avaya.com

Ethernet Routing Switch 5000 Series
Software Release 6.2.3

1. Release Summary

Release Date: 11-October-2011
Purpose: Software patch release to address customer and internally found software issues.

2. Important Notes before Upgrading to This Release

Please note that Release Notes for all prior releases 6.2.X are still applicable to this release.

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 6.2” (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_60014_diags.bin	Diagnostic image	2,468,024
5xxx_623010.img	Agent code image	18,432,648
5xxx_623011s.img	Agent code image (SSH)	19,180,252

5. Version of Previous Release

Software Version 6.2.2.

6. Compatibility

This software release is managed with Enterprise Device Manager.

7. Changes in This Release

7.1. New Features in This Release

7.1.1 SLPP Guard

The Switch Clustering implementations on the VSP9000, ERS8800/8600, and ERS5000 provide a Simple Loop Prevention Protocol (SLPP) packet, which operates to help prevent loops from occurring when Switch Clustering is used.

Simple Loop Prevention Protocol (SLPP) Guard can be used to provide additional loop protection to protect wiring closets from incorrect or faulty connections. When SLPP Guard is enabled, this loop prevention mechanism extends into and across multiple wiring closets. If an edge switch configured for SLPP Guard receives an SLPP packet on a port, the feature can immediately disable the port administratively, and generate appropriate log messages and SNMP traps.

New or Changed NNCLI List

To activate SLPP-guard and set the timeout value for a port the following command should be used in interface configuration mode:

```
[no|default] slpp-guard [port <port-list>][enable][timeout {0|<10-65535>}]
```

By default SLPP-guard is disabled and the timeout value is: 60 seconds.

To set the Ethernet type used to detect SLPP packets, the following command should be used in global configuration mode:

```
[default] slpp-guard ethertype [<hex>]
```

The default value for SLPP-guard Ethernet type is: 0x8102.

To obtain the current SLPP-guard settings, the following show command should be used:

```
show slpp-guard [<port-list>]
```

The output for the existing command ‘show interface <port-list> verbose’ was changed to contain info about SLPP-guard.

New or Changed EDM List

EDM interface will be available and will be based on the supported MIB objects listed in next section.

New or Changed SNMP List

Five new objects have been added in rcSlppMib to support SLPP-guard feature:

A scalar object was added in order to give read-write access to the SLPP-guard Ether type parameter:

```
rcSlppGuardEtherType OBJECT-TYPE
        SYNTAX        Integer32(1..'FFFF'h)
        MAX-ACCESS    read-write
        STATUS        current
        DESCRIPTION   "SLPP Guard ether type."
        DEFVAL        { '8102'h }
    ::= { rcSlppScalars 6 }
```

Four objects were added to the already existing rcSlppPortTable table to give access to SLPP-guard parameters configurable or accessible per port:

```
rcSlppPortGuardEnable OBJECT-TYPE
    SYNTAX    TruthValue
    MAX-ACCESS    read-write
    STATUS        current
    DESCRIPTION
        "Flag to indicate if SLPP-guard is enabled on the port."
    ::= { rcSlppPortEntry 8 }

rcSlppPortGuardTimeout OBJECT-TYPE
    SYNTAX    Integer32 (0|10..65535)
    MAX-ACCESS    read-write
    STATUS        current
    DESCRIPTION
        "This value specifies the time period for which a port will remain
        disabled.  When SLPP-guard disables a port, after this time period
        expires, the port will become re-enabled.  A value of 0 means ports
        will never be re-enabled."
    ::= { rcSlppPortEntry 9 }

rcSlppPortGuardStatus OBJECT-TYPE
    SYNTAX        INTEGER {
                      none(1),
                      monitoring(2),
                      blocking(3)
                  }
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
        "The object indicates the SLPP-guard status of a port."
    ::= { rcSlppPortEntry 10 }

rcSlppPortGuardTimerCount OBJECT-TYPE
    SYNTAX        Integer32 (0..65535)
```

```
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION
        "This value specifies the time period that has passed since
         a port was administratively disabled by SLPP-guard.  When this
         object reaches the timeout value (rcSlppPortGuardTimeout),
         the port will become re-enabled."
    ::= { rcSlppPortEntry 11 }
```

One notification object and two notifications were added to support the traps generated by SLPP-guard:

```
rcSlppGuardPortIfIndex OBJECT-TYPE
    SYNTAX        InterfaceIndex
    MAX-ACCESS    accessible-for-notify
    STATUS        current
    DESCRIPTION   "Port on which the SLPP-guard packet is received."
    ::= { rcSlppNotificationObjects 6 }

rcnSlppGuardHoldDownExpired NOTIFICATION-TYPE
    OBJECTS     { rcSlppGuardPortIfIndex }
    STATUS      current
    DESCRIPTION
        "Indicates that the SLPP-guard hold-down timer has expired on a port
        on which SLPP-guard is enabled, and the port has been re-enabled."
    ::= { rcSlppNotifications 4 }

rcnSlppGuardPacketReceived NOTIFICATION-TYPE
    OBJECTS     { rcSlppGuardPortIfIndex }
    STATUS      current
    DESCRIPTION
        "Indicates a SLPP packet has been received on a port on which
        SLPP-guard is enabled. The port has been disabled."
    ::= { rcSlppNotifications 5 }
```

7.2 Old Features Removed From This Release

None.

7.3 Problems Resolved in This Release

Stack upgrade failure from 6.1.4.011s to 6.2.1.003s with a large config file (**wi00882592**)

Loss of IST VLAN on three unit stack after a base unit failure (**wi00885609**)

Some links get disabled after upgrade from 5.1.x to 6.x (**wi00731564**)

IST Peers FDB table were out of sync (**wi00892974**)

"show spanning-tree rstp port role" command displayed 'Oper Status' incorrectly as "disabled" after reboot (**wi00899325**)

After upgrading from 5.1.4 to 6.2.1 EDM routing/IGMP/SNOOPING table expanded indefinitely causing high CPU utilization (**wi00886347**)

Using show running-configuration with 744 VLANs configured, spiked the CPU utilization to 100% for about 12-15 minutes (**wi00907462**)

7.4 Problems Resolved in 6.2.2

5xxx v6.2.2.022/23 enabling IPFIX on ports causes severe performance degradation (**wi00902841**)

Inconsistency between CLI MAC_Security Addr & MAC_Addr_Table (**wi00895275**)

MAC- security MAC-Address table would not clear when disabling port or turning off Mac-Security (**wi00895279**)

After Upgrading from 6.1.1 to 6.2.1, QoS configurations were lost (**wi00838747**)

IST stack Ping recovery takes up to 2 minutes when moving PC (**wi00822726**)

Unicast acknowledge (option 85) changed to multicast acknowledge by DHCP-relay agent (**wi00835596**)

Autonegotiation could not be disabled (**wi00824799**)

EAPOL table entries showed MACs that were aged out (**wi00831481**)

In a stack configuration and after adding ports (from a newly added switch) to an existing VLAN, the stack became unstable (**wi00731609**)

SMLT/FDB tables were not completely synchronized when one of the IST peers was reset (**wi00774925**)

SLPP packets were sent with priority 0 (**wi00555285)**

Not able to set PID of Vlan protocol_userdef to 24577 to 24585 (**wi00848161**)
This fix allows the creation of protocol VLANs using decOtherEther2 protocol PIDs or of using the PIDs for decOtherEther2 protocol VLANs, but not both. The protocol PIDs are 24576 to 24578, 24581 to 24585, 32824.

Incorrect ghost SMLT was created when IST/SMLT stats were displayed (**wi00601469**)

After upgrading from 5.0.5 to 6.2.0, ARPs were not properly generated (**wi00851317**)
This issue was a byproduct of the use of IPFIX on a single port. A fix was implemented for the 5600 HW but, due to HW differences, cannot be implemented for the 5500. A workaround is to use more than one port when using IPFIX. The issue only appeared for the port using IPFIX.

IGMP static member (mrouter port) not forwarding multicast after port down/up (**wi00895225**)

Switch does not learn MAC of format xx:59:xx:xx:xx:xx (**wi00870510**)

Units reset when PIM is enabled (**wi00848276**)

Cannot give an IP address to the switch with the last octet as "0" (**wi00872983**)

IST peer 5632 HD encountered memory leak one hour after upgrade to 6.2.1 (**wi00859217**)

QoS BPDU Blocker settings were not saved on unit 2 after it was rebooted (**wi00872260**)

5600 ports become unresponsive under certain conditions with no packets transmitted out with “drop on no resources” counter incrementing (**wi00854625)**

8. Outstanding Issues

None

9. Known Limitations

When utilizing VRRP as part of the system configuration, it is important to select a correct VRRP Fast Advertisement Interval. As configurations become more complex and have a large number of VRRP instances (or other configuration factors requiring high switch/stack CPU involvement), there may be VRRP bounces due to loss of VRRP communication between Master and Backup switches/stacks within the FAI time interval. To correct this, the FAI may need to be adjusted to a higher value. VRRP bounces are recorded in the switch/stack log file. The default FAI setting is 200 ms.
Note that changing the FAI value will require changing it on both the VRRP Master and Backup switches/stacks **(wi00837115).**

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 .