Ethernet Routing Switch 5000 Series
Software Release 6.3.5

1. Release Summary

Release Date: May 15, 2015
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 5510/5520/5530/5698TFD (-PWR)/5650TD (-PWR)/5632FD.

4. Notes for Upgrade

Please see “Ethernet Routing Switch 5000 Series, Configuration – System, Software Release 6.3”, available at http://www.avaya.com/support. Click Products, select Ethernet Routing Switch 5000 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)
5xxx_60021_diags.bin	Diagnostic image	2,472,272
5xxx_635024.img	Agent code image	19,240,252
5xxx_634025s.img	Agent code image (SSH)	20,032,180

5. Version of Previous Release

Software Version 6.3.4.

6. Compatibility

This software release is managed with Enterprise Device Manager.

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

wi01218307 – Stack instability after connecting a client with the VRRP IP

wi01173896 - Aastrai760E & 5380 IP Phones were not getting IP addresses from the DHCP server.

Wi01178743 – After upgrading to 6.3.3, DHCP offer packets from the server were being dropped when DHCP snooping was enabled globally,

wi01171284 - Unicast EAPoL packets were not processed properly by the switch

wi01218318 - The switch is now compliant with the TIA 1057 standard where LLDP - MED specific TLV sets transmission from a network device will only begin after an LLDP-MED device has been detected on that port

wi01190400 - LLDP neighbors did not show up on Cisco switch whereas on the Cisco switch ERS information on LLDP neighbor was correctly reflected.

wi01187624 - Not able to ping CLIP IP configured on the device

wi01196686 – MAC address was not learned correctly on VRRP master core stack

wi01218319 - SSL Poodle Vulnerability (NanoSSL) is now addressed in this release

Wi01204175 - Task tL3Mgr was suspended on unit 3 stack of 4 causing connectivity issues

wi01208586 - PC EAP client was authenticated as NEAP phone and traffic was directed to the voice VLAN

wi01210598 - While trying to remove only one Interface of active MLT, the entire VLAN configuration was lost for all VLANs except the highest numbered VLAN

wi01210775 - Default gateway ARP/MAC entry after IP conflict between management and non-management VLANs

wi01204837 - Stacks instability and the console getting hung was observed after upgrading to 6.3.4

wi01189871 – A base unit reboot with data access exception in "tDHCP" task is now resolved

wi01205362 - DHCP snooping table entries did not get purged after device obtained a different IP address

wi01199852 - ARP Packets were discarded with an error of invalid IP/MAC binding dropped on untrusted port

wi01218442 - EAP response was not processed properly after shut/unshut command on a port

wi01209870 - Ping loss due to MAC flapping

wi01212013 - IGMP group depletion is now addressed in this release

wi01217383 - In multihost unicast mode, upon receiving a Disconnect-Request from RADIUS server for an EAP authenticated client, the switch correctly sent out an EAP-Failure to terminate the session and blocked the port and the client's MAC was removed from the authentication list. But the client's MAC remained in the MAC address table

7.4 Problems Resolved in Diagnostic Firmware

wi01206283 - NVRAM issues on multiple 5650TD units

The 6.0.0.21 diagnostic provides a means of checking the degradation level of the various flash regions in the switch. This tool may be accessed through the diagnostic break menu (via pressing ctrl-c shortly after device boots) or from an internal menu within the diagnostic code. Note that the menu characters used to access the test differ between 55xx and 56xx devices.

Error Indications and Displayed Information
If the time is above the warning threshold, the sector address, time, and the letter ‘e’ for erase and ‘p’ for program are displayed:

```
FE020000:  856e
```

If the time is above the fatal error threshold, the sector address, time, and the letter ‘e’ for erase and ‘p’ for program are displayed, followed by ‘–F’ for fatal error:

```
FED40000:  862e-F
```

Time values are in milliseconds for erase and 5usec units for program.
It is also possible to get an error while restoring the flash section to its original content, with a message indicating address and expected and found values:

```
Flash Bad Copy @04000000 Sb=EB  @FDA00000 Is=FF
```

A summary message for each tested flash area indicates PASSED or FAILED for that area:

```
AuditLog:  FDEA0000-FDEDFFFF - PASSED
Config-1:  FFA00000-FFBFFFFF - FAILED
```

Examples of the flash check output for passing and failing flash are shown below.
Passing (from 56xx):

```
Check Flash Erase, Program Times?  (non-destructive)  y/N [ N ]: Y
Wait..
Zeroing     - Wait 27 sec..
Erasing     - Wait 16 sec..
Programming - Wait 11 sec..
```

```
Config-1:  FFA00000-FFBFFFFF - PASSED

Zeroing     - Wait  3 sec..
Erasing     - Wait  2 sec..
Programming - Wait  1 sec..

AuditLog:  FDEA0000-FDEDFFFF - PASSED

Zeroing     - Wait 27 sec..
Erasing     - Wait 16 sec..
Programming - Wait 11 sec..

Config-2:  FDA00000-FDBFFFFF - PASSED
```

Flash Check Output with Warnings and Failures

```
Check Flash Erase, Program Times?  (non-destructive)  Y/N [ N ]: Y
Wait..
Zeroing     - Wait  3 sec..
FDEA0000: 3179e    FDEC0000: 2641e
Erasing     - Wait  2 sec..
FDEA0000: 2896e    FDEC0000: 2701e
Programming - Wait  1 sec..
AuditLog:  FDEA0000-FDEDFFFF - PASSED

Zeroing     - Wait 27 sec..
Erasing     - Wait 16 sec..
FFA00000: 3935e    FFA20000: 4232e-F  FFA40000: 3159e    FFA60000: 4177e-F
FFA80000: 5938e-F  FFAA0000: 3857e    FFAC0000: 3060e    FFAE0000: 5691e-F
FFB00000: 3846e    FFB20000: 4195e-F  FFB40000: 3104e    FFB60000: 3371e
FFB80000: 3881e    FFBA0000: 2571e    FFBC0000: 3392e    FFBE0000: 3651e
Programming - Wait 11 sec..

Config-1:  FFA00000-FFBFFFFF - FAILED

Zeroing     - Wait 27 sec..
FDA00000: 8250e-F  FDA20000: 6497e-F  FDA40000: 7855e-F  FDA60000: 3725e
FDA80000: 3067e    FDAA0000: 8500e-F  FDAC0000: 3117e    FDAE0000: 3639e
FDB00000: 4152e-F  FDB20000: 5467e-F  FDB40000: 5477e-F  FDB60000: 3275e
FDB80000: 3041e    FDBA0000: 3768e    FDBC0000: 2792e    FDBE0000:11881e-F
  Flash Bad Copy @04000000 Sb=EB  @FDA00000 Is=FF

Config-2:  FDA00000-FDBFFFFF - FAILED
```

```
Zeroing     - Wait 27 sec..
FDC00000: 4499e-F  FDC20000: 3486e    FDC40000: 3832e    FDC60000: 3516e
FDC80000: 4222e-F  FDCA0000: 2810e    FDCC0000: 4297e-F  FDCE0000: 3791e
FDD00000: 3730e    FDD20000: 5120e-F  FDD40000: 5409e-F  FDD60000: 3230e
FDD80000: 6416e-F  FDDA0000: 6459e-F  FDDC0000: 3093e    FDDE0000: 4382e-F
  Flash Bad Copy @04000000 Sb=EB  @FDC00000 Is=FF

Config-3:  FDC00000-FDDFFFFF - FAILED

Press any key to continue..
```

8. Outstanding Issues

None.

9. Known Limitations

wi01218442 - EAP response was not processed properly after shut/unshut command on a port
Avaya recommends setting the ports to spanning-tree fast learning mode because if the ports are configured to spanning-tree normal learning mode the PCs may not be authenticated after a shut / no shut command.

wi01222772 - Not all IGMP reports are learned during stress L2 traffic conditions
In the case of hashing conflicts, some loss of service is expected. To circumvent this, the possible workarounds are:
- When the L2 table is empty, the DMAC/DIP of the stream(s) for which service is impaired should be changed;
- With an (almost) full L2 table, it should be investigated whether the unit should have the table full in the first place, and if this is caused by a network problem, fixing the source of the problem should restore multicast service.

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).

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.