Ethernet Routing Switch 8600

Readme

Software Release 5.1.5.0

Table of Content

Software Release 5.1.5.0

Release Date: March 04th, 2011

Purpose: Software maintenance release to address externally found customer issues.

Important Notices

Avaya Inc has acquired the Enterprise Solutions business from Nortel. This acquisition includes the ERS 8600 and software described in this document. During the transition of all assets and support infrastructure of products and services to Avaya, Nortel provides certain infrastructure support. As such, you will find the Nortel name, and pointers to Nortel support locations on the Internet being referenced intermixed with Avaya in this document.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled as it enables a software monitoring capability to detect and respond to abnormal software loop conditions. The flag setting can be checked via the command "show config". NOTE: Enabling this flag only takes effect after a reboot and must be saved in the config prior to reboot.

The display should be similar to the following:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potentially false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true which can be accomplished through JDM by following the menu option sequence "Edit Chassis" -> "System Flags" and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled.

To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpset -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0 1

Where x.x.x.x = some IP address associated with the switch.

To view the setting via SNMP use:

snmpget -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

In prior releases, the SNMP timer task could potentially crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it was recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

This is resolved in the 5.1.2.0 release, and the retry value can now be set to values greater than zero. (Q02052753)

Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependent on the presence of the High Performance (HP) Backplane. There is an orderable (and chargeable) upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

NOTE: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

Please refer to the following documents for extra details and as reference material in addition to this Readme:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Readme for Ethernet Routing Switch 8600 Series Switch Software Release 5.0.5.0. Release 5.1.2.0 has equivalent CR fix functionality as Release 5.0.5.0.
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation – Modules, for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)
- Nortel Ethernet Routing Switch 8600 Administration, for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance, for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

NOTE: If upgrading to 5.1.4.0 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 5.1.0.0 or the 5.0.1.0 Release Notes for specific details.

File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file	Deliverables (includes images that also contain encryption software)	pr86_5150.tar.gz	62586189
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5150.img	1141372
Run-time image	Run-time image	p80a5150.img	12793707
Run-time image for R modules	Image for R modules	p80j5150.dld	1615040
Run-time image for RS modules	Run-time image for RS modules	p80k5150.dld	1672064
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5150.img	12895814
3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5150.img	55928
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and DES	p80c5150.aes (this image includes the DES image)	26947
MIB	MIB files	p80a5150.mib	4391086
MIB (zip file)	Zip file containing MIBs	p80a5150.mib.zip	694794
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5150.md5	1358
Runtime image for ATM	Runtime image for the ATM module	p80t5150.dld	906024
Runtime image for POS	Runtime image for the POS module	p80p5150.dld	701771
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	Foq267.xsvf	5320469
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2640266
DPC for R modules	Dual port Controller FPGA firmware	dpc194.xsvf	2642001
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2284578
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4538368

PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	60183
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	78173
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	79891
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	54441
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5140.pkg	5988896
SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5140.img	7528448
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5140.upgrade	1481
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5140.install	2895
SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5140.diag	19460381
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	Wsm1003400_mp.img	845560
WebOS binary	WSM WebOS v10.0.34.0 binary image	Wsm1003400_bin.img	1376256
WebOS boot image	WSM WebOS v10.0.34.0 boot image	Wsm1003400_boot.img	43004
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6200_solaris_sparc.sh	
Microsoft Windows image	Device Manager software image	jdm_6200.exe	
Linux image	Device Manager software image	jdm_6200_linux.sh	
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-ROM	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery Module TPS	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	
	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	

	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	
Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

NOTE: dpc194.xsvf is a new DPC FPGA image for R-modules that can only be used with post 5.1.3GA release. Do not use this DPC FPGA image with pre5.1.3 releases; it may result in R-modules not booting up successfully and one may need RMA to get the card back in good state.

Version of Previous Release

Software Versions **5.1.4,5.1.3, 5.1.2, 5.1.1.1** and **5.0.5.0.**

Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

Changes in This Release

New Features in This Release

ACLI

Old Features Removed From This Release

None.

Problems Resolved in This Release

Platform

- An infrequent, but potentially service impacting timing interaction with auto-negotiation has been identified with 1000BaseT ports on R and RS modules running release 5.1.4.0. This issue may be encountered after link state transitions and could result in significant degradation of link throughput. There is no visible

indication of this problem being present on the switch and is only detected through symptoms of link throughput degradation. This issue has been resolved in release 5.1.5.0.

- MGID exhaustion error messages were displayed in some conditions during Vlan port enable/disable. A logic error in validating MGID allocation during port enable and disable functions has now been corrected. (Wi00732528).
- A table synchronization issue between the master and slave CPU in HA mode has been corrected. Previously there was the potential for some QOS mapping configuration elements to not be sync'd between Master and Slave after HA Failover. (Wi00698375).
- If the rlogin flag is disabled on the system, new TCP connections could still be established (although not active) on the rlogin port. This issue is resolved by blocking TCP from accepting any new connections for rlogin port when the rlogin flag is disabled on the switch. (wi00837637).
- Following a switch reboot, TCP connections would previously be accepted on the HTTP port when the webserver is disabled on the switch. This issue is resolved by blocking TCP from accepting any new connections for http port when webserver is disabled. (wi00816539).
- In case of network running PIM, there is a possibility of memory corruption happening while processing the mroute list. This issue is resolved by ensuring the memory is accessed correctly. (Wi00508085, Wi00508269).
- The configuration command "config/bootconfig/net/mgmt# ip default" now properly sets the net mgmt IP to default ip address. (wi00730804).
- Performing an SNMP walk with XFP's inserted into the switch would result in significant delay in SNMP response. This has been resolved through the implementation of a more efficient query of data elements for the XFP. (wi00518708).
- Since Rel 4.1, when a user defines filter redirection action, the availability of the next hop for the redirect was only validated at configuration time. Code changes have now been implemented to dynamically validate the redirect next hop's availability at run time (WI00834842).
- Deleting a filter containing the action next-hop-redirect without first disabling the filter would no longer results in sending continuous ARP requests. (Wi00834842).
- A scenario was been identified where repeated Packet Memory Refresh events occurring on a specific card could lead to a system outage due exhaustion of the switch fabric memory (reported as "Fab Memory Full" errors). Diagnostic improvements have now been added to avoid the system outage which will take the card offline if 5 Packet Memory Refresh events are encountered within a 50 second window or 15 encountered within a 210 second window. (Wi00731139).

VRRP

- In a square SMLT setup, power-cycle of one VRRP backup node could result in VRRP state transitions in the other VRRP nodes during switch recovery. VRRP advertisements from the lower priority VRRP node are now properly handled in this scenario.(Wi00704114).

DHCP

- In 5.1.x release the number of DHCP Relay instances was reduced to 512. The number of configurable DHCP relay instances has now been increased to 1024 (Wi00716374).
- A DHCP relay agent reply handling failure scenario was identified in the 5.1.4.0 load which has now been addressed. Switches configured to provide DHCP relay agent capabilities with DHCP clients connected via S/MLT may experience hardware error logs indicating an invalid port reference: HW ERROR

portGetPortNum: invalid physical port <portNumber>. On switches without an IST configured this error may also be associated with DHCP reply failures. (wi00852552)

IP Multicast

- In some routed ANYCAST topologies IP multicast traffic was impacted for up to 60 seconds when the primary path was removed due to deletion of the mroute entry. Handling of this scenario has now been corrected. Note that a alternate route must also be present in the alternate routing table in order to minimize routing convergence delay.(WI00564776, Wi00822532).
- MSDP error messages indicating “AS number not found” were seen if the route to the peer is learned through an IGP. In this scenario the local AS number is now used. (Wi00733871).
- In some scenarios, the IGMP querier was not set properly after receiving the query message. This issue has now been resolved.(Wi00730185).
- Multicast traffic was forwarded to CP in some conditions in an IST/SMLT condition. This scenario has been addressed by adding a missing discard entry when the source RPF check fails (Wi00747850).
- IGMP static entries did not work properly after CPU switchover with PIM-SSM. Sequencing interactions between IGMP and PIM-SSM configuration and event handling during CPU switchovers have now been addressed. (Wi00564255).
- An IGMP table corruption scenario has been addressed where the (S,G) entry was not properly updated when multicast source VLAN was taken down. (Wi00564227).

MLT / SMLT

- Fragmented TCP/UDP packets were not hashed through the same MLT link. Fragments with TCP/UDP port info were forwarded based on L4 hashing while the remaining fragments were forwarded based on L3 hashing. All TCP/UDP fragments in a fragmented datagram will now be forwarded based on L3 hashing (Wi00564807).
- An rare scenario was identified where an FDB mismatch was observed during MAC movement between 2 MLTs. A consistency check has now been added to prevent this scenario from occurring. (Wi00601530).
- In SMLT environments, the MAC entries in both the IST peers were previously marked as SMLT Remote TRUE when the IST synchronization occurred on an existing MAC address that had transitioned to a different port. This scenario now properly reflects which switch last updated the MAC address destination.. (Wi00686043).
- In SMLT environments, packets arriving on IST can be sent on SMLT links instead of being blocked. These scenarios have been addressed by discarding the packets from the IST with unknown srcMac, or the dstMac is learned through the same IST. (Wi00852559).

BGP/VRF

- Supermezz image loading failure would previously result in all the VRF VLANs being configured under the global router as the VRF configuration requires a mezz card and would not be activated. To avoid potential service impact, all I/O cards will now be taken offline and configuration loading blocked if configuration elements requiring the mezz card are present and the mezz card failed to load. The CPU will still boot up on the base CPU. (Wi00774936).

VLACP

- The “time-out” scale for VLACP protocol to bring the port down was miscalculated and taking twice the time of configured value. This issue has been rectified. (Wi00728743).

- The periodic timer interval for sending VLACP Hellos was miscalculated and taking twice the time of configured value. This issue has been rectified. (Wi00728749)

Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified outstanding issues.

- A potential packet handling issue has been identified specific to 8648GTR and 8648GTRS cards for configurations where an MLT port is defined on ports 41 through 48. In this scenario, an ingress packet that needs to be flooded within the VLAN could potentially be incorrectly forwarded back the other link in the MLT. This is a pre-existing issue and will be addressed in a future release. (wi00856177)

Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified as operation not to be changed.

Documentation Corrections

None.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web hosted by Nortel: http://www.nortel.com/support

Software Release 5.1.4.0

Release Date: December 03rd, 2010

Purpose: Software maintenance release to address externally found customer issues.

Important Notices

Avaya Inc has acquired the Enterprise Solutions business from Nortel. This acquisition includes the ERS 8600 and software described in this document. During the transition of all assets and support infrastructure of products and services to Avaya, Nortel provides certain infrastructure support. As such, you will find the Nortel name, and pointers to Nortel support locations on the Internet being referenced intermixed with Avaya in this document.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled as it enables a software monitoring capability to detect and respond to abnormal software loop conditions. The flag setting can be checked via the command "show config". NOTE: Enabling this flag only takes effect after a reboot and must be saved in the config prior to reboot.

The display should be similar to the following:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potentially false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true which can be accomplished through JDM by following the menu option sequence "Edit Chassis" -> "System Flags" and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled.

To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpset -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0 1

Where x.x.x.x = some IP address associated with the switch.

To view the setting via SNMP use:

snmpget -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

In prior releases, the SNMP timer task could potentially crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it was recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

This is resolved in the 5.1.2.0 release, and the retry value can now be set to values greater than zero. (Q02052753)

Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependent on the presence of the High Performance (HP) Backplane. There is an orderable (and chargeable) upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

NOTE: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

Please refer to the following documents for extra details and as reference material in addition to this Readme:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Readme for Ethernet Routing Switch 8600 Series Switch Software Release 5.0.5.0. Release 5.1.2.0 has equivalent CR fix functionality as Release 5.0.5.0.
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation – Modules, for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)
- Nortel Ethernet Routing Switch 8600 Administration, for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance, for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

NOTE: If upgrading to 5.1.4.0 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 5.1.0.0 or the 5.0.1.0 Release Notes for specific details.

File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file Tar file of all software	Deliverables (includes images that also contain encryption software)	pr86_5140.tar.gz	62067142
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5140.img	1140094
Run-time image	Run-time image	p80a5140.img	12639154
Run-time image for R modules	Image for R modules	p80j5140.dld	1525240
Run-time image for RS modules	Run-time image for RS modules	p80k5140.dld	1586120
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5140.img	12740040
3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5140.img	55928
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and DES	p80c5140.aes (this image includes the DES image)	26947
MIB	MIB files	p80a5140.mib	4150092
MIB (zip file)	Zip file containing MIBs	p80a5140.mib.zip	674875
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5140.md5	1358
Runtime image for ATM	Runtime image for the ATM module	p80t5140.dld	906024
Runtime image for POS	Runtime image for the POS module	p80p5140.dld	701771
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	Foq267.xsvf	5320469
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2640266
DPC for R modules	Dual port Controller FPGA firmware	dpc194.xsvf	2642001
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2284578
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4538368

PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	60183
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	78173
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	79891
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	54441
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5140.pkg	5988896
SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5140.img	7528448
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5140.upgrade	1481
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5140.install	2895
SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5140.diag	19460381
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	Wsm1003400_mp.img	845560
WebOS binary	WSM WebOS v10.0.34.0 binary image	Wsm1003400_bin.img	1376256
WebOS boot image	WSM WebOS v10.0.34.0 boot image	Wsm1003400_boot.img	43004
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6200_solaris_sparc.sh	239157758
Microsoft Windows image	Device Manager software image	jdm_6200.exe	215146471
Linux image	Device Manager software image	jdm_6200_linux.sh	218350078
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-ROM	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery Module TPS	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	
	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	

	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	
Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

NOTE: dpc194.xsvf is a new DPC FPGA image for R-modules that can only be used with post 5.1.3GA release. Do not use this DPC FPGA image with pre5.1.3 releases; it may result in R-modules not booting up successfully and one may need RMA to get the card back in good state.

Version of Previous Release

Software Versions **5.1.3, 5.1.2, 5.1.1.1** and **5.0.5.0.**

Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

Changes in This Release

New Features in This Release

VLACP HOLD Enhancement

During SMLT node failure scenarios, traffic loss may be observed in certain scaled SMLT configurations with hundreds of SLTs, hundreds of ports and tens of VLANs. The root cause for the traffic loss was that the ERS8600 ports would come up prematurely at the physical layer causing the remote end to start sending traffic toward the ERS8600 that just came up. On the ERS8600 that just rebooted, the communication between the line cards and the CP may take several seconds in such scaled configurations. This resulted in black-holing the traffic arriving on such ports which were physically up but all operational configuration was not yet performed on those ports by the CP. The VLACP SUBTYPE HOLD feature introduces a new VLACP PDU with a new subtype HOLD to help reduce traffic loss in such scenarios.

The goal of this new implementation is to "hold down" all VLACP enabled links for a specific period of time after a reboot. This prevents remote VLACP enabled devices that understand the new VLACP HOLD PDU from sending data to the ERS8600. This will ensure that all VLACP enabled ports on the ERS8600 have had sufficient time to come up with all operational configuration and are ready to receive and forward the ingress traffic.

ERS8600 switches with 5.1.4.0 release are capable of both sending and receiving VLACP HOLD PDUs. Future code revisions of the Baystack switch family will support receipt and processing of VLACP HOLD PDUs, but will not

generate them. Please refer to the applicable product release notes for information regarding product specific software levels required for support of this VLACP enhancement. VLACP is an Avaya proprietary protocol and hence this enhancement in not applicable when connecting to switches from other vendors.

By default, the VLACP HOLD feature will be disabled. The feature is enabled by configuring a positive value for VLACP HOLD Time. The VLACP Hold Time value configured should be selected based on the specific recovery implementation requirements, size and recovery characteristics for your network implementation.

The following new CLI commands are introduced to support:

```
ERS-8610:6/config/vlacp#?

Sub-Context:
Current Context:

    disable
    enable
    info
    hold-time <seconds>


ERS-8610:6/config/vlacp# hold-time ?
value in seconds for hold time
Required parameters:
<seconds>        = vlacp hold time {0..60}
Command syntax:
hold-time <seconds>



ERS-8610:6/config/vlacp# info
                  Vlacp           : enable
                  Vlacp hold-time : 20



ERS-8610:6/show/vlacp# info

================================================================================
```

```
                                Vlacp Global Information
========================================================================
                SystemId: 00:18:b0:5c:a0:00
                    Vlacp           : enable
                    Vlacp hold-time : 20
```

SLPP Enhancement

- **Introduced New EtherType for SLPP PDU:**

  From this release EtherType 0x8104 is replaced by 0x8102 as the default EtherType for SLPP PDUs. SLPP EtherType can still be configured through CLI. Old EtherType 0x8104 will be processed to handle the backward compatibility and upgrade scenarios.

  If the received ether type is old default ether type (0x8104) or current default ether type (0x8102) or currently configured ethertype, then the packet is classified as SLPP PDU.

  The Ethertype can be displayed using following existing CLI command.

  CLI Command:

```
config slpp info
Sub-Context:
Current Context:
                        add :
            etherType (hex) :  0x8102
                  operation :  disabled
              tx-interval   :  500
```

- **Re-Arm per port SLPP PDU Receive Counter issue:**

  Currently per-port SLPP PDU receive counter is never reset, resulting in shutting down links wrongly after months of running when the counter hit the pre-defined limit. This issue has been addressed in this release by resetting the counter if the switch not received expected number of SLPP packets on the port in a certain period of time. This timer is set to 24 hours.

Old Features Removed From This Release

None.

Problems Resolved in This Release

Platform

- 8648GTR and 8648GTRS modules do not negotiate speed and duplex as expected once Customizable Auto-negotiation Advertisements (CANA) has been used on to limit link speed on a port and is subsequently disabled on that port. This issue is resolved (wi00518718)
- When PCAP is enabled and disabled, a control bit in fast path was not cleared correctly. This results in packets received on the port that had been monitored through PCAP being forwarded to the CP incorrectly and potentially cause high CPU utilization. This issue is resolved (wi00564156)
- In prior releases, a timing issue existed in single CPU systems where physical reseating of the CPU card would result in a COP-SW Exception event to be copied to the CPU during switch recovery. To avoid this scenario, the chassis should be power cycled rather than reseating the single CPU. (wi00508448)
- Port based shaper functionality may be disabled in hardware for R/RS modules after a port state change. This issue is resolved (wi00564813)
- SNMP get failed on rcIpfixExporterStatsTable since the length field passed in the OID is not supported by the agent code. This issue is resolved (wi00564237).
- For tagged ports, the QoS queue mapping for Layer 3 packets received on R/RS modules has been corrected to align with E-modules. (wi00518702).
- In prior releases, a very rare scenario exists where the system monitor could potentially incorrectly detect the tTrapD task to be in an infinite loop and initiate recovery action. This issue is resolved (wi00508402).
- If ‘ctrl-C’ is entered at certain points in the boot up sequence the normal boot sequence is aborted and the user is entered into the shell access level of the switch. Sending ‘ctrl-C’ no longer results in user access to the shell level. (wi00675102).
- TFTP packets egressing out of line card port are marked with dscp 0x30, instead of default value. This issue is resolved (wi00564778).
- Executing the 'show sys pluggable-optical-modules info' command no longer results in repeated GBIC inserted messages being generated. (wi00564844).
- PIM mroute flapping could potentially be encountered in networks configured with short timer values for the multicast forward cache timeout. This was only encountered for multicast streams with low data rates in MLT or SMLT topologies and was dependent on which link in the S/MLT the data stream was active. Mroute flapping will no longer be encountered in this scenario. (wi00564358)

CLI/NNCLI

- Executing the ‘show fulltech’ command in NNCLI mode in some configurations would previously lead to unexpectedly high CPU utilization. Optimizations in the execution flow have now been made to minimize the impact of running the show ‘fulltech’. (wi00564789).

IP

- Deletions of VLAN IP did not previously remove the associated IP records in the HW. This could lead to initial connectivity failure if the deleted VLAN IP address were re-used on a different device until an ARP request was issued by the new device. This issue is resolved (wi00564233).
- Routed ipv6 packets were previously dropped when ECMP was configured for IPv4. This issue is resolved (wi00564341).

- When changing the IP address of a VLAN, the previous VLAN IP address would still be advertised to adjacent devices in the topology tables. This resulted in the “show sys topology” command from the adjacent boxes still displaying the previous IP address of the neighbour until a cold boot of the neighbour was performed. This issue is resolved (wi00507312)

DHCP

- DHCP Replies are flooded by Relay Agent instead of sending unicast DHCP reply packet. This issue is resolved (wi00564847).

IP Multicast

- A PIM message received on a specific port was discarded if the egress towards the source is on the same port but different VLAN. This issue is resolved. (wi00564777)
- In multicast over SMLT environments, aggregation switches could never age out certain S,G entries even after the source stopped sending multicast traffic. These stale entries would eventually prevent new entries from being created and could also result in high cpu utilization. This issue is resolved (wi00697430)

MLT / SMLT

- An infrequent scenario has been identified which could result in a CPU reset in the SMLT module during upgrades to 5.1.2.0. This issue is now resolved. (wi00564781).
- The VLAN MAC addresses of an IST peer switch should be learned only via IST links in a normal operating environment. It has been noted in some transient network scenarios that flooded control plane packets may be reflected and result in these addresses being learnt temporarily on SMLT links. SMLT behaviour has now been enhanced to ensure that the IST peer switch VLAN MAC addresses are never learnt on SMLT links. (wi00733200).
- In full mesh SMLT with both LACP and VLACP configured, a higher than expected number of VLACP packets may be forwarded to the CPU. This issue is resolved (wi00564193).
- In ERS 8600 with static-mcast mac configured in a SMLT setup, when the links are disabled/enabled, the error message "rarIsPortInMgid(4095): Invalid Mgid" was seen. This issue is resolved (wi00564321).
- When both aggregation switches in an IST pair are rebooted with SMLT ports disabled in the saved configuration file, the SMLT state will remain “normal” on one of the switches when the SMLT ports are subsequently restored. This issue is resolved (wi00564214).
- In an LACP SMLT, the SMLT status would incorrectly remain in SMLT state if the established LACP aggregation times out on the link without a link failure. This issue is resolved (wi00828218)
- In scenarios where packets generated by an IST peer are reflected back on an SMLT link, the "self" mac address associated with IST peer will no longer be learnt on an SMLT link and will remain properly programmed on the IST MLT. This improves resiliency during transient conditions, such as network convergence, that may result in packet(s) being reflected back to the IST peer on an SMLT link. (wi00733200)

BGP/VRF

- Disable/enable of route-policy configured within a VRF results in a crash because of NULL pointer dereference. This issue is resolved (wi00564289).
- On disabling/re-enabling BGP or doing BGP restart on the VRF, routes updates were not being processed properly in configurations where VRF 1 was not configured. This issue is resolved (wi00564348).

Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified outstanding issues.

- If there is a static route/static default route entry in intermediate switches and ospf is disabled at the multicast source vlan, pim and igmp tables are updated to point to static route/static default route on the intermediate switches. If the static route/static default route direction does not point to the multicast source then multicast traffic will not resume even after enabling ospf at the multicast source vlan. (wi00564227)
- QoS ingress-map configuration entries may not be synchronized properly to the slave CPU in HA-CPU configurations and could potentially be lost on CPU failover. This will be addressed in a future release. (wi00698375)
- The option to reset the switch Out of Band management IP address currently responds with an error indicating the subnet mask is invalid. (wi00730804)
- For SMLT/MLT setup, while L4 hashing is done for Jumbo packets, the last fragment of the packet does not follow the same link as the rest of the fragments. So, there will be chances of fragments reaching the destination out of sequence, which may lead to packet drop at the application layer. (wi00564807)
- In a PIM-SSM network, the configuration of static IGMP entries will not function properly after a CPU failover. The static entry can be recovered by deleting and re-adding the static igmp configuration or disabling and re-enabling the ssm-channel. (Wi00564255)
- In an ANYCAST RP routed square topology, a traffic interruption may be encountered when the link which is a part of the primary routed data path is toggled. The traffic impact will last a maximum of 60 seconds until the next MSDP SA is received. (Wi00564776)
- As part of the enhanced support for virtualization, the total number of DHCP instances supported has been limited to 512 although DHCP relay may be enabled on more than 512 VLANs. (wi00716374)
- VLACP PDU transmission and processing will behave at double the configured timer values in systems with CPU mezz cards. (wi00728743, wi00728749)

Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified as operation not to be changed.

- ERS8600 might have an I/O module COP (I/O co-processor) crash in an HA configuration, if the master/standby SF/CPU reset/reboot interaction is not properly performed. When resetting or rebooting the master, always allow the standby to take over as new master before any additional resets or reboots are attempted. When resetting or rebooting the standby, always make sure the master recognizes the standby is now off-line (5-10 seconds generally) before any additional reset or reboot activity on master is performed. (Q02068289)
- The ERS 1600 will not pass IP packets that contain a received IP header checksum value of 0xffff. The ERS 8600 E/M modules will potentially create and pass such packets. The RFC regarding this area of operation is not 100% clear as to how a product should behave, and what is valid. Therefore it is now recommended to not connect an ERS 1600 running in L3 operation to the egress port of an E/M module of an ERS 8600, to avoid the potential for this situation to be seen. If seen, the application will fail, as the required packet passing will

always be dropped. In these situations, the user must now design their network differently (such as use R/RS modules instead), and not at Avaya's expense. (Q02154661)

- It is not good practice to pull master CPU card in dual CPU environments. The recommended method is to failover to the standby before removing the "old" master CPU. For single CPU systems, or when removing the second CPU in dual CPU system, it is recommended to power cycle as part of the switch recovery.

Documentation Corrections

None.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web hosted by Nortel: http://www.nortel.com/support

Software Release 5.1.3.0

Release Date: August 06th, 2010

Purpose: Software maintenance release to address externally found customer issues.

Important Notices

Avaya Inc has acquired the Enterprise Solutions business from Nortel. This acquisition includes the ERS 8600 and software described in this document. During the transition of all assets and support infrastructure of products and services to Avaya, Nortel provides certain infrastructure support. As such, you will find the Nortel name, and pointers to Nortel support locations on the Internet being referenced intermixed with Avaya in this document.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled as it enables a software monitoring capability to detect and respond to abnormal software loop conditions. The flag setting can be checked via the command "show config". NOTE: Enabling this flag only takes effect after a reboot and must be saved in the config prior to reboot.

The display should be similar to the following:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potentially false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true which can be accomplished through JDM by following the menu option sequence "Edit Chassis" -> "System Flags" and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled.

To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpset -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0 1

Where x.x.x.x = some IP address associated with the switch.

To view the setting via SNMP use:

snmpget -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

In prior releases, the SNMP timer task could potentially crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it was recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

This is now resolved in this release, and the retry value can now be set to values greater than zero. (Q02052753)

Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependant on the presence of the High Performance (HP) Backplane. There is an orderable (and chargeable) upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

NOTE: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

Please refer to the following documents for extra details and as reference material in addition to this Readme:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Readme for Ethernet Routing Switch 8600 Series Switch Software Release 5.0.5.0. Release 5.1.2.0 has equivalent CR fix functionality as Release 5.0.5.0.
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation – Modules, for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)
- Nortel Ethernet Routing Switch 8600 Administration, for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance, for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

NOTE: If upgrading to 5.1.3.0 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 5.1.0.0 or the 5.0.1.0 Release Notes for specific details.

File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file Tar file of all software	Deliverables (includes images that also contain encryption software)	pr86_5130.tar.gz	62054115
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5130.img	1138987
Run-time image	Run-time image	p80a5130.img	12637666
Run-time image for R modules	Image for R modules	p80j5130.dld	1523484
Run-time image for RS modules	Run-time image for RS modules	p80k5130.dld	1581868
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5130.img	12736768
3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5130.img	55928
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and DES	p80c5130.aes (this image includes the DES image)	26947
MIB	MIB files	p80a5130.mib	4149831
MIB (zip file)	Zip file containing MIBs	p80a5130.mib.zip	674828
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5130.md5	1358
Runtime image for ATM	Runtime image for the ATM module	p80t5130.dld	906024
Runtime image for POS	Runtime image for the POS module	p80p5130.dld	701771
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	Foq267.xsvf	5320469
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2640266
DPC for R modules	Dual port Controller FPGA firmware	dpc194.xsvf	2642001
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2284578
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4538368

PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	60183
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	78173
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	79891
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	54441
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5130.pkg	5988896
SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5130.img	7528448
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5130.upgrade	1481
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5130.install	2895
SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5130.diag	19460381
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	Wsm1003400_mp.img	845560
WebOS binary	WSM WebOS v10.0.34.0 binary image	Wsm1003400_bin.img	1376256
WebOS boot image	WSM WebOS v10.0.34.0 boot image	Wsm1003400_boot.img	43004
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6200_solaris_sparc.sh	239157758
Microsoft Windows image	Device Manager software image	jdm_6200.exe	215146471
Linux image	Device Manager software image	jdm_6200_linux.sh	218350078
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-ROM	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery Module TPS	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	
	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	

	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	
Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

NOTE: dpc194.xsvf is a new DPC FPGA image for R-modules that can only be used with 5.1.3GA release. Do not use this DPC FPGA image with pre5.1.3 releases; it may result in R-modules not booting up successfully and one may need RMA to get the card back in good state.

Version of Previous Release

Software Versions **5.1.2, 5.1.1.1** and **5.0.5.0.**

Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

Changes in This Release

New Features in This Release

None.

Old Features Removed From This Release

None.

Problems Resolved in This Release

Switch management

- The command “show ports stats show-all” was previously not displaying all of the associated port statistics information. The ERS 8600 now will display the proper information. (Q02012952-01)
- The egress queue service rates configured in NNCLI mode were previously getting lost after a reboot. The egress queue service rates configured are now retained after a reboot. (Q02116358)
- In NNCLI mode “show qos egress-queue-set <queue-set-id>” command was showing no output. ERS 8600 now displays the proper output on executing this command. (Q02116618)

- Previously initiating a traceroute via JDM to an unknown destination while other ping or traceroute activites were being performed simulatenously from the same switch could potentially lead to system instability. This situation has now been addressed. (Q02137566)

Platform

- In specific scenarios with filters and port mirroring being used simulataneously, the ERS8600 will no longer see an increase in CPU utilization due to packets being sent improperly to CPU. (Q02141867)
- In some specific ACL configurations with default-action specified, the ERS8600 previously blocked certain traffic patterns improperly. The situation has now been addressed. (Q02068243)
- Previously links on an R-module could stay up for 60 seconds when the primary SF/CPU (of a dual non-HA SF/CPU configuration only) was not properly removed (module pulled out without prior master reset or switchover). The ERS 8600 now ensures that the links are brought down immediately when the primary SF/CPU is removed, for this configuration. (Q02102654)
- The radius secret key will now be stored as encrypted in the shadov.txt file. Before upgrading to 5.1.3.0, it is now required of the user to delete the radius secret key and then re-add it after the up-grade is complete to avoid accessibility problem with RADIUS. This situation has already been addressed in v7.0 code release. (Q01881817-03)
- When multiple failovers are performed on an ERS 8600 in HA environments, some R module I/O modules could come back up off-line. This situation is now addressed in the 5.1.3.0 code release but also requires the use of the new updated DPC FPGA image (see File Names section). Associated with this 5.1.3.0 Release, the DPC firmware image must be upgraded for all R-module I/O modules to the dpc194.xsvf firmware image. If the firmware image is not upgraded, the user will receive a warning log message upon any re-boot of 5.1.3.0 code release, warning them that DPC FPGA firmware image is out of revision. (Q02053766-01)
- On E/M module cards, receiving 802.3x pause frames on gigabit Ethernet ports ,could previously result in port level resets. This situation is now addressed. (Q02101087)
- For an ERS 8600 running with 8692 SF/CPU with SuperMezz, the SuperMezz physical LED will now display properly . (Q02102364)
- During boot-up, the potential for 8612XLRS 10Gig port flapping will no longer occur. (Q02138423)
- An error in loading configuration file previously resulted in all of the line cards being disabled. This behavior was added in 5.1 code. This behavior is now changed such that the rest of the correct config will be loaded and all the remaining line cards will not be disabled, but only the line card associated with the improper configuration will be disabled. This situation is different than an “invalid config file, with verify-config flag enabled”, in which case the system will not load the config and will bring up the system with all I/O modules disabled (versus loading the default config). This situation has already been addressed in v7.0 code release. (Q02056382-01)
- A power usage calculation error has been corrected for 8648TXE and 8691SF cards which previously lead to improper warnings being generated in some configurations indicating that the chassis was running on low power. (Q02072016)
- The value of the ingress records was showing improper values via the command show ip mroute-hw resource usage. This has been now been addressed and the proper values for these records are now displayed. (Q02120442)
- The Software power tables embedded in the ERS 8600 were out of sync with the Power Supply Calculator posted via the web. This inconsistency has now been addressed. This situation has already been addressed in v7.0 code release. (Q02020261-01)

RSTP/MSTP

- It had been seen that there was an outage of 30sec in some RSTP setups when one of the root ports was disabled. This situation has now been addressed and the ERS 8600 re-converges within the proper time interval. (Q01984762-02)
- IN RSTP mode, the log file transfer feature was not working properly. This situation has been addressed and the log file transfer feature is now working as expected when RSTP mode is enabled. (Q02101565-01)

IP Unicast

BGP

- In a specific aggregation scenario, when an ERS 8600 forms a neighbour relationship with Cisco, the BGP session will no longer go down due to a malformed AS path. (Q02085844-01)
- During some specific BGP transition scenarios, system instability was previously seen for the ERS 8600. This situation is now addressed. (Q02134841)
- BGP instabilities are no longer observed associated with a HA failover. (Q02135118)
- After an HA failover with a BGP route policy enabled, some BGP routes could be rejected and not re-advertised by the ERS 8600. This situation has been addressed. (Q02136224)

IP Multicast

- ERS 8600 now ensures that when an IP Multicast sender and the receiver are connected to the same ERS 8600, that SPM (Source Path Messages – specific message type within PGM) packets are no longer dropped. This is independent of PGM being enabled or not, as PGM packet flows can function with PIM-SM enabled. (Q02119454)

MLT / SMLT

- ERS8600 will now deterministically (and properly) hash traffic flows for IPVPN traffic on MLT links. (Q02142913)
- MLTs will now come up properly when the LACP Min Link feature is enabled. (Q02034692-02)
- In some rare network events, it is possible to learn the fdb-entry for an IP interface of the peer aggregation in a Switch Cluster on the SMLT associated port instead of the IST_MLT. In this scenario, the fdb-entry will now be properly updated afterward to correctly point to the IST_MLT. (Q02142730)
- CPU high buffer utilization and associated IST instabilities will no longer be observed in specific situations for the ERS 8600. (Q02109963)
- The 8632TXE module will now properly do offline in the scenario where both master and slave CPU's are removed in systems running with smlt-on-single-cp enabled. (Q02123052)

OSPF

- After an upgrade it is now ensured that the OSPF Md5 keys are no longer lost. (Q02127996)

VLACP

- If a mismatching VLACP configuration exists on two ends of a connection associated with a SLT, the SLT will no longer show as SMLT up improperly after a reboot. (Q02119095)

VRRP

- Enabling and then disabling the IST protocol will no longer lead to improper values displayed in the VRRP records. (Q02106080-01)

BFD

- On a ERS8600 running both BGP and BFD, when one tries to enable BGP first and then BFD on the BGP neighbour, the BFD related config can now be set properly. (Q02141063)

Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified outstanding issues.

- For a tagged R/RS module port, the ERS 8600 will improperly not honor the QoS marking of incoming packets that need to also be copied to the CPU, i.e. network control packets. These packets will instead be sent to the default queue for the CPU. This situation only has the potential to create operational issues for situations where the CPU utilization is already abnormally high, which is a situation that always needs looking at to start with. (Q02131463)
- In HA-CPU environments, when the Master CPU card is pulled out and re-inserted, some line cards may lose communication with the master CPU and may have to be re-inserted. Physical removal of the master SF/CPU is not a recommended or supported action. A switchover to secondary CPU is recommended to be performed first. (Q02128408)
- System instability has been reported infrequently during handling of OSPF updates. Analysis of the system data related to this issue indicates a strong correlation to the infrequent memory corruption already addressed in 5.1.2.0 under Q02093533 and Q02106560. A similar intermittent instability has been reported within SNMP which is also currently believed to be linked to the memory corruption addressed in 5.1.2.0. (Q02125441, Q02118856)
- Statistics related to ACE filters for R/RS modules may not increment/decrement properly. When running the “show filter acl statistics port” command, the fields for “the number of packets” and “bytes” may show up as all zeros. This is seen in all 5.1.x, not just 5.1.3.0. (Q02128334)
- In ERS 8600, certain routes may get deleted in the IP routing table on deleting/adding both a route policy and triggering a soft restart of an associated BGP peer. If encountered, this can be recovered by restarting the BGP session to the peer, or disable/enable BGP globally. (Q01976477)
- A very unlikely timing scenario can result in the system monitor falsely detecting tTrapd task in loop. (Q02120700)
- In highly scaled configurations with large number (hundreds) of SLTs and VLANs, one may encounter few seconds of traffic loss upon recovery of an aggregation switch after a reboot.(Q02138421)
- With static multicast MAC configured and no port configured on the static multicast mac, one may notice “HW ERROR rarIsPortInMgid: Invalid Group (4095)!” line in the log file (Q02144094)

- 8648GTR and 8648GTRS modules do not negotiate speed and duplex as expected once Customer Auto-negotiation (CANA) is enabled on these ports. (Q02139324)
- ERS8600 does not recognize ERS4550GT in the CLI topology database (Q02012675).
- In NNCLI mode, with scaled routes (thousands), one may notice that routes are not relearned after they are cleared with clear ip route command (Q02119580)
- PIM join message received on specific port is discarded if the egress towards the source is on the same port but on a different VLAN. In this specific case, multicast traffic may not work as expected (Q02142356)
- In SMLT configurations with both aggregation switches having SMLT ports disabled when the switch comes up after reboot and when the ports are enabled, the MLT type remains norm on one of the switches. Disabling and re-enabling the SMLT port will recover from the problem. (Q02150122)
- In a setup with BGP running on VRFs, on disabling and re-enabling BGP or doing a BGP restart globally or on the BGP neighbor, one may notice that BGP sessions do not bring up routes successfully. Having a vfrf id of 1 with BGP enabled alleviates the problem. (Q02153885)
- In systems with RS modules, when pcap is enabled and then disabled, a particular bit in the hardware in RS modules ends up with an incorrect value. This results in unintended packets hitting the CPU causing high cpu utilization. (Q02160154)
- When using XFPs with RS modules and while performing queries for certain rcPlug MIBs, the switch may experience high cpu utilization and one may notice inconsistancies in related statistics. (Q02138919)
- The commands “config ip forwarding disable” does not work (Q02140861)
- In HA-mode, following a CPU switch-over, IGMP Static entries, if configured, in a PIM-SSM config, will not be active on the new master CPU (Q02141640)
- In Microsoft NLB cluster and layer2 environments, one may not be able to ping the cluster IP from a client if IGMP snooping is enabled and the ingress port on the ERS8600 is a R-module (Q02145862)
- In BGP environments with VRFs, a switch may experience a crash upon disabling and re-enabling a route policy. The problem can be avoided by using vrf id 1 (Q02156040)
- Upon enable and disable of pcap feature on RS modules, one may notice unintended packets reaching the cpu causing high cpu utilization.(Q02160154)
- In a square SMLT with LACP enabled on the SMLT, when one of the aggregation switches is rebooted, SMLT may enter into normal state in one of the aggregation switches in the opposite pair of aggregation switches. Toggling LACP on the affected switch recovers the SMLT. (Q02156133)
- High CPU utilization may be observed on a box running HA with Mezz present and enabled after Primary CP is failed and the Standby CP takes over with the following traffic pattern. The traffic arriving to an end station which is directly connected to the HA box (VRF2) via routing and this end station was disconnected from the network for a while (Q02165596)

Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified as operation not to be changed.

- ERS8600 might have an I/O module COP (I/O co-processor) crash in an HA configuration, if the master/standby SF/CPU reset/reboot interaction is not properly performed. When resetting or rebooting the master, always allow the standby to take over as new master before any additional resets or reboots are attempted. When resetting or rebooting the standby, always make sure the master recognizes the standby is now off-line (5-10 seconds generally) before any additional reset or reboot activity on master is performed. (Q02068289)

- The ERS 1600 will not pass IP packets that contain a received IP header checksum value of 0xffff. The ERS 8600 E/M modules will potentially create and pass such packets. The RFC regarding this area of operation is not 100% clear as to how a product should behave, and what is valid. Therefore it is now recommended to not connect an ERS 1600 running in L3 operation to the egress port of an E/M module of an ERS 8600, to avoid the potential for this situation to be seen. If seen, the application will fail, as the required packet passing will always be dropped. In these situations, the user must now design their network differently (such as use R/RS modules instead), and not at Avaya's expense. (Q02154661)
- It is not good practice to pull master CP card in HA-CPU environments. The recommended way is to failover to the standby before removing the "old" master CP.
- It is not good practice to pull all CP out of the chassis and re-insert them WITHOUT power cycling the box.

Documentation Corrections

None.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web hosted by Nortel: http://www.nortel.com/support

Ethernet Routing Switch 8600

Readme

Software Release 5.1.2.0

Table of Content

Software Release 5.1.2.0

Release Date: April 16, 2010

Purpose: Software maintenance release to address externally found customer issues.

Important Notices

Avaya Inc has acquired the Enterprise Solutions business from Nortel. This acquisition includes the ERS 8600 and software described in this document. During the transition of all assets and support infrastructure of products and services to Avaya, Nortel provides certain infrastructure support. As such, you will find the Nortel name, and pointers to Nortel support locations on the Internet being referenced intermixed with Avaya in this document.

NOTE: For those customers who were part of the 5.1.2.0 Controlled Release program, an upgrade to this GA code release is recommended but is not required. The CRs listed in italic in the Problem Resolved section are the CRs changes between the CA release and the final GA release. Upgrading is left as a recommended option to the end user.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled as it enables a software monitoring capability to detect and respond to abnormal software loop conditions. The flag setting can be checked via the command "show config". NOTE: Enabling this flag only takes effect after a reboot and must be saved in the config prior to reboot.

The display should be similar to the following:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potentially false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true which can be accomplished through JDM by following the menu option sequence "Edit Chassis" -> "System Flags" and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled.

To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpset -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0 1

Where x.x.x.x = some IP address associated with the switch.

To view the setting via SNMP use:

snmpget -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

In prior releases, the SNMP timer task could potentially crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it was recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

This is now resolved in this release, and the retry value can now be set to values greater than zero. (Q02052753)

Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependant on the presence of the High Performance (HP) Backplane. There is an orderable (and chargeable) upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

NOTE: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

Please refer to the following documents for extra details and as reference material in addition to this Readme:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Readme for Ethernet Routing Switch 8600 Series Switch Software Release 5.0.5.0. Release 5.1.2.0 has equivalent CR fix functionality as Release 5.0.5.0.
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation – Modules, for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)
- Nortel Ethernet Routing Switch 8600 Administration, for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance, for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

NOTE: If upgrading to 5.1.2.0 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 5.1.0.0 or the 5.0.1.0 Release Notes for specific details.

File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file Tar file of all software	Deliverables (includes images that also contain encryption software)	pr86_5120.tar.gz	62008946
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5120.img	1138842
Run-time image	Run-time image	p80a5120.img	12617368
Run-time image for R modules	Image for R modules	p80j5120.dld	1519012
Run-time image for RS modules	Run-time image for RS modules	p80k5120.dld	1579496
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5120.img	12719925
3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5120.img	55928
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and DES	p80c5120.aes (this image includes the DES image)	26947
MIB	MIB files	p80a5120.mib	4149424
MIB (zip file)	Zip file containing MIBs	p80a5120.mib.zip	674759
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5120.md5	1358
Runtime image for ATM	Runtime image for the ATM module	p80t5120.dld	906024
Runtime image for POS	Runtime image for the POS module	p80p5120.dld	701771
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	foq267.xsvf	5320469
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2640266
DPC for R modules	Dual port Controller FPGA firmware	dpc184.xsvf	2583454

PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2284578
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4538368
PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	60183
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	78173
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	79891
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	54441
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5120.pkg	5988896
SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5120.img	7528448
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5120.upgrade	1481
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5120.install	2895
SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5120.diag	19460381
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	wsm1003400_mp.img	845560
WebOS binary	WSM WebOS v10.0.34.0 binary image	wsm1003400_bin.img	1376256
WebOS boot image	WSM WebOS v10.0.34.0 boot image	wsm1003400_boot.img	43004
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6200_solaris_sparc.sh	239157758
Microsoft Windows image	Device Manager software image	jdm_6200.exe	215146471
Linux image	Device Manager software image	jdm_6200_linux.sh	218350078
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-ROM	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	

Module TPS	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	
	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	
Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

Version of Previous Release

Software Version **5.1.1.1** as well as **5.0.5.0. 5.1.2.0** contains all CRs now implement in **5.0.5.0.**

Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

Changes in This Release

New Features in This Release

None.

Old Features Removed From This Release

None.

Problems Resolved in This Release

Switch management

- The SNMP trap for rcIpBgpPeerLastError will now be sent with a proper byte string length such that the last bye will no longer be lost. This could previously cause operational issues with some SNMP management stations. (Q02092718)
- ERS 8600 will no longer observe system instability associated with configuration changes to switch parameters involving SNMP settings. (Q02094258)

- Previously the ERS 8600 was applying a local Access Policy to IPv6 routed SSH packets. Now the system will route these packets and apply Access Policies to only local destination policy type (SSH, Telnet, HTTP) IPv6 packets. This will no longer cause inappropriate connection issues to remote hosts. (Q02070640-01)
- *SNMP GET/GET NEXT under certain conditions associated with the MAC (FDB) table was previously not working properly. These conditions lead to an issue that NetIQ PVQM would not function properly with an ERS 8600. This is now resolved. (Q02113802)*
- ERS8600 has been modified to now allow proper communication with NetQOS Management Device (generally used for IPFix data collection) via SNMPv3. (Q02049612-01)

Platform

- With both filtering and ingress mirroring enabled on the ERS8600, system instability could be seen under certain traffic conditions. This is now resolved. (Q02078239-01)
- IP fix traffic from the switch to an external collector will no longer be sent with an improper QoS marking of QOS=7, but instead sent with QOS=0, now placing these packets into the proper default egress queue. Previously this traffic could potentially interfere with other system management traffic leading to the potential for system instability when IPFix was enabled. (Q02044640-01)
- High CPU utilization on an I/O module co-processor (therefore R/RS only) will no longer result in a loss of messaging synchronization with the 8692 SF/CPU, which previously could have led to system instability. (Q02085085)
- ERS 8600 will no longer show system instability in while writing to the PCMCIA card with CLI Logging enabled. (Q02006689-01)
- ERS 8600 R and RS module card ports will now initialize multicast and broadcast bandwidth limiting values properly when these features are enabled. (Q02074960)
- *Previously when an 8630GBR experienced SW messaging instability to the CP (COP to CP messaging) that would required a module reset to resolve, the far end port could stay up for 20 seconds, which could lead to a 20 second SMLT blackhole. This was associated with the MAC chip not turning off its laser when the module was reset. This situation is now resolved, and the 20 second SMLT blackhole will no longer be seen. (Q02112285)*
- ERS 8600 will now properly handle IPX packets with a broadcast destination MAC of type RIP or SAP. Previously this could create a potential issue for routing IPX for E/M modules (R/RS modules do not support IPX Routing). (Q01997486-04)
- Packet throughput performance for jumbo frames at line rate has been improved for the 8612XLRS modules. (Q02075673)
- Filter pattern definitions for HTTP packet streams will no longer impact other protocol traffic. (Q02089688)
- Users will now be able to connect to an ERS 8600 using Secure Copy (SCP) with access-level rwa when access-strict true is also configured. Previously SSH worked, but SCP did not. (Q01767930-01)
- ERS 8600 will no longer encounter link flapping upon reboot of an OM1400 edge device running SFFD when connected to 8630GBR ports. Avaya continues to recommend the use of VLACP over SFFD, except in cases where the Avaya (or ex-Nortel) product does not support VLACP, such as the OM1400. (02014236-01)
- ERS8600 will now properly forward DHCP packets with the DHCP-relay agent configured as the VRRP virtual IP when the DHCP request has the broadcast flag set. Avaya best practice recommendation continues to be to configure the DHCP-relay agent IP address as the VLAN physical address and not use the VRRP IP address. (Q02059607-01)

- Reliability of R and RS series line card recovery after CPU resets (normally seen during switch software upgrades) has been improved due to enhancements in SF/CPU to I/O module co-processor message communication and synchronization. (Q02091485/ Q01997485)
- ERS 8600 will no longer silently drop packets when the number of ACEs with debug count enabled is such that system resources are at their maximum, but instead the filters will now all function properly. (Q02045086)
- *A memory corruption scenario has been identified which previously led to intermittent system instability and log messages relating to data manipulations of the rarHashBin data structure in some environments (log messages would contain RAR wording). The underlying cause of the memory corruption leading to the instabilities has now been resolved. (Q02093533, Q02106560)*

RSTP/MSTP

- Enhanced MSTP/RSTP logging information which was previously added in release 4.1.3.0 was not present in any 5.x code. This functionality has now been properly added. Q02053232)
- The VLAN interface on an ERS8600 in RSTP/MSTP mode will no longer be brought up unless a port first becomes active in the VLAN. This matches the existing VLAN interface behaviour in STP mode. (Q02083039)
- Packet loss on an MLT with RSTP enabled will no longer been seen after a CPU reset/switchover with HA mode enabled or after a complete switch re-boot. (Q02003158-01)
- ERS 8600 will properly retain the MLT path-cost configuration over reboots when configured for RSTP/MSTP mode. (Q02048253)
- ERS8600 will now properly show the MSTP CIST port path cost info when "show port info mstp" is executed. (Q02048252)

IP Unicast

UDP

- The configured filter action is now properly observed for ACL's configured to match UDP source and destination port ranges between 32752 and 32767. (Q02076252-01)

Static Routes

- ERS 8600 will no longer encounter system (DRAM) memory exhaustion with DHCP-relay configured on a Layer 2 VLAN or at the port level for a non-brouter port. (Q02076879)

BGP

- ERS 8600 will now properly learn the default routes from eBGP peers even after the failover or toggling of the physical port connection. (Q02094999)

IP Multicast

- ERS 8600 will no longer observe periods of sustained high CPU utilization associated with the forwarding of multicast traffic. (Q02067852)
- ERS 8600 will now properly recover its DVMRP status for an ATM interface when a Port/Fiber Fault occurs, and is then restored. (Q02041428)

MLT / SMLT

- Connectivity to NLB servers single homed to one ERS8600 in an IST pair will now function properly for SMLT connected devices when using an nlb-mode of unicast or with arp multicast-mac-flooding enabled. Configurations using nlb-mode of multicast were not affected. (Q02037778-01)
- *When the lowest member port of an SMLT is in an operationally down state during SMLT recovery, ARP records would previously be programmed incorrectly during the database synchronization and cause connectivity failures until the SMLT port was recovered. ARP records are now properly programmed for this scenario. (Q02124545)*
- SLPP will now disable the correct SMLT port when a loop is detected on an SMLT link where the smlt-id configured is not the same as the mlt-id value configured. (Q02089994)
- On ERS8600, FDB and ARP entries will point correctly to SMLT after IST peer reboots. Previously entries learnt on SMLT ports could very occasionally point incorrectly to the IST. (Q02091486)

RSMLT

- With ICMP redirect enabled on RSMLT peer switches, packets destined to the RSMLT-peer's MAC address will now be forwarded correctly and not dropped as ICMP-redirect packets. (Q02091034)
- In RSMLT environments, ERS8600 will no longer add the RSMLT-peer's MAC address to its Router MAC table. This will result in packets destined to the IP interface of RSMLT-peer to forward properly. (Q02091350)

SLPP

- *Previously SLPP would fail to detect a loop if the port uptime was between 24.8 and 49.7 days. After 49.7 days, and then again at 24.8 days, the same situation would repeat - the faulty state would cycle between working to non-working, back to working, etc. based upon the days time period. This is now resolved. A work-around to this situation previously is either a switch reset/re-boot, or port disable/enable prior to 24.8 days of operation. (Q02113609)*
- For non-routed VLANs, SLPP will now use a source MAC address equal to the Base Mac Address of the ERS8600 plus the ID of the VLAN. This will ensure that received SLPP packets are processed against the correct non-routed VLAN when a loop is present in the network and avoid erroneous warning messages. (Q02081719)

VLACP

- ERS 8600 will now always bring down a port via VLACP within the configured timeout value when its VLACP peer goes down. Previously one end of the link would take an extra timeout cycle before downing the port in some scenarios. (Q02088710)
- In scenarios where a port was taken down by VLACP and then the far end switch is rebooted or VLACP recovered to recover the port, Persistent VLACP port flapping will no longer occur. (Q02088709)
- On E-mode enabled switches in full mesh SMLT topologies, protocol traffic will now flow properly on the second MLT link when the first MLT link is disabled. (Q02089615)

VRRP

- Disabling and re-enabling the IST session on an IST switch pair with VRRP configured between them will no longer result in both switches reporting VRRP master ownership. (Q02104773)

Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified outstanding issues.

- Repeated HA-CPU failovers may result in R-modules going offline. It is recommended to not 'force' repeated HA-CPU failovers. (Q02053766)
- Upgrade of the software from 4.1.x to 5.1.2.0 has been reported to result in configured OSPF Md5 keys being corrupted. For this situation, users with MD5 keys configured on OSPF adjacencies should reconfigure the MD5 keys after the upgrade if this issue is encountered. (Q02127996)
- With the smlt-on-single-CP feature enabled, 8632TXE ports are not taken offline when both the Master CPU and Slave CPU are pulled out. (Q02123052)
- IP Multicast packets of type PGM-SPM will get dropped when the multicast sender and the receiver are connected to the same ERS 8600. At this time such designs to pass this type of traffic require the sender and receiver to be connected to different ERS 8600s. (Q02119454)
- In a triangular SLT setup with VLACP enabled only on the core boxes, if the ERS 8600 is rebooted, the SLT port is not properly taken offline despite VLACP making the ports offline. Such a configuration is not recommended as VLACP should be enabled on both core and edge connected devices. (Q02119095)
- For a tagged R or RS module ports, the ERS 8600 will not properly honor the QoS marking of incoming packets that need to also be copied to CP, i.e. network control packets. These packets will instead be sent to the default queue setting for the port. This situation only has the potential to create operational issues for situations where the CP utilization is already high. (Q02131463)
- ERS 8600 may experience system instability when certain types of vulnerability scans, are run against it. It is suggested that any vulnerability scans be tested first against a lab switch prior to those scans being performed against production usage switches. (Q02110359)
- In ERS8600, links on both R or RS modules currently remain up for 60 seconds after the primary SF/CPU is removed in a non HA mode. Removing the primary SF/CPU is a non-supported action. User should first either boot, reset, or force a switchover to secondary, before removal of the primary SF/CPU. Under these approved mechanism the improper 60 second status will not be seen. This operation will be improved in a future release. Q02102654)
- Intermittently after several card-pull actions, I/O modules and the CP may lose communication and line cards may be restarted by the CP. This operation will be improved in a future release. Repeated card pull/insert operation is not a recommended activity; if performed, the slot should be disabled first. (Q02091483)
- In HA-CPU environments, when master CPU card is pulled out and re-inserted, some line cards may lose communication with the master CPU and may have to be re-inserted. Physical removal of the master SF/CPU is not a recommended or supported action. A switchover to secondary CPU is recommended to be performed first. (Q02128408)
- System instability has been reported infrequently during handling of OSPF updates. Analysis of the system data related to this issue indicates a strong correlation to the infrequent memory corruption addressed under Q02093533 and Q02106560. A similar intermittent instability has been reported within SNMP which is also currently believed to be linked to the memory corruption addressed in 5.1.2.0. (Q02125441, Q02118856)

- In systems 8692 with Supermezz, pulling out and re-inserting line cards may result in instability that may cause traffic loss. (Q02120668)
- Statistics related to ACE filters for R/RS modules may not increment/decrement based on traffic. When running “show filter acl statistics port” command, the fields “the number of packets” and “bytes” may show up as all zeros. This is seen in all 5.1.x. (Q02128334)
- Incorrect values are displayed under the “ingress rec in-use” column while executing the CLI command “show ip mroute-hw record-usage”. This appears to be introduced in 5.1.x code stream. (Q02120442)
- In ERS 8600, certain routes get deleted in the IP routing table on deleting/adding the route policy and triggering a soft restart of the BGP peer. If encountered, this can be recovered by restarting the BGP session to the peer, or disable/enable BGP globally. (Q01976477)

Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified as operation not to be changed.

- ERS8600 might have an I/O module COP (I/O co-processor) crash in an HA configuration, if master/standby SF/CPU reset/reboot interaction is not properly performed. If resetting or rebooting the master, allow the standby to take over as new master before any additional resets or reboots are attempted. When resetting or rebooting the standby, make sure the master recognizes the standby is now off-line (5-10 seconds generally) before any additional reset or reboot activity on master is performed. (Q02068289)
- On upgrading an ERS 8600 from v5.1.2.0 to v7.0.0.0, there can be a corruption seen in the Radius Secret Key. This is because the new encryption/decryption algorithm meant for Radius Secret Key file (added in v7.0.0.0) is not supported in 5.1.2.0. (Q02113877)

Documentation Corrections

None.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Avaya Technical Support on the web hosted by Nortel: http://www.nortel.com/support

AVAYA

NORTEL

Ethernet Routing Switch 8600 Software Release 5.1.1.1

Software Release 5.1.1.1

1. Release Summary

Release Date: October 2009

Purpose: Software maintenance release to address software issues found both in the field and internally.

2. Important Notes before Upgrading to This Release

If upgrading to 5.1.1.1 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 4.1.8.2 Readme or 5.0.1.0 RN for specific details.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled. The flag setting can be checked via the command, show config. The display should be something like:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potentially false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true (requires a reboot to take affect), which can only be accomplished by JDM, Edit Chassis -> System Flags and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled. To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpset -v 1 -c public <ip address> enterprises.2272.1.4.41.0 1

Where <ip address> is an IP address associated with the switch. Change the SNMP community “public” in this example to the SNMP read-write community used on this switch.

To view the setting via SNMP use:

snmpget -v 1 -c public <ip address> enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

REGARDLESS OF SOFTWARE VERSION, the SNMP timer task may crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it is recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

(Q02052753 – the fix for this will be in the future 5.1.2.0 code)

3. Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependant on the presence of the High Performance Backplane. There does exist an upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

Please refer to the following documents for details on the Platforms Supported:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation - Modules Manual for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)

- Nortel Ethernet Routing Switch 8600 Administration Manual for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance Manual for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Note: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

4. Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

5. File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file Tar file of all software	Deliverables (includes images that also contain encryption software)	pr86_5111.tar.gz	61981964
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5111.img	1138336
Run-time image	Run-time image	p80a5111.img	12606645
Run-time image for R modules	Image for R modules	p80j5111.dld	1518464

Run-time image for RS modules	Run-time image for RS modules	p80k5111.dld	1578012
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5111.img	12709219
3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5111.img	55928
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and 3DES	p80c5111.aes (this image includes the 3DES image)	26947
MIB	MIB files	p80a5111.mib	4149308
MIB (zip file)	Zip file containing MIBs	p80a5111.mib.zip	674714
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5111.md5	1358
Runtime image for ATM	Runtime image for the ATM module	p80t5111.dld	906024
Runtime image for POS	Runtime image for the POS module	p80p5111.dld	701771
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	foq267.xsvf	5320469

BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2640266
DPC for R modules	Dual port Controller FPGA firmware	dpc184.xsvf	2583454
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2284578
Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4538368
PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	60183
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	78173
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	79891
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	54441
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5111.pkg	5988896

SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5111.img	7508448
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5111.upgrade	1481
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5111.install	2895
SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5111.diag	19460381
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	wsm1003400_mp.img	845560
WebOS binary	WSM WebOS v10.0.34.0 binary image	wsm1003400_bin.img	1376256
WebOS boot image	WSM WebOS v10.0.34.0 boot image	wsm1003400_boot.img	43004
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6180_solaris_sparc.sh	237137138
Microsoft Windows image	Device Manager software image	jdm_6180.exe	213143936
Linux image	Device Manager software image	jdm_6180_linux.sh	216329458
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	

	ROM		
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery Module TPS	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	
	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	
	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	
Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

6. Version of Previous Release

Software Version **5.1.1.0**

7. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

8. Changes in This Release

New Features in This Release

None.

Old Features Removed From This Release

None.

Problems Resolved in This Release

Switch management

- Network reachability testing via ICMP/ping will no longer show different results when used via either Out of Band connectivity (console or OOB Ethernet port) or when used via an Inband (telnet/SSH, etc.) connection, as was previously seen. (Q02057984-01)

Platform

- Previously certain IST message handling could be delayed by other system functions, thereby potentially causing IST instability (up/down/up). As well, system instability associated with SMLT (IST Peers) in association with high CPU utilization and potentially SLPP operations have both now been resolved. For those who disabled SLPP on their systems/network, SLPP can now be re-enabled with the 5.1.1.1 release. (Q02055292-02/Q02053200/Q02055101/Q02066500)

MSTP

- For an MSTP enabled system, port disable and enable scenarios, where the cistforceport state is disabled on the port, will now be handled properly and in turn OSPF will behave normally. (Q02064812)

IP Unicast

Static Routes

- Static routes usage in a VRF configured system for non-default VRFs (non-VRF 0 usage) will no longer cause a spike in CPU utilization. Now even after reboot all the static routes will remain active and CPU utilization will remain normal. This situation was introduced in 5.1.1.0 code, so only applies to that specific release. (Q02060978-03)

MLT / SMLT

- Previously unicast traffic could be flooded with the VLAN when some SMLT/RSMLT associated link failed; this is now resolved. (Q02037171)

9. Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.1.0. No new outstanding issues have been found in regards to the 5.1.1.0/5.1.1.1 releases.

10. Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. No new known limitations have been found in regards to the 5.1.1.0/5.1.1.1 releases.

11. Documentation Corrections

Dual MLTs in SMLT designs are supported, as long as only one is configured as an IST_MLT (system will not allow mis-configuration), and as long as any use of any form of spanning tree and the VLANs/ports associated with this form of spanning tree, remain solely on the non-IST_MLT; there can be no association or interaction with the IST_MLT. (Q02047748)

Ethernet Routing Switch 8600 Software Release 5.1.1.0

Software Release 5.1.1.0

1. Release Summary

Release Date: 7 August 2009

Purpose: Software maintenance release to address software issues found both in the field and internally.

2. Important Notes before Upgrading to This Release

If upgrading to 5.1.1.0 code within any SMLT designed network from a release prior to 4.1.8.2 or 5.0.1.0, i.e. a release which runs the 'older' SMLT architecture, then care should be taken to follow the proper upgrade steps. Please review the 4.1.8.2 Readme or 5.0.1.0 RN for specific details.

REGARDLESS OF SOFTWARE VERSION, the system-monitor flag should be checked on all systems to be sure it is enabled. This flag should always be enabled. The flag setting can be checked via the command, show config. The display should be something like:

```
ERS8600:6# show config
Preparing to Display Configuration...

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true (enabled)          or potential false (disabled)
#!flags regular-Autoneg false
#!record-reservation filter 4096
```

If the system-monitor flag is set false, then it should be changed to true (requires a reboot to take affect), which can only be accomplished by either JDM, Edit Chassis -> System Flags and then look under "System Monitoring" at the bottom of the screen. Checked equals enabled. To set via SNMP use:

MIB is rapidCity.rcMgmt.rcChassis.rcChasSystemMonitorEnable

snmpget -v 1 -c public x.x.x.x enterprises.2272.1.4.41.0

Output is either:

FALSE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 2 (disabled)
TRUE - SNMPv2-SMI::enterprises.2272.1.4.41.0 = INTEGER: 1 (enabled)

REGARDLESS OF SOFTWARE VERSION, the SNMP timer task may crash if the SNMP retry counter is set to a value greater than zero and multiple concurrent SNMP inform events are generated which do not receive an acknowledgement. While multiple factors and conditions need to align in order to encounter this SNMP task crash, it is recommended to set the SNMP retry count within the snmp-v3 target-address to zero in order to avoid the issue altogether. An example of such a configuration is (see the bolded entry):

Config snmp-v3 target-addr create "NNM" 10.10.10.1:162 "TparamV2" tdomain ipv4_tdomain timeout 1500 **retry 0** taglist informTag mms 484

(Q02052753 – the fix for this will be in future 5.1.x code)

3. Platforms Supported

All Ethernet Routing Switch 8600 modules are supported in the 8006, 8010, and 8010co Chassis. Full slot support for all modules may be dependant on the presence of the High Performance Backplane. There does exist and upgrade option for the HP Backplane.

The following modules are not supported in the 8003 chassis:

- 8692SF/CPU
- All R/RS modules

Please refer to the following documents for details on the Platforms Supported:

- Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 (Doc # NN46205-402, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 5.1 Upgrade Manual (Doc # NN46205-400, Rev 3.01)
- Nortel Ethernet Routing Switch 8600 Installation - Modules Manual for Software Release 5.1 (Doc # NN46205-304, Rev 3.02)
- Nortel Ethernet Routing Switch 8600 Administration Manual for Software Release 5.1 (Doc # NN46205-605, Rev 2.03)
- Nortel Ethernet Routing Switch 8600 Routine Maintenance Manual for Software Release 5.1 (Doc # NN46205-312, Rev 2.01)

Note: R/RS-series modules are supported in the 8010co chassis only with a High Performance Backplane installed.

4. Notes for Upgrade

Please see Upgrade Guide and Release Notes for the Ethernet Routing Switch 8600 Series Switch Software Release 5.1.0.0 available at www.nortel.com/support.

5. File Names for This Release

Module or file Type	Description	File name	Size in bytes
Software tar file Tar file of all software	Deliverables (includes images that also contain encryption software)	pr86_5110.tar.gz	59 M
Ethernet Routing Switch images			
Boot monitor image	CPU and switch fabric firmware	p80b5110.img	1.1 M
Run-time image	Run-time image	p80a5110.img	12 M
Run-time image for R modules	Image for R modules	p80j5110.dld	1.4 M
Run-time image for RS modules	Run-time image for RS modules	p80k5110.dld	1.5 M
Run-time image for Enterprise Enhanced SF/CPU Daughter Card (SuperMezz)	Image for the SuperMezz card	p80m5110.img	12 M

3DES	Encryption module for privacy protocol with Secure Shell (SSH)	p80c5110.img	55K
AES	Encryption module for privacy protocol for SNMPv3. Includes AES and 3DES	p80c5110.aes (this image includes the 3DES image)	26 K
MIB	MIB files	p80a5110.mib	4.0 M
MIB (zip file)	Zip file containing MIBs	p80a5110.mib.zip	659 K
MD5 checksum file	md5 checksums of all Release 5.1 software files	p80a5110.md5	1.3 K
Runtime image for ATM	Runtime image for the ATM module	p80t5110.dld	885 K
Runtime image for POS	Runtime image for the POS module	p80p5110.dld	685 K
Firmware images			
FOQ for R modules	Feedback output queuing FPGA firmware	foq267.xsvf	5.1 M
BMC for R modules	BAP memory controller FPGA firmware	bmc776.xsvf	2.5 M
DPC for R modules	Dual port Controller FPGA firmware	dpc184.xsvf	2.5 M
PIM8630GBR	Programmable I/O module FPGA firmware; for the 8630GBR only	PI_769.xsvf	2.2 M

Firmware for RS modules	Contains FOQ, BMC, DPC, mirroring, and loopback images	rs_dpm_fpga.bin	4.3 M
PIM images for RS modules	PIM FPGA firmware required for 8612XLRS module only	pim8612XLRS.bin	59 K
	PIM FPGA firmware required for 8634XGRS module only	pim8634XGRS.bin	76 K
	PIM FPGA firmware required for 8648GBRS module only	pim8648GBRS.bin	78 K
	PIM FPGA firmware required for 8648GTRS module only	pim8648GTRS.bin	53 K
SSL images			
SSL cluster upgrade	Ethernet Routing Switch 8600 clustered SSL modules self-installing runtime image/upgrade	p80s5110.pkg	5.7 M
SSL boot monitor	Ethernet Routing Switch 8600 SSL module boot monitor	p80s5110.img	7.2 M
SSL upgrade instructions	Ethernet Routing Switch 8600 SSL upgrade instructions	p80s5110.upgrade	1.4 K
SSL installation instructions	Ethernet Routing Switch 8600 SSL installation instructions	p80s5110.install	2.8 K

SSL diagnostics	Ethernet Routing Switch 8600 SSL diagnostics	p80s5110.diag	19 M
WSM images for Ethernet Routing Switch 8600			
WebOS firmware image	WSM WebOS v10.0.34.0 firmware image	wsm1003400_mp.img	826 K
WebOS binary	WSM WebOS v10.0.34.0 binary image	wsm1003400_bin.img	1.3 M
WebOS boot image	WSM WebOS v10.0.34.0 boot image	wsm1003400_boot.img	42 K
Device Manager images			
Solaris for SPARC image	Device Manager software image	jdm_6180_solaris_sparc.sh	237137138
Microsoft Windows image	Device Manager software image	jdm_6180.exe	213143936
Linux image	Device Manager software image	jdm_6180_linux.sh	216329458
Service Delivery Module images			
Service Delivery Module Firewall	Boot ISO for the NSF Service Delivery Module Firewall booting from CD-ROM	NSF5100_2.3.7.0_SDM_R60.iso NSF5100_2.3.7.0_SDM_R65.iso	
	Upgrade package for the NSF Service Delivery Module Firewall	NSF5100_2.3.7.0_SDM_R60.pkg.gz NSF5100_2.3.7.0_SDM_R65.pkg.gz	
Service Delivery Module TPS	Boot image for TPS Intrusion Sensor	Nortel_TPS_Intrusion_Sensor-SDM-v4.5.0-627-Install.iso	
	Boot ISO for TPS Defense Center booting from CD-ROM	NortelTPSDefenseCenter_2x70v4.5.0_627_Install.iso	
	Upgrade script (patch) to upgrade TPS IS from 4.5.0 to 4.5.1.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh	
	IS upgrade download verification file.	Nortel_TPS_IS_Upgrade_4.5.0_to_4.5.1_Upgrade-47.sh.md5	

Trace files			
MPLS trace file	Trace file for MPLS. This is auto generated and appears on the PCMCIA after upgrade.	nbpdtrc.lo0	variable

6. Version of Previous Release

Software Version **5.1.0.0**

7. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.1.8.0 or higher.

This software release supports the Web Switching Module (WSM) release WebOS 10.0.34.0. This code is found on Nortel web site under Content Networking -> Web Switches -> Ethernet Routing Switch Web Switch Module.

This software release supports SDM FW Release up to 2.3.7.0. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660, which provides a link to CheckPoint web site.

This software release supports SDM TPS Release up to 4.7.0.2. This code is found on Nortel web site under Security & VPN -> Service Delivery Module 8660.

To download any of these code releases requires valid Nortel support web access, as well as valid CheckPoint support site access for most FW code.

8. Changes in This Release

New Features in This Release

With this release, ERS 8600 introduces new commands to better handle receiving bad OSPF LSAs. The Switch will have an option to configure the way the router behaves on receiving a bad LSA. There are now different options on how to handle a received BAD LSA (with hole in mask). This can affect how adjacency is form to other routers in the network. (Q01997413)

The following commands have been implemented for this new functionality:

config ip ospf bad-lsa-ignore <enable|disable>

To enable the Switch to keep accepting the bad LSAs (with hole in mask) use the following CLI command (default behavior is disable):

config ip ospf bad-lsa-ignore enable

Alternatively use the following NNCLI command:

bad-lsa-ignore enable

Other associated NNCLI commands would be:

no bad-lsa-ignore [enable]

default bad-lsa-ignore [enable]

Setting the ospf bad-lsa-ignore parameter to enabled maybe required to maintain adjacency with other non-Nortel switch/routers, especially Cisco models.

The same commands under VRF configuration mode are for CLI:

config ip vrf <vrf-id> ospf bad-lsa-ignore <enable|disable>

and for NNCLI:

```
ip ospf bad-lsa-ignore enable
```

as well as:

```
no ip ospf bad-lsa-ignore enable
default ip ospf bad-lsa-ignore [enable]
```

To execute these commands OSPF needs to be disabled globally first.

There is no JDM support for these commands at this time.

Old Features Removed From This Release

None.

Problems Resolved in This Release

Switch management

- ERS 8600 will no longer experience VRRP transitions, ping failures or potential OSPF slowdown or failure when there is binary transfer of a file via FTP or TFTP with a file size greater than the free memory available on the flash. ERS 8600 could previously experience these issues while its CPU utilization was high. (Q01978884-02)

- Switch will no longer show system instability on quitting from a SSH session, even if a SSH File Transfer Window is opened from the existing SSH session more than once. However the ERS 8600 still does not support any File Transfers from a SSH session. (Q01856195-03)

- ERS 8600 no longer allows adding a route in net mgmt table, if the same route already exists in the normal routing table (due to some routable VLAN or static configuration). (Q01987429-02)

Platform

- ERS 8600 no longer allows (a guard rail has been added) port mirroring from Legacy Port to GTR/GTRS port in “Rx mode” and “both mode”. An invalid port number or failed message will be returned to the user. This operation is allowed for Tx mode only. (Q01790729-02)

- ERS 8600 no longer experiences unexpected Mezz CPU failover with the Mezz card enabled and then saving the configuration via JDM. (Q01981161-01)

- The potential for traffic interruption associated with the Gig ports on the 8634XGRS module has now been resolved. (Q02010160-03)

- ERS 8600 console will now no longer spool repeated messages of AA1419049-E6 (LX) SFP insertion after a switch reboot. (Q01940440-02)

- ERS 8600 will now be able to properly detect all versions of the AA1419049-E6 SFP (1000Base-LX) even after any switch reboot. (Q01980528-02)

- Link flap detect feature is now supported for R-modules cards. (Q01783494)

IP Unicast

RIP

- For ERS 8600, the set metric parameter in a route-policy will now take effect for RIP. (Q01959361-02)

BFD

- On an ERS 8600 running a BFD session over a static route, when a BFD failure occurs the static route will no longer get learned in the routing table, even when the ARP for next-hop is present until the BFD session gets re-established again. (Q02010174)

BGP

- Operational problems with BGP software that could have led to system instability issues have been resolved. (Q02026274 and Q01972590)

OSPF

- OSPF routes will no longer get improperly deleted even while routes are getting added with ECMP enabled. (Q02021239)

MLT / SMLT

- In RSMLT edge support enabled mode, the creation of a new RSMLT enabled VLAN interface ***only on one aggregation box*** will no longer cause the static default route to get deleted from the hardware, and thereby affect RSMLT forwarding and re-convergence time. (Q02005454-02)

- In a dual SF/CPU configuration, when the last CP card is pulled out or fails, the RS I/O modules will now have their entire ports drop link automatically. This will help in any SMLT designed network to provide better and faster recovery. (Q01991517-02)

- The ERS 8600 will now check for the SMLT status of an MLT only if it is configured as an SMLT, while sending a MAC-address-learn message for any MAC learnt on the MLT. If the MLT is not configured for SMLT, then SMLT status will not be checked and an MAC-address-learn message will be sent to the IST peer. (Q02036964)

- 8600 will now update the ARP when a MAC learn message is received from IST peer, irrespective of whether the MAC is already existing as local or not. This reduces the chances of improper forwarding in SMLT/RSMLT designed networks. (Q02044582)

Multicast Routing Protocol

PIM

- ERS 8600 will now properly forward packets to the DR when the egress port to the DR is the same as the incoming port and the port to the DR changes for some reason. (Q01907611-04)

9. Outstanding Issues

Please refer to the Outstanding Issues Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues will be fixed in a future release.

Platform

- The change for CR 1767930 which is related to proper operation of SCP (Secure Copy) while using Access Policies, which was fix in the 4.1.x stream back in 4.1.6.3, is missing from all 5.x streams. This will be resolved in all future 5.x code streams, but is still missing in 5.1.1.0.

Configuration

- While configuring ds-field under “config ip traffic-filter filter <filter-id> match”, if we give the six dscp bits, it is taking the command improperly. (Q02056382)

MLT

- An MLT with LACP enabled along with min-link configured, may not have ports added to the MLT properly. (Q02034692)

STATIC ROUTE

- When a static route is created within the non-default VRF, it may not become active and high number of such static routes may lead to increased CPU utilization. For system running with only the default VRF (VRF 0) this is of no concern. For those running with multiple VRFs, use of static routes in the non-default VRF (outside of VRF 0) should be limited or not used at all; instead use some routing protocol, such as OSPF or RIP. (Q02060978)

10. Known Limitations

Please refer to the Known Limitations Section of the Release Notes for Ethernet Routing Switch 8600 Software Release 5.1.0.0. Additionally, the following issues have also been classified as operation not to be changed.

Switch management

- "Secret" is no longer the default SNMP community string for read/write access. Instead there is none and it needs to be configured via CLI before SNMP can be used. This has been the operation for some time now, not just introduced with 5.1.1.0 code. (Q02049550)

- Clients may loose connectivity when filters are applied on tagged ports, with default port action of drop. Such a configuration is not supported. Instead use filter configuration of default port action of forward and drop filters. (Q01906338-02)

- SNMP-generated traps are not being processed by the MDM Carrier Management station, due to a checksum error in the UDP packets. This situation will NOT be seen if the source IP used in the SNMP Sender-IP parameter is some Circuitless IP address. (Q02047909)

11. Documentation Corrections

Dual MLTs in SMLT designs are supported, as long as only one is configured as an IST_MLT (system will not allow mis-configuration), and as long as any use of any form of spanning tree and the VLANs/ports associated with this form of spanning tree, remain solely on the non-IST_MLT; there can be no association or interaction with the IST_MLT. (Q02047748)

The command config sys set snmp-ip no longer will accept an IP address of value 0.0.0.0, which would be illegal to start with. (Q02062013)

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support