Ethernet Routing Switch 4800 Series
Software Release 5.9.5.052/053

1. Release Summary

Release Date: 16-March-2017
Purpose:

- Software patch release to address customer and internally found software issues.
- **This release replaces release 5.9.5.022/023**

2. Important Notes before Upgrading to This Release

Below note applies only for customers running 5.9.5.022/023

Customers running **5.9.5.022/023** release can encounter the following issue **that should be corrected as described below before upgrading to 5.9.5.052/053. Correcting the issue will prevent it from being inherited after upgrade.**

ERS454800-2619 - System-id is set to 0000.0000.0065 if booting in SPBM mode at default

Problem Description: Enabling SPB on a system with the factory default configuration (a new system) running 5.9.5.022/023 will cause the box to erroneously generate a SysID equal to 0000.0000.0065 instead of the MAC.65 format

- Customers enabling SPB for the first time on a box running 5.9.5.022/023 can encounter this issue.
- This scenario covers the situation when a customer extended his SPB network by adding new nodes running 5.9.5.022/023.
- **Important:** Issue is visible only if the customer is using the self-generated SysID and does not manually configure the SysID!

Problem Detection: Issue 'show isis system-id' on the box will indicate that the SysID is erroneously generated
Example:

```
(config)#sh isis system-id
=======================================
             ISIS System-Id
=======================================
SYSTEM-ID
=======================================
0000.0000.0065
```

Problem Correction:

- Disable ISIS;

- Issue ‘default system-id’ under router isis config. This will correctly generate the SysID with the format MAC.65. Verify this by using ‘show isis system-id’.

```
(config-isis)#default system-id
(config-isis)#show isis system-id
=======================================
            ISIS System-Id
=======================================
SYSTEM-ID
=======================================
fca8.41fe.dc65
```

- Change the SPBM nickname
- Enable ISIS

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 5.9.2, 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_58001_diag.bin	Diagnostic image	1,934,853
4800_595052.img	Agent code image	12,088,216
4800_595053s.img	Agent code image (Secure/SSH)	12,392,604

5. Version of Previous Release

Software Version 5.9.4.

6. Compatibility

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

7. Changes in This Release

New Features in This Release

ERS454800-2523 - Stack of ERS 4850GTS with a Duplicate Nickname Connected to Existing SPB Domain, Removing it Caused Network Outage

- SPBM ISIS Duplicate System Id/Nickname Detection.
  - 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

Old Features Removed From This Release

None.

Problems Resolved in This Release

ERS454800-2155 - 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

ERS454800-2476 - CVE-2008-5161 vulnerability & others reported via Nessus Scans

ERS454800-2487 - 4850GTS: Power Status Unavailable and port poe status as Deny Low Priority

ERS454800-2491 - Display Error On EDM for MTU Size When the Switch Jumbo Frame Setting Is Disabled

ERS454800-2507 - Client do not communicate with EAP and SPB when fail-open-vlan is configured

ERS454800-2508 - 10-15 % CPU spike after software upgrade to 5.9.3

ERS454800-2511 - SNTP time synchronization has 1 hour difference

ERS454800-2597 - Ports added to vlans from 4001 and so on are not seen in Running configuration

ERS454800-2534 - ERS4800: Unable to authenticate via radius

ERS454800-2538 - ERS 4800: EDM Incorrectly Displays SFP uplink port as Copper port

ERS454800-2540 - List of CVEs found by the NESSUS vulnerability scanner run by the customer

ERS454800-2619 - System-id is set to 0000.0000.0065 if booting in SPBM mode at default

8. Outstanding Issues

None.

9. Known Limitations

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

- **Applicability**: Only customers replacing a faulty BU **on an SPBM enabled stack** will be affected by this issue.
- **Description**: After a BU fails, the stack will continue to run with unit 2 acting as TBU. The recommendation is to replace the faulty BU with a new BU. The new unit will enter the stack (and run as NBU) and the stack will continue to run with unit 2 acting as TBU. Rebooting the whole stack will make the new unit act as BU. At this point, ISIS will be disabled on the stack and all traffic will be dropped.
- **Procedure to work around this limitation**:
    - Schedule a MW before rebooting the entire stack
    - Disable ISIS: *(config)#no router isis enable*
    - Copy config to nvram: *(config)#copy config nvram*
    - Reboot the stack so that the newly replaced unit will act as BU
    - Change the SPBM sysid:
        - If using manual configured sysid, change it under *"router isis"* config:
          (config-isis)#system-id …
        - If using self-generated sysid, generate a new one under *"router isis"* config:
          (config-isis)#default system-id
    - Change the SPBM nickname under *"router isis"* config:
      (config-isis)#spbm 1 nick-name …
    - Enable ISIS: *(config)#router isis enable*.
- **Warning**: Customers replacing a faulty BU are advised to schedule a MW as soon as possible after the BU replacement, in order to perform the workaround (including boot the entire stack) and avoid the uncontrolled situation where the stack reboots due to a power outage. **Failure to follow this recommendation can result in traffic outage.**

ERS454800-2556 - 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.

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).