

Part No. 212629-B
July 2002

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1000 Series Software Release 2.0.7.9

212629-B

NORTEL
NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. July 2002.

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.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

LinkSafe and Nortel Networks are trademarks of Nortel Networks.

Passport and Accelar are registered trademarks of Nortel Networks.

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

All other trademarks and registered trademarks are the property of their respective owners.

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.

Introduction

These release notes for Passport® software release 2.0.7.9 describe bug fixes in the Nortel Networks™ Passport 1000 Series switch software that have been implemented since release 2.0.7.8. This document also describes known issues and bugs that still exist in Passport software release 2.0.7.9.

These release notes contain the following topics:

- [“Upgrading your software,”](#) (next)
- [“Recommendations and feature-specific information about release 2.0.7.9”](#) on page 5
- [“Bugs fixed in release 2.0.7.9”](#) on page 14
- [“Known issues”](#) on page 17
- [“Related publications”](#) on page 19
- [“Hard-copy of technical manuals”](#) on page 20
- [“How to get help”](#) on page 20

Upgrading your software

Software release 2.0.7.9 includes updates to the run-time software and boot monitor software as follows:

- Run-Time Software Version 2.0.7.9 (p10a2079.img)
- Boot Monitor Software Version 2.0.7.9 (p10b2079.img) supplied as a Boot Monitor Updater
- Java Device Manager (JDM) Version 5.5 (for Microsoft ® Windows ® 95, Windows 98, Windows 2000, and Windows NT ®: jdm_win.exe; for UNIX: jdm_unix.tar.Z)



Note: Before upgrading your software from earlier versions, back up your current configuration file. Version 2.0.7.9 configuration files contain configuration options that are not compatible with run-time options in software version 2.0.7.0 or earlier. It is important to back up the current configuration file before upgrading in case you must revert to a previous version of the run-time image.

For the latest information about software issues, always refer to the Passport Products documentation site from the Nortel Networks Web page (<http://www.nortelnetworks.com/documentation>) or contact Nortel Networks Customer Support at 1-800-4NORTEL.



Warning: Software release 2.0.7.9 requires 32 MB of DRAM. If you do not have 32 MB of DRAM, an error message appears when you boot up the Passport 1000 Series switch.

The memory upgrade kit (AA0011017) is available for the XLR1297SF module and increases DRAM to 32 MB. If your Passport 105x or 11x0 routing switch has 16 MB of DRAM, contact your Nortel Networks sales representative or authorized reseller to upgrade your switch.

- Access Policies have been modified.



Note: The behavior of the access policies has been modified, see related sections [see “Access policy support for TFTP” on page 13](#). Nortel Networks recommends taking this into consideration before upgrading your switch.

Recommendations and feature-specific information about release 2.0.7.9

This section describes basic recommendations and miscellaneous information and pertinent feature-related information about the Passport 1000 Series switch software release 2.0.7.9, and includes the following topics:

- [Recommendations and miscellaneous information](#)
- [Multicast in release 2.0.7.9](#)
- [STG and BPDU clarification](#)
- [High-priority switching](#)
- [Console and Telnet screen message displays](#)
- [Clarification on MLT/STP pathcost](#)
- [Disabling IPX NetBIOS propagation](#)
- [Flash commands](#)
- [IPX RIP and IPX SAP pacing \(frame rate\)](#)
- [Access policy support for TFTP](#)
- [Access level authorization for SNMP, rlogin and telnet](#)

Recommendations and miscellaneous information

Note the following recommendations and miscellaneous information about Passport 1000 Series switch software release 2.0.7.9:

- Before using the configuration files from previous software releases, Nortel Networks recommends that you ensure that the `Polycyname` and the `TrustedHostUserName` fields are populated for access policies.
- Changes have been made to Passport 1000 series switches from software release 2.0.7.3 onwards in terms of selection of the best path to an ASBR if more than one path exists.



Note: Due to these changes, Nortel Networks recommends that you not interconnect a switch running software release 2.0.7.3 or higher to a switch running a software release 2.0.7.2 or lower. (Q00168665)

- Passport 1000 Series switch software release 2.0.7.9 does not support global filters. Configuration information relating to global filters is ignored. When booting up with software version 2.0.7.9, the following message is displayed on the screen:

```
Global filters are not supported in this release.
```
- When you create a MultiLink Trunking (MLT) group through the command line interface (CLI), the resulting MLT is put into the default VLAN (VLAN 1). The MLT should then be assigned to other VLANs as appropriate.
- Always set a specific Enforce Operational Configuration (EOC) mode (refer to the Passport 1000 Series switch software release 2.0 release notes for more information) instead of allowing the default EOC mode (which is to the lowest-level module in the switch) in order to avoid losing functionality in case a lower-revision module is installed in the switch.
- Terminology has been modified in Device Manager and the CLI so that “trunk” is used only in reference to MultiLink Trunking (MLT). What were previously referred to as *trunk ports* (in contrast to access ports) are now referred to as *tagged ports*.
- Gigabit LinkSafe™ configurations must have autonegotiation enabled. Setting autonegotiation to False is not supported on gigabit LinkSafe modules in *redundant* configurations. However, autonegotiation can be set to False if a gigabit LinkSafe module is connected in a nonredundant setup to a gigabit module not supporting autonegotiation.

- Nortel Networks recommends against configuring VRRP on IP-subnet-based VLANs because there is no hardware support for this configuration in the I/O modules and all traffic forwarding must be handled by the CPU. This situation can cause high CPU utilization and affect performance. (105851-1)
- VRRP running over IEEE 802.1Q tagged ports requires ARU3 modules (-B hardware). (115732-1, 130826-1)
- On a Passport 1000 Series switch, IP forwarding is enabled by default. (142874-1)

Multicast in release 2.0.7.9

The two software features DVMRP and IGMP have known problems that can cause general operational issues with Passport 1000 Series switches. Therefore, IP Multicast is not supported in release 2.0.7.9 or earlier releases.

STG and BPDU clarification

The following two controls regulate the behavior of the Spanning Tree Protocol (STP) in a spanning tree group (STG) on a Passport 1000 Series switch:

- A global parameter to enable or disable STP at the STG level
- Port parameters to enable or disable STP on individual ports

When the STP is globally disabled on the STG, received bridge protocol data units (BPDUs) are handled like a MAC-level multicast and flooded out the other ports of the STG. Note that an STG can contain one or more VLANs. Remember that MAC broadcasts are flooded out on all ports of a VLAN; a BPDU is a MAC-level message, but the BPDU is flooded out on all the ports in the STG, which may encompass many VLANs.

When STP is globally enabled on the STG, BPDU handling depends on the following STP setting of the port:

- When STP is enabled on the port, received BPDUs are processed in accordance with STP.
- When STP is disabled on the port, the port will always be in a forwarding state, received BPDUs are dropped and not processed, and no BPDU is generated.

To configure STP on STGs with the CLI, use this command:

```
config stg <sid> group-stp <enable/disable>
```

To configure STP on a port with the CLI, use this command:

```
config ethernet <ports> stg <sid> stp <enable/disable>
```

To configure STGs with Device Manager, choose VLAN > Stg > Configuration. To configure STP on a port with Device Manager, choose the port and the spanning tree tab.

High-priority switching

The Passport 1000 Series switch operates in one of two modes: Best Effort mode or High Priority mode. The factory default setting is Best Effort mode; in this mode, all traffic is treated with the same priority. In High Priority mode, high-priority traffic flows through the switch fabric using a high-priority data path; output buffers are reserved for high-priority traffic. This does not apply to IEEE 802.1P packets.

Nortel Networks recommends that you enable High Priority mode on switches in very heavy traffic situations. Enabling High Priority avoids delaying vital high-priority network traffic, including BPDUs and routing protocol information. To enable High Priority mode using the CLI, enter:

```
config sys set flags highpriomode true
```



Note: The switch must be rebooted before this change takes effect.

Console and Telnet screen message displays

Table 1 describes the messages that are not displayed on the console or Telnet screens using the `config log screen on` command.



Note: Even though these messages are not displayed, they are still added to the log file.

Table 1 Non-displayed CLI messages

```
cpu switch over, stand-by CPU become master
Link Down
Dual Connector Link Down
Link Up
Dual Connector Link Up
Card Down
Card Up
Spanning Tree New Root
Spanning Tree Topology Change
BackupConnectorDown
BackupConnectorUp
Ospf Nbr State Change trap:
OspfIfConfigError trap:
OspfIfAuthFailure trap:
OspfIfStateChange trap:
OspfVirtNbrStateChange trap:
OspfVirtIfConfigError trap:
OspfVirtIfAuthFailure trap:
OspfVirtIfStateChange trap:
Power Supply Down
Fan Down
Link Oscillation
Mac Violation
Power Supply Up
```

Clarification on MLT/STP pathcost

This section describes behavior of the MLT/STP pathcost when adding or removing ports in a MLT group.

- When adding ports to a MLT group configured with default pathcost, the pathcost value is equally distributed among the MLT ports; the higher the number of ports in a MLT, the lesser the path cost.
- When the pathcost value of any one enabled MLT port is administratively configured, or if an enabled port with an administratively configured pathcost is added to a MLT group, the remaining MLT ports exhibit the same pathcost value.
- When adding or removing a port from a MLT group, the pathcost value of all the ports in a MLT revert to the default value. (Q00072320)
- Adding or removing a disabled port to a MLT causes the pathcost of the port to be 65535.



Note: To assure desired traffic flow, Nortel Networks recommends to verify the path cost after adding or removing ports in a MLT group when using non-default values for pathcost.

Disabling IPX NetBIOS propagation

With the release of Passport 1000 Series switch software version 2.0.4 and higher, you can disable IPX NetBIOS (type 20) propagation. You can enable or disable IPX NetBIOS (type 20) propagation globally, that is, on all IPX interfaces in the entire chassis.

You can configure this feature using the CLI. The CLI command to enable or disable IPX NetBIOS (type 20) propagation is

```
config ipx set netbios <on/off>
```

To view the current state of IPX NetBIOS propagation, use the `config ipx set info` command.



Note: The option to enable or disable IPX NetBIOS propagation is associated with IPX routing, so it is relevant only to switches with the ARU3 module (Rev B) and with IPX enabled.

Flash commands

The verbiage in the flash commands `format`, `squeeze`, and `recover` is changed to accurately indicate the behavior when leaving the command—the operation is not canceled when selecting to continue; rather the operation continues in the background. Any attempt to access or manage the flash command during processing will fail. (115397-1, 116199-1)

The following is an example of the revised wording:

```
Passport 1000 Series switch-1000# format fl
```

```
Format will erase all files.
```

```
Do you wish to continue? (y/n)? y
```

```
formatting...Press any key to push operation to background.
```

When you press any key, the following text is displayed on the screen:

```
Note: If you push operation to background you will not be advised as to the result of the operation.
```

```
Do you wish to continue (y/n)? n
```

```
formatting ... success
```

```
Passport 1000 Series switch-1000# format fl
```

```
formatting ... Press any key to push operation to background.
```

When you press any key, the following text is displayed on the screen:

Note: If you push operation to background you will not be advised as to the result of the operation.

```
Do you wish to continue (y/n) ? y
```

```
formatting ... operation pushed to background
```

```
Passport 1000 Series switch-1000#
```

IPX RIP and IPX SAP pacing (frame rate)

This frame rate is used to control the number of frames per second for IPX RIP and IPX SAP. The default is 20 frames per second. In Device Manager, the frame rate is controlled by the pace parameter; and in the CLI, it is controlled by the update-delay parameter. (118350-1)

The “pace” is the number of packets per second. The “update-delay” is expressed in milliseconds.

For example:

pace = 50 (packets per second)

update-delay = 20 milliseconds (1000/pace)

To make changes to the pace parameter:

- ➔ From the Device Manager menu bar, choose Routing > IPX > RIP or Routing > IPX > SAP.

To make changes to the update-delay parameter:

➔ In the command line interface (CLI), use the following commands:

```
config ipx rip update-delay <ipx-network-number>
<delay-timer>
```

or

```
config ipx sap update-delay <ipx-network-number>
<delay-timer>
```

where:

ipx-network-number is the network number in hexadecimal format.

delay-timer is a value in milliseconds (1...1000).

Access policy support for TFTP

You can enable or disable access-policies for TFTP service. To enable TFTP service for a specified access-policy, enter the following command:

```
config sys access-policy policy <pid> service
tftp<enable|disable>
```

This command configures specific policy IDs, *where*

<pid> is the policy ID. Enter a value from 1 to 65535

enable|disable enables or disables the specified access policy for TFTP service.

In addition, the CLI command **sh config verbose** now shows the access-policy information for TFTP service.



Note: This feature is not supported in Device Manager.

Access level authorization for SNMP, rlogin and telnet

Access policies for SNMP, rlogin and telnet now properly authorize access levels. The access level specified within the access policy is used as a base when authenticating users accessing the switch.

For example, assigning an access level of ro allows users with ro, rw, and rwa permissions to access the policy. Access policies now have a default level of 'ro', and accept access from users with login criteria equal to or higher than the current policy access level. If you configure multiple access policies with the same settings for network/ mask, host, precedence, and username (username applies only to rlogin policy), then the policy with the lowest access policy ID (PID) takes precedence.



Note: The default access level for the access policies has been changed from 'rw' to 'ro'. The user needs to be careful during upgrading. If the previous config file has 'rw' access level saved pertaining to a particular access policy, it will get changed to 'ro'.

Bugs fixed in release 2.0.7.9

This section describes bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.9, and includes the following bugs-fixed topics:

- “IP” next
- “IPX” on page 15
- “OSPF” on page 15
- “Miscellaneous” on page 17

IP

This section describes the IP bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.9.

- The source IP address in the UDP packets sent out of the egress interface of a Passport 1200 now correspond to the egress interface IP addresses. (Q00170994-02)
- On a Passport 1000 Series switch, when the default route exist, an IP Filter entry pointing to a dynamic route is no longer deleted when the dynamic route is deleted. (Q00043950, Q00043955)
- When a Passport 1000 Series switch pings the network address of a subnet, an ARP request is generated. The ARP responses for the network address are now properly discarded.(Q00169482-02)
- On a Passport 1000 Series switch, the following error message is now given while adding a static route which is more specific than an existing local route. (Q00284589)
“Failed adding a route <IP ADDRESS> in RTBL”
- On a Passport 1200 switch, now only one router can be configured on a port. (Q00302834, Q00302840).
- On a Passport 1000 Series switch, the port in the default route record will now be updated only if the same MAC address is learned over any port on the same VLAN. (Q00279152)

IPX

The following IPX bugs have been fixed in Passport 1000 Series routing switch software release 2.0.7.9.

- On a Passport 1000 Series switch, IPX traffic is restored across reboots on a port that is a member of a protocol-based VLAN and has a port number higher than another active port in that VLAN. (Q00289208)
- On a Passport 1000 Series switch, an IPX network number that is larger than the valid length is no longer accepted. (Q00227898-02)

OSPF

The following OSPF bug has been fixed in Passport 1000 Series routing switch software release 2.0.7.9.

- OSPF area aggregation with a network IP address of 0.0.0.0 and any non-zero mask can no longer be configured. (Q00209497)
- Across reboots with an ASCII configuration file, the area range configured on the backbone is now restored. (Q00229248)
- On a Passport 1000 series switch, when OSPF is enabled on a VLAN, re-enabling OSPF does not change the OSPF status of the ports in that VLAN. (Q00286263)
- OSPF ASE routes are no longer lost when the backbone interface port link state is toggled. (Q00420068)
- OSPF area aggregation for LSA Type 7 can no longer be created on the backbone area. (Q00283898-01)
- A static route is no longer announced after it is deleted. (Q00209499)
- For an external route destination for which both inter-area and intra-area routes exist, the Passport 1000 Series switch now chooses the non-backbone intra-area route even if the inter-area route has a lower cost. (Q00415202-02)

MLT

The following MLT bugs were fixed in Passport 1000 Series routing switch software release 2.0.7.9.

- On a Passport 1000 series switch, MLTs configured on protocol-based VLANs are now restored properly when upgrading from earlier software releases. Software release 2.0.7.8 erroneously defaulted the MLT configuration when upgrading with configuration files that were generated from releases prior to release 2.0.7.8. (Q00321460)
- When ports of an MLT belonging to a policy-based VLAN are added as not allowed members of that VLAN, they are no longer potential members of that VLAN. (Q00108115)

Miscellaneous

This section describes miscellaneous bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.9.

- On a Passport 1000 series switch, log messages are now properly stored in the syslog file after the syslog file is deleted and recovered. (Q00208255)
- When doing reboots with an ASCII configuration file, no ports are added to the default VLAN and to the default STG, if no ports were initially assigned to them. (Q00170883-01)
- The Passport 1000 series switch no longer allows creation of an STG with a Tagged-Bpdu-Vlan-Id the same as that of an existing STG. (Q00208842)
- The static ARP entry corresponding to a protocol-based VLAN is no longer lost across reboots. (Q00089518)
- A Passport 1200 Series switch no longer allows the invalid MAC address 00:00:00:00:00:00 to be added to the allow-MAC table from JDM. (Q00212676).
- UDP forwarding is now allowed only if IP forwarding is enabled.(Q00227835)
- When a dynamic ARP entry for an interface is replaced by a static ARP entry, all of the parameters in the dynamic ARP entry are replaced by the user-specified parameters. (Q00207059, Q00110910)
- Changes have been made to the Telnet implementation to make it more robust. (Q00250016)
- On a Passport 1000 series switch, CDP packets are now properly handled. (Q00411060)
- A port which is a 'notallowedtojoin' member of a policy-based VLAN is now removed from that VLAN, if the port is removed from the STG to which the VLAN belongs. (Q00173789, Q00216346-01)
- An incorrect network mask and IP address combination is no longer allowed when configuring access policies. (Q00283883-02)
- The Tagged-Bpdu-Vlan-Id of an STG will now be restored properly across reboots with an ASCII configuration file. (Q00458070)
- The SNMP Non-Unicast Packet-Counter now returns a correct value. (Q00433702-02)

Known issues

The following sections describe issues known to exist in the Passport 1000 Series switch software release 2.0.7.9, and include the following topics:

- [“Miscellaneous” on page 17](#)
- [“IP” on page 19](#)

Miscellaneous

The following miscellaneous known issues exist in the Passport 1000 Series switch software release 2.0.7.9:

- An interoperability issue has been observed under the following conditions that cause the Passport 1000 Series switch to reset:
 - A Dell or Compaq laptop PC using Windows 2000 is repowered while connected to the console port of the Passport 1000 Series switch.
 - A Dell or Compaq laptop PC using Windows 2000 is connected to the console port of the Passport 1000 Series switch for an extended period of time without running an active application such as hyperterm. (Q00064666/138370-1)
- The rcStatBridgeOutBroadcastFrames counter is not supported. (113124-1)
- In a Passport 1000 Series switch, sourcing a pre-2.0.7.4 ASCII configuration containing STG information results in errors due to a change in the configuration order. (Q00052243/141807-1)
- In a Passport 1000 Series switch, when an IP filter is applied to a port in a MLT, it is not automatically applied to all ports in the MLT. For the filter action to take place, it must be applied individually to all the ports in the MLT. (Q00045276/145942-1)
- The ifOutBroadcastPkts counter is not supported. (Q00086882)
- Only 100 Add-Allow-Mac entries will be restored across reboots with a binary configuration file.
- In Passport 1000 Series switches, any changes made to the access-level in an access-policy, take effect immediately even if the access-policies are globally disabled. (Q00476989)

IP

The following IP issue exists in the Passport 1000 Series switch software release 2.0.7.9:

The Passport switch does not use a dynamically learned route (RIP/OSPF) when a static route for that network becomes inactive.
(Q00055362/115167-1, 121564-1)

Related publications

Refer to the following Passport documentation for additional information:

- *Reference for the Passport 1000 Series Management Software Switching Operations* (part number 208964-A)

This publication describes how to use Device Manager to configure and manage layer 2 (switching) functions in a Passport switch.

- *Reference for the Passport 1000 Series Management Software Routing Operations* (part number 208965-A)

This document describes how to use Device Manager to configure and manage layer 3 (routing) functions in a Passport switch.

- Various addenda to the release notes for software release 2.0 for Passport (and Accelar) 1000 Series products (part numbers 206494-A through 206494-Z and 212629-A)
- *Release Notes for the Accelar 1000 Series Products Software Release 2.0* (part number 896-00181-E)
- *Networking Concepts for the Passport 1000 Series Routing Switch* (part number 205588-B)
- *Reference for the Accelar 1000 Series Command Line Interface Software Release 2.0* (part number 202086-B)
- *Installing the Accelar 1000 Series Chassis* (part number 893-01051-D)
- *Using the Accelar 1050/1051 Routing Switch* (part number 201603-C)
- *Using the Accelar 1100/1150 Routing Switch* (part number 893-01050-C)
- *Using the Accelar 1200/1250 Routing Switch* (part number 893-01049-C)
- *Upgrading to Accelar 2.0 Software* (part number 206077-A)

Hard-copy of technical manuals

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* at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader*.

You can purchase selected documentation sets, CDs, and technical publications through the Internet at the www1.fatbrain.com/documentation/nortel/ URL.

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 one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
EMEA	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

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 www12.nortelnetworks.com/ URL and click ERC at the bottom of the page.