Part No. 206494-N
July 2000

4401 Great America Parkway
Santa Clara, CA 95054

Addendum to the 2.0 Software Release Notes for Passport 1000 Series Products Release 2.0.7.2

NORTEL NETWORKS™

Copyright © 2000 Nortel Networks

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.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Passport, LinkSafe, and Nortel Networks are trademarks of Nortel Networks.

Accelar 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.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA 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

This release note addendum for Passport™ 1000 Series routing switch software release 2.0.7.2 describes the enhancements and bug fixes to the Passport 1000 Series routing switch software that have been implemented in release 2.0.7.2. This document is an addendum to the *Release Notes for the Accelar 1000 Series Products Software Release 2.0* (part number 896-00181-E). The 2.0 release notes and addendums are available on the 2.0 Software CD and on the Nortel Networks™ Customer Service Documentation Web page (*http://support.baynetworks.com/library/tpubs/nav/rtswitch/accelar.htm*).

Note: To consolidate and leverage marketing investments, simplify brand promise and reach customers again and again with a simple message - Nortel Networks will transition the Accelar family of products into the Passport brand. All product model numbers will remain the same.

The Passport 1000 Series products were formerly called the Accelar 1000 Series products. This software release is compatible with all previously released Accelar 1000 Series switch modules, as well as current Passport 1000 Series modules.

Software release 2.0.7.2 includes updates to the run-time software only. The latest software components are:

- Run-Time Software Version 2.0.7.2 (p10a2072.img)
- Boot Monitor Software Version 2.0.5 (ac10b205.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 2.0.7.2 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.

Note: Boot Monitor Software Version 2.0.5 is equivalent to Boot Monitor Software Version 2.0.1. Existing configurations with Boot Monitor Software Version 2.0.1 can continue to use this boot monitor with the Run-Time Software Version 2.0.7.2. Configurations with boot monitor software versions prior to 2.0.1 must upgrade to Boot Monitor Software Version 2.0.5.

For the latest information about software issues, always refer to the Passport Products site from the Nortel Networks Web page (*www.nortelnetworks.com*) or contact Nortel Networks Customer Support at 1-800-2LANWAN.

This addendum includes the following sections:

Note: Many of the new features in release 2.0 and above require modules and chassis (Accelar 1100/1150 routing switches) to be -B versions or above with ASICs that are ARU3 or above. Hardware with ARU1 or ARU2 ASICs does not support these features.

Warning: Software release 2.0.7.2 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 routing 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 information about release 2.0.7.2

Note the following recommendations and miscellaneous information about Passport 1000 Series routing switch software release 2.0.7.2:

- Passport 1000 Series routing switch software release 2.0.7.2 does not support global filters. Configuration information relating to global filters is ignored on boot-up when you use software release 2.0.7.2. Upon booting up with software version 2.0.7.2, the following message appears on the screen:

  ```
  Global filters are not supported in this release.
  ```

  If you attempt to configure global filters using software version 2.0.7.2, the following error message appears on the screen:

  ```
  Operation not allowed.
  ```

- DVMRP support requires chassis and modules that are -B versions. The -A version chassis and modules do support IGMP snooping.
- When you create a Multi-Link Trunking (MLT) group, the resulting MLT is put into the default VLAN (VLAN 1). The MLT should then be assigned to other VLANs as appropriate.

- The new XLR1298SF SSF module has 32 megabytes (MB) of dynamic random access memory (DRAM). Release 2.0.7.2 requires 32 MB of DRAM, so you must upgrade your XLR1297SF module to increase memory. If you do not have 32 MB of DRAM, an error message appears on boot-up. A memory upgrade kit (AA0011017) is available for the XLR1297SF module to increase DRAM to 32 MB.
- Always set a specific Enforce Operational Configuration (EOC) mode (refer to the Passport 1000 Series routing 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 command line interface (CLI) so that “trunk” is used only in reference to Multi-Link 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)
- VRRP running over IEEE 802.1Q tagged ports requires ARU3 modules (-B hardware). (115732-1, 130826-1)

Multicast limitations in release 2.0.7.2

DVMRP in the 2.0.7.2 release has known issues when running with other features such as OSPF and VRRP. These issues may cause high CPU utilization in meshed networks. The resulting high CPU utilization can cause general operational issues with the routing switch.

The ARU3 ASICs (-B version modules and chassis) introduced the ability to replicate a multicast stream over a tagged port by generating one copy for each VLAN that requires receipt of the multicast stream. This feature also works when deployed over an MLT link.

The above feature is limited to -B version modules and chassis; therefore, using this feature may affect the suitability of -A modules and chassis when deploying a multicast-enabled network.

Note: DVMRP is not supported on ARU2/QUID4 Enforce Operational Configuration (EOC) mode. ARU2/QUID4 mode is considered suitable for IGMP snooping and proxy operation.

An additional consideration is that, because some IP multicast MAC addresses share the MAC address used by the reserved range of 224.0.0.x, IP multicast sessions with destination MAC 01-00-5E-00-00-xx are not processed and are flooded in the VLAN. The affected address ranges are 225 to 239.0.0.x and 224 to 239.128.0.x (108919, 108920). Whenever possible, configure IP multicast applications to not use these address ranges.

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 routing 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 many VLANs. Remember that MAC broadcasts are flooded out all ports on 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 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 BPDUs are generated.

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

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

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

```
config ethernet <ports> stp <sid> <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 routing switch operates in either of two modes: Best Effort 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 issue 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.

Disabling IPX NetBIOS propagation

With the release of Passport 1000 Series routing 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.

Configuring

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 `config ipx set info`.

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 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 routing switch-1200#

Passport 1000 Series routing switch-1200# format fl

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

When you press any key, the following text appears 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 routing switch-1200#



Passport 1000 Series routing switch-1200#

Passport 1000 Series routing switch-1200# format fl

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

When you press any key, the following text appears 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 routing 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>
  ```

  ```
  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).

Bugs fixed in release 2.0.7.2

The following sections list bugs that were fixed in Passport 1000 Series routing switch software release 2.0.7.2.

Miscellaneous

The following miscellaneous bugs were fixed in the Passport 1000 Series routing switch software release 2.0.7.2:

- The Passport 1000 Series routing switch flash file system no longer reports negative free space. (96872-1)
- If an MLT group has STP set to false and a port that has STP set to true is added to the MLT group, the port no longer keeps STP set to true. (98949-1)
- The counters for Frame Too Short, Alignment Error, FCS, and Runt Errors now increment correctly on Passport 1216TF modules. (102833-1)
- You can now add the same port to two user-defined protocol-based VLANs configured on a Passport 1000 Series routing switch using either Device Manager or the CLI, after the VLANs have been created. (105043-1)
- Ports of newly inserted boards will no longer belong to VLANs other than the default VLAN. (116312-1)
- An internal loopback test is now possible to run on a port that is part of an MLT. (120931-1)
- The port configuration in the `show config` command now shows the correct STG (Spanning Tree Group) number. Previously, it displayed the highest STG number configured on the device.(120934-1)
- The CLI command `config Ethernet IP Traffic-filter` will now properly recognize “DIS” as abbreviated action for “Disable.” (121149-1)
- MLT groups that are members of an SRC-MAC VLAN can now be changed from *tagged* to *access*. (121152-1)
- CLI and Telnet sessions will now show a more accurate port utilization. (126028-1)

- The Passport 1000 Series routing switch now has an option to configure the time period over which the CPU utilization is averaged. The default is 1 second. (124648-1)

  To configure the option, use the command:

  ```
  config sys set cpu-util-average <seconds>
  ```

  To view the current setting, use the following command:

  ```
  show sys set cpu-util-average
  ```

- Tagging now functions properly on IRPs (Isolated Routing Ports) after a hot-swap of the I/O module. (125729-1)
- When modifying a nonexistent port, the error message that is returned no longer has incorrect spelling. (126851-1)
- When using a Telnet session to transfer very large files from the secondary SSF to the primary SSF, the session no longer times out. The problem was fixed by changing the TFTP time-out from 1 to 4 minutes. (123725-1)
- For formatting a device, an additional confirmation step was added to prevent the accidental deletion of files. (97918-1)
- Parameter information is now saved when ports are added to a newly created spanning tree group (STG). The port level spanning tree parameters such as the STP state, Fast Start state, or path cost are modified when saved to NVRAM. (114362-1)
- When Trap receivers are configured with broadcast addresses, some additional IP address checking for illegal addresses such as 0.x.x.x, 127.x.x.x, and some well-known multicast addresses has been added. (95212-1)
- The Web server passwords for all permission levels could be seen using the `show web-server` command for a CLI or Telnet session with Read Only (RO) permissions. This will now require Read Write Access (RWA) permission.(106197-1)
- MLT ports in a blocking state no longer trigger ARU events. This change avoids unnecessary CPU utilization.(120671-1)
- The TRAPD process no longer keeps other processes from running after running out of frame buffers.(129271-1)

CLI

The following CLI bugs were fixed in Passport 1000 Series routing switch software release 2.0.7.2:

- After deleting a file and running the `squeeze flash` command, the content of the log file could not be seen with the `show log file` command. (121646-1)
- Telnet CLI sessions no longer fail to respond when an access policy is configured on the switch and the policy is displayed using the `show sys access-policy info` command. (123334-1)
- The command `config ip ospf interface info` no longer displays garbage characters after the authentication key. (120869-1)
- The router port's broadcast address can now be seen by using the `show port info` CLI command. (82430-1)

IP

The following IP bugs were fixed in Passport 1000 Series routing switch software release 2.0.7.2:

- A static route or a default route no longer becomes inactive when there is a dynamically learned route that is less specific (than the local route covering the next hop of that static route or default route) and the dynamically learned route goes away. (125581-1)
- A static route or default route no longer points at the wrong next hop when there is a route that is less specific in the routing table pointing at a different next hop. (125968-1)
- The Passport 1000 Series routing switch now correctly handles two or more filters with the same destination and source IP address mask. (120551-1, 125995-1)
- A change in state of a local interface now causes a triggered RIP update. (123090-1)
- Static routes no longer take preference over local routes after rebooting the Passport 1000 Series routing switch. (123174-1)
- IP static routes marked as inactive in the routing table can now be deleted from the table. (123183-1)

- IP policies created using an ASCII configuration file no longer become corrupt after they have been edited with Device Manager and saved to NVRAM. (120551-1)
- The ARP process has been optimized to reduce CPU load. When there is an outstanding ARP request, traffic for the unresolved IP destination is handled in the I/O module and no longer requires CPU interaction. (125502-1)

  This functionality is enabled by default.

  To disable this functionality, use the following CLI command:

  ```
  conf ip arp hwarpdiscard <disable>
  ```

Note: It is important to save the configuration and reboot the switch to assure that the hardware tables are properly reinitialized.

OSPF

The following OSPF bugs were fixed in the Passport 1000 Series routing switch software release 2.0.7.2:

- When a RIP learned route on an Autonomous System Boundary router (ASBR) disappears and an alternative route is available through another ASBR, the switch no longer fails to populate the routing table when the total cost of the alternative route is greater than or equal to 16. (125302-1)
- Changes to the OSPF announce policy, Netlist, are now dynamically applied. (106783-1)
- OSPF redundant ABRs will no longer learn the same summary-link LSAs for each other. (110040-1)
- Disabling OSPF on a VLAN will no longer disable OSPF on a tagged port if that port belongs to other VLANs with OSPF still enabled. (115412-1)
- The ASCII configuration file now shows the correct value of the cost of the OSPF host route. (119683-1)
- Auto virtual links are no longer saved in the ASCII configuration files. (120356-1)

IP Multicast

The following IP Multicast bug was fixed in the Passport 1000 Series routing switch software release 2.0.7.2:

- Source groups are now properly tracked, assuring that correct source groups are removed when becoming inactive.

IPX

The following IPX bugs were fixed in the Passport 1000 Series routing switch software release 2.0.7.2:

- The Passport 1000 Series routing switch now has the option to populate the routing table with the received hop count rather than to increment the hop count first.(113909-1)

  To enable or disable the hop count, increment use the following command:

  ```
  config ipx set learnafterincrement <enable|disable>
  ```

  The default is enabled.

  To view the current value, use the following commands:

  ```
  show config
  ```

  or

  ```
  config ipx set info
  ```

- Entering the same IPX static route on two separate port-based VLANs no longer causes the route to disappear. (107134-2)
- The IPX SAP table is now updated when the advertising host changes for the same service. (121232-1)

- The Passport 1000 Series routing switch can be configured to respond to GNS requests alphabetically or in a round-robin manner. For round-robin, the device responds with the SAP that is least used. (114741-1)

  To configure the SAP GNS response, use the following command:

  ```
  config ipx sap sapgnstiebreaker <alphabetical or
  round-robin>
  ```

  To show the current setting use the following command:

  ```
  show config
  ```

- IPX routing no longer fails on IPX protocol-based VLANs after reset. (117575-1)

VRRP

The following VRRP bugs were fixed in the Passport 1000 Series routing switch software release 2.0.7.2

- Removing the VRRP backup interface did not change the state to initializing. The status stayed as backup. (108266-1, 122485-1)

  The VRRP master IP address field displayed the wrong value when the VRRP state transitioned to backup as a result of the critical IP being down. VRRP continued to display it's own IP address instead of the master IP address. The field also displayed the previous IP address when the VRRP state transitioned to initialize from either master or backup.

  This problem is fixed by displaying the correct master IP address when the VRRP state transitions to backup because the critical IP address is down and by displaying 0.0.0.0 in the master IP address field when the VRRP state transitions to initialize. (122932-1)

- The command `show port stat vrrp extended` no longer displays the error message "...Invalid get option...". (127611-1)
- When the link on a VRRP port is lost, the state of the port transitions from backup to initialize and returns to backup when the link is restored. The VRRP Master Timer is now reset to zero. (124184-1)

Known issues

The following sections list known issues in the Passport 1000 Series routing switch software release 2.0.7.2.

Miscellaneous

The following miscellaneous known issues exist in the Passport 1000 Series routing switch software release 2.0.7.2:

- Some resources are reserved when using software release 2.0.x in QUID5/ARU3 mode. As a consequence, this configuration supports a maximum of 100 VLANs where software release 1.3.x supports up to 124 VLANs.

  In both cases (software versions 1.3.x and 2.0.x), the maximum VLAN number is reduced by the number of STG groups (1 per STG group) and MLT links (4 per MLT link). Using software version 1.3.x, the maximum VLAN number is further reduced by the number of IGMP snoop groups (1 per group).
- The rcStatBridgeOutBroadcastFrames counter is not supported. (113124)
- Disabling OSPF on a VLAN may cause OSPF to be disabled on a tagged port if there are other VLANs with OSPF still enabled. To recover from this situation, reenable OSPF on the tagged port.
- When heavily oversubscribed, the 2-port Passport 1000 Series routing switch Gigabit Ethernet module may experience intermittent connectivity loss. To avoid this issue, distribute traffic over multiple Passport 1000 Series routing switch Gigabit Ethernet modules.
- SNA-802.2 protocol-based VLANs do not support DSAP/SSAP values other than 0x04. (118821-1)

IP

The following known IP issue exists in the Passport 1000 Series routing switch software release 2.0.7.2:

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

VRRP

The following known VRRP issue exists in the Passport 1000 Series routing switch software release 2.0.7.2:

- ICMP support for the VRRP virtual IP address is limited. Future releases of software will allow you to disable this functionality to avoid problems with fragmentation (108271-1), traceroute (109230-1), and access to own virtual address (122482-1).

Multicast

The following known multicast issues exist in the Passport 1000 Series routing switch software release 2.0.7.2:

- IGMP snooping may forward multicast data to the wrong VLAN in a situation when multiple snoop VLANs exist and a multicast data stream first ingresses a snoop VLAN that does not have the lowest VLAN ID. The multicast data gets forwarded to the receiver's VLAN with the lowest VLAN ID. (109720)
- When ports are moved between VLANs, the multicast data stream for the moved port may be dropped. (109721)
- If there are multiple snoop-enabled VLANs and the VLAN that a multicast stream first ingressed gets disabled and then reenabled, that VLAN may never learn the sender(s). (109822)
- Using DVMRP, senders are aged out at 5-minute intervals rather than aged out dynamically. This situation may cause a periodic interruption of multicast sessions. (110522)

- When you use IGMP snooping and a querier moves from an active multicast router port to a statically configured port, the old querier port may be left in an active multicast router state after the move. The workaround is to disable and then reenable IGMP snooping on the VLAN. (109510)
- ARP entries can be removed from the ARP table after the multicast stream is started on a given port. This situation may cause a loss of subsequent unicast traffic. (110042)
- You cannot add a static multicast receiver after inserting a multicast access filter for the same multicast group. (97499)

Related publications

For additional information about the Passport 1000 Series routing switch products, refer to the documents found at *http://support.baynetworks.com/library/tpubs/nav/rtswitch/* on the World Wide Web.