

Part No. 212358-D
August 2002

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1000 Series Switch Software Release 2.1.5.0

NORTEL
NETWORKS™

Copyright © 2002 Nortel Networks

All rights reserved. August 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, the Nortel Networks logo, the Globemark, Unified Networks, and [other Nortel trademarked product names] are trademarks of Nortel Networks.

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

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Passport is a registered trademark of Nortel Networks.

The asterisk after a name denotes a trademarked item.

Introduction

These release notes for Nortel Networks* Passport* 1000 Series software release 2.1.5.0, describe bug fixes since software release 2.1.4.0, 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—2.1.4 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. 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 2.1.5.0 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 2.1.5.0”](#) on page 5
- [“Access policy support for TFTP”](#) on page 6
- [“Access level authorization for SNMP, rlogin and telnet”](#) on page 7
- [“Bugs fixed in release 2.1.5.0”](#) on page 8

- [“Known issues in release 2.1.5.0” on page 12](#)
- [“Related publications” on page 17](#)
- [“Hard-copy technical manuals” on page 18](#)
- [“How to get help” on page 18](#)

Software updates

This software release includes updates to the following components:

- Boot Monitor Software Version 2.1.5.0 (p10b2150.img)
- Run-Time Software Version 2.1.5.0 (p10a2150.img)
- Java Device Manager (JDM) Version 5.5.3 (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 2.1.5.0 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 5.5.3 for Passport 1000 Series software release 2.1.5.0 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*.

- Access Policies have been modified.



Note: The behavior of the access policies has been modified, [See “Access policy support for TFTP” on page 6](#). Nortel Networks recommends taking this into consideration before upgrading your switch.

Recommendations and information about release 2.1.5.0

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 `Polycyname` 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.

- Nortel Networks does not recommend that you perform a TFTP operation to the flash or PCMCIA on a secondary telnet session from the primary SSF. It is also not recommended that you perform simultaneous TFTP operations to the flash or the PCMCIA from the primary and secondary SSF under high traffic conditions.
- When configuring the time-offset parameter for NTP, a positive offset from Greenwich Mean Time (GMT) or Coordinated Universal Time (UTC) indicates west of Greenwich and a negative offset indicates east of Greenwich. (Q00488473-01)

Access policy support for TFTP

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. The default value for `tftp service` is `disable`.

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.

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 switch. 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.



Caution: The default access level for the access policies has been changed from `rw` to `ro`. Take care when upgrading, if the previous config file has `rw` access level saved pertaining to a particular access policy, it will get changed to `ro`.

Since the user-configured `rw` access levels will also be changed to `ro`, make sure to configure them to the desired access level after upgrading.

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.

UDP forwarding configuration clarification

There are three possible options when configuring a UDP broadcast forwarding address:

1 Address of server

The UDP Broadcast is forwarded as an IP unicast, MAC unicast.

2 Address of router interface

The UDP Broadcast is forwarded as an IP local network broadcast (255.255.255.255), MAC broadcast.

3 Subnet broadcast address for address of router interface

The UDP Broadcast is forwarded as an IP subnet broadcast MAC broadcast.

Bugs fixed in release 2.1.5.0

This section describes bugs fixed in the Passport 1000 software release 2.1.5.0, and includes the following topics:

- [“RMON,” next](#)
- [“Miscellaneous” on page 9](#)
- [“IP” on page 10](#)
- [“IPX” on page 11](#)
- [“OSPF” on page 11](#)
- [“VRRP” on page 12](#)

RMON

This section describes the RMON bugs fixed in Passport 1000 Series Routing software release 2.1.5.0.

- RMON timestamps are now logged correctly in the RMON log messages and RMON event information. (Q00249556)
- When RMON memsize changes are made after enabling RMON from the CLI for the first time, the following warning message is displayed:

```
WARNING!!! For this change to take effect please disable
rmon, save and reset the device.
```

After a reset, you need to re-enable RMON and re-configure the alarms in accordance to the new memsize.

(Q00283844)

- RMON configurations now load properly across reboots with an ASCII configuration file. (Q00121927)

Miscellaneous

This section describes the miscellaneous bugs fixed in Passport 1000 Series Routing Switch software release 2.1.5.0.

- On a Passport 1000 series routing switch, now only one brouter can be configured on a port. (Q00302834, Q00302840).
- The remote end of an LR Module with GMAC version 3 when used in non-redundant configurations now detects the `port admin down` even if auto-negotiation is turned off. (Q00284391)
- On a Passport 1000 series switch, CDP packets are now properly handled. (Q00411060)
- On a Passport 1000 Series switch without a Real Time clock, the timestamp in the syslog now displays the time since boot correctly. (Q00416804)
- On a Passport 1000 Series switch, when a configuration file containing UDPFWD entries is saved and the switch rebooted, the `fwdId` and `fwdListId` are no longer changed. (Q00084642-01)
- An incorrect network mask and IP address combination is no longer allowed when configuring access policies. (Q00283883)

- The SNMP Non-Unicast Packet-Counter string now returns a correct value. (Q00433702-01)
- Reply messages are now displayed for RADIUS server Accept and Reject cases. (Q00320794)
- Port parameters are now restored across reboots with an ASCII configuration file when the port is locked. (Q00411331)
- NTP update time now takes effect immediately after it has been changed. (Q00472408-01)
- When one of the ports of a MLT is down, the `arp` entry is now updated with another active port of the MLT. (Q00477097)
- A Passport 1200 switch, which is not directly connected to another L3 device (for example, through a hub), no longer logs an error message when the ARP entry corresponding to local next-hop of a static route ages out. In addition, even if the `fdb-aging` timer is the same as the `arp-aging` timer, the ARP entry corresponding to the local next-hop is aged out successfully. (Q00483580)
- The user configured values for `STG Forward Delay` and `MaxAge` are now restored successfully when the switch is booted with an ASCII configuration file. (Q00482386-01)

IP

This section describes the IP bugs fixed in Passport 1000 Series Routing Switch software release 2.1.5.0.

- ARP aging now works properly when IP traffic from the same IP source address is received on two different ports. (Q00030556-01)
- When IP traffic from the same IP source address is received on two ports in different spanning tree groups, the Passport 1000 Series routing switch now properly processes the traffic. (Q00026697-01)
- A change in state of local interface now causes a triggered RIP update. (Q00065979-03)

- On a Passport 1000 Series switch, the port in the default route record is now updated only if the same MAC address is learned over any other port on the same VLAN. (Q00279152-01)
- A Subnet mask of 0 should now be used for creating and deleting the default route. (Q00030843-02)
- The source IP address in the UDP packets sent out of the egress interface of a Passport 1200 now corresponds to the egress interface IP addresses. (Q00170994-03)

IPX

This section describes the IPX bugs fixed in Passport 1000 Series Routing Switch software release 2.1.5.0.

- When IPX encapsulation is changed, it will take effect immediately on the RIP routes. (Q00286957)
- 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. (Q00227898-01)

OSPF

This section describes the OSPF bugs fixed in Passport 1000 Series Routing Switch software release 2.1.5.0.

- 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. (Q00286263-01)
- OSPF area aggregation for LSA Type 7 can no longer be created on the backbone area. (Q00283898)
- External routes announced into NSSA area now have a proper forwarding address. (Q00453203)
- 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. (Q00415202-04)

VRRP

This section describes the VRRP bug fixed in Passport 1000 Series Routing Switch software release 2.1.5.0.

The following error message is now displayed when you preempt the hold-down timer which is not active:

```
Error: vrrpOperTblConsistencyCheck FAILED. Action allowed  
only on VR with active holddown state
```

(Q00287299-02)

Known issues in release 2.1.5.0

The following sections describe known issues with the Passport 1000 Series Routing Switch software release 2.1.5.0, and include the following topics:

- [“Miscellaneous,”](#) next
- [“IPX protocol-based VLANs”](#) on page 14
- [“IP Multicast”](#) on page 15
- [“Unknown MAC discard”](#) on page 15
- [“Large frame support”](#) on page 15
- [“TOS-based priority forwarding”](#) on page 16
- [“Java Device Manager”](#) on page 16

Miscellaneous

The following miscellaneous issues exist in release 2.1.5.0:

- On a Passport 1000 Series switch, when group STP is disabled in the STG in which MLT ports are members, BPDUs are flooded on only one port of the MLT. So if these MLT ports are connected to a non-root bridge with STP enabled in the group, then the ports that do not receive BPDUs will remain in Listening state on the remote switch. (Q00462377)

- 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 session
 - On a windows 95/98/NT4 system running telnet to the switchUse 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 all TX/FX ports, 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.
 - 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)

IPX protocol-based VLANs

If a IP protocol-based VLAN and IPX protocol-based VLAN have a common port as the potential member with traffic ingressing on it, deleting and recreating the IPX protocol based vlan using the same vlan ID may give the following message:

```
[08/02/2002 05:18:29] WARNING: Code=0x0 Task=tCppRxTask:  
vlanProcessFrame: port=6/9 frame's pid=1 does not match  
VLAN's pid=7!
```

If this occurs, the IPX protocol-based VLAN should be deleted and recreated using a unique VLAN ID. (Q00496145)

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 2.1.5.0:

- 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.
- Only 100 Allow-Mac entries are restored across reboots with a binary configuration file. (Q00284650)

Large frame support

The following large frame forwarding support issue exists in release 2.1.5.0:

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 2.1.5.0:

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 2.1.5.0:

- 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.*
- *Release Notes for the Passport 1000 Series Switch Software Release 2.1.4.0*
- *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.