

Part No. 212358-C
April 2002

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1000 Series Switch Software Release 2.1.4.0



NORTEL
NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. April 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 NA 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, Autotopology, and BaySecure are trademarks of Nortel Networks.

Passport is a registered trademark 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.

Introduction

These release notes for Nortel Networks* Passport* 1000 Series software release 2.1.4.0, describe bug fixes since software release 2.1.3.0, and describe known issues that exist in this software release. These release notes are to be used in conjunction with the previously released Passport 1000 Series 2.1—2.1.3 release notes available on the Nortel Networks documentation Web site at the www.nortelnetworks.com/documentation/ URL; search terms: Data and Internet and Passport 1000 Series.



Warning: This software release requires 32 megabytes (MB) of dynamic random access memory (DRAM). The system will not boot using less DRAM. A memory upgrade kit (AA0011017) is available for the XLR1297SF module to increase DRAM to 32 MB. If your Passport routing switch has less than 32 MB of DRAM, contact your Nortel Networks sales representative or authorized reseller for upgrade options for your switch.

Do not upgrade to release 2.1.4.0 using only 16 MB of RAM. Doing so can cause the Passport switch to crash and block all types of access, including console access and monitor mode access.

These release notes contain the following topics:

- “Software updates,” next
- “Recommendations and information about release 2.1.4.0” on page 5
- “Access policy support” on page 5
- “Bugs fixed in release 2.1.4.0” on page 6
- “Known issues in release 2.1.4.0” on page 10
- “Related publications” on page 15
- “Hard-copy technical manuals” on page 15
- “How to get help” on page 16

Software updates

This software release includes updates to the following components:

- Boot Monitor Software Version 2.1.4.0 (p10b2140.img)
- Run-Time Software Version 2.1.4.0 (p10a2140.img)
- 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: As a precaution, before you upgrade your software from versions 2.0.7.x, 2.1.x, or earlier, back up your current configuration file. Release 2.1.4.0 configuration files contain configuration options that are not compatible with the run-time options of previous versions. Back up the current configuration file before upgrading, in case you must revert to a previous version of the run-time image.

JDM version 5.5 for Passport 1000 Series software release 2.1.4.0 supports:

- Windows 95, Windows 98, Windows 2000, and Windows NT
- HP-UX, AIX
- Solaris

To run JDM, install the JDM software and the Java Run-Time Environment (JRE) software. For instructions on installing the software, refer to *Reference for the Passport 1000 Series Management Software Switching Operations Release 2.1*.

Recommendations and information about release 2.1.4.0

Note the following recommendations and miscellaneous information about Passport 1000 Series software release 2.1.x.x:

- Before using the binary configuration files from previous releases, ensure that the `PolicyName` and the `TrustedHostUserName` fields are populated for the access policies.
- Always set a specific enforced operational configuration (eoc) mode to the highest level of hardware (ARU2 or ARU3) in the chassis, instead of allowing the default eoc mode (which is to the lowest level module in the switch). This setting prevents functionality loss in case a lower revision module is installed in the switch.
- 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.
- The use of VRRP on IP subnet-based VLANs is not supported.
- You can now create a maximum of **101** VLANs using software release 2.1 and up; previously, you could create a maximum of 123 VLANs. This number is further dependent on the number of MLTs and STGs configured for the Passport switch.
- To initiate a Telnet session from the console, use the CLI command **`config sys telnet-client enable`**. By default `telnet-client` is disabled on the switch. (Q00054813/145983-1)

Access policy support

To enable TFTP service for a specified access-policy, enter the following CLI 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 **show config verbose** now shows the access-policy information for TFTP service.



Note: This feature is not supported in Device Manager.

Bugs fixed in release 2.1.4.0

This section describes bugs fixed in the Passport 1000 software release 2.1.4.0, and includes the following topics:

- “Miscellaneous,” next
- “CLI” on page 8
- “DHCP” on page 8
- “IP” on page 8
- “IPX” on page 9
- “OSPF” on page 9
- “RADIUS” on page 10
- “VRRP” on page 10

Miscellaneous

This section describes the miscellaneous bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- An access MLT configuration based on a protocol based VLAN is now properly restored when upgrading to Passport 1000 Series software release 2.1.4.0 when using a pre-2.1.3.0 binary configuration file. (Q00321460)
- In a Passport 1200 switch, changes have been made to the telnet implementation to make it more robust. (Q00250016)

-
- The Passport 1000 series switch is no longer impacted by SNMP vulnerability issues documented on February 12, 2002 by CERT/CC in their SNMP advisory. (VU#107186 and VU#854306)
 - The length of the RMON owner, description and community fields are now restricted to 48 characters. (Q00283833)
 - In this Passport 1000 Routing Switch Series software release, default values are populated for `Polycyname` and `TrustedHostUserName`, if the access policies are created from Device Manager without supplying values to these fields. (Q00301387)
 - A CPU synchronization failure message is no longer displayed on a Passport 1000 Series Switch with a single SSF when the `date` CLI command is executed. (Q00168275)
 - The message `Transfer Timed Out` is no longer erroneously displayed after you terminate a TFTP transfer. (Q00086736)
 - When a policy-based VLAN having no active members is deleted, or its IP address is deleted, the static ARP entry corresponding to this VLAN is now purged from the ARP table. (Q00173788)
 - The default access policy can no longer be deleted. (Q00157142)
 - If the port goes down, a potential member of a policy-based VLAN is now removed from the active membership of the VLAN. (Q00035785)
 - Port members of a STG are now added as potential members of a policy-based VLAN based on that STG, even if the same policy-based VLAN exists in another STG. (Q00156752)
 - The Passport 1000 Series Switch no longer allows creation of a STG with a tagged bpdv VLAN ID the same as that of an existing STG. (Q00208842)
 - Across 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)
 - A port which is not allowed to join 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)
 - The static ARP entry corresponding to a protocol-based VLAN is no longer lost across reboots. (Q00089518)
 - The following error message is displayed when you attempt to add more than 500 static routes on the Passport 1000 Series Switch:

```
Max 500 Static Routes Allowed, cannot add the route
```

(Q00086970, Q00091867)

CLI

This section describes the CLI bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- The range for valid values of IP traffic filter IDs is now properly displayed as 1-767. (Q00091995-01)
- VLAN interfaces are now displayed correctly when the **show ip vrrp stats** CLI command is executed.(Q00249574)

DHCP

This section describes the DHCP bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- When DHCP is disabled, all the forwarding paths pertaining to that interface are now deleted. (Q00032689-04)
- DHCP can no longer be enabled on an interface which is not assigned an IP address. (Q00093563-03)
- DHCP parameters can not be set when DHCP is not enabled on an interface. (Q00093563-03)
- The Passport 1000 series switch now uses the ingress port information in the `source IP address` field of the DHCP request packet. (Q00208249)

IP

This section describes the IP bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- 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)
- A filter route entry for the same destination as an existing OSPF/static route now is added to the main routing table, once the OSPF/ static route is deleted. (Q00091868, Q00108739)
- UDP forwarding no longer occurs if IP forwarding is disabled on a Passport 1000 Series switch. (Q00227835)

IPX

This section describes the IPX bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- In Device Manager, you can no longer create an IPX static route with a metric of 16. (Q00029863)
- An IPX static route entry now replaces a similar dynamic SAP entry in the main routing table even if it is configured after the dynamic entry was learned. (Q00024852-04)
- An IPX static route can now be added even though a local route exists for the same IPX network. The static route will be added to the static-routing table as inactive. As a result of this, inactive static routes are now restored properly across reboots with ASCII configuration files. (Q00170790)
- The RIP Out policy now updates the ticks and the hop count of the matching IPX route irrespective of the global routing-method value, provided the tick or hop count is not zero in the matching policy. (Q00171433-01)
- On a Passport 1200 switch, you can now successfully add an IPX static SAP entry with a dynamically learned host network. (Q00093097)
- The parameter `learnafterincrement` is now saved properly across reboots with ASCII configuration files (Q00157150)
- Changes in IPX max-route and max-static-route no longer require a reboot to take effect. (Q00093873, Q00093874)

OSPF

This section describes the OSPF bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- All external routes through a NSSA are now announced properly into the backbone. (Q00217037)
- OSPF area aggregation for network IP address 0.0.0.0 with any non-zero mask can no longer be configured. (Q00209497-01)
- OSPF area ranges configured in the backbone area are no longer lost across reboots with ASCII configuration files. (Q00229248-01)
- Area aggregation based on type 3 and type 7 LSAs for the same network is now possible. (Q00176066-01)

RADIUS

This section describes the RADIUS bugs fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

- The Passport 1000 Series switch is no longer impacted by the RADIUS vulnerability documented by CERT/CC in their RADIUS advisory, VU#589523. The Passport 1000 was not impacted by the second documented vulnerability, VU#936683/
- In a Passport 1000 Series switch, the total size of all the instances of RADIUS reply-message attributes in an Access-Challenge response can now be up to 2000 characters. (Q00248238)

VRRP

This section describes the VRRP bug fixed in Passport 1000 Series Routing Switch software release 2.1.4.0.

The same IP address can no longer be created on two virtual routers on an interface. (Q00173068)

Known issues in release 2.1.4.0

The following sections describe known issues with the Passport 1000 Series Routing Switch software release 2.1.4.0, and include the following topics:

- “Miscellaneous,” next
- “IP Multicast” on page 12
- “Unknown MAC discard” on page 12
- “Large frame support” on page 13
- “TOS-based priority forwarding” on page 13
- “Java Device Manager” on page 13

Miscellaneous

The following miscellaneous issues exist in release 2.1.4.0:

- In a Passport 1200 switch, there is IPX connectivity loss on a port of a protocol-based VLAN when the VLAN becomes active before the port's admin-state is enabled. To restore connectivity, reenable IPX forwarding on the switch. (Q00289208).
- If the routing table contains a more specific non-local route and also a less specific route to a network, then the Passport 1200 switch drops traffic to that interface. This is usually the result of a disjointed network configuration. (Q00041599-02)
- When the large size frame feature is enabled, the hardware counter is not aware of the larger allowed frames and continues to count all frames larger than 1514 bytes or when tagged 1518 bytes as “too large.” (125185-1)
- A port name can only be saved in an ASCII configuration file. The port name will not be saved if a binary configuration is used. (126196-1)
- The CLI up and down arrow keys do not work with the history commands in the following instances:
 - On a Solaris system using the command tool to connect to a tip or Telnet session
 - On a Windows NT4 system running JDM to open a Telnet sessionUse Ctrl-P and N instead of arrow keys. (117470-1)
- The CLI will not accept question marks (?) or semicolons (;) in command strings. This rule applies to the loginprompt, passwordprompt, and prompt. Use the following formats when entering commands:
 - `config cli loginprompt <string>`
 - `config cli passwordprompt <string>`
 - `config cli prompt <string>`(117489-1)
- Progress indicators do not work when copying a file from PCMCIA to flash or from flash to PCMCIA. (117491-1)
- For MLT counters, the outgoing broadcast packets are counted as outgoing multicast packets and the outgoing broadcast counter remains at zero. The outgoing multicast packet counter is incremented. (121756-1)

- Passport switches cannot detect link flaps with less than a 0.5 second interval. (129252-1)
- 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.
 - 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)

IP Multicast



Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform. If your network design requires the use of multicast protocols, contact your sales representative to discuss possible Passport 8000 solutions.

Unknown MAC discard

The following unknown MAC discard issues exist in release 2.1.4.0:

- An ARP request or reply from any station will not cause the MAC address to be AutoLearned. (107649)
- After enabling AutoLearn on a port, previously existing ARP entries and fdb entries must be flushed; otherwise, they will not be reachable or AutoLearned. To remedy this situation, flush the MAC fdb tables and the ARP cache for the AutoLearn port.
- BootP and DHCP traffic will not be autolearned. Rather, an IP address will be assigned but will not be able to communicate unless the MAC address of the client is manually added to the allowed MAC table.

Large frame support

The following large frame forwarding support issue exists in release 2.1.4.0:

Using the large frame support and the tagging feature simultaneously on 10/100 Mb/s Ethernet interfaces in the following situations corrupts the frames so that the frames all reach 1600 bytes:

- Untagged large frames (1536 to 1596 bytes) passing through tagged ports
- Tagged large frames (1544 to 1596 bytes) passing through untagged ports

Gigabit ports do not experience this problem. (126418-1)

TOS-based priority forwarding

The following TOS-based high-priority forwarding issue exists in release 2.1.4.0:

The threshold is checked on the frame's ingress, and the value is not rechecked afterwards. If you change the priority after the frame ingresses the port, that change remains ineffective. (117891-1)

Java Device Manager

The following Device Manager issues exist when used with Passport 1000 Series software release 2.1.4.0:

- The following restrictions apply when selecting multiple ports using `Ctrl+Click`.
 - Redundant Gigabit ports cannot be selected along with ports without redundancy, for example, an SX port and SR port cannot be selected at the same time.
 - Ports on a Passport 1216FX module cannot be selected along with any other type of port except for 10/100Mbps TX port.

In such cases, use the following Device Manager workaround to select multiple ports of different types:

- Select one set of similar ports you want to edit or graph.
- Select the next set of similar ports you want to edit or graph.

The Device Manager screens and dialog boxes are displayed so you can view them side-by-side for comparisons. (139953-1)

- To flush a sender's table in Device Manager:
 - Select the first entry in the sender table.
 - Select the last entry in the sender table using the Shift key to highlight all table entries.
 - Press Delete.

All highlighted entries are deleted.

To sort a table, click the column heading. This action provides an entry sequence if you want to delete multiple tables. A maximum of 200 entries can be selected at any time. (137882-1)

- When working with pull-down menus, sometimes you cannot deselect the menu item after you have selected it.

To deselect the menu item, press [Ctrl] + right-click on the mouse. (126629-1)

- The path to the xterm binary needs to be added to the PATH variable to allow Device Manager telnet sessions. (120711-1)
- The port names do not appear in most displays or in statistics, logs, or traps. These names appear on the Edit Port tab. The port names also appear when using the CLI command **show ports info name [<port>]**.
- Inactive IPX static routes are not displayed in Device Manager.
- The IPX route table from Device Manager does not provide the number of routes used by the table. To see the number of routes used, click the Refresh button at least once. (144839-1)

Related publications

For additional information, refer to the following Passport 1000 Series documentation available on the Nortel Networks Customer Service Documentation Web page (www.nortelnetworks.com/documentation):

- *Reference for the Passport 1000 Series Management Software Switching Operations Release 2.1*
- *Reference for the Passport 1000 Series Management Software Routing Operations Release 2.1*
- *Release Notes for the Passport 1000 Series Switch Software Release 2.1.2.0.*
- *Release Notes for the Passport 1000 Series Switch Software Release 2.1.3.0.*
- *Using the Passport 1000 Series Switch*

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*.

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.