sflow uses the configured address when it sends its sflow packets
CVE-2016-20009	Vulnerability found against VxWorks code For more information, please visit VN-2021-461 – “NAME:WRECK” (CVE-2016-20009)

KNOWN LIMITATIONS:

None.

For other previously known issues, please refer to the product release notes and technical documentation available from the Extreme Networks Support web site at: www.extremenetworks.com/support/.

DOCUMENTATION CORRECTIONS

None.

TROUBLESHOOTING

As good practices of help for troubleshooting various issues, we recommend:

- configuring the device to use the Simple Network Time Protocol to synchronize the device clock;
- setting a remote logging server to capture all level logs, including informational ones. (#logging remote level informational).

GLOBAL SUPPORT:

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.

Legal Notice

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

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

Trademarks

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks