# Ethernet Routing Switch 5000 Series
## Software Release 6.1.5

## 1. Release Summary

Release Date: 29-November-2010
Purpose: Software patch release to address customer and internally found software issues.

## 2. Important Notes Before Upgrading to This Release

For customers upgrading from older software versions, a series of upgrades are required to prevent configuration corruption under certain circumstances. Customers upgrading to release 6.0.1 and later versions from software versions prior to Release 6.0, must first upgrade to Release 6.0. Please see “Ethernet Routing Switch 5000 Series Release Notes - Release 6.0” for details on how to upgrade your Ethernet Routing Switch to Release 6.0.

## 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 6.1” (NN47200-500, 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_60009_diags.bin | Diagnostic image | 2,464,972 |
| 5xxx_615014.img | Agent code image | 15,857,860 |
| 5xxx_615015s.img | Agent code image (SSH) | 16,391,864 |

## 5. Version of Previous Release

Software Version 6.1.4

## 6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.2 or later.

## 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 new unit config control feature (NUQC) did not work properly, for instance, when a third unit was added to the stack, it was not correctly configured (**wi00554951**).

A SW exception in the SNMP task that caused a base unit reset is now addressed (**wi00554965**).

An EAP enabled port with User based Policy configured timed out when a PC client went to sleep mode (**wi00554946**).

With LACP configured, some times the standby links were not properly recognized (**wi00600984**).

Some times POE powered IP phones would get the wrong VLAN ID after a stack reset (**wi00686407**).

A security vulnerability to DoS attack has now been fixed (**wi00496350**).

A memory leak that caused stack instability is resolved (**wi00555049**).

The LACP link was not properly removed from the aggregation during a unidirectional link failure (**wi00488102**).

A static route that went inactive, did not recover until a unit reset (**wi00692259**).

A log message was not generated when SLPP disabled a port (**wi00554966**).

The DHCP snooping entries were not properly removed with IP source guard configured (**wi00554988**).

The OutDiscards were wrongly counted as filtered packets (**wi00692574).**

Some times the GBIC info was not displayed on remote units if the GBIC was removed (**wi00555110**).

With EAP enabled ports at default values, the authentication failed on the first attempt (**wi00691680**).

The RIP updates with the destination address of 255.255.255.255 were not recognized (**wi00703945**).

Certain laptops did not work properly with DHCP snooping enabled (**wi00733255**).

Some VRRP Configurations were lost when a non-base unit was powered off and then the base unit was powered off/on (**wi00731771**).

The static ARP entries were removed after clearing ARPs or a power loss (**wi00733359**).

When a SFP was connected to a non-base unit and then removed, it would still show up at its original location (**wi00827484**).

The switch became unresponsive when displaying PIM configuration in “show running-config” **(wi00555038).**

A problem with updating the remote GBIC info caused a SW exception, this issue is now resolved **(wi00824536).**

Some times rebooting the non-base unit caused a broadcast storm on remaining DMLT links **(wi00496279)**

The Dynamic ARP inspection/DHCP snooping blocked certain clients during PXE boot (**wi00692082**).

The Switch becomes unresponsive when displaying PIM configuration (**wi00555038**).

## 8. Issues Resolved in Two Prior Releases

### 8.1 Problems Resolved in 6.1.4

Base unit crashed with data exception in PP task (**Q02119687**)

Invalid binding entries via DHCP engineering menu caused fluctuations in the binding table within seconds. (**Q02143834**).

IGMP reports received from Client with TTL greater than 1 were forwarded and when an ERS 8600 connected to an ERS 5520 received the IGMP report with TTL set any value but 1, it dropped the packet (**Q02141971**).

Problems changing switch passwords (**Q02132910**).

Custom user password profiles were not consistently applied to all units in the stack (**Q02143365**).

TACACS authentication caused an exception (**Q02126732**).

In a Triangular IST/SMLT environment, with ERS 8300 as core and ERS 5520 as edge switches, with ARP Inspection enabled, the edge switches lost Arp entry for its default gateway and thus the gateway was no longer reachable. (**Q02153086**).

Under certain conditions, broadcast traffic looped into the stack could generate a broadcast storm (**Q02162104**).

## 8.2 Problems Resolved in 6.1.3

After upgrading from 6.0 to 6.1, interface names for the non-base unit were lost (**Q02024643, Q02019044**).

Using filters on multicast traffic caused OSPF control packet drops (**Q02103672-01**).

The switch did not properly pass MIB values for port security Auth Status to JDM (**Q02011169-02**).

A specific type of multicast packet on 56xx caused sporadic resets with out logging an exception (**Q02094042**).

When the switch has a route to a network that is learned from an OSPF neighbor and it is equal to one of its downed local interfaces, the switch will hang when that interface is brought up (**Q02075419-02**).

Link doesn't come up when AA1419069-E6 and AA1419070-E6 parts are used on 55xx (**Q01966044-02**).

In an SMLT Full Mesh environment, Traffic was lost when the core stack was powered down/rebooted (**Q02101874**).

With IGMP Snooping enabled, multicast traffic was not properly forwarded on Non-EAP ports (**Q02109643**).

With MAC Security enabled, there were unwarranted writes to NVRAM without any configuration changes (**Q02126138**).

In a RADIUS setup, the switch sends continuous authentication requests to the user “Nortel” (**Q02113703-02, Q02120164**).

The switch returns incorrect value for SNMP request for ifHCOutUcastPkt (**Q02119264**).

Locked Telnet sessions some times caused stack instabilities (**Q01899506-01**).

The 'radius-server password fallback' defaulted to “No” after upgrading to 6.1.2 (**Q02119855**).

Addressed a data exception error: “Data Access Task Name ‘tIdt’ “(**Q02024889-02**).

Support for creating user-defined protocol VLANs with SNAP encapsulation, unable to create a user defined VLAN using AppleTalk PIDs. (**Q02128054**).

Fixed an issue when the IST could not be enabled thru JDM (**Q02126805**).

I2004 Phase 2 set connected to an EAPoL/ADAC configured port of the switch got the “Server Unreachable” error (**Q02135088**).

The link did not come up with BX SFPs between two ERS5530 switches (**Q02116585**).

Base Unit in an ERS5600 Stack running v.6.1.1.016 leaves and then later rejoins the stack while traffic is flowing at 1% bandwidth (**Q02106434**).

Stack instability occurred when adding a unit with traffic flowing (**Q02101619**).

LACP Aggregations were lost after base unit reset (**Q02106430**).

## 9. Known Limitations

None.

## 10. Documentation Corrections

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 .