Ethernet Routing Switch 4000 Series
Software Release 5.6.4

1. Release Summary

Release Date: 09-December-2013
Purpose: Software feature pack to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4000 (all models).

4. Notes for Upgrade

Please see "Ethernet Routing Switch 4000 Series, Configuration – System, Software Release 5.6" (available at http://www.avaya.com/support . Click Products, select Ethernet Routing Switch 4000 Series from the A-Z list, then select Documentation > View All Documents) for details on how to upgrade your Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
4000_564026.img	Agent code image	8,724,856
4000_564027s.img	Agent code image (Secure / SSH)	9,121,644

5. Version of Previous Release

Software Version 5.6.3

6. Compatibility

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

7. Changes in This Release

7.1. New Features in This Release

None.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

The switch stopped sending OSPF hello packets after a time period (**WI01088809**)

SNMP walk produced inconsistent results for the field ipAddressifIndex (**WI01140417**)

Data access exception tIdt occurred on the non-base unit (**WI01081161**)

VLACP was not working properly with ethertype 0x8125 (**WI01102848**)

After a successful MAC based authentication, if an EAP supplicant on the same device tried and failed to authenticate, after about 2 minutes the device lost network access. (**WI01105899**)

If a device successfully EAP authenticated and at the same time its MAC is also MAC-based authenticated, the switch will see the device as two separate authenticated clients (**WI01105902**)

Snmpgetnext for ifIndex, ifInOctets and ifType returned incorrect ifInOctets data (**WI01118979**)

Base unit instabilities with 'bcmRX' and 'Unknown Task ID' exceptions were resolved (**WI01140419**)

After a device authentication period expired and a NEAP re-authentication was rejected, the device was still able to access the network (**WI01119845**)

Incorrect user level authentication by TACACS on EDM (**WI01119434**)

Some amount of packet loss occurred for a specific MAC address after MAC-flap when using MLT (**WI01120015**)

Switch did not forward BOOTP requests from different VLANs to the DHCP server (**WI01119751**)

A data access exception in tHttpT_3 was corrected in this release (**WI01112471**)

When the stack was part of a cluster, the management VLAN was unreachable after the peer MAC address was cleared (**WI01140422**)

Mac Security Auto-Learning with MaxMacs reported a violation when there were fewer MACs learned on the port than the configured maximum threshold (**WI01116184**)

After a SW upgrade, "VLAN NVRAM read error" was sometimes displayed (**WI01140423**)

4850GTS-PWR+ TDR testing returned incorrect cable length and also rendered the port inoperable (**WI01122063**)

DHCP traffic caused a switch reset due to DHCP memory leak (**WI01088068**)

When the stack was part of a cluster, a tDRPMgr software exception occurred, causing stack instability (**WI01140425**)

A high CPU utilization by task "tLAC" (67% of the CPU), was resolved in this release (**WI01140428**)

8. Outstanding Issues

None.

9. Known Limitations

A DHCP memory leak issue was addressed in this release that included a change in the DHCP packet header. In code versions prior to 5.6.4, the code added 4 bytes to each egressing DHCP packet without changing the total length value of the packet thus creating a malformed DHCP packet. The 5.6.4 release will now discard these packets when DHCP snooping is enabled.
This fix may create unexpected loss of DHCP packets when the 4k is connected to other ERS switches running prior code. The affected ERS switches are 2500/3500, 4k running code prior to 5.6.4, and 5k running code prior to 6.3.3.
The workaround is to disable DHCP snooping until this fix is propagated to all ERS switches.

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).