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

Release Notes for the Passport 1600 Series Switch Software Release 1.1

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 1.1 software, its file names, download process, and supported software and hardware capabilities. They also describe the new security features, documentation corrections and enhancements and known issues and bugs that still exist in release 1.1.

The following topics are discussed in this document:

File names for this release

The Passport 1600 Series Switch software release 1.1 contains the following files

Note: The Passport 1600 Series Switch software release 1.1 contains two different images.

One image contains the SSH encryption algorithms: **p16c1100.img**

One image does **not** contain the SSH encryption algorithms: p16a1100.img. SSH cannot be configured using this image.

Please see "Downloading the SSHv2 (server) encryption image" on page 15 for instructions on obtaining the SSH encryption image.

Name	Description
p16c1100.img	Run-time image file with SSH encryption algorithms
p16a1100.img	Run-time image file without SSH encryption algorithms
jdm_578.exe	Supported PC JDM version (Windows 95 and later)
jdm_578.sh	Supported Unix JDM version (Solaris SPARC only)
p16a1100.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.

Name	Description
Framework.mib	The SNMP management architecture MIB
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
synro185.mib	Nortel/SynOptics root MIB release 1.7.5
** 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
rfc1493.mib	Definitions of managed objects for bridges
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
rfc2021.mib	Remote network monitoring MIB Version2 using SMIv2
rfc2096.mib	IP forwarding table MIB
rfc2233.mib	The interfaces group MIB using SMIv2

Name	Description
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)
802.3x (Flow Control)	802.1D (MAC bridges/Spanning Tree Protocol)
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)	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 Release 1.1. 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	1
Aggregation groups*	7
Ports per MLT group	up to 4 per aggregation group
IP interfaces	64
VRRP IDs **NOTE:** Refer to Virtual Router Redundancy Protocol (VRRP) below for details on the interaction between VRRP and other protocols.	32
Static IP routes	up to 512 with configuration
RIP routes	1918 (see Table 4 on page 34)
OSPF areas per switch	4
OSPF adjacencies (neighbors) per switch	32
OSPF routes per switch	1918 (see Table 4 on page 34)
OSPF virtual links per switch	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 1.1 of the Passport 1600 Series switch software.	

In this release, 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).

Downloading release 1.1 software

To download the Passport 1600 Series switch release 1.1 software, please go to the Nortel Networks support site: http://www.nortelnetworks.com.

After you have downloaded the software, to install, reinstall or replace release 1.0 or later software with release 1.1 software, please follow the download instructions included in this section:

Caution: Before replacing release 1.0 software or re-installing release 1.1, be sure to back up the configuration file.

1. To backup the current configuration file currently used by the Passport 1600 Series Switch, use the following command:

   ```
   #save
   ```

2. To upload the configuration file, use the following command:

   ```
   #upload config <tftp_server_ip> <path_filename>
   ```

3. To load the Passport 1600 Series Switch version 1.1 software, execute this case-sensitive CLI command:

   ```
   #download firmware <tftp_server_ip> <path_filename>
   ```

   Example:

   ```
   #download firmware 10.10.10.2 \image\p16a1100.img
   ```

4. After the download is complete and the device boots up, execute a **reset system**.
5. Re-configure the management IP.
6. Download your original configuration which was uploaded at Step 1.

Downloading the SSHv2 (server) encryption image

The SSHv2 server will not function properly without the use of the special image (p16c1100.img) to scramble the data. However, due to export restrictions Nortel Networks cannot bundle the encryption algorithms into the Passport 1600 Series switch software image, and a different image must be downloaded.

To download the Passport 1600 SSHv2 encryption image:

1. Go to the Nortel Networks http://www.nortelnetworks.com
2. Click "Login" and enter your Nortel Networks user name and password.
3. If your default home page is set to the "Customer Support" web page and you see this page, proceed to step 5
4. Go to the "Customer Support" web page http://www.nortelnetworks.com/cs
5. Select the Product Family e.g. "Passport"
6. Locate the product (e.g. "Passport 1648T") and click on "Software"
7. Click on the specific software name (select appropriate version)
8. Click on the file name you wish to download. Note that you will be required to complete a questionnaire.
9. Downloaded and save the image file.
10. Copy the *p16c1100.img* image file to the Passport 1600 Series switch CPU.

Note: To protect the integrity of your switch, it is recommended that you use the Command Line Interface (console) to change the passwords after a software image upgrade.

Emergency download using Z-modem

In case your existing switch image becomes corrupted during the course of the 1.0.1.1 software download, perform the following steps to recover normal operation:

1. Save a copy of the image onto the local hard drive.
2. Establish a terminal session to the switch console using the following settings.
   - 9600
   - 8
   - n
   - 1
3. Power cycle the switch. As it powers back on, wait until the switch displays the following message:

   ```
   Power On Self Test
   ```

   Hold down the Shift and 3 keys simultaneously while the switch is running this self-test. Be sure to complete this step before the diagnostic is 60% complete. If successful the following message displays:

   ```
   Please change your baud rate to 115200 for Z-modem or
   press CTRL-C to go to the boot menu.
   ```

4. Disconnect the terminal session and change the baud rate to 115200.
5. Once the change is done, reinitiate the terminal session.
6. Select the image file that you wish to download to the switch.
7. Click Send.
8. Once the image is downloaded and saved to the switch, disconnect the terminal session and change the baud rate back to 9600.
9. Log into the switch.
10. Manually reboot the switch to ensure it will boot properly with the new image you just downloaded.

New features in release 1.1

Platform

1000BaseT SFP

Passport 1600 Series Switch Software release 1.1 now supports 1000BaseT SFPs (Small Form Factor). The Nortel Networks part number for this item is AA1419043.

CP Limit Feature

This feature has been introduced to prevent the CPU from being overloaded by excessive multicast or broadcast control or exception traffic. For example, traffic generated by a network loop introducing broadcast storms of BPDUs in a network will not impact the stability of the system by blocking/disabling one interface. This feature protects the CPU, if enabled, from receiving more than 1700 broadcast control/2000 multicast control or exception packets within a duration of 1 second. The feature can be enabled per port and the user can configure the amount of broadcast and/or multicast control or exception frames per second to be allowed to reach the CPU before the responsible interface is blocked and disabled.

IP Routing memory size configuration

The Passport 1600 Series Switch has introduced a parameter, **`asic unicast_multicast_ratio`** `{100_0|75_25|50_50}`**`,`** that is used when booting the switch. This parameter is configured using the CLI only and allows the user to allocate memory size to be used for routing tables.

This parameter is not dynamic. Therefore, when changing the value of the parameter, the switch must be rebooted. The default value is 75/25, that is 75% to be used for unicast traffic and 25% for multicast traffic. This default value is the value if you have already a 1.0 code installed.

Unicast traffic: If you use only unicast traffic, set this parameter to 100/0. In this case all memory will be allocated for unicast traffic.

Unicast and multicast traffic: If you plan to use a mix of unicast and multicast traffic, do not change anything. Use the default setting of 75/25.

Multicast traffic: If you plan to use your switch in a configuration where multicast plays a large role, use a 50/50 configuration according to the following CLI command example:

```
PP1648_40.20:4# config asic unicast_multicast_ratio
50_50
```

Table 2 on page 19 displays the ratio between unicast and multicast traffic.

Table 2 Unicast/multicast ratios for dynamic and static iproute and arp values

Unicast/ multicast ratio of 50/50	Dynamic IP routes	Static IP route(s)	Dynamic arp	Static arp
	911	0	1372	32
	879	32	1372	32
	847	64	1372	32
	783	128	1372	32
	655	256	1372	32
	399	512	1372	32
Unicast/ multicast ratio of 75/25	**Dynamic IP routes**	**Static IP route(s)**	**Dynamic arp**	**Static arp**
	1404	0	1372	32
	1372	32	1372	32
	1340	64	1372	32
	1276	128	1372	32
	1148	256	1372	32
	892	512	1372	32
Unicast/ multicast ratio of 100/0	**Dynamic IP routes**	**Static IP route(s)**	**Dynamic arp**	**Static arp**
	1918	0	1372	32
	1886	32	1372	32
	1854	64	1372	32
	1790	128	1372	32
	1662	256	1372	32
	1406	512	1372	32

If you plan to use 64 S,Gs, Nortel Networks recommends that you configure the switch with the 50%/50% ratio.

The maximum number is 64 S,Gs but depending on the actual IP addresses used, this number could be smaller. IP addresses that are sequential in nature take up less of the available memory (e.g. 239.10.10.1, 239.10.10.2, 239.10.10.3, etc are examples of sequential addresses). Addresses which are random take up more memory.

Since a block of memory is allocated in a tree structure when the 1st address is learned, values which are sequential (up to 256) will simply use up the allocated block and not take up any more memory until you cross over the boundary (in which case another block of memory must be allocated). At one point, another block of memory cannot be allocated due to memory constraints and that address will not be learned. A log message will be created to notify the user.

Since address learning cannot be controlled, it is possible to run out of memory for new blocks but still have open spaces in existing blocks. Therefore, receiving the log messages does not mean that other addresses cannot be learned.

Nortel Networks recommends that network administrators control the multicast group addresses that are being used by the multicast applications to ensure sequential addresses are used as much as possible. It is also recommended that you keep the number of S,G on the network to 64 or less.

Layer 2

Protocol-based/Policy-based VLANs

Protocol-based (often called "policy-based”) VLANs allow network managers to isolate traffic coming from different protocols and to reduce the broadcast rate generated by these different protocols, thus enhancing the level of security. Classification is based on the Ethernet "Ethertype" field. Nortel Networks allows you to configure a large list of different protocols.

Both tagged port and untagged port can be a member of multiple port-based, IP subnet-based, or protocol-based vlans if there's no setting conflict.

The configuration rules are as follows:

- An untagged port can be part of one port-based VLAN only

- Once an untagged port is assigned to an IP protocol-based VLAN, it can not be assigned to an IP subnet-based VLAN, and vice versa.
- An untagged port can belong to multiple protocol-based VLANs only if those protocol types are different
- Port tagging is required for a port to be a member of multiple protocol-based VLANs if those VLANs are set up for the same protocol types.

The operation rules are as follows:

- Once an untagged frame is received by a port, if ingress checking allows to process it, the frame will be applied to IP subnet-based VLANs classification first; then Protocol-based VLANs classification; then Port-based VLANs classification.
- Once a tagged frame is received by a port, if ingress checking allows to process it, the frame will be processed base on tag or PVID.

The Passport 1600 can support up to 2048 VLANs, either port-based or protocol-based. However, only 11 records (EtherType or DSAP-SSAP values) are available. One protocol-based VLAN may use one or multiple records. For instance, AppleTalk uses 2 different records (0x809B and 0x80F3), meaning once an AppleTalk Protocol-based VLAN is configured, only 9 records remain available.

Note: An ARP protocol record (0x0806), is always reserved once a device is booted up and is not considered as one of the 11 available. Therefore, an IP Protocol-based VLAN will use 1 more protocol record (0x0800). Please refer to Table 3 on page 21 below for more details.

Table 3 EtherType or DSAP-SSAP values used by Protocol-based VLAN

Protocol	EtherType	DSAP/SSAP	SNAP-PID
IP	0x0800, 0x0806		
IP RARP	0x8035		

Table 3 EtherType or DSAP-SSAP values used by Protocol-based VLAN

Protocol	EtherType	DSAP/SSAP	SNAP-PID
IPv6	0x86DD		
IPX 802.3 Raw		0xFFFF	
IPX 802.2		0xE0E0	
IPX SNAP			0x8137, 0x8138
AppleTalk	0x809B, 0x80F3		0x809B, 0x80F3
DecLat	0x6000		
DecOther	0x6009		
SNA 802.2		0x0404	
SNA Ethernet v2	0x80D5		
NetBIOS		0xF0F0	
XNS	0x0600, 0x0807		
VINES	0x0BAD		

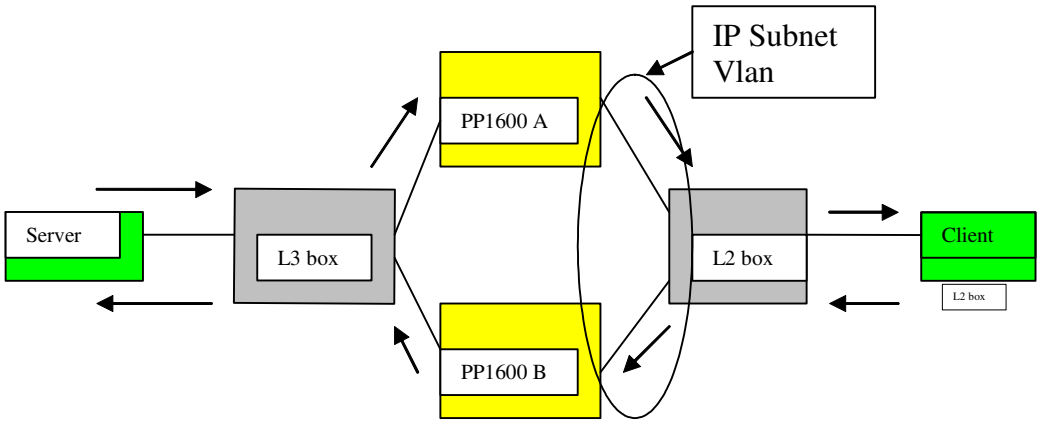
Please refer to the document *Configuring Layer 2 Operations: VLANs, Spanning Tree, and Multilink Trunking using Device Manager* (316856-B) for a complete description and configuration.

IP Subnet Based VLANs

IP Subnet Based VLANs provide a way to separate and/or isolate the traffic coming from edge devices in your network based on the source IP address (subnet). Routing can be done in hardware by the Passport 1600 at the aggregation/core layer between the different VLANs. Note that this feature can be used to filter some traffic, by configuring one or several IP Subnet Based VLANs with different source subnets on the same port. At the difference of regular port-based VLANs, frames coming with different source subnets will be dropped if the port-based VLAN does not have a configured IP address.

You need to assign an IpSubnetArpClassId when creating the first IP subnet-based VLAN. IpSubnetArpClassId defines a VLAN ID for the ARP protocol classification. The setting range is 1 to 4094 but should not conflict with any existing VLAN ID.

Once you create the first IP Subnet Based VLAN, one ARP protocol record, named "vlan-arp", will also be created for all IP Subnet Based VLANs. The ARP record is visible, and looks like a VLAN with 'byProtocolId=arpEther2, but can not be modified. It will be automatically removed once the last IP subnet-bases VLAN is deleted.



- Due to the current implementation, in a network with redundant characteristics (as above), where the IP unicast traffic flows in only one direction through the switch, the PP1600 A will not learn the ARP and MAC entries for the proper VLAN. The result is that Unicast traffic flowing through PP1600 A to Client will be routed by the switch's CPU. If you have this situation, it is recommended to not use IP Subnet Based VLANs. Nortel Networks is currently working on a solution to this problem. (Q00886326)

  Please refer to the document *Configuring Layer 2 Operations: VLANs, Spanning Tree, and Multilink Trunking using Device Manager* (316856-B) for a complete description and configuration.

Layer 3

Virtual Router Redundancy Protocol (VRRP)

VRRP (Virtual Router Redundancy Protocol), following the RFC2338, is the standard protocol which provides redundancy if one router fails in the network. Two (or more) routers are sharing a virtual MAC address which is used as the MAC to forward the routed packets by the hosts connected on the subnet. If one router fails, one of the backup routers takes precedence (default time = 3s), and provides redundancy. Nortel Networks 1600 VRRP implementation provides full support of the standard (preempt mode, MD5 authentication) plus the notion of "critical IP address". This critical IP associated to the VRRP ID, can help trigger a VRRP transition from master to backup even if the router is still exchanging the VRRP messages in a timely manner with its peer(s), based on a local or remote address configured on the master router. Please refer to the document *Configuring IP Routing Operations using Device Manager* (316853-B) for a complete description and configuration.

Filtering enhancements (source/destination IP range)

With the 1.1 release, Passport 1600 allows you to define filters based on the combination of source and destination IP subnets/addresses. Please refer to the document *Configuring IP Filters and QoS using Device Manager* (316854-B) for a complete description and configuration.

Scalability of static routes

With the 1.1 release, Passport 1600 allows you to configure up to 512 static routes. Note that static and dynamic routes are part of the same "pool", so adding static routes reduces the number of dynamic routes. See Table 2 on page 19 for a description of the scalability of static routes.

Multicast

IP Multicast Operations: Layer 3 IGMP and DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a distance vector type of multicast routing protocol. It advertises shortest-path routes to multicasting source networks—that is, any network containing hosts that have the capability to issue multicast datagrams. (In this respect, DVMRP is the opposite of RIP, which advertises all routes to destination networks.) Coupled with IGMP, membership for a multicast stream is learned from both the routers and directly attached hosts.

DVMRP constructs a different distribution tree for each source and its destination host group. The distribution tree provides a shortest path between the source and each multicast receiver in the group, based on the number of hops in the path. A tree is constructed on demand, using a broadcast and prune technique, when a source begins to transmit messages to a multicast group. DVMRP assumes that initially every host on the network is part of the multicast group. The designated router on the source subnet (the router that has been selected to handle routing for all hosts on the subnet) begins transmitting a multicast message to all adjacent routers. Each of these routers then selectively forwards the message to downstream routers until the message is eventually passed to all multicast group members. In the selective forwarding process during the formation of the multicast tree, when a router receives a multicast stream, it checks its DVMRP routing tables to determine the interface that provides the shortest path back to the source. If that was the interface over which the multicast stream arrived, the router enters state information to identify the multicast stream and its source in its internal tables and forwards the multicast message to all adjacent routers except to the ones that are on the same interface. If the interface was not on the optimal one receiving the multicast stream, the stream is discarded. This mechanism, called reverse path forwarding, ensures that there are no loops in the tree and that the tree includes the shortest path from the source to all recipients.

The pruning feature of the protocol eliminates branches of the tree that do not lead to any multicast group members. The IGMP running between hosts and their immediately neighboring multicast routers is used to maintain group membership data in the routers. When a router determines that no hosts beyond it belong to the multicast group, it sends a prune message to its upstream router. Routers update source and destination group state

information in their tables to reflect which branches are eliminated from the tree, resulting in a minimum multicast tree. If a router later learns of new group memberships from the hosts or downstream routers, it sends a graft message upstream to retract the prune sent earlier.

After the multicast tree is constructed, it is used to transmit multicast messages from the source to multicast members. Each router in the path forwards messages over only those interfaces that lead to group members. Because new members can join the group at any time and these members may depend on one of the pruned branches to receive the transmission, DVMRP periodically re-initiates the construction of the multicast tree.

The Passport 1600 DVMRP implementation is based on the following IETF draft: draft-ietf-idmr-dvmrp-v3-11.txt.

Please refer to the document *Configuring IGMP and DVMRP using Device Manager* (316858-B) for a complete description and configuration.

Security features

SSHv2 (server only)

The Passport 1600 Series switch software release 1.1 now supports the Secure SHell Version 2 (SSHv2) protocol as a server. SSH is a protocol that specifies the way to conduct secure communications over a network.

The SSHv2 protocol supports the following security features:

— *Authentication* This determines in a reliable way to identity the SSHv2 client. During the login process the SSHv2 client is queried for a digital proof of identity.

— *Encryption* The SSH server uses encryption algorithms to scramble data and render it unintelligible except to the receiver.

Encryption algorithms provided are:

- Symmetric: 3DES, BlowFish, TwoFish(128,192,256 bits), AES(128,192,256 bits), ArcFour, Cast128. Data Integrity algorithms are MD5 and SHA-1. The symmetric encryption mode is cipher block chaining mode. The key exchange algorithm is Diffie-Hellman.

- Asymmetric: 2 algorithms are supported: RSA and DSA. The key length is 1024 bits.

— *Integrity* This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

Note: There are two image versions available. One image provides the SSHv2 server, and the other image does not. The default image loaded in the Passport 1600 does NOT contain the SSHv2 server. The SSHv2 server is available only by download from the Nortel Networks web site. See Downloading release 1.1 software above for instructions on downloading new images from the web.

Note: Configuration and maintenance of the SSHv2 feature is available only through the Command Line Interface (CLI). Please refer to *Command Line Interface Reference Guide for the Passport 1600 Series Layer 3 Switch* (316862-B).

Password protection

With release 1.1, all passwords and community strings are encrypted to provide a higher level of security. Please see *Installing and Using Device Manager* (316857-B) for information about using this feature.

Syslog

Syslog provides a mechanism to send events (logs) to a remote station (which has to implement a syslog daemon). Please see *Installing and Using Device Manager* (316857-B) for information about using this feature.

TACACS+

TACACS+ (Terminal Access Controller Access Control System Plus) is, like RADIUS, a security application that provides centralized validation of users attempting to gain access to a switch/router. Passport 1600 provides validation for console, telnet and SSHv2 access. Please see *Installing and Using Device Manager* (316857-B) for information about using this feature.

Bugs fixed in this release

- This release adds a new feature that provides prevention of flooding of unregistered multicast. This will prevent up to 512 unregistered streams from being flooded. Please refer to *Command Line Interface Reference Guide for the Passport 1600 Series Layer 3 Switch* (316862-B). (Q00678675 and Q00793618)
- Device Manager now supports 7 aggregation groups (static 802.3ad). (Q00757589)
- When you were connected to a 1600 Series switch via the console port and a telnet session, if you did a save on the console and then save on the telnet session, the telnet session properly displayed a message indicating that it was locked by the other session. However, the completion percentage would start appearing in the telnet session, rather than on the console. (Q00712057)
- When you created or deleted a route redistribution policy, it would cause the switch's routing table to be re-learned. This would happen with both RIP and OSPF. In addition, creating or deleting the OSPF route redistribution policy would cause the OSPF neighbors to re-form their adjacencies. (Q00615860)
- After you insert a route distribution policy via JDM, a timeout message would appear. Routing to the switch would then go down for 5 seconds. When it became operational again, the redistribution change would appear and the switch would operate normally. This issue is related to Q00615860 which involves creating or deleting a route redistribution policy and the routing table re-learn operation it causes. (Q00681739)
- With the Passport 1600 Series switches, the display for the template rules for the source IP filter table no longer shows the full 32 bits instead of the subnet only. (Q00725044).
- In Release 1.0, STP could sometimes become unstable under extreme traffic conditions and be unable to recover in a loop condition. This condition is fixed in Release 1.1 (Q00889177)
- In the previous OSPF implementation, in some cases with redistribution, the Passport 1600 Series switch would not always clear the LSDB related to the neighbor that is down. The LSDB is synchronized once more when the neighbor becomes operational again. (Q00692383)
- External OSPF route selection now operates correctly. (Q00729712)
- In an OSPF triangle or square topology, a PP1600 which is not an ABR (Area Border Router) now correctly builds the routing table with external routes after losing a link to the ABR. (Q00806211-02)

- When the ARP table is full and a topology change occurs, the PP1600 now correctly inserts a static route in the routing table. (Q00808927)
- When IP Forwarding is disabled, the PP1600 will now stop forwarding (routing) IP traffic, even if an ARP entry is present for the source and destination stations on different attached subnets. (Q00799926-01)
- The PP1600 now correctly forwards DHCP requests when a VRRP IP Address is used as Next Hop. (Q00817939-01)
- In a clustering service scenario on servers (such as: Novell, Unix, Windows) where the same IP virtual address is shared between several MAC addresses, the MAC entry in the ARP table which is pointing to the new server after the failover is now reachable, without having to flush or clear the ARP table. (Q00833204)
- In a particular case, OSPF As-External LSA received with the "forwarding address" set no longer causes the PP1600 to add a routing table entry with the next-hop address pointing to the 1600's own IP address. (Q00841902)
- JDM now correctly prevents you from adding the same untagged port in two different VLANs. If you attempt this same task using the CLI, the message *Untagged ports overlapped!* displays. (Q00731969)
- You can use the `config arp aging_time` command to set the ARP aging time in the CLI. By default, it is 20 minutes. There is now a similar option in the JDM to ensure that Dynamic Learnt ARPs are being purged when the connection is lost, for example. (Q00627397-01)
- The following problem has been fixed in the 1.1 release: "Currently, for AS external routes, the Passport 1600 switch only checks the combined metric and selects the LSA with the lowest metric to use it in its routing table. It does not check whether the path to the ASBR is an intra-area or inter-area path. This is not correct and the problem will happen again if two ASBRs advertise the same OSPF External network N1 with different metrics. For example, router A advertises N1 with a lower metric, and router B advertises N1 with a higher metric. The Passport 1600 switch can reach route A through an inter-area path, and reach route B through an intra-area path. In this case, the Passport 1600 switch still selects the wrong route, through router A, because the metric is lower." (Q00729712)
- When you insert a row/entry using the IP Routing > Filter > Destination Ip Filter, MAC Priority, and FDB Filter options, the Passport 1600 Series switch no longer requests an index number. (Q00719660)
- Adding an entry to Trusted Host table is now dynamic. If a host is removed and it is already connected, it will be disconnected immediately. (Q00799804)

Known issues and considerations

Release 1.1 issues and considerations

Changes to Documentation

- *Configuring IP Filters and QoS using Device Manager*, 316854-B.pdf

  On the top of page 22, the Note states that "you can only configure a single source IP address for security source IP filters. Should you wish to enter a range of IP addresses, you should enter them one at a time." Please ignore this note. (Q00876798)

Platform

- On certain SX GBICs, the Passport 1600 software will see a link up event even though no fiber is connected to the GBIC. This situation arises when (a) the port (x) is set to 1000 Full Duplex instead of Autonegotiation, and (b) an adjacent GBIC port (usually x+1) is also populated by an SX GBIC (of a different vendor type). If the port in question is a member of an aggregation group, this can pose problems as the switch will hash traffic in the direction of a missing link. To prevent this situation, leave Autonegotiation enabled on the port. (Q00885732)

Bandwidth Management

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)

QOS

- Nortel Networks Service Classes define values for DSCP (DiffServ Code Point) and 802.1p (priority) bits. By using the following example configuration, the incoming traffic will automatically be 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)

Layer 2

- 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)

Layer 3

VRRP

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

Table 4 Combinations of VRRIDs, OSPF routes, LSDB entries and Areas

VRRIDs	OSPF routes	LSDB entries	Areas
4	485	2857	4
8	480	2749	4
16	450	2569	4
24	430	2449	4
32	400	2253	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 can not 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, you should 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 will remain unchanged (even though the number should be one less). (Q00804959)

IP

- The configuration of the number of static routes can be done only using CLI (console/telnet), but not through SNMP (JDM). (Q00869870)
- In a protocol-based VLAN or IP-subnet VLAN, you cannot use JDM to configure a static IGMP snoop router port. Please use the CLI to perform this operation. (Q00873442)

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)

Network Management

- When an SNMP `get` request is sent from an SNMP device to one interface of the Passport 1600, the Passport 1600 may use a different interface IP address in the SNMP response. This only occurs if the routing table of the Passport 1600 has a different interface to the SNMP device. Since some SNMP applications are address sensitive to the `get` response, loss of communication may be reported. (Q00878800)
- 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)
- 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 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)

- 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)
- A telnet session will automatically expire, 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)
- When viewing trusted-host from the web interface under the Basic Setup > Network Management > Management Station IP tab, the 4th through 6th IP addresses display in a wrong column, and the 7th through 10th IP addresses are not visible. Please use the CLI command `show trusted_host` or Device Manager (JDM) to see these IP addresses. (Q00866713)
- The SNMP agent fails when a space is inserted within the System Contact, Name or Location string when using Device Manager (JDM) interface. Please use the Command Line Interface (console/telnet) to enter information with spaces in the strings. (Q00873350)
- There are either missing hyperlinks or incorrect hyperlinks for the following help files in the Device Manager interface (JDM)
  - Edit/Ports/STP/Help
  - Graph/Chassis/System
  - IP Routing/IGMP/Snoop Group Ports

  (Q00873772)

- The Device Manager uninstaller will give an out-of-memory exception. The following steps provide a work around to uninstall JDM.

  1. Go to the installation directory, e.g., 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).

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)

Release 1.0 issues and considerations

The following chart describes issues known to exist in the Passport 1600 Series Switch software release 1.0 and in the 1.1 release:

Hardware and platform

- You need to 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 that the Passport 1600 Series switch will respond to is 1472 bytes. (Q00672839)
- On the 1600 Series switch, a port counter wraps to zero once it reaches 43,000,000. (Q00628251)
- With 2 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)

CLI

- 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)

Layer 2

- The Series 1600 switches support only 1 Spanning Tree Group (STG). As a result, if the 1600 is connected to a switch that supports multiple STGs, tagged BPDUs received for these other STGs are silently dropped. The default STG uses untagged BPDUs. (Q00614132)

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:

  — Tagged 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

QoS

- 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: RTR Link, you may expect to see the total number of RTR Links. However, the total is actually the total of all OSFP LSDB interfaces.
- 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)

JDM

- 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)
- If the 1600 Series switch reboots while JDM is connected, the JDM *Java Null Pointer* error message appears. If this happens, close JDM, reopen, and then connect to the switch once more. (Q00682375)
- 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 will 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.

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. You need to do this through the CLI since 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)

IP

- 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 will pick RIP instead of OSPF for those OSPF external routes. (Q00566603-01)

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 will be enabled too. (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)

Related publications

For more information about the Passport 1600 Series switch 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, 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.