Ethernet Routing Switch 5000 Series
Software Release 6.6.2

1. Release Summary

Release Date: July 23, 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 5698TFD(-PWR)/5650TD(-PWR)/5632FD.

4. Notes for Upgrade

Please see "Release Notes for Avaya Ethernet Routing Switch 5000 Series, Software Release 6.6.1", available at http://support.avaya.com 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_662012.img	Agent code image	10,816,068
5xxx_662013s.img	Agent code image (SSH)	11,078,820

5. Version of Previous Release

Software Version 6.6.1.

6. Compatibility

This software release is managed with Enterprise Device Manager.

7. Changes in This Release

7.1. New Features in This Release

Source Interface enhancement for Circuit-less IP feature

The existing Circuit-less IP (CLIP) feature was enhanced with the Source Interface functionality.

Source Interface for management/client applications

You can use a loopback interface IP as the source IP address for some applications that generate packets. This is useful when more than one path exists between the switch sending the packets and the server receiving them. This is possible since traffic filters constructed on the server can take into account only the CLIP address, which is reachable regardless of the path used.
The following applications support the use of a loopback interface IP as source IP address:

- RADIUS
- Syslog
- TACACS
- SNMP traps
- SSH
- TELNET

By default, each application uses the VLAN/management IP according to its normal behavior. To use a CLIP source for a specific application, you must set the required interface using the ip source-interface command.

Setting a CLIP interface as source IP address
Use the following command to set a CLIP interface to be used as source IP address for a specific application.

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Set the CLIP interface to use as source IP address:

```
ip source-interface {radius|syslog|tacacs|snmp-traps|ssh|telnet|all}
{loopback <1-16>}
```

3. To disable the use of a CLIP interface as source IP, enter the following command:

```
no ip source-interface {radius|syslog|tacacs|snmp-traps|ssh|telnet|
all}
OR
default ip source-interface {radius|syslog|tacacs|snmp-traps|ssh|
telnet|all}
```

Displaying source interface configuration
Use the following command to display the source interface configuration.

1. Enter Privileged EXEC mode:

```
enable
```

2. Display source interface configuration:

```
show ip source-interface
```

Configuring source interface from EDM
Use the following procedure to set a loopback interface IP as source IP address for a specific application.

1. From the navigation tree, double-click IP.
2. In the IP tree, click **IP**.
3. In the work area, click the **Source Interface** tab.
4. In the table, double-click the cell under the **InterfaceType** column heading for setting a CLIP interface.

5. Click **loopback**.
6. Repeat steps 4 and 5 as required.
7. In the table, double-click the cell under the **InterfaceId** column heading.
8. Type a numerical value from 1 to 16.
9. Repeat steps 7 and 8 as required.
10. On the toolbar, click **Apply**.

Variable definitions
The following table describes the fields for the Source Interface tab

Field	Description
AppId	- Indicates the source interface for radius, syslog, tacacs, snmp-traps, ssh, and telnet.
InterfaceType	- Indicates the interface type and you can assign loopback for the source interface.
InterfaceId	- Indicates the loopback interface identifier. Values range from 1 to 16.

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

wi01178900 – When ADAC is configured on the switch with one of the MLT ports as an up-link port, upon reboot of the stack, the second MLT port was disabled and the ADAC VLAN membership was removed from that port

wi01179124 - A memory leak in the base unit made it unresponsive and resulting in failover when WoL (wake on Lan) was performed on many clients

wi01226787 - After "snmp-server view xxx +1.3.6.*" a CLI freeze was observed and next session failed to perform 'conf t'

wi01178903 - In a setup with phone terminal and PC (connected through the phone) and EAP used for PC authentication, there was a delay on shutting down and moving traffic between data and guest VLAN if dhcp-snooping was used or if mac-max values for the port were changed.

wi01226791 – Connectivity issues were observed after connecting a client with IP of VRRP (VLAN 600)

wi01183289 – Unsuccessful attempts with ERS5600 running 6.6.1 code to use a semi-colon and comma when configuring the "snmp-server contact" attribute.

wi01226803 – With Aastrai760E & 5380 IP Phones used, these devised were not getting IP address from DHCP server

wi01177887 – A memory depletion problem is now fixed in this release.

wi01171286 - Unicast EAPoL packets were not properly processed by the switch

wi01167272 - 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 wi01193325 – EAP Documentation inconsistency between CLI and EDM.Disable snmp object dot1xAuthTxPeriod

wi01226813 – An EAP interoperability issue with Odyssey (Juniper) supplicant is now resolved.

wi01200287 – The switch action is now more consistent when a supplicant in 'authentication state' sends an eap-start to the authenticator

wi01197724 - SSH, SLAMON, Poodle Vulnerability is now addressed in this release.

wi01226816 - When trying to bring up a PC via EAP authentication, the PC was initially authenticated (machine authenticated) and put in the data VLAN (via RAV) correctly. However after some minutes, the PC's MAC showed up under the list for authenticated NEAP phone and the MAC was added to voice VLAN resulting in the loss of connectivity on the PC.

wi01208274 - Unable to see SNMP port labels when using Solarwinds

wi01210601 - While trying to remove only one Interface of an active MLT, the entire VLAN configuration was lost for all VLANs except the highest numbered VlAN

wi01210776 – Default gateway ARP/MAC entry after IP conflict between management and non-management VLANs

wi01215549 – With ARP-inspection enabled, unicast ARP packets coming from non-base units to the base unit were blocked when the clients were EAP authenticated and put into same RAV

wi01226819 - EAP response was not processed properly after a port is shut/no shut

wi01214506 - IGMPV2, IGMPV3 and IPV6 Multicast Listener reports hitting the CPU causing VLACP link flaps

wi01209871 - Ping loss due to MAC flapping is now fixed in this release.

wi01226820 – The switch EAP behavior is more consistent when transitioning with eap-start, eap success and eap failures

wi01226822 - 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. Although the client's MAC was removed from the authentication list, the client's MAC remained in the MAC address table causing EAP-Request ID not be sent.

wi01221845 - DHCP packets were getting copied to CPU and dropped when the dhcp-relay was enabled globally

wi01190403 - LLDP packets from switch, triggered by fast start, sometimes did not have the network policy TLV.

wi01190401 – The switch LLDP neighbors did not show up on a Cisco device whereas the ERS information was properly displayed on Cisco

wi01226823 - Two UBP filter were applied to a port for the same PC thus blocking user traffic

wi01224174 - 100BASE-FX(LC) AA1419074-E6 was not working in ERS 5632FD

wi01213552 - A "tDHCP" data exception is now fixed in this release

wi01227891 - VlanIds field displays "NaN" instead of VLAN ID after VLAN ID is assigned to a port

wi01228237 - tL3Mgr task sometimes got suspended causing connectivity loss

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

wi01223778 – The CPU utilization reaches 100% when the switch receives IGMP Membership Reports at 600 fps

wi01228515 - EDM Offbox: EAPOL Ports tab does not work

9. Known Limitations

wi01226819 - EAP response is not processed after port is shut / no shut
Avaya recommends setting the ports (where PCs are connected) to spanning-tree learning fast because if the ports are configured to spanning-tree learning normal the PCs may not be authenticated after a shut / no shut

wi01227258 - Approximately 20% of multicast traffic is lost in a PIM setup using 900 groups with multicast traffic

10. Documentation Corrections

wi01189979 - ERS stackable RADIUS documentation needs to provide additional details on how RADIUS reachability works

wi01225892 - RIP:update-timer range for RIP in official documentation is 0– 360 seconds instead of the correct 1– 360

wi01223945 - The transmit-interval parameter needs to be removed from NN47200-501_07_03_Configuration_Security.pdf (Configuring Security on Avaya Ethernet Routing Switch 4000 Series)

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.