Part No. 316859-F Rev 01
October 2004
4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1600 Series Switch Software Release 1.2

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

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 Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and PASSPORT are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

IPX is a trademark of Novell, Inc.

SSH is a trademark of SSH Communication Security.

TACACS+ is a trademark of Cisco Systems.

SecureCRT is a trademark of VanDyke Software, Inc.

SecureNetterm is a trademark of InterSoft International, Inc.

AbsoluteTelnet is a trademark of Celestial Software.

PenguiNet is a trademark of Silicon Circus Ltd.

F-Secure is a trademark of F-Secure Corporation.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed

by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS),

WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Introduction

These release notes describe the Nortel Networks* Passport 1600 Series switch 1.2 software, its file names, download process, and supported software and hardware capabilities. They also describe the new Spanning Tree Protocol features, documentation corrections and enhancements, and known issues and bugs that still exist in software release 1.2.

The following topics are discussed in this document:

File names for this release

The Passport 1600 Series switch software release 1.2 contains the following files:

Note: The Passport 1600 Series switch software release 1.2 contains two different images.

One image contains the SSH encryption algorithms: **p16c1200.img**

One image does **not** contain the SSH encryption algorithms: p16a1200.img. SSH cannot be configured using this image.

Name	Description
p16c1200.img	Run-time image file with SSH encryption algorithms
p16a1200.img	Run-time image file without SSH encryption algorithms
jdm_584.exe	Supported PC JDM version (Windows 95 and later)
jdm_584.sh	Supported Unix JDM version (Solaris SPARC only)
p16a1200.mib.zip	MIB zip file
Supported MIB files	
Private MIBs	
SSH.mib	Secure Shell MIB
Commgmt.mib	Structure of common management information for the proprietary enterprise
dvmrp.mib	MIB module for management of DVMRP routers (Experimental)
AAC.mib	System access authentication control
Framework.mib	SNMP management architecture MIB

Name	Description
iana-rtproto.mib	IANAipRouteProtocol and IANAipMRouteProtocol textual conventions for use in MIBs which need to identify unicast or multicast routing mechanisms
L2mgmt.mib	Structure of Layer 2 network management information for the proprietary enterprise
L3mgmt.mib	Structure of Layer 3 network management information for the proprietary enterprise
PriL3mgmt.mib	Proprietary definitions
rapid_city.mib**	Nortel/Rapid-City communications enterprise MIB
s5emt103.mib	Nortel/SynOptics 5000 Ethernet multi-segment MIB release 1.0.3
s5roo114.mib	Nortel/SynOptics 5000 root MIB release 1.1.4
s5tcs112.mib	Nortel/SynOptics 5000 common textual conventions MIB release 1.1.2
nnmst000.mib	Nortel Networks MSTP proprietary MIB
draft-bridge.mib	STP path cost
RapidSTP.mib	Nortel Networks RSTP proprietary MIB
synro204.mib	Replaces synro185.mib to add some new definitions.
s5age.mib	Nortel Networks SNTP proprietary MIB
** The Passport 1600 switch software implements only a limited portion of the rapid_city.mib.	
Standard MIBs/RFCs related to network management	
rfc1213.mib	MIB for network management of TCP/IP-based internets: MIB-II
rfc1215.mib	A convention for defining traps for use with the SNMP
rfc1513.mib	Token ring extensions to the remote network monitoring MIB
rfc1643.mib	Definitions of managed objects for the Ethernet-like interface types
rfc1724.mib	RIPv2 MIB extension
rfc1757.mib	Remote network monitoring MIB (support of alarms, events, statistics and history groups)
rfc1850.mib	OSPFv2 MIB

Name	Description
rfc2021.mib	Remote network monitoring MIB Version2 using SMIv2
rfc2096.mib	IP forwarding table MIB
rfc2233.mib	The interfaces group MIB using SMIv2
rfc2674.mib	Definitions of managed objects for bridges with traffic classes, multicast filtering and virtual LAN extensions
rfc2787.mib	VRRP MIB. Partial implementation and some proprietary extensions
rfc2932.mib	IPv4 multicast routing MIB
rfc2933.mib	Internet Group Management Protocol MIB

Supported Standards	
802.3 CSMA/CD Ethernet (ISO/IEC 8802-3)	802.3i 10BaseT (ISO/IEC 8802-3)
802.3u 100BaseT (ISO/IEC 8802-3)	802.3z (Gigabit Ethernet)
802.1Q and 802.1p (VLAN tagging & Prioritization)	802.3ab (Gigabit Ethernet Over Copper)
802.1w RSTP (Rapid Spanning Tree Protocol)	802.1s MSTP (Multiple Spanning Tree Protocol)
802.1D (MAC bridges/Spanning Tree Protocol)	802.3x (Flow Control)
Supported RFCs	
rfc768 (UDP protocol)	rfc783 (TFTP protocol)
rfc791 (IP protocol)	rfc793 (TCP protocol)
rfc826 (ARP protocol)	rfc854 (Telnet protocol)
rfc1542(BootP)	rfc1058 (RIP version 1)
rfc1112 (IGMPv1)	draft-ietf-magma-snoop-10 (IGMP Snoop)
rfc1583 (OSPFv2)	rfc1723 (RIPv2)
rfc1724 (RIPv2 extensions)	rfc1812 (Router Requirements)

rfc1866 (Hypertext Markup Language v2.0)	rfc 2030 (Simple Network Time Protocol (SNTP))
rfc2068 (Hyper Text Transfer Protocol)	rfc2131 (Dynamic Host Control Protocol (DHCP))
rfc2236 (IGMPv2)	rfc2178 (MD5 encryption for OSPF)
rfc2338 (Virtual Router Redundancy Protocol)	draft-ietf-idmr-dvmrp-v3-11 (Distance Vector Multicast Routing Protocol)

The Passport 1600 Series Switch MIB files can be found on the Nortel Networks Web site:

http://www.nortelnetworks.com.

To access the MIB files:

1. Under Support, select Software Downloads.
2. Under Software, choose Passport.
3. Under Passport 1600 Layer 3 Switch, choose Software.

Supported software and hardware capabilities

Table 1 lists the current values for supported capabilities for software release 1.2. Unless otherwise noted, values represented in this table are maximum values. Actual values are dependent on implementation.

Table 1 Hardware and software capabilities

Hardware/Software	Capabilities
Hardware records - MAC	8000
Dynamic ARP entries	1372
Static ARP entries	32
VLANs	2048
Protocol-based VLANs	11
IP Subnet-based VLANs	12
Spanning Tree Group	8 (MSTP) (includes CIST)
Aggregation groups*	7
Ports per MLT group	up to 4 per aggregation group
IP interfaces	64
VRRP IDs	32
Static IP routes	up to 512 with configuration
RIP routes	1918 (see Table 2 on page 13)
OSPF areas per switch	4
OSPF adjacencies (neighbors) per switch	32
OSPF routes per switch	1918 (see Table 2 on page 13)
OSPF virtual links per Area	4
MTU**	1518 (1522 for tagged ports)
Multicast streams	64 (S, G)
DVMRP routes	1024
DVMRP interfaces	64 (same as IP interface maximum)

Hardware/Software	Capabilities
IGMP Snoop VLANs	256
* Aggregation groups are statically compliant with the IEEE 802.3ad standard.These groups should be of the same type. ** Jumbo frames are not supported in release 1.2 of the Passport 1600 Series switch software.	

Table 2 Maximum supported hardware and software routes for RIP and OSPF

Hardware size			
Ratio	**UC prefix (entry)**	**MC prefix (entry)**	
100/0	1916	0	
75/25	1404	64	
50/50	892	64	
Software Size			
Ratio	**Route entry**	**Arp entry**	**IPMC entry**
100/0	1884/32	1884/32	0
75/25	1372/32	1372/32	64
50/50	860/32	860/32	64
Note: Route entry and Arp entry values indicate dynamic routes/static routes. For example, the 75/25 ratio for Route entry indicates 1372 dynamic routes with 32 static routes.			

In software release 1.2, the Passport 1600 Series switch supports the following SFP (Small Form-factor Pluggable) modules:

- AA1419013 1-port 1000Base-SX connector type: LC
- AA1419014 1-port 1000Base-SX connector type: MT-RJ
- AA1419015 1-port 1000Base-LX connector type: LC
- AA1419025 1-port 1000BaseCWDM- 1470nm wavelength- 40km
- AA1419026 1-port 1000BaseCWDM- 1490nm wavelength- 40km
- AA1419027 1-port 1000BaseCWDM- 1510nm wavelength- 40km
- AA1419028 1-port 1000BaseCWDM- 1530nm wavelength- 40km

- AA1419029 1-port 1000BaseCWDM- 1550nm wavelength- 40km
- AA1419030 1-port 1000BaseCWDM- 1570nm wavelength- 40km
- AA1419031 1-port 1000BaseCWDM- 1590nm wavelength- 40km
- AA1419032 1-port 1000BaseCWDM- 1610nm wavelength- 40km
- AA1419033 1-port 1000BaseCWDM- 1470nm wavelength- 70km
- AA1419034 1-port 1000BaseCWDM- 1490nm wavelength- 70km
- AA1419035 1-port 1000BaseCWDM- 1510nm wavelength- 70km
- AA1419036 1-port 1000BaseCWDM- 1530nm wavelength- 70km
- AA1419037 1-port 1000BaseCWDM- 1550nm wavelength- 70km
- AA1419038 1-port 1000BaseCWDM- 1570nm wavelength- 70km
- AA1419039 1-port 1000BaseCWDM- 1590nm wavelength- 70km
- AA1419040 1-port 1000BaseCWDM- 1610nm wavelength- 70km
- AA1419043 1-port 1000BASE-T Small Form Pluggable (SFP), 8-pin modular connector (RJ-45).

New features in release 1.2

Multiple Spanning Tree Protocol groups

The Passport 1600 Series switches support the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

Starting with software release 1.2**,** the Passport 1600 Series switches support multiple Spanning Tree Groups (STGs), based on the 802.1s standard (MSTP). The Passport 1600 Series switches support a maximum of 8 STGs. Multiple STGs provide multiple data paths, which can be used for load-balancing and redundancy. Enable load balancing between two Passport 1600 Series switches using multiple STGs by configuring each path with a different VLAN and then assigning each VLAN to a separate STG**.** Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

Note: The 802.1s implementation in software release 1.2 is not compatible with the pre 802.1s implementation called “Nortel STGs” done by the Passport 8600. You must use a special version of software, called Passport 8600 3.7.0.2, to support the 802.1s standard. Please contact your Nortel Networks representative for more information.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLANs). With software release 1.2, the Passport 1600 Series switches support multiple instances (8) of STGs running simultaneously.

The Passport 1600 Series switches with software release 1.2 support a maximum of 2048 VLANs. With a maximum of 8 STGs, on average, each STG can have 256 VLANs.

In the default configuration of the Passport 1600 Series switches, a single STG with the ID of 0, called the *instance 0* or *CIST,* includes all ports on the switch. Although a VLAN can be added to or deleted from the default STG, the instance 0 (STG0) itself **cannot** be deleted from the system.

The tagging for the BPDUs from STG0, or the default STG, is user-configurable (as are tagging settings for all STGs). However, by default STG0 sends out only untagged BPDUs in order to operate with all devices that support only one instance of STP.

All other STGs, except the Default STG, must be created by the user. To become active, each STG must be enabled by the user after creation. Each STG will be assigned an ID number from 1 to 7 (the Default STG is assigned the ID number 0). You assign a VLAN or VLANs to an active STG. However, a port that is not a member of a VLAN will not be allowed to join an STG.

When you no longer need a particular STG, disable and delete that particular one. The procedure is to disable the STG, delete all VLAN and port memberships, and then delete the STG.

STG configuration guidelines

This section provides important information on configuring STGs:

- An STG must be created in the following order:
  - — Create the STG.
  - — Add the existing VLAN and port memberships.
  - — Enable the STG.
- When you create a VLAN, that VLAN automatically belongs to STG 0, the default STG. If you want the VLAN in another STG, you must move the VLAN by assigning it to another STG.
- To move a newly created VLAN to an existing STG:
  - — Create the VLAN.
  - — Add the VLAN to an existing STG.
- You can move default VLAN from instance 0 to another instance.

- VLANs must be contained **within** a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.
- All VLANs in the same shared database (SVL) must be assigned to the same STG.
- All members of a particular MultiLink Trunking (MLT) group must be assigned to the same STG.

Rapid Spanning Tree Protocol

Prior to the Passport 1600 Series switch software release 1.2, the Spanning Tree implementation is based on IEEE 802.1d which is slow to respond to a topology change in the network (for example, a dysfunctional link in a network).

The Rapid Spanning Tree protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains a backward compatibility with the IEEE 802.1d which was the Spanning Tree implementation prior to RSTP. In certain configurations the recovery time of RSTP can be reduced to less than 1 second.

RSTP also reduces the amount of flooding in the network by enhancing the way the Topology Change Notification (TCN) packet is generated.

The Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s) allows you to configure multiple instances of RSTP on the same switch. Each RSTP instance can include one or more VLANs.

RSTP and MSTP enable the Passport 1600 Series switch to achieve the following:

- Reduce converging time from 30 seconds to less than 1 or 2 seconds when there is topology change in the network (that is, port going up or down).
- Eliminate unnecessary flushing of the MAC database and flooding of traffic to the network, with the new Topology Change mechanism.
- Under MSTP mode, 8 instances of RSTP can be supported simultaneously. Instance 0 or CIST is the default group which includes default VLAN 1. Instances 1 to 7 are called MSTIs 1-7.

- The user can configure the switch to run MSTP, RSTP, or STP configuration.

Interoperability with legacy STP

RSTP provides a new parameter ForceVersion for backward compatibility with legacy STP. The user can configure a port in either STP compatible mode or RSTP mode.

- An STP compatible port transmits and receives only STP BPDU. Any RSTP BPDU that the port receives in this mode will be discarded.
- An RSTP compatible port transmits and receives only RSTP BPDU. If an RSTP port receives an STP BPDU, it becomes an STP port. User intervention is required to bring this port back to RSTP mode. This process is called Port Protocol Migration.

Differences between STP and RSTP

Differences in port roles

RSTP is an enhanced version of STP. These two protocols have almost the same set of parameters.

Table 3 lists the differences in port roles for STP and RSTP. STP supports two port roles while RSTP supports four port roles.

Table 3 Differences in port roles for STP and RSTP

Port Role	STP	RSTP	Description
Root	Yes	Yes	This port is receiving a better BPDU than its own and it has the best path to reach the Root. Root port is in Forwarding state.
Designated	Yes	Yes	This port has the best BPDU on the segment. Designated port is in Forwarding state.

Table 3 Differences in port roles for STP and RSTP

Port Role	STP	RSTP	Description
Alternate	No	Yes	This port is receiving a better BPDU than its own BPDU and there is a Root port within the same switch. Alternate port is in Discarding state.
Backup	No	Yes	This port is receiving a better BPDU than its own BPDU and this BPDU is from another port within the same switch. Backup port is in Discarding state.

Edged Port

Edged port is a new parameter that is supported by RSTP. When a port is connected to a non-switch device, such as a PC or a workstation, it must be configured as an Edged port. An active Edge port goes directly to the Forwarding state without any delay. An Edged port becomes a non-Edged port if it receives a BPDU.

Path cost values

RSTP and MSTP recommend new path cost values that support a wide range of link speeds. Table 4 lists the recommended path cost values.

Table 4 Recommended path cost values

Link speed	Recommended value
Less than or equal 100Kb/s	200 000 000
1 Mb/s	20 000 000
10 Mb/s	2 000 000
100 Mb/s	200 000
1 Gb/s	20 000
10 Gb/s	2 000
100 Gb/s	200
1 Tb/s	20
10 Tb/s	2

Rapid convergence

In RSTP and MSTP the environment root port or the designated port can ask its peer for permission for going to the Forwarding State. If the peer agrees then the root port can move to the Forwarding State without any delay. This procedure is called Negotiation Process.

RSTP and MSTP also allow information received on a port to be sent immediately if the port becomes dysfunctional instead of waiting for the Maximum Age time.

The following example illustrates how an RSTP port state can move rapidly to the Forwarding state without the risk of creating a loop in the network.

Switch A: ports 1 and 2 are in full duplex. Port 2 is an Edged port

Switch B: ports 1, 2 and 3 are in full duplex. Port 2 is an Edged port.

Switch C: ports 1 and 2 are in full duplex. Port 2 is an Edged port

Switch A is the Root.

Negotiation Process

After power up, all ports assume the role as Designated ports. All ports are in the Discarding state except Edged ports. Edged ports go directly to the Forwarding state without delay.

Switch A port 1 and switch B port 1 exchange BPDUs and switch A knows that it is the Root and switch A port 1 is the Designated port. Switch B learns that switch A has better priority. Switch B port 1 becomes Root port. Both switch A port 1 and switch B port 1 are still in the Discarding state.

Switch A starts the negotiation process by sending BPDU with proposal bit set.

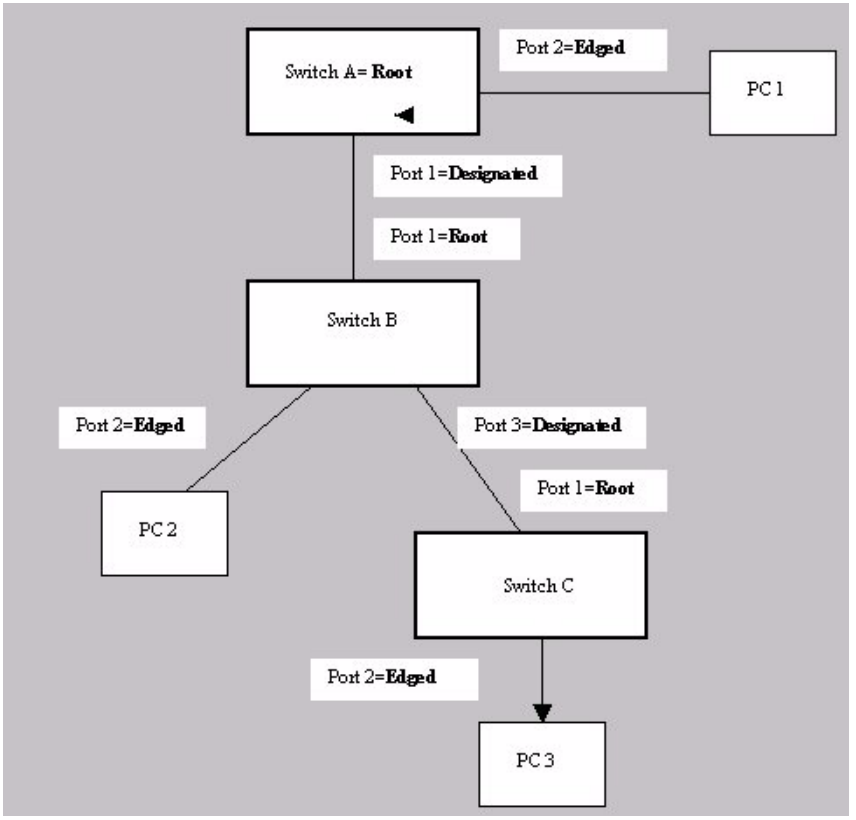
Switch B receives proposal BPDU and it will set its non-Edge ports to the Discarding state. This operation is the sync to synced process.

Switch B sends a BPDU with the agreement bit set to switch A.

Switch A sets port 1 to Forwarding and switch B sets port 1 to the Forwarding state. PC 1 and PC 2 can talk to each other.

- The negotiation process now moves down to switch B port 3 and its partner port.
- PC 3 cannot talk to either PC 1 or PC 2 until the negotiation process between switch B and switch C is complete.

Figure 1 Negotiation process



The RSTP convergent time depends on how quickly the switch can exchange BPDUs during the Negotiation process, and the number of switches in the network. For a Passport 1600 switch, the convergent time depends on the hardware platform and the number of active applications running on the switch.

Configurable Telnet banner

The Passport 1600 Telnet banner is now configurable. Setting the default banner parameter to true uses the default banner. Otherwise, the Passport 1600 displays the banner specified by the *string* parameter. (Q00893786)

The syntax for this feature is as follows:

```
config banner {add < banner_string 255> | default
< TRUE| FALSE>| delete }
show banner
```

Static ARP entries with multicast MAC addresses

The Passport 1600 Series switch now supports configuring static ARP entries with multicast MAC addresses. (Q00944053)

Simple Network Time Protocol (SNTP)

The Passport 1600 Series switch now implements the SNTP protocol following RFC 2030.

Secure Password Optional

Passport 1600 series software release 1.2 once again supports ampersand (@) and tilde (~) in the password. This is the default operation. Whether this is allowed is controlled by the same CLI command which controls High Secure mode. The CLI command to configure high secure mode on Passport 1600 series is:

```
config secure_mode [normal| high]
```

When creating a new account in the High Secure mode, the user's password can contain any of 62 standard alphanumerical characters, 0-9, a-z, and A-Z (note, this does not include @ or ~, among others). In the Normal (that is, not High Secure) mode, there is no limitation related to user's password.

During the login process, if the secure mode is set to High, the system checks the user's password and if there is at least one non-alphanumerical character in the password, the system displays a warning message and asks the user to change the password. However, the system allows a user with administrator rights to change the password right away. When secure mode is set to Normal, Passport 1600 series does not check the user’s password.

Bugs fixed in this release

Platform

General

- The Passport 1600 will no longer go into an unstable condition randomly on which certain L3 functions were not possible. (Q00910146)
- In some extremely rare cases, for very large files that use a specific traffic pattern, a transmission error occurs, causing a file transfer failure. This extremely rare problem is now fixed in software release 1.2. For customers who are using software releases 1.1.0, 1.1.1 or 1.1.2 and do not want to use release 1.2, Nortel Networks recommends using release 1.1.3. Please contact your local representative for more information. (Q00989527-01)

Hardware

GBICs

- On certain SX GBICs, the Passport 1600 will no longer see a link-up event when no fiber is connected to the GBIC. (Q00885732-01)

Layer 2

Bridge

- The Passport 1600 Series switch now bridges the traffic through the correct path when a downstream BayStack 470 link fails. This condition is also true on a link recovery. (Q00925622-01)

MLT

- The Passport 1600 now adds a static MAC address to all participating ports of an MLT. This guarantees that the traffic is redirected to other MLT ports if the forwarding port fails. (Q00943647-01)

VLANs

- In a protocol-based VLAN or IP-subnet VLAN, you can now use JDM to configure a static IGMP snoop router port. (Q00873442)
- Passport 1600 series will no longer lose the configuration of IP subnet-based VLANs. (Q00950643-01)

IP Unicast

General

ARP

- Routes will no longer be lost while updating ARP entries during a failover. (Q00975504)

Bootp

- The Passport 1600 Series switch no longer drops bootP packets with a broadcast destination address. (Q00877401)

OSPF

- The OSPF neighbor state condition no longer stays at exchangestart after the primary link fails. (Q00927373-01)

TFTP

- The Passport 1600 Series switch now transfers config files to servers through TFTP successfully. (Q00928287-01)

IP Multicast

General

- While routing IP multicast packets, Passport 1600 series now decrements TTL value of the packets correctly. (Q00928766-01)

Network management

- If the 1600 Series switch reboots while JDM is connected, the JDM *Java Null Pointer* error message no longer appears. (Q00682375)
- The SNMP agent no longer fails when a space is inserted within the System Contact, Name or Location string when using the Device Manager (JDM) interface. It is no longer necessary to use the Command Line Interface (console/telnet) to enter information with spaces in the strings. (Q00873350)
- When viewing trusted-host from the web interface under the Basic Setup > Network Management > Management Station IP tab, the 4th through 6th IP addresses no longer display in a wrong column, and the 7th through 10th IP addresses are now visible. It is no longer necessary to use the CLI command `show trusted_host` or Device Manager (JDM) to see these IP addresses. (Q00866713)
- When an SNMP `get` request is sent from an SNMP device to one interface of the Passport 1600, the Passport 1600 no longer uses a different interface IP address in the SNMP response. (Q00878800)
- Java Device Manager (JDM) now correctly displays the device's serial number. (Q00968969)
- There are no longer missing hyperlinks or incorrect hyperlinks for the following help files in the Device Manager interface (JDM) (for versions 579 and higher):
  - Edit/Ports/STP/Help
  - Graph/Chassis/System
  - IP Routing/IGMP/Snoop Group Ports

(Q00873772)

Known issues and considerations

Release 1.1 issues and considerations

The following chart describes issues known to exist in the Passport 1600 Series Switch software release 1.1 and in the 1.2 release:

Hardware and platform

- You must have auto-negotiation set to Auto to determine the port type (MDI/MDIX) at the far-end link, or else use the correct type of cable (straight-through or crossover). (Q00615939)
- The largest Ping packet the Passport 1600 Series switch responds to is 1472 bytes. (Q00672839)
- On the 1600 Series switch, a port counter wraps to zero once it reaches 43,000,000. (Q00628251)
- With two connected ports on 1600 Series switches, if you change force mode on the first switch to 1 Gigabps, the link goes down immediately on the other. The only way to make the link operational again is to change force mode on the second switch to 1 Gigabps, or change it on the first one back to Auto. (Q00712333)

Layer 2

- The predefined protocol sna802dot2 option has been programmed to identify SNA frames by looking in the DSAP and SSAP fields of an LLC frame for the values 04 and 04.

  This means that both fields have to be set to 04 in order for the frame to be accepted in sna802dot2 protocol based vlan.

  In SNA a client initiates a session by sending out a test poll with DSAP and SSAP field set to 04 and 00 respectively. The Host then responds with a Test Poll Response with DSAP and SSAP fields set to 04 and 01 respectively. Furthermore as seen on traces taken of a SNA session between a host and a client, different control frames from the host may have DSAP and SSAP set for 04 and 05 respectively.

  A workaround is possible by overlapping 3 protocol based vlans on top of the standard sna802dot2 as shown below:

```
config vlan default delete 1-8
#
create vlan SNA0404 vid 20 type protocol-sna802dot2
config vlan SNA0404 add untagged 1-8
#
create vlan SNA0004 vid 21 type protocol-userDefined
0x0004 enc llc
config vlan SNA0004 add untagged 1-8
#
create vlan SNA0401 vid 22 type protocol-userDefined
0x401 enc llc
config vlan SNA0401 add untagged 1-8
#
create vlan SNA0405 vid 23 type protocol-userDefined
0x405 enc llc
config vlan SNA0405 add untagged 1-8
```

  In the example above ports 1-8 have been configured as part of the workaround protocol based SNA as long as the four vlans are treated as one, the Passport will be able to keep all the different types of SNA frames under control. (Q00912053, Q00912070)

- IP subnet VLANs can be configured either with all the ports to be untagged or all the ports to be tagged. This means that no tagged/hybrid port can be a member of a subnet-based VLAN when it is configured with untagged ports. (Q00952328)
- After creating the protocol-based VLAN, you can not dynamically change the EtherType or Protocol ID. You must first delete the VLAN, then recreate it with the new EtherType and Protocol ID. (Q00788268)
- With software release 1.2, PP1600 can support 3 spanning tree modes: STP-compatible (behaving as legacy STP), RSTP and MSTP.
  When PP1600 connects to a PP8600, regardless of which STP mode is used with PP1600, if PP8600 is configured as Nortel STG, then only the default STG (id=1) with untagged BPDU will be processed by PP1600. All other STGs (with tagged BPDU) will be silently dropped by PP1600.
- When the Passport 1600 Series switch is running in RSTP or MSTP mode, any port that receives a legacy STP BPDU will migrate to STP-compatible mode. However, the Passport 1600 series switch has no log event for this situation. Although the port has migrated to STP, in Device Manager (JDM), the port's OperVersion will not update to STP-compatible mode. JDM will continue to show the port operating in the original MSTP or RSTP mode. (Q01014687)

Caution:

1. When you connect two Passport 1600 switches and configure link aggregation on both of them, traffic transmits without any problem. However, if link aggregation is disabled on one of the switches, a network loop occurs since the switch with link aggregation enabled only sends out BPDUs on the master port. This causes all the ports on the switch with link aggregation disabled to go into forwarding mode, thus causing a network loop.

Be aware that this scenario only occurs when the Passport 8600 compatibility option is turned off. This option ensures that the Spanning Tree Protocol (STP) running over a Local Area Group (LAG) is compatible with the 8600. Ensure that this compatibility option is turned on. (Q00621524)

2. When a Passport 1600 Series switch and a Passport 8600 are connected with 2 MLT links, STP works properly as long as the 8600 is the designated root bridge. When 1600 is the designated root bridge, however, only one of the MLT ports on the 8600 side transitions to the appropriate STP state (forwarding), while the rest remain in the listening state. This can cause problems, such as the 8600 dropping control traffic received on the ports that are in listening state. It is strongly recommended that you use the option to make the 1600 work in 8600 compatibility mode, **and** configure the 8600 as the root bridge. Configuration **must** be performed using the Command Line Interface. You cannot configure this using the Device Manager (JDM). (Q00640319)

- In the Series 1600 switch, note that incoming mirrored packet tag information may be modified when received by the analyzer port. (Q00717990)

  The analyzer port can:

  — be either a member or a non member of the mirrored packets VLAN
  — be either selected as tagged or untagged per VLAN
  — perform either Tx, Rx or both mirroring of ports

The software permits you to use the tag/untag setting for VLANs for which the analyzer port is not a member. Thus, you may wish to place the analyzer port in its own VLAN, so that it is not receiving Multicast data from the VLANs to which it is a member.

The analyzer ports operate as follows:

1 For **L2 bridged traffic**:

- If the analyzer port is a member of the mirrored packets VLAN then tagging and untagging is based upon the analyzer port setting.
- If the analyzer port is **not** a member of the mirrored packets VLAN, then all packets will be sent **untagged** from the analyzer.

With L2 bridged traffic, when the analyzer port is a member of a VLAN:

- If the analyzer port is **untagged:**
  - The Rx packet is sent untagged, regardless of whether it is tagged or untagged on ingress
  - The Tx packet is sent untagged
- If the analyzer port is **tagged:**
  - The RX packet is sent tagged, regardless of whether it is tagged or untagged on ingress
  - The TX packet is sent tagged

With L2 bridged traffic, when the analyzer is not a member of a VLAN, all packets from the analyzer port are sent untagged.

2 For **L3 routed traffic:**

The determination for the VLAN is based upon the destination VLAN ID that the router is sending the packet to. The routed destination VLAN is used to determine if this is the same member VLAN as the analyzer port.

With L3 routed traffic, when the analyzer port is a member of a destination (routed) VLAN:

- If the analyzer port is **untagged:**

  The Rx packet from the analyzer port is sent:

  - untagged, regardless of tag or untag on ingress
  - pre-routed data

The Tx packet out of the analyzer port is sent:

— untagged

— post-routed data

- If the analyzer port is **tagged:**

  The Rx packet out of the analyzer port is sent pre-routed data. In addition, it is sent tagged with:

  — the routed destination VLAN, if the Rx packet is untagged

  — the ingress VLAN tag, if the Rx packet is tagged

  The Tx packet out of the analyzer port is sent:

  — τagged with the destination VLAN tag

  — post-routed data

With L3 routed traffic, when the analyzer is not a member of the destination (routed) VLAN, all packets are sent out the analyzer port **untagged.**

Examples

Without support for the tagging and untagging of the analyzer port for non-VLAN members, the default operation is untagged as follows:

VID= 1	VID= 2
Port 1	Port 12
Tagged/Untagged	**Tagged**
Tag VID 1, 3 in	Untag VID 1, 3 out
Tag VID 2 in	Tag VID 2 out
Untag VID 1 in	Untag VID 1 out
Tag VID 1, 3 in	Untag VID 1, 3 out
Tag VID 2 in	Untag VID 2 out
Untag VID 1 in	Untag VID 2 out

As shown in the previous example, it can be difficult to differentiate the traffic on the analyzer port, even though it is transmitted out. Setting the analyzer port to **tagged** for non-VLAN members produces the following:

VID= 1	VID= 2
Port 1	Port 12
Tagged/Untagged	**Tagged**
Tag VID 1, 3 in	Tag VID 1, 3 out
Tag VID 2 in	Tag VID 2 out
Untag VID 1 in	Tag VID 1 out
Tag VID 1, 3 in	Tag VID 1, 3 out
Tag VID 2 in	Untag VID 2 out
Untag VID 1 in	Tag VID 1 out

Layer 3

VRRP

Nortel Networks guarantees the following combination of VRRP and OSPF routes. (Q00804183)

Table 5 Combinations of VRRIDs, OSPF routes, LSDB entries and Areas

VRRIDs	OSPF routes	LSDB entries	Areas
4	760	4284	4
8	740	4164	4
16	715	4014	4
24	675	3885	4
32	650	3735	4

- When the MAC address corresponding to a multicast group is similar to one of the VRRP MAC addresses (xxx.0.0.18 ->01005E000012), VRRP cannot work correctly. This is something not specific to the Passport 1600 Series Switch, but to any switch/router. Please carefully choose the address of the multicast groups when you implement VRRP, and more specifically, do not use a multicast group that could use the following MAC addresses: 01-00-5E-00-00-04 (DVMRP Routers), 01-00-5E-00-00-05 (OSPF Routers), 01-00-5E-00-00-06 (OSPF Designated Routers), 01-00-5E-00-00-09 (RIP2), 01-00-5E-00-00-12 (VRRP). (Q00777777)
- When you implement VRRP between a Passport 1600 and a Passport 8600, do not configure the authentication field. Passport 8600 does not support VRRP authentication as defined in the RFC. If you enable authentication on the 1600, you could encounter a situation where both routers would be master (Q00803727).
- Once you modify an IP interface used for a VRRP, the VRRP interface will be removed. However, the total number of VRRP interfaces remains unchanged (even though the total number of VRRP interfaces should decrement by one). (Q00804959)

IP

- The configuration of the number of static routes can be done only using CLI (console/telnet), but not through SNMP (JDM). (Q00869870)
- The 1600 Series switch does not support an IP deny policy, and thus, cannot deny some unwanted routes. For RIP, the route preference is lower than OSPF external type 1 and 2 routes. Because of this, if the 1600 works as an Autonomous System Border Router (ASBR), it redistributes those OSPF external type 1 and 2 routes back to the OSPF network. Also, the ASBR picks RIP instead of OSPF for those OSPF external routes. (Q00566603-01)
- If the ARP aging timer is less than the MAC aging timer, note that the ARP timer is not triggered. The MAC timer must age out first. If it is set to a longer duration, this issue does not arise. (Q00663257)

RIP

When you create or modify a RIP interface, the status follows the RIP global state automatically. For example, if RIP is globally enabled, once you modify the interface, it is also enabled. (Q00718213)

OSPF

- The Hello and DeadInterval timers are the only OSPF timers supported on the 1600 Series switch CLI and JDM. The standard MIB contains other OSPF timers which are read/write and may be set with other SNMP tools. However, be aware that these are *not* supported.(Q00711011)
- When using GBICs in MLT configurations, OSPF may take a long time to be stable if the MLTs are configured in "force mode 1000_full" (Q00961939).

Multicast

- The accuracy of the CP limit feature for the multicast frames (IGMP & DVMRP) is plus or minus 100 frames. (Q00844463)
- In a multi-access LAN topology, a PP1600 may receive multicast traffic from multiple neighbors or from a neighbor which has been pruned. The traffic can not be pruned but will be discarded at ingress ports if the traffic does not come from its upstream neighbor. (Q00757983)

CLI

Caution: Care should be taken when modifying the max_static route size to ensure that other administrators are not concurrently modifying the configuration. This is because this command will automatically do a save and reboot. Others attempting to do a save will interfere with this process. (Q00872911)

- You can accidentally remove your IP address when executing the CLI `reset config` and `reset system` commands. In order to avoid this, use `reset` to keep the system IP address and `reset config` and `reset system` to set the IP address to default. (Q00599270)
- While the 1600 Series switch allows you to have multiple administrator accounts, you cannot delete or modify the default admin account username `rwa`. (Q00651775)
- When you attempt to use the up-arrow key to recall a CLI command whose length is over 80 characters, and either move the cursor or use <Backspace> to delete, the cursor moves up a line. This problem typically occurs when the Telnet session's window width is set to more than 80 characters. As a result, it is recommended that you set the window's width to 80. (Q00637504)

- The question mark (?) is not recognized by the CLI in the 1600 Series switch. Press <CR> to obtain help via the *Next possible completions* option. (Q00654586)
- You cannot partially disable link aggregation ports using the CLI `config ports state enabled/disabled` command. You must either disable or enable all of the ports. (Q00699418)
- When you disable STP ports using the CLI `config ports state disabled` command, it means that STP no longer works on the specified ports and they remain in the forwarding state. (Q00620617)
- When you enter the `show iproute` command, the route preference ranges and defaults that display as output are different in the Passport 1600 switches than they are in the Passport 8600. For example, the 8600 contains route preferences that range from 0 to 175, with 0 being the highest priority. By contrast, the 1600 route preferences range from 0 to 10, with 10 being the highest priority. Note that as far as the route protocol behavior is concerned, both the Passport 1600 and 8600 are the same. (Q00615078)
- Once you remove a port from an untagged port list, its PVID becomes 0. (Q00720617)

Bandwidth management

QoS

- Nortel Networks Service Classes define values for DSCP (DiffServ Code Point) and 802.1p (priority) bits. Using the following example configuration, the incoming traffic is automatically classified based on the incoming DSCP values to be prioritized according to the Nortel Networks Service Classes.

Example config

config flow_classifier template_id 2 mode_parameters qos_flavor dscp

config flow_classifier vlan default attach template_id 2

create qos_rule template_id 2 dscp 8 priority 1 dscp 8

create qos_rule template_id 2 dscp 10 priority 1 dscp 10

create qos_rule template_id 2 dscp 12 priority 1 dscp 12

create qos_rule template_id 2 dscp 14 priority 1 dscp 14

create qos_rule template_id 2 dscp 16 priority 2 dscp 16

create qos_rule template_id 2 dscp 18 priority 2 dscp 18

create qos_rule template_id 2 dscp 20 priority 2 dscp 20

create qos_rule template_id 2 dscp 22 priority 2 dscp 22

create qos_rule template_id 2 dscp 24 priority 3 dscp 24

create qos_rule template_id 2 dscp 26 priority 3 dscp 26

create qos_rule template_id 2 dscp 28 priority 3 dscp 28

create qos_rule template_id 2 dscp 30 priority 3 dscp 30

create qos_rule template_id 2 dscp 32 priority 4 dscp 32

create qos_rule template_id 2 dscp 34 priority 4 dscp 34

create qos_rule template_id 2 dscp 36 priority 4 dscp 36

create qos_rule template_id 2 dscp 38 priority 4 dscp 38

create qos_rule template_id 2 dscp 40 priority 5 dscp 40

create qos_rule template_id 2 dscp 46 priority 5 dscp 46

create qos_rule template_id 2 dscp 48 priority 6 dscp 48

create qos_rule template_id 2 dscp 56 priority 7 dscp 56

(Q00834858)

- It is recommended that you do *not* send data traffic to level 7 since control traffic will be impacted. Keep this in mind when you configure QoS or 802.1p on the port level. While you can change the QoS/ 802.1p level to level 7, this level is reserved for the network protocol only. Should you make this level change, the switch issues a warning message asking you to confirm it. (Q00614827)
- By default, all of the ports in the Passport 1600 are DiffServ enabled. (Q00719468)
- In the Passport 1600, all the (routing, bridging) traffic prioritization is based on the priority bit. (Q00719471)
- You can configure the L4_switch rule to drop packets based on SIP/DIP peers. However, the rules cannot drop fragmented frames. While you can set the global fragment flag to drop IP fragments, note that this only applies to VLANs to which filter templates are bound. (Q00698385)

Web Management interface

In the Web management interface, under Network Monitoring > Address Table > OSPF > OSPF LSDB table:

- If you filter by LSDB Type: ASExtLink, do not enter a value into the AREA ID since the external links are not associated with an area. (Q00718412)

Network Management

- In the Passport 1600 Series switch software release 1.1, community strings are stored in encrypted format and are no longer stored in the configuration file. If a configuration file saved prior to software release 1.1 is loaded, any saved community strings from the configuration file will not be recognized. If the switch is booted for the first time with the software release 1.1 image, the community strings are reset to default values. It's highly recommended to change the community strings immediately after the first reboot. (Q00806022)
- A telnet session automatically expires, triggered by the serial port logout timer (there is only one timer for both console and telnet sessions). To configure this timer, please use the CLI command, “config serial_port auto_logout never |2_minutes}5_minutes|10_minutes|15_minutes”. (Q00815285)

JDM

- Help files for MSTP, RSTP and SNTP have not been included with the 584 version of JDM. The help files will be added in a later JDM build.
- When you use JDM to add a new interface, if you have a large number of static routes, JDM may receive a response time out. Even though JDM timed out, the action was completed. (Q00874970)
- JDM uses caching to improve performance, however, in some cases, if CLI or another instance of JDM is used to modify the configuration, the cache will get out of sync with the switch. If this occurs, please close the JDM connection to the switch and reopen it. The specific area that gets out of sync is the interface name mapping to the IP Address. This is known for DVMRP and VRRP tables. (Q00801941)
- The Device Manager uninstaller gives an out-of-memory exception. The following steps provide a work around to uninstall JDM.

1. Go to the installation directory (for example, C:\Program Files\JDM).
2. Go to directory "UninstallerData" from the installation directory.
3. Edit the plain text file "Uninstall Java Device Manager.lax".
4. Search for the line, "lax.nl.java.option.java.heap.size.max=50331648".
5. Insert the character '#' (without the quotes) into the beginning of the line above.
6. Save the file and restart the Uninstall process.

(Q00873714).

- JDM shows multicast packets as NUcastPkts, or Non-Unicast packets. There are no separate rows for multicast and broadcast packets in the JDM graph. (Q00636659)
- System names are limited to 15 characters. (Q00728030)
- In the CLI, the IP routing table shows the gateway IP for the local subnet as the local IP interface. In the JDM, however, the next-hop for the local subnet displays as IP 0.0.0.0. (Q00715696)
- By default, the management port on the Passport 1612G and 1624G switches is part of the default VLAN. Thus, there is no way to manage this port from the JDM. Instead, it is recommended that you use the CLI. Note that this issue is not relevant for the Passport 1648T since it has no separate management port. (Q00719409)
- While installing JDM on a PC running Windows 98/2000/XP, you may see a *Fatal Application Error* appear on the screen followed by a message indicating that the application has unexpectedly quit. Be aware that this problem does not occur if you install JDM in a new folder.

  If the problem occurs after uninstalling the old JDM, it is recommended that you:

1. End the task.
2. Save the dm.ini file in the JDM install directory to another folder.

   This file contains the JDM configuration parameters, including the last opened IP address.

3. Delete the JDM install folder.
4. Reinstall JDM.

5 Copy the dm.ini file back to the JDM install folder. (Q00730381)

Caution: It is recommended that you uninstall JDM before upgrading to a new version.

Security

- The CLI command config authentication allows entry of a 3rd parameter, but returns an error message that the chosen authentication method cannot exceed two. (Q00872906)
- TACACS+ does not properly support authenticating Web access to the switch. Because the switch can handle this authentication locally, Nortel Networks recommends that you configure Web Access in this manner. (Q00797922)
- When you change security mode to “high”, the system automatically saves the switch configuration. Changing the security mode to “normal” however, does not automatically save the configuration. You should manually save the configuration file after changing the security mode to “normal”. (Q00798823)
- You must create a TACACS+ server prior to selecting TACACS+ as an authentication type in either the JDM or CLI. (Q00801010)

Miscellaneous

- The TCP port of a Telnet/Web connection cannot be configured using the Device Manager. To change a port number, you must use the CLI interface. (Q00800455)
- When you attempt to establish a connection using the Z-modem, you may see the following system message:

  ```
  Z-Modem: Can’t Establish Connection with Sender
  ```

  Disregard this message. The file transfer will still occur. (Q00694513)
- Be aware that the JDM and CLI use different terms to refer to ingress filtering. The JDM uses ingress filters while the CLI uses ingress checking. Both terms refer to the same set of features. (Q00718504)
- The Passport 1600 Series switch does not support the swL2IGMPMaxIpGroupNumPerVlan MIB. (Q00719351)

- If the management port is left in the default VLAN in the Passport 1600 switch, multiple packets are sent by the management port. This problem occurs because in the Passport 1600 default configuration all ports are in the same, default VLAN. Before you move all the ports out, those ports forward traffic to one another.

Caution: After connecting to the Passport 1612 and 1624, it is recommended that you isolate the management port by placing it in its own VLAN. Do this through the CLI, as JDM does not support this capability. To do so, use the following procedure:

1. Create a VLAN named mgmt or management with VLAN ID 4094 as follows:

```
create vlan mgmt vid 4094
```

2. Configure the System IP interface and attach it to VLAN mgmt as follows:

```
config ipif System ipaddress x.x.x.x/x vlan mgmt state
enable
```

3. Use the following CLI command to verify that the mgmt_port is in the VLAN mgmt:

```
show vlan
```

Note that this problem is related to Q00705437 which involves the same overall issue, with a different result. (Q00720343)

- The Tx counter for Bridge Protocol Data Units (BPDUs) on the Gigabit ports will not increment. This is true for the Gigabit ports on all three models of the 1600 Series switch. (Q00718397)

Related publications

For more information about the Passport 1600 Series switch software release 1.1, refer to the following publications:

Installation and User Guides

These guides provide instructions for installing the chassis, the Device Manager software, and finally describe the tasks involved in using the 1600 Series switch.

Installing the Passport 1600 Series Layer 3 Switch	316860-B
Installing and Using Device Manager	316857-B

Reference and Configuration Guides

These guides provide reference and configuration information, including:

Command Line Interface Reference Guide for the Passport 1600 Series Layer 3 Switch	316862-B
Configuring IP Routing Operations using Device Manager	316853-B
Configuring IP Filters and QoS using Device Manager	316854-B
Configuring Network Management and Diagnostics using Device Manager	316855-B
Configuring Layer 2 Operations: VLANs, Spanning Tree, and Multilink Trunking using Device Manager	316856-B
Configuring IGMP and DVMRP using Device Manager	316858-B

You can print selected technical manuals and release notes free of charge, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.