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

Customer Release Notes

Ethernet Routing Switch 3600 Series

Software Release 6.5.0
December 2020

INTRODUCTION:

This document provides specific information for version 6.5.0 of agent software for the Ethernet Routing Switch 3600 (All models).

The purpose of this version is to address customer and internally found software issues. This version of software also includes a few new features and feature enhancements as described in the New Features in This Release section of this document.

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

None.

PLATFORMS SUPPORTED

Ethernet Routing Switch 3600 (All models)

NOTES FOR UPGRADE

Please see "Configuring Systems on Ethernet Routing Switch 3600 Series", NN47213–506 available at https://documentation.extremenetworks.com/ERS_Series/ERS3600

FILE NAMES FOR THIS RELEASE

File Name	Module or File Type	File Size (bytes)
3600_6100_diags.bin	Diagnostic software	7,096,948
ers3600_650027s.img	SSH runtime image	16,444,180
ers3600v630_HELP_EDM.zip	EDM Help file zip	1,678,595
Ethernet_Routing_Switch_36xx_MIBs_6.5.0.zip	MIB definition files	1,683,951

VERSION OF PREVIOUS RELEASE

Software Version 6.4.2

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

Dynamic User Based Policies (UBP)

When a device is authenticated based 802.1X (EAP) or the source MAC address (Non-EAP), the RADIUS Access-Accept packet contains the specific attributes for the user. The existing User Based Policy attribute will be extended to support new values that will enable it to be created on the switch dynamically if it does not already exist.

Previously, the UBP had to be created on the switch:

```
3650GTS-PWR+(config)#qos ubp classifier name PrinterACL addr-type ipv4 src-ip
192.168.0.1/32 drop-action disable eval-order 1

3650GTS-PWR+(config)#qos ubp classifier name PrinterACL drop-action enable
eval-order 2

3650GTS-PWR+(config)#qos ubp set name PrinterACL set-priority 1 track-
statistics individual
```

The RADIUS server could specify the filter for the user via the UBP VSA (Vendor Specific Attribute), defined with code 110, as a String, under Vendor ID 562. Its current format is to specify either “UROL” or “UGRP” at the beginning of the RADIUS attribute so that the switch knows it received the UBP Name or its Group. Note that Group is purely cosmetic, it is the name that is used to identify the UBP created on the switch that must be installed on the client port.

In order to dynamically create the UBP, we must specify one or more Classifier statements and one Set statement. We will use “ACL” and “SET” at the start. The format of the statements will be identical to the one in CLI, minus the beginning consisting of “*qos ubp classifier/set name <Name>*”. We will still use the UROL string to identify the UBP name, in order to save space and allow longer rules. The maximum rule length will thus be 252, (255 max RADIUS attribute length, minus 3 characters are taken by the type, ACL or SET). So in order to dynamically create the above UBP and apply it for the client device, RADIUS will send the following (using FreeRadius text-based config as an example):

```
UBP = “UROLPrinterACL”,

UBP += “ACLaddr-type ipv4 src-ip 192.168.0.1/32 drop-action disable eval-
order 1”,

UBP += “ACLdrop-action enable eval-order 2”,

UBP += “SETset-priority 1 track-statistics individual”
```

Note that the conversion to RADIUS is easily done from the static configuration. The syntax is specific to FreeRadius, while GUI-based server applications might offer you a dialog box to enter without quotes for each line or commas at the end. That is the FreeRadius syntax for sending multiple instances of the same attribute.

The UBP will not be created if it already exists on the switch. It is stored in NVRAM and is deleted at soft reboot of the entire stack. Hardware reboot of the entire stack or the Base Unit will keep them. Soft reboot of the Base Unit will delete only those which were installed only on Base Unit ports. Hardware reboot of a Non-Base unit will delete them but if that unit itself becomes standalone, it will keep them. Because of their persistence upon hardware reboot, the CoA Request used to modify them also applies to static UBPs for more flexibility.

Once created, a UBP's rules cannot be modified via subsequent RADIUS authentication unless it is deleted dynamically once all clients using it are de-authenticated. It is possible to send a CoA message to delete and re-create a dynamic (or static) UBP with the new rules.

Refer to the "Configuring Quality of Service on Ethernet Routing Switch 4900 and 5900 Series" and "Configuring Security on Ethernet Routing Switch 4900 and 5900 Series" documents from the 7.8.0 release of ERS4900/5900 for more details related to this feature.

Note that 3600 does not have the "QoS Double Wide" enhancement for UBP, so certain combinations of fields in a UBP Classifier will not work. Examples include Source IP + Destination MAC, Destination IP + Source MAC or any combo of IPv6 and MAC. Also, the UBP Filter-on-MAC option introduces the source MAC field of the client to all classifier rules in a UBP and can lead to these unsupported combinations.

Change of Authorization (CoA) for Fabric Attach (FA), CoA Re-Authenticate and CoA for Non-EAP clients

Previously, CoA requests on ERS3600 were only possible for authenticated EAP (802.1X) clients. This release extends support of all CoA attributes from EAP to Non-EAP clients and also supports new attributes to be sent.

For FA, the attributes Fabric-Attach-ISID (VSA code 171 under Vendor ID 562) and Auto-Create-VLAN (code 170) are now supported both for EAP and Non-EAP clients, just as they are on ERS 4900/5900.

Another CoA attribute now supported is Re-Authentication-Request (code 190). If sent, it will re-authenticate the client in question, skipping other attributes. It effectively functions as a third type of CoA and can also be included in Disconnect requests. This is possible both for EAP and Non-EAP clients.

Refer to the "Configuring Quality of Service on Ethernet Routing Switch 4900 and 5900 Series" and "Configuring Security on Ethernet Routing Switch 4900 and 5900 Series" documents from the 7.8.0 release of ERS4900/5900 for more details related to this feature.

TLS-min-version configurable

This feature allows to configure the minimum TLS version for web-server as either TLSv11 or TLSv12.

Configuring TLS-min-version using ACLI
Use the following procedure to set the TLS-min-version as either TLSv11 or TLSv12.
The default TLS-min-version is TLSv12.

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:

```
Switch(config)#show web-server
WEB Access: Enabled
TLS-minimum-version : TLSv12
WEB IP List Access Control: Enabled
Allowed Source IP Address  Allowed Source Mask
-------------------------  ------------------
```

Increase of port mirroring instances to 4

The maximum number of port mirroring instances was increased to four in this release. Depending on the switch model, you can have up to three ingress and one egress or two ingress and two egress instances. ERS 3626GTS or ERS 3626GTS-PWR+ support one egress instance and ERS 3650GTS and ERS 3650GTS-PWR+ support two egress instances (one for ports 1-24 and one for ports 25-48).

The egress modes are: ManyToOneTx, ManyToOneRxTx, Xtx, XrxOrXtx, XrxOrYtx

On the ERS 3626GTS and 3626GTS-PWR+, 2 egress instances don't work at the same time if they are any of the modes Xtx, ManyToOneTx, ManyToOneRxTx, XrxOrXtx, XrxOrYtx.

In a stack of ERS 3626GTS and 3626GTS-PWR+, 2 or more (up to 4) egress instances (Xtx, ManyToOneTx, ManyToOneRxTx, XrxOrXtx, XrxOrYtx) can be active if configured on different units in the stack.

OLD FEATURES REMOVED FROM THIS RELEASE

None.

PROBLEMS RESOLVED IN THIS RELEASE

ERS3600-898 - Switch could reboot with exception when DHCP option 82 packet is processed
ERS3600-905 - NEAP port state change causes re-authentication of all NEAP clients on the switch
ERS3600-871 - RADIUS authenticated NEAP client (no RAV) MAC address not learned if RADIUS assigned VLAN is disabled
ERS3600-888 - A NEAP client using an RAV, in an FA-enabled switch which automatically configures VLAN/I-SID bindings through FA on the uplink towards the switch, fails to do so after a two-unit stack reverts to a standalone unit.
ERS3600-861 - When USB drive removed from switch, CPU elevates to approx 60% and remains until switch is rebooted
ERS3600-851 - Backing up the binary configuration file through TFTP when the SNMP notify is configured could result in the failure of establishing connections through SSH/Telnet/HTTP or in some cases frozen CLI
ERS3600-845 - Intermittently the fans start running at full speed when switching to low power mode. This can happen either at startup when low power mode has been previously configured, or when changing the power mode during normal operation
ERS3600-838 – Non base unit FA uplink in redundant LACP configuration stays disabled following reboot/rejoin of non base unit to stack

KNOWN LIMITATIONS:

ERS3600-556 - EDM: Users can't connect on switch via secure EDM using Chrome version 59.
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: Use Firefox (v74 or older), IE (v11 or older), Edge (v44 or older) or Chrome (v58 or older)

ERS3600-902 - FA with LACP: Non-base-unit (NBU) uplink port, member of a two link LAG, is administratively disabled after stack transitions to standalone and back to stack in an FA Proxy standalone topology
Problem description: After rebooting units 1 and 3, unit 2 goes through a standalone state and when it rejoins the stack, the static tagging set by FA Proxy Standalone on the uplink trunk is not kept for the unit 2 trunk port. This leads to the unit 2 trunk link being shut down because inconsistent VLAN settings are detected across the same trunk links. This is specific to standalone proxy because it uses static VLAN settings applied by FA. Static VLAN settings are compared between ports at stack join.
Recovery procedure: Remove the FA uplink setting (*'no fa uplink'*), re-enable the trunk port (*'no shutdown'*) and set the FA uplink trunk again.

ERS3600-904 - After disabling LACP on an interface with Fabric Attach and shutting it down, FA VLAN membership and VLAN tagging settings are not removed.
Recovery procedure: Reboot the stack.

ERS3600-907 – The *tls-min-ver* is not the same on all units if the value is changed while another unit in the stack is rebooting. There is no operational impact because the TLS-min-version value from Base-unit (BU) is used for the web-server connection.
Recovery procedure: Set the *tls-min-ver* to the desired value from the Base-unit (BU) console and this will propagate the change across all units in the stack.

ERS3600-908 – EDM: EDM doesn't work for ERS3600 when configured with tls-min-ver tlsv11 and a Temporary-base-unit (TBU) had a power cycle.
Recovery procedure: Disable/enable SSL using *no ssl*; *ssl*

ERS3600-910: When a stack of two becomes a standalone switch as a result of the first unit being rebooted or reset, Dynamic User Based Policy (UBP) ACLs are removed from the remaining unit.
Note that this may only be observed if the standalone unit was the previous Non-base-unit (NBU).
Recovery procedure: Disable UBP from QoS with "*qos agent ubp disable*" and re-enable it with "*qos agent ubp low-security-local/high-security-local*". Then re-authenticate the clients.

DOCUMENTATION CORRECTIONS

None.

For other 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/

TROUBLESHOOTING

As good practices of help for troubleshooting various issues, Extreme Networks recommends:

- 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).
- enabling timestamps on all `show` commands using the `cli timestamp enable` command

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.