Ethernet Routing Switch 8300

Software Release 3.0.x.x

Ethernet Routing Switch 8300

Software Release 3.0.2.0

1. Release Summary

Release Date: Mar 30 2007
Purpose: Software maintenance release to address customer found software issues.

2. Important Notes before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 8300 modules in 8010 and 8006 chassis.
Ethernet Routing Switch 8300 modules in 8306 and 8310 chassis.

4. Notes for Upgrade

Please see the *Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0* and *Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0* (Part No : NN46200-401and Part No : NN46200-400) available at http://www.nortel.com/support , (select Ethernet Routing Switch family) for details on how to upgrade your Ethernet Routing Switch 8300.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
p83b3020.img	Boot monitor image	1075149
p83a3020.img	Runtime image	6698433
p83f3020.img	Pre-Boot monitor image **See IMPORTANT Note below	230786

** Nortel recommends that the Pre-Boot Image ONLY be upgraded if the system is currently running a Pre-Boot Monitor Software Rel 3.6. Systems running a Pre-Boot image Rel 3.7 should not be upgraded as there have been no changes to the Pre Boot Image for this release. Please use the CLI command **'show sys sw'** to know the Pre-Boot Monitor Software version.

p83r3020.dld	Ethernet module image (Required for I/O) cards	2222332
p83c3020.aes	Encryption module for SNMPv3 (DES)	26960
p83c3020.img	Encryption module for SSH (3DES)	52424
p83a3020.mib	MIB file (Private)	3045022
p83a3020.mib.zip	MIB (zip file)	486593
p83a3020.md5	md5 checksum file	524

5. Version of Previous Release

Software Version **3.0.1.0**

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.0.2.0**.**

7. Changes in This Release

New Features in This Release

None

Old Features Removed From This Release

None

Problems Resolved in This Release

Switch Management

General

The description of GBIC ports on CP cards is now correctly displayed. (Q01504488)
The "Cold-start / Warm-start" trap message now can be received while trap-receiver is in inband connection (i.e. the net management is configured on the IO cards). (Q01534395)

Secure Shell

The ERS8300 is now able to clean up the broken SSHv1 sessions caused by port disabling. (Q01512693).

Platform

General

The POE I/O cards are now able to handle the larger than normal ElectroStatic Discharge(ESD) or Cable Discharge (CD) events. (Q01559866)
Note: A larger than normal ESD or CD directly into the port may cause POE management chipset to reset. Though the ERS8300 can handle it, it is recommended

that the customer or operator takes all precautions to eliminate or reduce ESD event to avoid unnecessary confusion.

Layer 2 switching

MLT/SMLT

The multicast traffic received from IST is now prevented to be forwarded to SMLT ports. (Q01498518)

MLT designated port now is null if there are no ports in UP status in this MLT group. (Q01491190)

The “smlt-remote” flags of learned MAC entry on the aggregation switches now are correctly set when the SMLT ports that connect to the closet switch are disabled and enabled. (Q01481762)

The “smlt-remote” flags of learned MAC entry on the aggregation switches now are correctly set when the same packet is exceptionally sent to both aggregation switches. (Q01489313)

The FDB entries learnt via IST-MLT now can be purged out correctly. (Q01504767)

IP Unicast

General

The ERS8300 now can correctly process the DHCP offer message received from IST. (Q01579460)

When performing DHCP relay function, the aggregation switch is now able to correctly handle the wrong DHCP offer message, inside which the offered address is the same as the VRRP IP address itself, from misconfigured DHCP server. (Q01504398)

8. Outstanding Issues

None.

9. Known Limitations

This section describes issues known to exist in the 8300 Series Software Release 3.0.2.0 in the following categories:

Topic
Configuring ACL/ACE filters
Smlt-remote flags of learned MAC entry

Configuring ACL/ACE filters

Use the following guidelines when you configure ACL/ACE filters over ports.

Always use an ACT with only the proper attributes selected. If you must add ACEs with attributes that are not in the original ACT, you must create a new ACL associated with the new ACT.

For multiple ACEs that perform the same task, for example: deny or allow IP addresses, or UDP/TCP-based ports, you can configure one ACE to perform the task with either multiple address entries, or address ranges, or a combination of both. You can now use this one ACE instead of using multiple ACEs.

For ERS8300, the user can apply only one ACG per port, but the user can apply the same ACG on multiple ports. At the same time, the maximum number of ACEs that are contained by all the applied ACGs is 128 (If the ACG is applied to multiple ports, it is

considered as one ACG). If the following messages appear on the console or in the log, it is likely that there is an excessive number of active ACEs configured within an ERS8300. Therefore, review and reduce the number of active ACEs, keeping the guidelines, noted above, in mind.

CPU5 [12/14/06 12:20:34] QOS ERROR gtcmCreateTcEntry: Failed, status = 20!

For ERS8300, a maximum of 128 ACEs per ACG are supported. This maximum may not be achievable depending on the type of attributes used within an ACE. For example, an ACE containing the logical operator “NON EQUAL” will definitely reduce the maximum number of ACEs per ACL. In these cases, to help ensure stable system operation, reduce the number of ACEs or optimize the ACE, and follow the previous guidelines.

Smlt-remote flags of learned MAC entry

Please also see “**Known limitations and considerations in this release**” of “Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0” (Part No: NN46200-401) and the Known Limitations section of Readme for Ethernet Routing Switch 8300 Software Release 3.0.1.0.

10. Documentation Corrections

None

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

Ethernet Routing Switch 8300

Software Release 3.0.1.0

1. Release Summary

Release Date: 20 Dec 2006
Purpose: Software maintenance release to address customer found software issues.

2. Important Notes before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 8300 modules in 8010 and 8006 chassis.
Ethernet Routing Switch 8300 modules in 8306 and 8310 chassis.

4. Notes for Upgrade

Please see the *Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0* and *Nortel Ethernet Routing Switch 8300 Upgrades - Software Release 3.0* (Part No : NN46200-401and Part No : NN46200-400) available at http://www.nortel.com/support , (select Ethernet Routing Switch family) for details on how to upgrade your Ethernet Routing Switch 8300.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
p83b3010.img	Boot monitor image	1075234
p83a3010.img	Runtime image	6699018
p83f3010.img	Pre-Boot monitor image **See IMPORTANT Note below	230786

** Nortel recommends that the Pre-Boot Image ONLY be upgraded if the system is currently running a Pre-Boot Monitor Software Rel 3.6. Systems running a Pre-Boot image Rel 3.7 should not be upgraded as there have been no changes to the Pre Boot Image for this release. Please use the CLI command **'show sys sw'** to know the Pre-Boot Monitor Software version.

p83r3010.dld	Ethernet module image (Required for I/O) cards	2221508
p83c3010.aes	Encryption module for SNMPv3 (DES)	26960
p83c3010.img	Encryption module for SSH (3DES)	52424
p83a3010.mib	MIB file (Private)	3044990
p83a3010.mib.zip	MIB (zip file)	486584
p83a3010.md5	md5 checksum file	524

5. Version of Previous Release

Software Version **3.0.0.0**

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.0.2.0**.**

7. Changes in This Release

New Features in This Release
None

Old Features Removed From This Release
None

Problems Resolved in This Release
IP

General

The traceroute utility (i.e. Window command “tracert”) will no longer time-out on the first hop when the first hop is the ERS8300 itself. (Q01393096)

ERS 8300 does now respond to ARP query from Alteon firewall. (Q01502526)

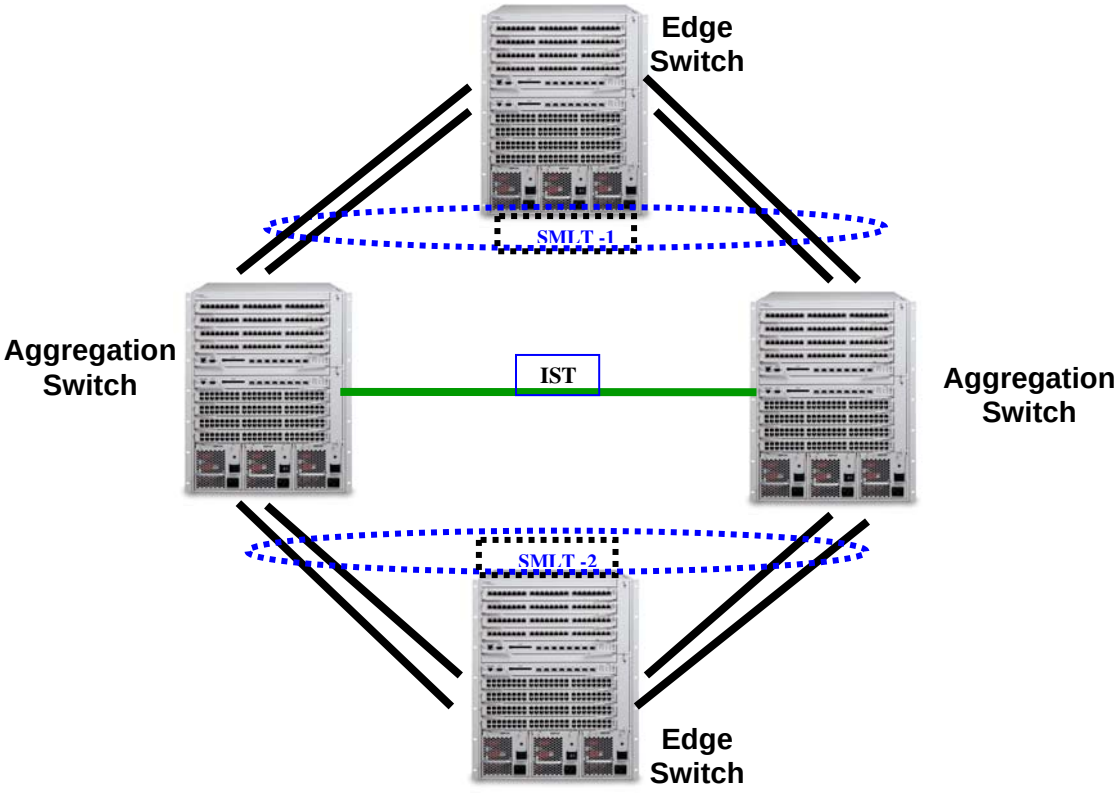
Layer 2 switching

MLT/SMLT

There is now about 4 seconds traffic loss during the system booting time or system recovery time of the SMLT active switch. (Q01360780, Q01404355)

In a diamond SMLT topology consisting of 4 ERS8300 devices, the booting with factory default configuration of the edge switch now doesn't cause the system instability of the aggregation switch. (Q01475259)

Note: Here is a example for the diamond SMLT topology



The “smlt-remote” flag of SMLT MAC entry is now correctly set if this MAC is learnt via pinging from edge switch in SMLT topology. (Q01490170)
The FDB entries are now in sync between aggregation switches when SMLT ports are disabled. (Q01483556)

Platform

General

The following message is now displayed on the console when the RSA key is generated successfully using the CLI command “config sys set ssh action rsa-keygen” (Q01398088)

> Generating RSA keys. This may take a while. Please wait...
> SSH INFO RSA private/public Host key pair successfully generated

The Gigabits ports on CP card (i.e. 8393) and 8348GB card will no longer go active until the system is ready to accept traffic from network. (Q01399804, Q01474912)
The ping-snoop message, i.e. “CPU INFO ICMP Request received on…”, will no longer display unreadable characters. (Q01455449)
When the TFTP IP address is configured for the management network, a class based route now no longer gets added in the management network. (Q01461908)
There is now no SEEPROM error (error message: “seepromGetInfo: Failed 2”) while booting the ERS8300. (Q01485593)

EAP

The data flow with same MAC address on two different “MAC centralization” enabled ports now doesn’t prevent this MAC address being populated into FDBentry. (Q01465709)
The VLAN now can’t be deleted if one of its ports has an active EAPOL session. (Q01460640)

Switch Management

General

The syslog maximum number of hosts (syslog max-host) is now preserved after reboot. (Q01395367)

The VLAN name is now shown correctly even when its length is more than 14 characters. (Q01416621-01)

The MIB walk on lldpLocManAddrTable now doesn't cause system instability on ERS8300. (Q01487381)

Added support bits in license for some CLI commands in basic package. (Q01471509)

8. Outstanding Issues

None

9. Known Limitations

This section describes issues known to exist in the 8300 Series Software Release 3.0.1 in the following categories:

Topic
Software

CR Reference	Description
Software	
Q01498518	When the MLT ID of IST is greater than 7, the multicast traffic received from IST will be forwarded to SMLT ports at 8348TX / 8348TX-POE / 8324FX cards. There is a hardware limitation on these 3 kinds of cards: the hardware can only support as much as 7 MLTs synchronously. So, the MLT ID of the IST can't be greater than 7, if there are any existing SMLT containing ports of 8348TX / 8348TX-POE / 8324FX cards. Similarly, if the MLT ID of existing IST is greater than 7, it is forbidden to create a SMLT containing ports of 8348TX / 8348TX-POE / 8324FX cards, or add this kinds of ports into existing SMLT.
Q01504767	In a diamond SMLT topology consisting of 4 ERS8300 devices, after one aggregation switch reboots and comes up, the FDB entries learnt by this aggregation switch via IST-MLT may not be purged out as expected.
Q01481762, Q01485041	The "smlt-remote" flags of learnt SMLT MAC entry is TRUE on both aggregation switches when the SMLT links connected to edge switch are disabled and enabled.
Q01489313	The "smlt-remote" flag of one learnt SMLT MAC entry of 5520 SONMP packets are TRUE on two aggregate switches.

Please also see "**Known limitations and considerations in this release**" of "Nortel Ethernet Routing Switch 8300 Release Notes - Software Release 3.0" (Part No: NN46200-401).

11. Documentation Corrections

None

12. SNMP Access policies – Clarification

There is a new feature in release 2.3.1.0, and its name is “Support for SNMP service in access policy”. The SNMP access policy will always be disabled by default during the upgrading from older releases (older than release 2.3.1.0). The following is the complementary clarification about this feature.

How to configure access policy for snmp in release 2.3.1 or newer release?

1) Enable the access-policy globally:
   config sys access-policy enable true
2) Create the policy:
   config sys access-policy policy 2 create

   The following parameters will be having default values when an access policy is created. User can change them if required. Below is the explanation of the parameters with examples:

   name -- Used to set the name of the access-policy
   config sys access-policy policy 2 name policyName
   policy enable – Used to enable or disable the policy
   config sys access-policy policy 2 enable
   mode – Used to determine whether access be allowed or denied to an incoming request if it matches the policy
   config sys access-policy policy 2 mode allow
   precedence – If more than one policies are matched for an incoming request, the value of precedence determines which one of them would be applied. Lower the precedence value, higher the priority.
   config sys access-policy policy 2 precedence 10
   network – If configured for a policy ,then the policy gets applied only in case the subnet of the source ip address of the incoming access request matches the configured network address.
   config sys access-policy policy 2 network 198.202.188.0/24
   host - If configured for a policy ,then the policy gets applied only in case the source ip address of the incoming access request matches the configured host ip address.
   config sys access-policy policy 2 host 198.202.188.174
   username – Used only in case of rlogin access.
   config sys access-policy policy 2 username nortel
   accesslevel – Determines the accesslevel which the user should have if he is to be granted access. If the user’s accesslevel is greater than the one configured for the policy, he would be granted access or not depending upon whether access-strict is set to true or false.
   config sys access-policy policy 2 accesslevel rw
3) Enable snmpv3 service in policy 2:
   config sys access-policy policy 2 service snmpv3 enable
4) Add the snmp-groups and the security model to the access policy. The default snmp-groups and the security models for allowing access to private and public community strings are:
   readgrp snmpv1
   readgrp snmpv2c
   v1v2group snmpv1
   v1v2group snmpv2c

   config sys access-policy policy 2 snmp-group-add readgrp snmpv1
   config sys access-policy policy 2 snmp-group-add readgrp snmpv2c

config sys access-policy policy 2 snmp-group-add v1v2grp snmpv1
config sys access-policy policy 2 snmp-group-add v1v2grp snmpv2c

5) Login to the switch with public & private.
6) If a new community name is to be granted access through a policy, then the snmp-group corresponding to the community string and the security model should be added to the access policy.

config snmp-v3 community create third nortel readview
config sys access-policy policy 2 snmp-group-add readgrp snmpv1
config sys access-policy policy 2 snmp-group-add readgrp snmpv2c

Upgrading from previous load to release 2.3.1

Access Policies need to be disabled at the global level before upgrading from previous loads to release 2.3.1.0 or newer release if access via JDM required immediately after upgrade:

CLI Command

config sys access-policy enable false

NNCLI

access-policy disable

After upgrade, an access policy for the SNMP group needs to be created, and add the snmp-groups and the security model to this access policy (Access Policies SNMP Groups table) before enabling Access Policies at the global level.