



# Ethernet Routing Switch

## 8300

### Software Release 2.3.x.x

Software Release 2.3.2.0 .....	2
Software Release 2.3.1.0 .....	13



# Ethernet Routing Switch

## 8300

### Software Release 2.3.2.0

## 1. Release Summary

Release Date: 22 June 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 *Release Notes for the Ethernet Routing Switch 8300 Software Release 2.3 and Upgrading to Ethernet Routing Switch 8300 Software Release 2.3* (Part No : 316811-F and Part No : 318769-D) 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)
p83b2320.img	Boot monitor image	1071856
p83a2320.img	Runtime image	6479079
p83f2320.img	Pre-Boot monitor image **See IMPORTANT Note below	230786
p83r2320.dld	Ethernet module image (Required for I/O) cards	2213680

\*\* 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.

p83c2320.des	Encryption module for SNMPv3 (DES)	8638
p83c2320.img	Encryption module for SSH (3DES)	55976
p83a2320.mib	MIB file (Private)	2124589
p83a2320.mib.zip	MIB (zip file)	338544
p83a2320.md5	md5 checksum file	477

## **5. Version of Previous Release**

Software Version **2.3.1.0**

## **6. Compatibility**

This software release is managed with Java Device Manager (JDM) release **5.9.5.0**

## **7. Changes in This Release**

### **New Features in This Release**

### **Old Features Removed From This Release**

None.

### **Problems Resolved in This Release**

#### **Switch management**

##### **General**

- When an access policy with SSH service enabled exists, the configured value of access-level is now applied to SSH users accessing the switch with RSA/DSA public key authentication. (Q01281360)
- Access policies can only be configured by users with RWA access level. (Q01325130)
- The access policy usage counters are now updated properly when telnetting to the peer CPU card on a ERS 8300 switch with dual CPU cards. (Q01305174)
- The *show sys access-policy snmp-group-info* command now displays the snmp groups without causing switch instability. (Q01381069)

#### **Platform**

##### **General**

- The EAP port state can now be set to force-auth from either force-unauth or auto when EAP is disabled globally. (Q01313950)
- An EAP enabled tagged port now moves from the guest VLAN to the authenticate VLAN after successful authentication. (Q01326368)
- In CLI mode, when a syslog host is in disabled state and the ERS 8300 switch is rebooted in NNCLI mode, the disabled state of the syslog host is retained. (Q01296753)
- Simultaneous link state changes on multiple ports are now logged properly.(Q01343042-02)
- When VLAN id and TCP/UDP destination port are selected and 12 other octets are configured for a PCL template, the TCP/UDP destination port is now matched with the incoming packets. (Q01322891-01)
- Configuring a syslog host with a severity level of INFO no longer causes system instability. (Q01374779-01)

## **8. Outstanding Issues**

- When a tracert (Windows traceroute utility) initiated from one host to another, connected using a 8348 GTX module, the traceroute times-out on the first hop, but is able to reach the destination. (Q01393096)

## **9. Known Limitations**

Please see Known limitations and considerations in this release section of Release Notes for the Ethernet Routing Switch 8300 Software Release 2.3 (Part No: 316811-F) and the Known Limitations section of Readme for Ethernet Routing Switch 8300 Software Release 2.3.1.0.

## **10. Documentation Corrections**

None

---

Copyright © 2006 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globe mark, and Ethernet Routing Switch 8100/8300/8600 are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

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 2.3.1.0

#### 1. Release Summary

Release Date: 20<sup>th</sup> March 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 *Release Notes for the Ethernet Routing Switch 8300 Software Release 2.3 and Upgrading to Ethernet Routing Switch 8300 Software Release 2.3* (Part No : 316811-F and Part No : 318769-D) 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)
p83b2310.img	Boot monitor image	1071460
p83a2310.img	Runtime image	6477917
p83f2310.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.

p83r2310.dld	Ethernet module image (Required for I/O) cards	2214136
p83c2310.des	Encryption module for SNMPv3 (DES)	8638
p83c2310.img	Encryption module for SSH (3DES)	55976
p83a2310.mib	MIB file (Private)	2124589
p83a2310.mib.zip	MIB (zip file)	338544
p83a2310.md5	md5 checksum file	477

## **5. Version of Previous Release**

Software Version **2.3.0.0**

## **6. Compatibility**

This software release is managed with Java Device Manager (JDM) release **5.9.5.0**

## **7. Changes in This Release**

### **New Features in This Release**

#### **Support for EAP (Extensible Authentication Protocol) on tagged ports (Q01209997-01)**

The Ethernet Routing Switch 8300 implements EAP for authenticating devices connected to access (untagged) ports. This feature extends the support for EAP to tagged ports. With IP phones implementing 802.1x supplicant, it is required to support tagged frames coming from the IP phone.

This feature allows the user to enable EAP on tagged ports. The enhancement also provides guest VLAN support and multiple clients per port, on tagged ports. The Guest VLAN feature allows the users connected on the port with EAP enabled to have guest network access on the switch until they are authenticated. With multi-host feature enabled, more than one client can be connected on an EAP enabled port. Each of these clients has to be authenticated in order to gain network access on the switch.

#### **Support for SNMP service in access policy (Q01071373-03, Q01190776-01)**

The access policy feature in Ethernet Routing Switch 8300 determines the access level for the users connecting to the switch with different services like FTP, TFTP, Telnet, rlogin etc. The system access-policy feature is based on the access-levels and the network address of the user. It covers services like TFTP, HTTP, SSH, rlogin, SNMP. However with SNMP-v3 engine, the community names do not map on to an access-level but the access privileges are determined only through the VACM (Variable Access Control Model) configuration.

The new enhancement allows the user to specify groups for the SNMP access policy which enables SNMP to be covered under the access policy services. Since the access restriction is based on groups defined through the VACM model, the synchronization will be made using the snmp-v3 VACM configuration. This feature enables the administrator to bind these groups along with the security level to an access-policy.

### Feature Specifics

- All users associated with the groups configured under access policy when snmp service is enabled will be covered through this policy. The access privileges will be based on access allow/deny and if allow then based on the VACM configuration the mib-views for access are determined.
- The SNMP service will be by default disabled for all access-policies
- The access-level configured under “access-policy policy <id>” will not affect SNMP service. The SNMP access rights are determined by VACM configuration.

### Command Line Interface:

To add a group under access policy snmp service:

```
Passport-8310:5/config sys access-policy policy 2# snmp-group-add <snmp-v3 group name> <snmpmodel>
```

To delete a group under access policy snmp service:

```
Passport-8310:5/config sys access-policy policy 2# snmp-group-del <snmp-v3 group name> <snmpmodel>
```

The info command

```
Passport-8310:5/config sys access-policy policy 2# snmp- group-info snmpv3-groups:
GroupName Snmp-model
group1 snmpv1
group2 usm
```

To see the list of entries in the access-policy snmp service table,

```
Passport-8310:5#5/show/sys/access-policy# snmp- group info [<polname>]
```

```
=====
SNMP Groups under Access Policy <PolName>
=====
```

```
GroupName snmp-model
group1 snmpv1
group2 usm
-----
```

**Note:** SNMP access policy will always be disabled by default while upgrading from older releases. The user must enable access policy and add appropriate configuration to use the snmp service with the access policy feature.

## LLDP Link Layer Discovery Protocol (Q01287849)

### Overview

A new protocol, defined by the IEEE as the Link Layer Discovery Protocol (LLDP) allows stations connected to a LAN to exchange capabilities and build the topology of the network. The information distributed using this protocol is stored by the different stations which support this protocol (as defined by IEEE in the 802.1ab standard). These can include PCs, IP Phones,

switches, routers or any interconnecting device in a standard Management Information Base (MIB), making it possible for the information to be accessed by a network management system (NMS) or application.

### Functionality

The following functions apply to this new feature:

- LLDP communicates connectivity and management information about the local station to an adjacent station on the same 802 LAN
- Receives network management information from adjacent stations on the same 802 LAN. Information received from remote LLDP agents is stored in the LLDP remote systems MIB.
- Establishes a network management information schema and object definitions that are suitable for storing connection information about adjacent stations.

### Operation

Each time a port is up, if the tx option is enable for that port, the switch sends an LLDP Data Unit (LLDPDU) to the new neighbor. If the neighbor supports the protocol and also sends an LLDPDU, the information received by the switch can be seen by SNMP using the show lldp neighbors CLI command.

The information fields for each LLDP frame are contained in a LLDPDU as a sequence of short, variable length, information elements known as TLVs. Each LLDPDU also includes four mandatory TLVs (a Chassis ID TLV, Port ID TLV, A Time To Live TLV, an End Of LLDPDU TLV), plus five optional TLVs as selected by the network management.

### Capabilities

The current implementation supports the core TLV set.

The information communicated includes the following:

- *Mandatory TLV*: Chassis ID, port ID, TTL and End of LLDPDU.
- *Optional TLV*: System description, system name, system capabilities, port description and local management address.

**Note:** 802.1, 802.3 and MED TLVs set in 2.3.1 are NOT supported. They are considered as "Unknown" TLVs.

### Configuration

#### **Note:** show CLI & NNCLI – below CLI=NNCLI

LLDP allows the transmitter and the receiver to be separately enabled, making it possible to configure an implementation to restrict the local LLDP agent to either transmit only or receive only, or to allow the local LLDP agent to both transmit and receive LLDP information.

The user can configure the state for the receiving/transmitting (rx/tx) machines by SNMP and CLI commands and also configure if the optional TLVs have to be sent or not. The mandatory TLVs are configured by default to be sent. To configure other TLV to be sent, the lldp tx-tlv ... CLI command and SNMP is used.

### User Interface



The SNMP and NNCLI/CLI can be used to configure this feature and also to view the local storage database that contains information about the device's neighbors.

## NNCLI Commands

```
Passport-8306:6(config)#lldp ?
notification-interval interval for notification
reinit-delay          reinitiation delay
tx-delay              transmission delay
tx-hold-multiplier    transmission hold multiplier
tx-interval           transmission interval

Passport-8306:6(config)#show lldp ?
interface             Display LLDP Interface Information
local-sys-data        Lldp local system data
mgmt-sys              mgmtsys
neighbor              neighbor of lldp
neighbor-mgmt-addr    neighbor-mgmt-addr of lldp
rx-stats              rx-stats of lldp
stats                 stats
tx-stats              tx-stats of lldp
tx-tlv                tx-tlv
<cr>
```

```
Passport-8306:6(config-if)#lldp ?
config-notification configuration notification
port                  Port number(s) which are to be changed
status                status of lldp
tx-tlv                transmission tlv
```

```
Passport-8306:6(config-if)#lldp tx-tlv ?
local-mgmt-addr       transmission addr
port-desc             port desc for tx-tlv
sys-cap               sys cap for tx-tlv
sys-desc              sys desc for tx-tlv
sys-name              sys name for tx-tlv
```

## CLI Commands

```
Passport-8306:6# config lldp ?
```

Sub-Context:

Current Context:

```
info
notification-interval <seconds>
reinit-delay <seconds>
tx-interval <seconds>
tx-hold-multiplier <seconds>
tx-delay <seconds>
```

```
Passport-8306:6# show lldp ?
```

Sub-Context:

Current Context:

local-sys-data  
mgmt-sys  
neighbor [<portlist>]  
neighbor-mgmt-addr [<portlist>]  
rx-stats [<portlist>]  
stats  
tx-stats [<portlist>]

Passport-8306:6# config eth <portlist> lldp ?

Sub-Context: tx-tlv  
Current Context:

config-notification <enable|disable>  
info  
status <tx|rx|txandrx|disabled>

Passport-8306:6# config eth <portlist> lldp tx-tlv ?

Sub-Context:  
Current Context:

info  
local-mgmt-addr-tx <enable|disable>  
port-desc <enable|disable>  
sys-cap <enable|disable>  
sys-desc <enable|disable>  
sys-name <enable|disable>

Passport-8306:6# show lldp local-sys-data

```

=====
                        lldp local-sys-data Chassis
=====
chasis      sys      sys
id          Name      Desc
-----
00:13:0a:1d:e0:00 Passport-8306 Passport-8306 (2.3.1.0)

```

```

=====
                        lldp local-sys-data port
=====
port port      port
Num  Id          Desc
-----
1/1  00:13:0a:1d:e0:40 1000BaseTXPOE

```

Passport-8306:6# show lldp mgmt-sys

```

=====
                        lldp mgmt-sys-data
=====
MgmtAddr      MgmtAddrId  MgmtAddrOID

```

-----  
134.177.220.125 447          1.3.6.1.4.1.2272.1.100.2.1.1.447

Passport-8306:6# show lldp neighbor

=====  
=====

LLDP NEIGHBOR

=====  
=====

PORT NUM	INDEX	CHASSIS SUBTYPE ID	CHASSIS SUBTYPE ID	PORT ID	PORT ID
1/11	1	Network	Addr	172.192.202.100	MAC      00:0a:e4:6f:be:67
Nortel IP Phone			Nortel IP Telephone 2004, F2		

=====  
=====

lldp Remote-sys-data Sys Capabilities

=====  
=====

Repeater	Bridge	WLAN	Router	Telephone	DOCICS	Station	Other
	Access Pt		Cable	Only			
	(Supported/Enabled)						

-----  
No/No   Yes/Yes   No/No   No/No   Yes/Yes   No/No   No/No   No/No

### SNMP MIBs

List any new MIBs that will be available for this feature:

lldp.mib

### Performance

An active LLDP agent enabled for transmission will initiate an LLDP frame transmission whenever either of the following events occurs:

- Expiration of the transmission countdown timing counter, txTTR, associated with the LLDP local system MIB, or
- A condition (status or value) change in one or more objects in the LLDP local system MIB.

To prevent a series of successive LLDP frame transmissions during a short period due to rapid changes in the LLDP local systems MIB objects and to increase the probability that multiple, rather than single changes are reported in each frame, the local LLDP limits the LLDP frame transmission rate through the use of a variable transmit delay timer that may be set by the network management.

The actual transmission intervals for different ports on the same multi-port implementation are staggered to prevent synchronization effects.

### **Thresholds**

The default (recommended) thresholds for LLDP configuration are:

```
tx-interval : 30
tx-hold-multiplier : 4
reinit-delay : 2
tx-delay : 2
notification-interval : 5
```

### **Troubleshooting**

The amount of space needed in the LLDP remote systems MIB to accommodate the creation of several new MIB structures may be too large. It may not always be possible to accommodate another new neighbor in implementations with limited memory. The solution when presented with this scenario is to ignore and not process the new neighbor's information.

## Old Features Removed From This Release

None.

## Problems Resolved in This Release

### Switch management

#### General

- There will no longer be problem of CPU utilization going higher while processing SNMP packets. (Q01158832-02)
- The default access policy can no longer be deleted. (Q01200901-01)
- Access policy can now be created from JDM without enabling any service. (Q01200902-01)
- On Ethernet Routing Switch 8300, the last entry in the access policy list will no longer be lost after reboot (Q01304306).
- Ethernet Routing Switch 8300 will now display a message when user connection is established or disconnected via FTP (Q01183804-01/Q01295814).

#### Secure Shell

- Setting the SSH mode to Secure through Java Device Manger will no longer cause any system instability (Q01250458).
- The RSA key generated when SSH is enabled, will no longer be printed on the CLI. (Q01201638-01)

### Platform

#### General

- STP now converges properly after CPU failover (Q01243757, Q01232899)
- The RSA key generated when SSH is enabled, will no longer be printed on the CLI. (Q01201638)
- The allocated power for PoE no longer shows a negative value. (Q01237128)
- The port utilization values are now calculated properly by including the Preamble and Inter-Frame Gap. (Q01189519)
- Changes to NTP interval will now take effect from the next synchronization cycle. Also changes to NTP interval will take effect properly across reboot. (Q01254489)
- The 8348TX and 8348TXPoE modules will no longer erroneously report InternalMacReceiveErrors upon toggling the link state (Q01193827).
- The maximum configurable value for RADIUS server retry time is now 20 seconds. (Q01234950-01)
- Non EAP Clients can now be authenticated successfully when multiple Radius servers are configured (Q01226753, Q01226761-01)
- CPU utilization values are now calculated correctly on an ERS 8300 (Q01265501)
- If an ACE is configured with both Acelid and Precedence set to the same value, the precedence value of an ACE will no longer be set to default value after reboot (Q01282637).
- On an ERS 8300, traffic from the management port will no longer be forwarded to the internal network (Q01237567-01).

### IP Unicast

#### General

- RIP version can now be configured as rip1 via NNCLI. (Q01205411-01)

- ERS 8300 will no longer display a warning message when a circuitless IP interface with 32 bit mask is deleted (Q01265965)
- The Ethernet Routing Switch 8300 will no longer allow route-discovery parameters to be set for a Non-routable VLAN (Q01148215-01).

## **8. Outstanding Issues**

- The statistics accumulated on the port will not being cleared when the LLDP status on the port is modified (Q01301623).
- The Ethernet Routing Switch 8300 will not send an LLDP shutdown frame when the port status is administratively disabled (Q01296071).

## **9. Known Limitations**

- JDM support is not provided for SNMP service for access policy. Modifying any access policy service via JDM will cause SNMP service to be disabled if it was previously enabled. (Q01249562)
- Creating IP Multicast groups in the xxx.0.0.xxx range will cause multicast streams to be flooded to all ports in the IGMP Snooping enabled VLAN even if there is a valid receiver configured. These IP multicast addresses map to IP Multicast Mac address which is used for control traffic (Q01314902).

Please see **Known limitations and considerations in this release** section of **Release Notes for the Ethernet Routing Switch 8300 Software Release 2.3 (Part No: 316811-F)**

## **11. Documentation Corrections**

None

---

Copyright © 2006 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globe mark, and Ethernet Routing Switch 8100/8600 are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

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>

## APPENDIX

### MIB Changes in Rel2.3.1.0 :

#### MIB Objects modified in this release

```
rcSysAccessPolicyService OBJECT-TYPE
    SYNTAX          INTEGER {
                    telnet(1),
                    snmp(2),
                    tftp(4),
                    ftp(8),
                    http(16),
                    rlogin(32),
                    ssh(64),
                    snmp-v3(128)
                    }
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION    "Is represented as bitset to indicate which protocol
                    this entry should be applied to."
    ::= { rcSysAccessPolicyEntry 5 }
```

#### MIB Objects added in this release

```
rcSysAccPolSnmpGrpTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF RcSysAccPolSnmpGrpEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION    "SNMP group list for access policy"
    ::= { rcSystem 95 }

rcSysAccPolSnmpGrpEntry OBJECT-TYPE
    SYNTAX          RcSysAccPolSnmpGrpEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION    "The table entry which covers the groups under SNMP service."
    INDEX { rcSysAccessPolicyId, rcSysAccPolSnmpGrpName, rcSysAccPolSnmpGrpModel }
    ::= { rcSysAccPolSnmpGrpTable 1 }

RcSysAccPolSnmpGrpEntry ::=
    SEQUENCE {
        rcSysAccPolSnmpGrpName SnmpAdminString,
        rcSysAccPolSnmpGrpModel SnmpSecurityModel,
        rcSysAccPolSnmpGrpRowStatus RowStatus
    }

rcSysAccPolSnmpGrpName OBJECT-TYPE
    SYNTAX          SnmpAdminString(SIZE(1..32))
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION    "The snmp-v3 group name"
    ::= { rcSysAccPolSnmpGrpEntry 1 }

rcSysAccPolSnmpGrpModel OBJECT-TYPE
    SYNTAX          SnmpSecurityModel
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION    "The snmp model"
    ::= { rcSysAccPolSnmpGrpEntry 2 }
```

```
rcSysAccPolSnmprGrpRowStatus OBJECT-TYPE
    SYNTAX          RowStatus
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION     "Row status"
 ::= { rcSysAccPolSnmprGrpEntry 3 }
```