

Part No. 896-00181-F
May 2001

4401 Great America Parkway
Santa Clara, CA 95054

Release Notes for the Passport 1000 Series Switch Software Release 2.1



NORTEL
NETWORKS™

Copyright © 2001 Nortel Networks

All rights reserved. May 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.

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. The software license agreement is included in this document.

Trademarks

NORTEL NETWORKS and LinkSafe are trademarks of Nortel Networks.

Accelar, Bay Networks, and Passport 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 describe the new features for the Nortel Networks™ Passport® 1000 Series software release 2.1, and add to the previously released Accelar® 2.0 documentation.



Note: The Accelar 1000 Series product line is now referred to as the Passport 1000 Series product line beginning with release 2.1. Legacy documents will continue to use the Accelar name. This document refers to the Passport 1000 Series products.

These release notes apply to the following products:

Obsolete product name	New product name
Accelar 1100 chassis	Passport 1100 chassis
Accelar 1150 chassis	Passport 1150 chassis
Accelar 1200 chassis	Passport 1200 chassis

This software release includes updates to the following components:

- Boot Monitor Software Version 2.1 (p10b2100.img)
- Run-Time Software Version 2.1 (p10a2100.img)
- Device Manager Version 5.2 (for Microsoft® Windows® 95, Windows 98, and Windows NT®: jdm_win.exe; for UNIX: jdm_unix.tar.Z)

The VLAN Manager is no longer included with Device Manager. VLAN configuration can be accomplished using Device Manager or the CLI.



Note: Before upgrading your software from version 2.0.3 or earlier, back up your current configuration file. Release 2.1 configuration files contain configuration options that are not compatible with version 2.0.3 or earlier run-time options. Back up the current configuration file before upgrading, in case you must revert to a previous version of the run-time image.

Device Manager (version 5.2) for software release 2.1 supports:

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

To run Device Manager, install the Device Manager 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*.



Note: Version 5.2 of Device Manager displays the following icons. The icons are located at the bottom of the applicable window. Not all icons are available with each action:

- Copy—Ctrl+C
- Paste—Ctrl+V
- Undo—Ctrl+Z
- Export data
- Print table



Passport software release 2.1 enhances the Accelar 2.0 software. These release notes are an addition to the 2.1 software documentation, which is available on the 2.1 Software CD and the Nortel Networks documentation Web site at the www25.nortelnetworks.com/library/tpubs/ URL.

Refer to “[Related publications](#)” on page 18 for more information about obtaining Accelar 2.0 documentation.

For the latest information about the Passport product line, refer to the Passport Products site from the Nortel Networks Web page (www25.nortelnetworks.com/library/tpubs/), or contact Nortel Networks Customer Support by accessing the URL (<http://www.nortelnetworks.com/documentation/>) or calling 1-800-4NORTEL.

These release notes contain the following sections:

- “[Recommendations and information about release 2.1](#)” on page 5
- “[New features in release 2.1](#)” on page 6

- [“Other enhancements” on page 10](#)
- [“New and revised CLI commands” on page 12](#)
- [“Known issues in release 2.1” on page 13](#)
- [“Related publications” on page 18](#)



Note: Many of the new features in release 2.1 require modules and chassis (Passport 11xx/12xx routing switches) to be -B versions or later.



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 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.

Recommendations and information about release 2.1

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

- Nortel Networks recommends using an ASCII configuration file.
- 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 at this time.
- You can now create a maximum of **101** VLANs using software release 2.1; previously, you could create a maximum of 123 VLANs. This number is dependent on the number of MLTs and STGs configured for the Passport Switch.

New features in release 2.1

Release 2.1 of the Passport 1000 Series software includes the following new features:

- RADIUS client support ([page 6](#))
- IP-directed broadcast suppression ([page 7](#))
- IP Static Routing Table Manager([page 7](#))
- VRRP hold down timer ([page 7](#))
- Unknown MAC discard security enhancements ([page 7](#))
- Broadcast SNMP trap receiver ([page 8](#))
- Link flap detection ([page 8](#))
- Port naming ([page 8](#))
- TOS-based high-priority forwarding ([page 8](#))
- Disabling IPX NetBIOS propagation ([page 9](#))
- Large frame support ([page 9](#))
- Autosave of boot parameters ([page 9](#))
- Layer 1 security login ([page 10](#))
- Multicast MAC filtering ([page 10](#))
- OSPF passive ports ([page 10](#))

RADIUS client support

Release 2.1 software provides Remote Authentication Dial In User Service (RADIUS) support, which allows a remote RADIUS server, rather than the Passport switch, to authenticate logins. The RADIUS server also provides access authority. For more information, refer to Chapter 5, “Management and security features,” in *Using the Passport 1000 Series Switch*.

IP-directed broadcast suppression

In Passport software release 2.1, the user can enable or disable directed broadcast traffic forwarding on an IP-interface basis. For more information, refer to Chapter 5, “Management and security features,” in *Using the Passport 1000 Series Switch*.

IP Static Routing Table Manager

The IP Static Routing Table Manager feature allows users to change static routes directly. This new table is separate from the System Routing Table, which the router uses to make forwarding decisions. Although the tables are separate, entries in the Static Routing Table Manager are automatically reflected in the System Routing Table if the next hop address in the static route is reachable and the static route is enabled. For more information, refer to Chapter 5, “IP Routing,” in *Networking Concepts for the Passport 1000 Series Switch*.

VRRP hold down timer

Software release 2.1 adds a timer to delay the preemption of the primary over the secondary, when the primary becomes available. This timer is called the hold down timer, and it has a default value of 0 seconds. Nortel Networks recommends that you set all your routers to the identical number of seconds for the hold down timer. For more information, refer to Chapter 5, “IP Routing,” in *Networking Concepts for the Passport 1000 Series Switch*.

Unknown MAC discard security enhancements

Passport software release 2.1 enhances the unknown MAC discard feature introduced in release 2.0. This security feature for high-security environments restricts access to the network based on the layer 2 media access control (MAC) address of the network devices connected to the Passport switch. This feature is enabled per port. Using unknown MAC discard, any frame originating from or sent to a MAC address that is not known by the Passport switch on that port is a security violation and is dropped. For more information, refer to Chapter 5, “Management and security features,” in *Using the Passport 1000 Series Switch*.

Broadcast SNMP trap receiver

Users can specify a directed broadcast address (for example, 10.10.40.255) as an SNMP trap receiver. For sites where multiple network management stations are located on a single subnet, the Passport 2.1 software sends SNMP trap messages to all network management stations with a single SNMP trap receiver entry. The subnet broadcast is used as the trap receiver address. Users no longer have to specify each network management station on a subnet as a trap receiver. For more information, refer to Chapter 5, “IP Routing,” in *Networking Concepts for the Passport 1000 Series Switch*.

Link flap detection

Link flap detection allows the user to set thresholds for the number and frequency of link state changes allowed on a physical port. The user can then take action if the thresholds are exceeded. If the link state change thresholds are exceeded, a log entry is generated. For more information, refer to Chapter 5, “Management and security features,” in *Using the Passport 1000 Series Switch*.

Port naming

Software release 2.1 supports port naming with strings of up to 20 alphanumeric characters. Named ports are useful for managing networks. Port names can only be saved in ASCII configuration. Use Device Manager to name the ports. For more information, refer to Chapter 3, “Configuring layer 2 switching operations,” in *Getting Started with the Passport 1000 Series Management Software*.

TOS-based high-priority forwarding

With Passport software release 2.1, users can prioritize IP traffic based on the IP TOS (Type of Service) precedence bits within the received IP packet. Use the command line interface (CLI) to enable TOS-based high-priority mode. For more information, refer to Chapter 8, “IP Filtering,” in *Networking Concepts for the Passport 1000 Series Switch*.

Disabling IPX NetBIOS propagation

IPX NetBIOS (type 20) propagation can be disabled globally. That is, on all IPX interfaces in the entire chassis. Use the CLI to enable or disable IPX NetBIOS (type 20) propagation. For more information, refer to *Reference for the Passport 1000 Series Command Line Interface Release 2.1*.

Large frame support

Although the Ethernet maximum frame size is 1514 bytes for nontagged ports and 1518 bytes for tagged ports, the Passport switch can support frame forwarding up to 1750 bytes for 10/100 megabits per second (Mb/s) and Gigabit Ethernet interfaces. Large frame support in Passport software is targeted for specific environments where a data encapsulation scheme is used on Ethernet. This scheme causes the frames to exceed the Ethernet standard frame size. Enabling large frame support as frames ingress a port allows oversized frames to be received from that port. Enabling large frame support is performed on a port-by-port basis and is disabled by default. For more information, refer to Chapter 4, “VLANs,” in *Networking Concepts for the Passport 1000 Series Switch*.

Autosave of boot parameters

In the Passport software release 2.1, changes to the boot configuration in the CLI or Device Manager are automatically saved in NVRAM. Previously, to save changes to boot parameters, users needed to execute a SAVE command in the run-time image, which saved both the boot configuration and the run-time configuration. Although the parameters are now saved automatically, these parameters are read only when the switch is booting. For more information, refer to *Reference for the Passport 1000 Series Command Line Interface Release 2.1*.

In Device Manager, you set the configuration file by choosing Edit > Chassis > Boot.

Layer 1 security login

A layer 1 (L1) security level has been added to device management security. Users with this security privilege can change parameters only at the physical port level while still being able to view most settings. The layer 1 security level complements the existing layer 2 and layer 3 security levels where users can change bridging and routing parameters, respectively. For more information, refer to Chapter 1, “Managing a Passport 1000 Series Switch,” in *Getting Started with the Passport 1000 Series Management Software*.

Multicast MAC filtering

Some network applications rely on a layer 2 multicast MAC mechanism for sending a frame to multiple hosts for processing (for example, mirroring). With Passport software release 2.1, a feature has been added to direct MAC multicast flooding to a specific set of ports. Because this feature is also effective for IP routed traffic, layer 3 functionality is also available. This filtering does not apply to BPDUs.

OSPF passive ports

Within a VLAN, users can enable or disable receiving OSPF traffic on a per port basis. This configuration applies to all VLANs on the configured port. The port continues to generate hello packets. For more information, refer to Chapter 5, “IP Routing,” in *Networking Concepts for the Passport 1000 Series Switch*.

This feature can be enabled and disabled using Device Manager or the CLI.

Other enhancements

This section describes other general and management enhancements included in this release. The enhancements are:

- Configurable login banner ([page 11](#))
- Previous and next history commands ([page 11](#))
- Setting the boot flags ([page 11](#))
- Progress indication during TFTP squeeze, format, and recover ([page 12](#))

- TFTP server enable/disable command ([page 12](#))
- Telnet client enable/disable command ([page 12](#))

Configurable login banner

In release 2.1, you can modify the login banner and the login/password prompts using the CLI. Login banners are most commonly used to post warnings against unauthorized access or to create a generic login/password prompt. The CLI login/password prompts are limited to 20 characters.

Release 2.1 also offers a “Message of the Day” (MOTD) feature. The MOTD typically appears after you log in to a device.



Note: Do not use a question mark (?) in the login banner, login/password prompt, or MOTD.

The login banner and MOTD can contain a total of eight lines, with 80 characters in each line, giving you an allowable limit of 640 characters. Additionally, an empty banner or MOTD is not allowed.

Previous and next history commands

Passport release 2.1 allows you to access the “previous” and “next” history commands using the Up and Down arrow keys. This feature works only on VT100 terminals or emulated-VT100 terminals.

Setting the boot flags

The default setting for the factory default flag is false. In previous software versions, when you booted the switch to factory defaults, the factory default flag remained set to true until you saved the run-time configuration.

With Passport software release 2.1, the factory default flag is automatically set to false when the run-time image is booted.

Progress indication during TFTP squeeze, format, and recover

Commands to `squeeze`, `format`, and `recover` flash devices take 30 seconds or more to complete on the Passport switch. While these commands are executing, a series of dots on the next line are displayed to indicate progress.

As a file is copied to the switch or flash memory, an indicator appears to show that a block of the file was successfully downloaded.

TFTP server enable/disable command

In release 2.1, if you are using the `rwa` login, you can enable or disable the TFTP server on the active Passport Silicon Switch Fabric (SSF). The output from the `show sys info` command displays the status of the TFTP server on the SSF.

Use the `config sys tftp-server <enable/disable>` command to enable or disable the TFTP server on the SSF using the CLI.

Telnet client enable/disable command

Using the `rwa` login, you can enable or disable a Telnet client on an active SSF. Run the `show sys info` command to display the status of the Telnet client on the active SSF.

To enable or disable the Telnet client on the active SSF, use the `config sys telnet-client <enable/disable>` command. To clear a Telnet session, use the `clear telnet <session-id>` command.

New and revised CLI commands

CLI commands that are new in this release or have added functionality are listed in boldface type in Appendix A of the *Reference for the Passport 1000 Series Command Line Interface Release 2.1*, part number 202086-C.

Known issues in release 2.1

The following sections describe known issues with the Passport 1000 software release 2.1.

Miscellaneous

The following miscellaneous issues exist in release 2.1:

- The path to the xterm binary needs to be added to the PATH variable to allow JDM (Java Device Manager) Telnet sessions. (120711-1)
- 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 1514/1518 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)
- 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)

- To initiate a Telnet session from the console use the CLI command **config sys telnet-client enable**. (145983-1)
- Tagged and untagged large frames are getting corrupted (extra bytes are added) passing through the Passport switch 10/100BASE-T ports. This problem occurs with untagged large frames of 1536 bytes to 1596 bytes and tagged frames of 1544 bytes to 1596 bytes. (115806-1)
- 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

To activate the arrow keys, press Ctrl-P and N. (117470-1)

- 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>` (117489-1)
- Progress indicators do not work when copying a file from PCMCIA to flash. (117491-1)
- When using the TOS feature so that a filter record modifies the TOS field, the resulting value cannot be read and used to prioritize based on the TOS threshold. Ingressing packets get examined only one time. (119845-1)
- 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)
- To flush a sender's table in JDM:
 - 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. (137882-1)

- To stop the inconsistency check error messages after rebooting a DUT, do a hard reset. (143294-1)
- If a VLAN is configured for both an IP and an IPX and the IPX VLAN definition is removed, leaving the VLAN as only an IP, the IP address for that VLAN does not respond to ping. (145508-1)
- The enable log stats function is not saved after rebooting the Passport switch. (147831-1)
- When upgrading NVRAM, the Telnet and FTP default configurations are disabled. These configurations should be enabled by default. (147864-1)

IP Multicast



Caution: Nortel Networks does not recommend or support IP Multicast with IGMP or DVMRP on the Passport 1000 platform.

The following IP Multicast issues exist in release 2.1:

- Multicast traffic may not be received if a single box has a DVMRP interface and a snoop VLAN interface. This problem is referred to as the ACB Index limitation. (145283-1)
- The user cannot change the IGMP version. (104591-1)
- MCAST data is not forwarded to a client on a snoop VLAN from a server that is on a DVMRP VLAN. To enable the client to receive MCAST data, change the snoop VLAN to a DVMRP VLAN. (135954-1)
- You cannot have two valid ingress interfaces for a particular multicast stream. That is, a user should not configure a switch in such a way that the same MCAST stream is sent to the switch using two interfaces. (136038-1)
- Layer 2 edge switch with IGMP snoop enabled remains unaware of multicast ingress link failure in the designated forwarder, which is also the querier switch. (143767-1)
- For IGMP snooping, if creating a static entry and marking the port as “not allowed to join,” the port is shown as a receiver on the receiver list even though the port is not a receiver. This port is blocked statically and will not receive MCAST data. (120883-1)
- Disabling DVMRP on a nondesignate router will cause problems for multicast traffic. Nortel Networks recommends that DVMRP remain enabled on VLANs spanning multiple switches. (108529-1)
- MCAST cannot be supported on an IP protocol-based VLAN. The hardware protocol VLAN record does not contain multicast flag information, and the hardware cannot identify the VLAN ID for an MCAST packet injected to the VLAN. (133669-1)
- When the server moves from one port to another across the same VLAN, the multicast traffic should resume. Currently, the multicast stream must be restarted at the server side for the traffic to resume. (135132-1)

- An mrouter duplication problem is causing large amounts of MCAST packets to go to every port on the same switch. To avoid this problem, customers cannot have redundancy in their edge for MCAST traffic if they have tagged ports in their snoop VLAN. (143820-1)
- Snoop VLAN does not forward all MCAST data to clients when MCAST data is sent to a VLAN through a port other than the querier port. (143977-1)
- Multicast traffic on the third DUT in an extended VLAN is not seen. (145283-1)
- Under certain circumstances, multicast group records are not updated for the current DVMRP routes, causing traffic to be dropped. (118794-1)

OSPF passive ports

The following OSPF passive port issue exists in release 2.1:

- When disabling OSPF on a port, making the port an OSPF passive port, the setting is saved only in ASCII format, not in the binary configuration.

VRRP

The following VRRP issue exists in release 2.1:

- VRRP allows a user to configure a priority of 255 without displaying an error message. (147877-1)

Unknown MAC discard

The following unknown MAC discard issues exist in release 2.1:

- 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:

- 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 portsThe gigabit ports do not have this problem. (126418-1)

TOS-based priority forwarding

The following TOS-based high-priority forwarding issue exists in release 2.1:

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

Java Device Manager

The following JDM issues exist in release 2.1:

- 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>]` .
- In JDM, when selecting multiple ports using Ctrl+Click, the ports must be in the same category (or java class). If you select a 10/100 port, you cannot also select a gigabyte port. A 10/100 Mb/s Ethernet port and a Gigabyte Ethernet port are different port types. That is, they are each a different Java class.

Use the following JDM workaround to select multiple ports of different types:

- Select the 10/100 Mb/s Ethernet ports you want to edit or graph.
- Select the Gigabyte Ethernet ports you want to edit or graph.

The JDM screens and dialog boxes will be displayed so you can view side-by-side comparisons. (139953-1)

- The IPX route table from JDM 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)
- In JDM, User Set Time does not display the system time and, when filled out and applied, does not apply the specified system time. System time must be observed and set from the CLI. (Q00019754)

Related publications

For additional information, refer to the following Passport 2.1 documentation available on the Nortel Networks Customer Service Documentation Web page (www25.nortelnetworks.com/library/tpubs/):

- *Reference for the Passport 1000 Series Management Software Switching Operations Release 2.1* (part number 211192-A)
- *Reference for the Passport 1000 Series Management Software Routing Operations Release 2.1* (part number 211193-A)
- 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 Passport 1000 Series Switch Software Release 2.0* (part number 896-00181-E)
- *Using the Passport 1000 Series Switch* (part number 212154-A)

Refer also to the following documents on the Accelar documentation CD:

- Networking Concepts for the Accelar Series 1000 Routing Switch Software Release 2.0 (part number 205588-B)
- *Reference for the Accelar 1000 Series Command Line Interface 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)
- *Upgrading to Accelar 2.0 Software* (part number 206077-A)