NORTEL

Nortel Ethernet Routing Switch 8600

5.1 to 7.0 Release Delta

Release: 7.0
Document Revision: 01.01

www.nortel.com

NN46205-205

Contents

Introduction

This document describes the new features and related changes for the Ethernet Routing Switch 8600 Release 7.0.

Navigation

New features

The following sections describe the new features for the Ethernet Routing Switch 8600 Release 7.0.

8003-R 3-slot chassis

Nortel Ethernet Routing Switch 8600 Release 7.0 supports the new 8003-R 3-slot chassis. The 8003-R chassis provides two slots for interface modules and one slot for the Ethernet Routing Switch 8692 SF/CPU (with SuperMezz) or the new 8695 SF/CPU. Only R and RS modules are supported in the interface slots.

For more information about the 8003-R chassis, see *Nortel Ethernet Routing Switch 8600 Installation — Chassis* (NN45205-303).

8695 SF/CPU

The new 8695 SF/CPU is an enhanced version of the 8692 SF/CPU with Super Mezzanine daughter card, redesigned to give better performance at a reduced cost. Feature changes include replacing the existing PCMCIA slot with a Compact Flash (CF) card and changing the existing Ethernet management port from 10/100 to 10/100/1000.

The 8695 SF/CPU module performs the same functions as the 8692 SF/CPU with SuperMezz.

For more information about the 8695 SF/CPU, see *Nortel Ethernet Routing Switch 8600 Installation — Modules* (NN46205-304).

Enterprise Device Manager (EDM)

Starting with Release 7.0, Enterprise Device Manager (EDM) replaces the Java-based Device Manager.

EDM is a Web-based graphical user interface (GUI) for element management and configuration of the Ethernet Routing Switch 8600. EDM is an embedded application on the Ethernet Routing Switch, and the EDM Web server is the switch itself. You do not have to install any additional client software and there is no operating system dependency. EDM comes with each Ethernet Routing Switch and enables you to directly manage your switch.

To access EDM, you must enable the Web server on the Ethernet Routing Switch 8600. By default, the Web server is disabled.

The default EDM username and password combination is rwa/rwa. From the initial login page, you also need to specify the name of the desired VRF to log on to. For the global routing instance (VRF 0), enter GlobalRouter.

> **ATTENTION**
> If you have configured a username and password for Web server access in a previous release, these configured values remain unchanged in Release 7.0. To access EDM, use these previously configured username and password values. In this case, the rwa/rwa default values do not apply.

For more information on EDM, see *Nortel Ethernet Routing Switch User Interface Fundamentals* (NN46205-308).

IP Multinetting

By using the IP Multinetting feature, the Ethernet Routing Switch 8600 can support the configuration of multiple interfaces and IP interfaces on a single VLAN. A new type of VLAN, IpMultinetting, which is the extension of port-based VLANs, is implemented for IP Multinetting.

For more information about IP Multinetting, see *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517).

BPDU Filtering

To prevent unknown devices from influencing the Spanning Tree topology, the Ethernet Routing Switch 8600 supports Bridge Protocol Data Unit (BPDU) Filtering for Nortel Spanning Tree Groups (STPG), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP).

With BPDU Filtering, the network administrator can achieve the following:

- Block an unwanted root selection process when an edge device (for example, a laptop running Linux and enabled with STP) is added to the network. This prevents unknown devices from influencing an existing spanning tree topology.

- Block the flooding of BPDUs from an unknown device.

The STP BPDU Filtering feature is not supported on MLT, IST, SMLT, and RSMLT ports.

For more information about BPDU Filtering, *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517).

DHCP snooping

Dynamic Host Configuration Protocol (DHCP) snooping provides security to the network by preventing DHCP spoofing. DHCP snooping classifies ports into two types:

- Untrusted: ports that are configured to receive messages from outside the network or firewall. Only DHCP requests are allowed.

- Trusted: ports, such as switch-to-switch and DHCP server ports, that are configured to receive messages only from within the network. All types of DHCP messages are allowed.

To eliminate the capability to set up rogue DHCP servers on untrusted ports, the untrusted ports allow DHCP request packets only. DHCP replies and all other types of DHCP messages from untrusted ports are dropped.

DHCP snooping dynamically creates and maintains an IP-to-MAC binding table. You can also configure static DHCP binding entries.

For more information about DHCP snooping, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets in the network. It intercepts, discards, and logs ARP packets with invalid IP-to-MAC address bindings.

Without Dynamic ARP inspection, a malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet (man-in-the-middle attacks). Dynamic ARP Inspection prevents this type of attack.

> **ATTENTION**
> For Dynamic ARP inspection to function, you must enable DHCP snooping globally and on the VLAN.

When you enable Dynamic ARP inspection, ARP packets on untrusted ports are filtered based on the source MAC and IP addresses. The switch forwards an ARP packet when the source MAC and IP addresses match an entry in the DHCP snooping IP-to-MAC binding table. Otherwise, the ARP packet is dropped.

Like DHCP snooping, Dynamic ARP Inspection supports MLT/SMLT ports as trusted ports only.

For more information about Dynamic ARP Inspection, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

IP Source Guard

IP Source Guard is a security feature that validates IP packets by intercepting IP packets with invalid IP-to-MAC bindings.

IP Source Guard works closely with DHCP snooping and prevents IP spoofing by allowing only IP addresses that are obtained through DHCP on a particular port. Initially, all IP traffic on the port is blocked except for the DHCP packets that are captured by DHCP snooping. When a client receives a valid IP address from the DHCP server, traffic on the port is permitted when the source IP and MAC addresses match a DCHP binding table entry for the port. Any IP traffic that does not match an entry in the DHCP binding table is filtered out. This filtering limits the ability of a host to attack the network by claiming a neighbor host's IP address.

> **ATTENTION**
> For IP Source Guard to function, you must enable DHCP snooping and Dynamic ARP Inspection globally and at the VLAN level. To enable IP Source Guard on a port, the port must be configured as untrusted for DHCP snooping and untrusted for Dynamic ARP Inspection.

IP Source Guard cannot be enabled on MLT/SMLT ports.

For more information about IP Source Guard, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

IGMP Layer 2 querier

In a multicast network, if the multicast traffic only needs to be Layer 2 switched, no multicast routing is required. However, for multicast traffic to flow from sources to receivers, an IGMP querier must exist on the network, a function that is normally provided by a multicast router.

To provide a querier on a Layer 2 network without a multicast router, you can use IGMP Layer 2 querier.

The IGMP Layer 2 querier provides the querier functions of a multicast router on the Layer 2 multicast network, forwarding queries for multicast traffic and processing the responses accordingly. On the connected Layer 2 VLANs, IGMP snoop continues to provide services as normal, responding to queries and identifying receivers for the multicast traffic.

To enable Layer 2 querier, you must configure an IP address for the querier, in order for it to receive forwarded report and leave messages.

In the Layer 2 multicast network, enable Layer 2 querier on one of the switches in the VLAN. Only one Layer 2 querier is supported in the same Layer 2 multicast domain. No querier election is available.

If a multicast router is present on the network, the Layer 2 querier is automatically disabled.

For more information about IGMP Layer 2 querier, see *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).

Multicast VLAN Registration (MVR)

With IGMP snoop enabled on a Layer 2 VLAN, all the ports, including receiver and source ports, are members of the same VLAN. When users in different VLANs join the same multicast group, the multicast router replicates one stream into multiple streams that are sent to these VLANs. Multiple streams waste bandwidth and decrease the performance of the multicast router.

The Multicast VLAN Registration (MVR) Protocol solves this problem. With MVR, the receiver ports remain in the IGMP Snoop VLAN, but one VLAN is designated as the MVR VLAN.

The MVR VLAN has a source port, which connects to the multicast router. After you bind several IGMP Snoop VLANs to the MVR VLAN, and a multicast data packet arrives from the source port, the switch replicates this packet and forwards it to all the IGMP Snoop VLANs that are bound to the MVR VLAN.

After you enable MVR globally, all IGMP control packages that are received from IGMP Snoop VLANs that are bound to the MVR VLAN (including report, leave, and query) are processed by MVR.

Each VRF on the Ethernet Routing Switch 8600 supports only one MVR VLAN.

You cannot enable MVR and Layer 2 querier on the same VLAN.

MVR is designed to work on the edge only. Do not enable MVR in the core network.

For more information about MVR, see *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).

PIM-SSM with SMLT

With Release 7.0, fast failover for multicast traffic in a PIM-SSM network is supported using SMLT/RSMLT. PIM-SSM is supported in triangle, square, and full mesh SMLT/RSMLT topologies.

For more information about PIM-SSM with SMLT, see *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).

Key Health Indicator (KHI) enhancements

Release 7.0 supports Key Health Indicators (KHI) that allow for the collection of statistics and information about the health of the system for troubleshooting purposes related to system failure. The Key Health Indicator (KHI) feature identifies a small number of key health indicators that allow quick assessment of the overall operational state of the Ethernet Routing Switch 8600. These indicators do not provide complete coverage of all possible failure scenarios. Rather, KHI is a diagnostic tool for the health of the switch. Further debugging is required to correctly understand the system state and actions required to remedy the situation.

KHI provides global health information for the switch, including:

- Chassis health indication
- CPU performance health indication
- Port state change indication
- Forwarding health indication
- IP interface configuration and operation information
- Protocol information
- Management information: Log, TCP, UDP and Users

For more information on KHI, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

Route Switch Processor Packet Tracing

Release 7.0 supports Route Switch Processor (RSP) Packet Tracing which provides support for co-processor (COP) debug commands.

When you enable Packet Tracing, the CP sends a message to the COP and Packet Tracing is internally enabled on the COP. Similarly, when Packet Tracing is disabled on the CP, it is disabled on the COP. By default the Packet Tracing is enabled for one second. After one second, the Packet Tracing is disabled internally. While enabling the Packet Tracing, RSP selection is based on port by default—a port number is internally converted into RSP-ID and Packet Tracing is enabled on that lane. Therefore, when Packet Tracing is enabled using one port, it displays enabled on all the ports in that lane. Packet Tracing is collected on the COP and it is sent to the CP when you enter the RSP dump trace command through the CLI or NNCLI.

For more information on RSP Packet Tracing, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

ERCD Records Dump

Release 7.0 provides support for Enterprise RSP Control Driver (ERCD) Records Dump for the following:

- ARP

- IP

- IP subnet

- MAC

- MAC_VLAN

- MGID

- Protocol

- VLAN

The dump ercdRecords command dumps the specified ERCD records. The ERCD records dump is requested by the CP to the COP and then the records are obtained at the COP and replied back to the CP. The CP displays the records on the CLI or NNCLI prompt.

For more information on ERCD Record dump, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

IPv6 RSMLT

While Nortel's Routed Split Multilink Trunk (RSMLT) functionality originally provided sub-second failover for IPv4 forwarding only, Release 7.0 extends RSMLT functionality to IPv6. The overall model for IPv6 RSMLT is essentially identical to that of IPv4 RSMLT. In short, RSMLT peers exchange their IPv6 configuration and track each other's state by means of IST messages. An RSMLT node always performs IPv6 forwarding on the IPv6 packets destined to the peer's MAC addresses. When an RSMLT node detects that its RSMLT peer is down, the node also begins terminating IPv6 traffic destined to the peer's IPv6 addresses.

With RSMLT enabled, an SMLT switch performs IP forwarding on behalf of its SMLT peer – thus preventing IP traffic from being sent over the IST.

IPv6 RSMLT supports the full set of topologies and features supported by IPv4 RSMLT, including SMLT triangles, squares, and SMLT full-mesh topologies, with routing enabled on the core VLANs.

With IPv6, you must configure the RSMLT peers using the same set of IPv6 prefixes.

Supported routing protocols include the following:

- IPv6 Static Routes
- OSPFv3

Note that the Ethernet Routing Switch 8600 does not support the configuration of an IST over IPv6. IST is supported over IPv4 only.

For more information about RSMLT over IPv6, see *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504).

IPv6 VRRP

To provide fast failover of a default router for IPv6 LAN hosts, the Ethernet Routing Switch 8600 supports the Virtual Router Redundancy Protocol (VRRP v3) for IPv6 (defined in draft-ietf-vrrp-ipv6-spec-08.txt).

VRRPv3 for IPv6 provides a faster switchover to an alternate default router than is possible using the IPv6 Neighbor Discovery (ND) protocol. With VRRPv3, a backup router can take over for a failed default router in approximately three seconds (using VRRPv3 default parameters). This is accomplished without any interaction with the hosts and with a minimum amount of VRRPv3 traffic.

The operation of Nortel's IPv6 VRRP implementation is similar to the IPv4 VRRP operation, including support for hold-down timer, critical IP, fast advertisements, and backup master. With backup master enabled, the backup switch routes all traffic according to its routing table. It does not Layer 2-switch the traffic to the VRRP master.

New to the IPv6 implementation of VRRP, you must specify a link-local address to associate with the virtual router. Optionally, you can also assign global unicast IPv6 addresses to associate with the virtual router. Network prefixes for the virtual router are derived from the global IPv6 addresses assigned to the virtual router.

For more information about VRRP over IPv6, see *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504).

BGP+

Ethernet Routing Switch 8600 extends the BGPv4 process to support the exchange of IPv6 routes using BGPv4 peering. BGP+ is an extension of BGPv4 for IPV6.

Note that the Ethernet Routing Switch 8600 BGP+ support is not an implementation of BGPv6. Native BGPv6 peering uses the IPv6 Transport layer (TCPv6) for establishing the BGPv6 peering, route exchanges, and data traffic. Native BGPv6 peering is not supported in Release 7.0.

Ethernet Routing Switch 8600 supports the exchange of BGP+ reachability information over IPv4 transport. To support BGP+, the Ethernet Routing Switch supports two BGP protocol extensions, standards RFC 4760 (multi-protocol extensions to BGP) and RFC 2545 (MP-BGP for IPv6). These extensions allow BGPv4 peering to be enabled with IPv6 address family capabilities.

The Ethernet Routing Switch 8600 implementation of BGP+ uses an existing TCPv4 stack to establish a BGPv4 connection. Optional, nontransitive BGP properties are used to transfer IPv6 routes over the BGPv4 connection. Any BGP+ speaker has to maintain at least one IPv4 address to establish a BGPv4 connection.

Different from IPv4, IPv6 introduces scoped unicast addresses, identifying whether the address is global or link-local. When BGP+ is used to convey IPv6 reachability information for inter-domain routing, it is sometimes necessary to announce a next hop attribute that consists of a global address and a link-local address. For BGP+, no distinction is made between global and site-local addresses.

The BGP+ implementation includes support for BGPv6 policies, including redistributing BGPv6 into OSPFv3, and advertising OSPFv3, static, and local routes BGPv6 (through BGP+). It also supports the aggregation of global unicast IPv6 addresses, as well as confederations and partial HA.

The basic configuration of BGP+ is the same as BGPv4 with one additional parameter added and some existing commands altered to support IPv6 capabilities. You can enable and disable IPv6 route exchange by specifying the address family attribute as IPv6. Note that an IPv6 tunnel is required for the flow of IPv6 data traffic.

BGP+ is only supported on the global VRF instance.

For more information about BGP+, see *Nortel Ethernet Routing Switch 8600 Configuration – BGP Services* (NN46205-510).

IPv6 RADIUS

The Ethernet Routing Switch 8600 supports RADIUS over IPv6 networks to provide security against unauthorized access.

For more information about RADIUS over IPv6, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

IPv6 DHCP Relay

The Dynamic Host Configuration Protocol (DHCP) for IPv6 (RFC 3315) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCP supports automatic allocation of reusable network addresses and of additional configuration parameters.

IPv6 DHCP clients use link-local addresses to send and receive DHCP messages. To allow a DHCP client to send a message to a DHCP server that is not attached to the same link, you must configure a DHCP relay agent on the client's link to relay messages between the client and server. The operation of the relay agent is transparent to the client.

A relay agent relays messages from clients and messages from other relay agents.

For more information about DHCP Relay over IPv6, see *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504).

Singular Record Operations

Release 7.0 provides support to flush single MAC records, single ARP records and single IP Multicast records. For more information, see *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517), *Nortel Ethernet Routing Switch 8600 Configuration — IP Routing* (NN46205-523) and *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501), respectively.

show debug generic

The `show debug generic [verbose]` command is mainly used for debugging purposes only. It displays information from multiple system shell commands. For more information, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

Feature impacts

This section describes the impacts of the new Release 7.0 features under the following categories:

Planning and engineering

Release 7.0 features can impact the planning and engineering of your network. For network design guidelines for Release 7.0, see *Nortel Ethernet Routing Switch 8600 Planning and Engineering — Network Design* (NN46205-200).

Upgrades and patches

The following are upgrade considerations for Release 7.0:

- Classic modules, including E and M modules, are not supported with release 7.0, and therefore must be removed before you perform an upgrade. You must also remove the nonsupported 8691 SF/CPU module and the 8692 SF/CPU module without SuperMezz (the 8692 SF/CPU module is supported if equipped with SuperMezz). For more information, see "Restrictions and limitations" (page 22) and *Nortel Ethernet Routing Switch 8600 Upgrades — Software Release 7.0* (NN46205-400).

- When booted with a software version older than Release 7.0, the 8692 SF/CPU does not recognize the 8003-R chassis or the high-speed fan (DS1411037-E5). This results in hardware warnings being continually generated on the console that makes it difficult to commission the node. As a result, if the 8692 SF/CPU is not running Release 7.0, you must upgrade the switch fabric for use with the 8003-R (3-slots chassis). For more information, see *Upgrading the switch fabric for use with the 8003-R (3-slot chassis)* (NN46214-901).

- As EDM replaces the Jave-based Device Manager, there is no longer any need to update Device Manager. However, to provide on-product help for EDM, you must download the latest EDM help file from the Nortel support portal and specify the location of this help file for EDM to access it. For more information, see *Nortel Ethernet Routing Switch User Interface Fundamentals* (NN46205-308).

Configuration

The new EDM graphical user interface (GUI) replaces the Java-based Device Manager. The paths used to access configuration tabs in EDM are similar to those used in Device Manager. For more information, see the relevant configuration guides for your features.

The following Release 7.0 features provide new CLI and NNCLI configuration commands on the Ethernet Routing Switch 8600. For more information on these commands, see the applicable configuration guide:

- IP Multinetting

  (See *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517).)

- BPDU Filtering

  (See *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517).)

- DHCP Snooping

  (See *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).)

- Dynamic ARP

  (See *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).)

- IP Source Guard

  (See *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).)

- IGMP Layer 2 Querier

  (See *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).)

- Multicast VLAN Registration (MVR)

  (See *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).)

- KHI, ERCD Records Dump, RSP Packet Tracing, and show debug generic

  (See *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).)

- IPv6 VRRP

  (See *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504))

- BGP+

  (See *Nortel Ethernet Routing Switch 8600 Configuration – BGP Services* (NN46205-510))

- IPv6 RADIUS

(See *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).)

- IPv6 DHCP Relay

    (See *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504))

- Singular Record Operations

    (See *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517), *Nortel Ethernet Routing Switch 8600 Configuration — IP Routing* (NN46205-523) and *Nortel Ethernet Routing Switch 8600 Configuration — IP Multicast Routing Protocols* (NN46205-501).

The following features do not introduce any new CLI/NNCLI configuration commands:

- PIM-SSM with SMLT
- 8003-R chassis (uses the same commands existing chassis)
- 8695 SF/CPU (uses the same commands as the 8692 SF/CPU)

    Note that the 8692 SF/CPU with SuperMezz displays the external flash card inserted in the PCMCIA slot as `/pcmcia`. The 8695 SF/CPU replaces the PCMCIA slot with a compact flash slot, but still displays the flash card as `/pcmcia` for backwards compatibility.

The IPv6 RSMLT feature does not introduce new configuration commands as it uses the same configuration commands provided for IPv4 RSMLT. However, there are some new IPv6-specific RSMLT tabs in EDM. For more information, see *Nortel Ethernet Routing Switch 8600 Configuration — IPv6 Routing* (NN46205-504)

Routine maintenance

The new 8003-R chassis introduces modified routine maintenance procedures, including the replacement of fan trays and power supplies. For more information, see *Nortel Ethernet Routing Switch 8600 Routine Maintenance* (NN46205-312). This document is also updated to refer to the new 8695 SF/CPU.

Accounting

The RADIUS feature, including RADIUS accounting, is implemented over IPv6. For more information, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

Administration and security

The following new features provide additional security capabilities on the Ethernet Routing Switch 8600.

- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- RADIUS over IPv6

For more information on these features, see *Nortel Ethernet Routing Switch 8600 Security* (NN46205-601).

In addition, the BPDU filtering feature provides additional security to Spanning Tree networks. For more information, see *Nortel Ethernet Routing Switch 8600 Configuration — VLANs and Spanning Tree* (NN46205-517).

Fault management

New logs have been added to the system for the new Release 7.0 features. For more information, see *Nortel Ethernet Routing Switch 8600 Logs Reference* (NN46205-701).

KHI, ERCD Records Dump, RSP Packet Tracing, and show debug generic are new troubleshooting features for 7.0. For more information, see *Nortel Ethernet Routing Switch 8600 Troubleshooting* (NN46205-703).

Performance management

Release 7.0 replaces the Java-based Device Manager with EDM, which affects the configuration of performance management, along with all other configuration screens previously accessible using Device Manager.

For more information, see *Nortel Ethernet Routing Switch 8600 Performance Management* (NN46205-704).

Restrictions and limitations

The following are some of the restrictions and limitations associated with Release 7.0. For detailed feature restrictions and limitations, refer to the appropriate guide for the specific features.

- The 8003 chassis is no longer supported. It is replaced by the 8003-R chassis.
- The 8003-R chassis and 8695 SF/CPU both require the minimum Release 7.0 software.

- With Release 7.0, the 8692 SF/CPU must be equipped with the SuperMezz daughtercard for proper operation. The 8692 SF/CPU without SuperMezz is not supported with Release 7.0.

- The 8001AC, 8002DC, 8003AC, and Breaker Interface Panel are no longer supported.

- Release 7.0 supports R/RS Modules only. The following Classic modules are no longer supported:
  — 8608GBE module
  — 8608GBM module
  — 8608GTE module
  — 8608GTM module
  — 8608SXE module
  — 8616GTE module
  — 8616SXE module
  — 8624FXE module
  — 8632TXE module
  — 8632TXM module
  — 8648TXE module
  — 8648TXM module
  — 8672ATME module
  — 8672ATMM module
  — 8683POSM module
  — 8690 SF/CPU module
  — 8691 SF/CPU module
  — WSM module
  — 8660 Service Delivery Module
  — Media Dependent Adapters for the 8672ATME and 8672ATMM Modules

- M mode is no longer supported. The software runs in R mode by default.

- IGMP Layer 2 querier is not supported with Multicast VLAN Registration (MVR) on the same VLAN.

- IPv6 RSMLT does not support IPv6 IST. The IST in IPv6 RSMLT must be an IPv4 IST.

- IPv6 VRRP, like IPv4 VRRP, cannot enable critical IP and backup master at the same time.

- BGP+ does not provide native IPv6 peering.

- BGP+ convergence in case of SMLT scenarios cannot be guaranteed. Nortel does not recommend to configure BGP peers between SMLT core routers or in between the core router and any switch connecting through SMLT links for the failover scenarios.

Nortel Ethernet Routing Switch 8600

5.1 to 7.0 Release Delta

Release: 7.0
Publication: NN46205-205
Document revision: 01.01
Document release date: 21 December 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com