Ethernet Routing Switch 4800 Series
Software Release 5.10.1

1. Release Summary

Release Date: 06-June-2017
Purpose:

- Software patch release to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4800 (all models).

4. Notes for Upgrade

Please see "Release Notes for Avaya Ethernet Routing Switch 4000 Series Release 5.10.0, NN47205-400", available at http://www.avaya.com/support for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
4000_58003_diag.bin	Diagnostic image	1,934,909
4800_5101039s.img	Agent code image	12,999,672

5. Version of Previous Release

Software Version 5.10.0.

6. Compatibility

This software release is managed with Enterprise Device Manager (EDM).

7. Changes in This Release

New Features in This Release

SPBM ISIS Duplicate System Id/Nickname Detection - ERS454800-2541 - Stack of ERS 4850GTS with a Duplicate Nickname Connected to Existing SPB Domain, Removing it Caused Network Outage

- Enhancements were made to the SPBM code in all products to help prevent network outages caused by duplicate misconfigurations of Nickname and/or System-id.
- The upgraded code has algorithms to detect duplicate system-id and/or Nickname when a node is introduced into the SPB network. When duplication is detected the newly added duplicate system is isolated from the SPBM network by automatically disabling ISIS and the existing SPBM nodes perform clean-up activities for the corruption introduced.
- The recovery procedure is as follows depending on which entity was duplicated:

   a. If both the Nickname and System-id were duplicated, then both need to be made unique and ISIS re-enabled
   b. If only the System-id was duplicated then the Nickname needs to be changed, the System-id needs to be made unique and ISIS re-enabled
   c. If only the Nickname was duplicated then:
      1. Either wait 20 minutes for the LSPs from that System-id to age out of the network, make the Nickname unique and re-enable ISIS
      2. Or if the node needs to be introduced into the network immediately, make the Nickname unique, change the System-id and re-enable ISIS

- To help administrators identify and avoid introducing a duplicate, the existing CLI command “show isis spbm nick-name” was augmented to include all system identifications that need to be unique:
  LSP-id /system-id, Nickname, Virtual BMAC and Host name.
- A CLI consistency check was introduced to prevent a virtual BMAC being erroneously configured equal to the “system-id” or the “IST peer’s system-id”.
- Two new SNMP Traps were introduced to indicate the occurrence of duplicate System-id and/or duplicate Nickname

Jumbo frames

Starting with this release, it is allowed to customize the jumbo frame size, and jumbo frames are enabled by default. A jumbo frame is an Ethernet frame that is larger than 1518 bytes.

Following are benefits of jumbo frames:

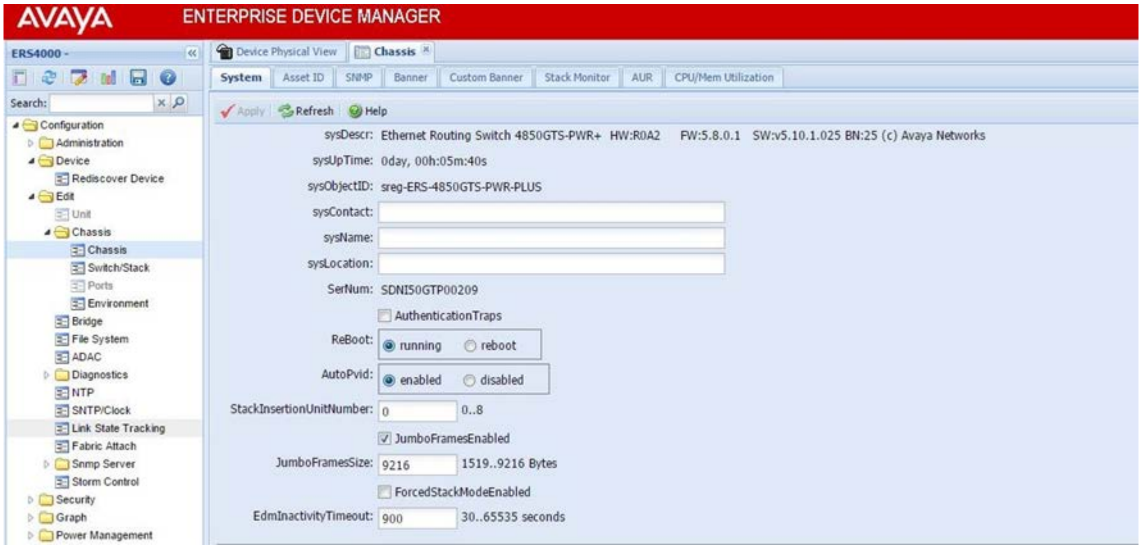
- Each frame carries a larger payload as the header sizes remain the same.
- There are fewer interrupts on the server due to less frames and a smaller CPU load.
- Larger frames provide better buffer utilization and forwarding performance in switches.

The default jumbo frame size is 9216 bytes. You can configure the jumbo frame size between 1519 and 9216 bytes. When jumbo frames are disabled, the maximum untagged frame size is 1518.

Configuring jumbo frames using ACLI:

```
(config)#no jumbo-frames enable
(config)#jumbo-frames enable
(config)#jumbo-frames size ?
  <1519-9216> Jumbo-frames size value
(config)#sh jumbo-frames
Switch Jumbo Frames:
MTU Size:  1518 bytes (1522 bytes for VLAN-tagged frames)
State:     Disabled
```

Configuring jumbo frames from EDM:



sysDescr: Ethernet Routing Switch 4850GTS-PWR+ HW:R0A2 FW:5.8.0.1 SW:v5.10.1.025 BN:25 (c) Avaya Networks
sysUpTime: 0day, 00h:05m:40s
sysObjectID: sreg-ERS-4850GTS-PWR-PLUS
sysContact:
sysName:
sysLocation:
SerNum: SDNI50GTP00209
□ AuthenticationTraps
ReBoot: ● running ○ reboot
AutoPvid: ● enabled ○ disabled
StackInsertionUnitNumber: 0 0..8
☑ JumboFramesEnabled
JumboFramesSize: 9216 1519..9216 Bytes
□ ForcedStackModeEnabled
EdmInactivityTimeout: 900 30..65535 seconds

Improved configurability for Enhanced Secure Mode

- Password Repeating turned off by default;
  The command to turn it on is:
  `password check-repeated enable`
- Password Consecutive turned off by default;
  The command to turn it on is:
  `password check-sequential enable`
- Password Change on first login turned off by default;
  The command to turn it on is:
  `password password-change-on-first-login enable`
- Transitions between Non-ESM and ESM will no longer default the configuration, except for the users settings which have to be defaulted;
- Banner indicates when the switch is in ESM mode.

Default settings for NNI ports

Starting with this release, the following default settings are automatically applied for a NNI port (ERS454800-2632):

- tagAll and filter-untagged-frames are enabled making untagged traffic coming to a NNI port to be discarded;
- PVID value is now 0 for a NNI port.

Changing the port from a NNI to a normal port will apply the previously used PVID; tagAll and filter-untagged-frames settings will remain enabled.

Other changes

RDS replay-protection is turned off by default starting with this release.

```
(config)#show radius dynamic-server replay-protection
RADIUS dynamic server replay protection: Disabled
```

To enable RDS replay-protection the following command can be used:

```
      (config)#radius dynamic-server replay-protection
```

Old Features Removed From This Release

None.

Problems Resolved in This Release

ERS454800-2677 - Several end users connected to the stack not able to reach the network

- False intruder logs inserted when a MAC is migrated between ports with mac-security and auto-learning enabled (issue reported when ports from different units with the same id are used or the same MAC is received on both ports in the same time)
- Counters for the number of Auto learned MAC addresses improper increase when the same Source MAC address reaches two ports at the same time

ERS454800-2616 – EDM displays inaccurate MTU size when Jumbo Frame setting is disabled

ERS454800-2518 - Client cannot reach devices in the assigned VLAN with EAP, SPB and fail-open-VLAN configured

ERS454800-2669 - Web session timeout didn't clear a record for Radius authenticated users, causing access to switch to be denied by Radius server

ERS454800-2670 - Unable to Login to the Switch CLI using SSH Radius Credentials

ERS454800-2531 - Flexoptix LR GBICs are not getting detected after upgrade.

ERS454800-2535 - Power Status Unavailable and port poe status as Deny Low Priority

ERS454800-2509 - ISIS Hello packets from adjacent switch incrementing the InDiscards/Filtered packets counter

ERS454800-2532 – SNTP time can have 1 hour difference when setting of Daylight Saving interval is used

ERS454800-2536 - Incorrect display of syslog message time field on EDM

ERS454800-2671 - ISIS manual area displayed incorrectly both in running config and in show isis manual-area command

ERS454800-2542 - EDM Incorrectly Displays SFP uplink port as Copper port

ERS454800-2555 - List of CVEs found by the NESSUS vulnerability scanner run by the customer - CVE-2008-5161, CVE-2016-2183, CVE-2016-6329, SSH Weak MAC Algorithms Enabled

ERS454800-2510 - CVE-2008-5161 vulnerability & others reported via Nessus Scans

ERS454800-2566 - SSH: number of sessions counter reaching maximum value (20) after connecting/disconnecting SSH sessions and the user can't connect anymore on SSH, Telnet or EDM

ERS454800-2569 - Users set to inactive after default 90 day period despite setting it to 0
Multiple users: User is disabled because a second corrupted timer starts ticking at first SNTP synchronization if inactive-period for that user is different than 0.

ERS454800-2571 - Not able to use character "|" in a password

ERS454800-2577 - The switch responds intermittently to the remote devices if accessed to the routed VLAN interface.

ERS454800-2541 - Stack with a Duplicate Nickname Connected to Existing SPB Domain, Removing it Caused Network Outage

ERS454800-2579 - Selecting ADAC uplink as SPBM is not possible using EDM. The only option EDM offers is to use physical ports.

ERS454800-2580 - Tagged packets seen while mirroring a port which is not tagged

ERS454800-2620 - System-id is set to 0000.0000.0065 on all DUTs in setup if booting in SPBM at default

ERS454800-2675 - FA Client VLANs removed from all ports in MLT on single port down event

ERS454800-2031 - Entries missing from the DHCP snooping table after a while and hence DAI dropping the device from the network

ERS454800-2587 - End-user /client loses network connection with DAI, ARP inspection, IP guard configuration

ERS454800-2622 - Unable to authenticate via radius

ERS454800-2630 - Multicast traffic loss when roaming IP Multicast sender in a non-SPBM environment, IGMP snooping & WLAN scenario

ERS454800-2624 – VLAN configuration loss after upgrade or reboot of the stack when there is a mismatched spanning-tree MSTP configuration for base units versus non base units

ERS454800-2633 - Ports added to VLANs from 4001 and so on are not seen in running configuration

ERS454800-2653 - The first "discovery" multicast packet send by a patient monitor is not forwarded making it unable to communicate with the patient monitoring server

ERS454800-2638 - L2 Ping and L2 Traceroute function not working correctly

ERS454800-2676 - PVID assignment ignored by the switch when assigned via Radius with Fabric Attach configured

ERS454800-2645 – Memory depletion when SNMP polling for USB related OIDs is used

ERS454800-2634 - Storm control feature shuts down port even if unicast traffic is flooded on port with threshold set only for multicast and broadcast

ERS454800-2629 - SPBM Guard rail: AAUR: ISIS disabled because of SYSID and NICKNAME duplicate detection after BU replacement and transition from TBU to BU

ERS454800-2700 – Non base unit software exception in task "tMCMgr" when a duplicate SPBM nickname triggered a spike of inter-module communication in stack

ERS454800-2736 - Intermittent base unit software exception in task "tMCMgr" when the virtual-bmac for an IST pair in the SPB network is changed back fast to a previously used value.

ERS454800-2711 - SSH Auth Retries value overwritten by an invalid value

ERS454800-2127 - SFP+ port not linking at 1Gb speed after upgrading from an image older than 5.7

8. Outstanding Issues

ERS454800-2644 - SPBM: Guard rail: Intermittently, IP shortcuts multicast traffic not recovering after new node with duplicate nickname is added to SPBM cloud.

- Workaround: flush IGMP on the nodes with the multicast source ("ip igmp flush all"). If the traffic does not recover, the ISIS protocol needs to be bounced on the IPSC Multicast receiver nodes.

9. Known Limitations

ERS454800-2636 - SPBM Guard rail: ISIS on SPBM node not disabled when setting an SYS-ID equal to a cluster's SMLT-VIRTUAL-BMAC

- The SPB Duplicate SysID/Nickname Detection mechanism does not cover the scenario when a new SPB node is added to the network and this node's SysID is equal with the SMLT Virtual BMAC of another IST cluster in the SPB domain.

ERS454800-2652 - SPBM Multicast: First packet from a multicast stream is still filtered by an ERS switch with SPBM Multicast and IP multicast shortcuts enabled.

- This limitation is related to ERS454800-2653, which was fixed for IGMP snooping and SPBM multicast (IGMP snooping enabled CVLANs).

ERS454800-2683 - Traffic is filtered when toggling spanning-tree learning on MLTs configured on UNI interfaces (SPBM).

- Workaround: Disable/Enable the MLT will recover the traffic flow.

10. Documentation Corrections

None.

For other known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support .

11. Troubleshooting

As good practices of help for troubleshooting various issues, AVAYA 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).

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Avaya.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web at: http://www.avaya.com/support.