

Part No. 206494-Z
October 2001

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1000 Series Software Release 2.0.7.7



NORTEL
NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. October 2001.

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 2.0.7.7 describe bug fixes in the Nortel Networks™ Passport 1000 Series switch software that have been implemented since release 2.0.7.6. This document also describes known issues and bugs that still exist in Passport software release 2.0.7.7.

These release notes contain the following topics:

- [“Upgrading your software,”](#) (next)
- [“Recommendations and feature-specific information about release 2.0.7.7”](#) on page 5
- [“Bugs fixed in release 2.0.7.7”](#) on page 14
- [“Known issues”](#) on page 19
- [“Related publications”](#) on page 20
- [“Hard-copy technical manuals”](#) on page 21
- [“How to get help”](#) on page 21

Upgrading your software

Software release 2.0.7.7 includes updates to the run-time software and boot monitor software as follows:

- Run-Time Software Version 2.0.7.7 (p10a2077.img)
- Boot Monitor Software Version 2.0.7.7 (p10b2077.img) supplied as a Boot Monitor Updater
- Device Manager and VLAN Manager Version 2.0.5 (for Microsoft® Windows® 95 or Windows 98 and Windows NT®: dm_205.exe; for UNIX: dm_2.0.5.tar.Z)



Note: Before upgrading your software from earlier versions, back up your current configuration file. Version 2.0.7.7 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 2.0.7.7 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.

Recommendations and feature-specific information about release 2.0.7.7

This section describes basic recommendations and miscellaneous information and pertinent feature-related information about the Passport 1000 Series switch software release 2.0.7.7, and includes the following topics:

- [Recommendations and miscellaneous information](#)
- [Multicast in release 2.0.7.7](#)
- [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 \(frame rate\)](#)

Recommendations and miscellaneous information

Note the following recommendations and miscellaneous information about Passport 1000 Series switch software release 2.0.7.7:

- Passport 1000 Series switch software release 2.0.7.7 does not support global filters. Configuration information relating to global filters is ignored. When booting up with software version 2.0.7.7, 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 1200 Switch, IP forwarding is enabled by default. (142874-1)

Multicast in release 2.0.7.7

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 2.0.7.7 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 all ports on 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 Priority mode. The factory default setting is Best Effort mode; in this mode, all traffic is treated with the same priority. In 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 Priority mode on switches in very heavy traffic situations. Enabling Priority avoids delaying vital high-priority network traffic, including BPDUs and routing protocol information. To enable Priority 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 following messages that are not displayed on the console or Telnet screens using the `config log screen on` command.



Note: Even though these message 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 clarifies 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 MLT port is administratively configured, or if a port with an administratively configured pathcost is added to a MLT group, the remaining MLT ports exhibit the same pathcost value.
- When removing a port from a MLT group, the pathcost value of all the ports in a MLT revert to the default value. (Q00072320)

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-1200# 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-1200#
```

```
Passport 1000 Series switch-1200#
```

```
Passport 1000 Series switch-1200# 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-1200#
```

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).

New access policy support in release 2.0.7.7

In this release you can enable or disable access-policies for TFTP service. Previously this option was available only for telnet, http, snmp and rlogin.

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.

Bugs fixed in release 2.0.7.7

This section describes bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.7, and includes the following bugs-fixed topics:

- [“Miscellaneous,”](#) next
- [“CLI](#)
- [“MLT”](#) on page 16
- [“IP”](#) on page 17
- [“IPX”](#) on page 17
- [“OSPF”](#) on page 17
- [“VRRP”](#) on page 18

Miscellaneous

This section describes miscellaneous bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.7.

- In the routing table, the IP filter now points to the default route next-hop when the route to the destination IP address is deleted. (Q00084326)
- When saved, the correct status of log-stats is now displayed across reboots. (147831/Q00043179)
- An enabled IP traffic filter now no longer is disabled when a Passport 1200 switch is rebooted with an ASCII config file. (Q00079759)
- With the secondary CPU booted to standby, the `savetostandbyNvram` CLI command now works properly when executed from the primary CPU. (Q00068300-01)
- A Passport 1200 switch now displays IP filter log-stats information when the `show ip traffic-filter active` CLI command is executed. (Q00043179)
- The UDPFWD configuration is now no longer lost when a Passport 1200 switch is booted with an ASCII configuration file. (Q00079034)
- A brouter port is now no longer created if a duplicate IP address is assigned to the brouter port. (Q00084320)

- The **show log file tail** CLI command now shows the correct set of log messages when a Passport 1200 switch is reset after the syslog file is cleared and a few messages are logged on to the new syslog file. (Q00084322)
- After an I/O card is removed, a Passport 1200 switch now no longer displays port information corresponding to a port on the card when the **show port info** CLI command is executed. (Q00044574)
- A condition has been resolved in which the Passport 1200 routing switch may erroneously imply high levels of memory fragmentation and eventually cause the Passport 1200 routing switch to believe it has run out of memory during frequent and prolonged SNMP polling. (Q00087373)
- The **config ether <ports> stg <stg-id> stp disable** CLI command drops the ports that do not belong to the specified STG and disables the STP on the other ports in the specified range. (Q00086728-01)
- The **show stg info status** CLI command now displays the correct number of ports present in the STG. (Q00084323)
- The connectivity between two hosts connected to a Passport 1200 switch now is restored successfully after the link to the host goes down and comes up, even if an IP filter with a default action of drop exists on the port connected to the host. (Q00088071)
- When the administrative state of a Gig link-safe port is brought down, the remote Gig link-safe port connected to this port also goes to a down state. (Q00086737)
- An ASCII configuration file containing UDPFWD Portfwdlist entries created in Device Manager with blank list names is now successfully loaded on a Passport 1200 switch. A default list name is given to these entries. (Q00103410)
- In a Passport 1200 switch, when a configuration file containing UDPFWD entries is saved and the switch rebooted, the forwarding ID, `portfwd`, no longer is changed. (Q00084642)
- A Passport 1200 switch now allows the deletion of old UDPFWD PortFwdList entries when the PortFwdList entry under an interface is changed to another value. (Q00079035)
- An ASCII file can now be successfully copied from active SSF to a standby SSF. (Q00106405)

CLI

This section describes CLI bugs that have been fixed in the Passport 1000 Series switch software release 2.0.7.7.

- You can now enable or disable IP filters using the CLI by entering the partial commands **en** or **di** respectively. You can also configure the default action for the filters by entering partial commands **f** for forwarding and **n** for none. (Q00047018)
- The CLI command **config sys set action getstandbycpuinfo** now displays the slot number of the stand-by CPU and its operating status (only if the standby CPU is present). (Q00069220-01)
- If all the ports belonging to a VLAN that contains a MLT group are disabled, the IP address of the VLAN is now no longer displayed as part of ARP table or the routing table when `advertise when down` is disabled. (Q00039992)
- The error message `Command not allowed on standby` is now generated when the CLI command **copy running <device>** is executed from the standby CPU. (Q00084655)
- The CLI command **show port info arp** now displays information about IRP ports. (Q00088533)
- In a Passport 1200 switch, correct values are now displayed for `IN_OCTETS` count when the **show port stats interface main** command is executed from the CLI. (Q00048140)
- The CLI command **config sys set action resetcounter** now resets the `Topology Changes` counter to 0. (Q00089598)

MLT

The following MLT bugs have been fixed in Passport 1000 Series routing switch software release 2.0.7.7:

- A Passport 1200 switch now allows a single MLT port to be removed from the VLAN or the STG to which it belongs, instead of first having to remove all the ports belonging to the MLT group. (148526-1)
- A Passport 1200 switch now no longer allows two VLANs belonging to two different STGs to be added to an access MLT. (Q00088534)

- A Passport 1200 switch now no longer allows the addition of a policy based VLAN to a MLT when the MLT already has a similar policy based VLAN with MLT ports as its active members. (Q00046182)
- The pathcost of a disabled port is now set to 100 after it is added and then removed from a MLT group. (Q00068026)
- The pathcost of a MLT port that is down, now remains constant across reboots and is set to 100. (Q00079760)
- A MLT port can now no longer be configured as an IP brouter nor can a VLAN associated with an IP brouter port be added to a MLT. (CR-Q00080811-01, CR-Q00085307)

IP

This section describes the IP bug that has been fixed in the Passport 1000 Series switch software release 2.0.7.7.

A local interface can now no longer be added as a next-hop for a static route even if the interface is down. (Q00043594)

IPX

The following IPX bug has been fixed in Passport 1000 Series routing switch software release 2.0.7.7:

A Passport 1200 switch now no longer allows an access port belonging to an IPX protocol based VLAN with a particular encapsulation to be added to a port-based VLAN with the same encapsulation and vice-versa. (Q00086723-01)

OSPF

The following OSPF bugs were fixed in Passport 1000 Series routing switch software release 2.0.7.7:

- When a Passport 1200 switch is connected to another switch through a common NSSA interface, the database description packets exchanged between them now have the NSSA bit set. (Q00103689)

- A Passport 1200 switch now displays the following message when the **show ip ospf lsdb** CLI command is executed before the OSPF has converged:
LSDB has changed please try the command later
(Q00085532-01)
- A VLAN now continues to remain in the same OSPF area after an IP address is assigned to it. (Q00075950-01)
- A Passport 1200 switch now announces static routes when rebooted with an ASCII config file. (Q00048203)
- A Passport 1200 switch now displays the error message
Error: Consistency check failed - OSPF interface not found when you attempt to add a non-existent interface to an OSPF area.
(Q00088559-01)
- A Passport 1200 switch now displays the correct neighbor area id under the NBAREAID field in ospf virtual neighbors table. (Q00079052)
- A Passport 1200 switch now accepts message-digest authentication for VLANs. (Q00072323)
- Device Manager no longer allows you to configure an authentication-key when the authentication-type is set to NONE. (Q00072322)
- If an area is configured as an NSSA, a Passport 1200 switch now no longer allows you to disable the import-summary option for the NSSA. (Q00084117)

VRRP

The following VRRP bugs were fixed in Passport 1000 Series routing switch software release 2.0.7.7:

- The VRRP virtual IP address now only responds to ICMP echo messages. (Q00046505-01)
- When a critical interface is deleted on a Passport 1200 switch that was originally the master, and the switch is rebooted, the switch no longer loses its VRRP configuration. (Q00084649-01)
- VRRP master to backup transition now happens when the critical interface is deleted. (Q00084645)
- In a Passport 1200 switch, the hardware records corresponding to VRRP in GIG revision -B boards are now initialized correctly so that IP unicast packets having a destination MAC address as VRRP Mac address are now properly treated. (Q00086170)

Known issues

The following sections describe issues known to exist in the Passport 1000 Series switch software release 2.0.7.7, and include the following topics:

- [“Miscellaneous” on page 19](#)
- [“IP” on page 20](#)

Miscellaneous

The following miscellaneous known issues exist in the Passport 1000 Series switch software release 2.0.7.7:

- An interoperability issue has been observed under the following conditions that cause the Passport 1200 Switch to reset:
 - A Dell or Compaq laptop PC using Windows 2000 is repowered while connected to the console port of the Passport 1200 Switch.
 - A Dell or Compaq laptop PC using Windows 2000 is connected to the console port of the Passport 1200 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 1200 Switch, sourcing a pre-2.0.7.4 configuration ASCII file containing STGs gives errors as the file attempts to set the port-based parameters for STG IDs even before the STGs are created. (Q00052243/141807-1)
- In a Passport 1200 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)

IP

The following IP issue exists in the Passport 1000 Series switch software release 2.0.7.7:

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-W)
- *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 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.

