Part No. 206494-J
January 2000

4401 Great America Parkway
Santa Clara, CA 95054

Addendum to the Release Notes for the 2.0 Software Release for Accelar 1000 Series Products

Software Release 2.0.5.6

206494-J

NORTEL NETWORKS™

Introduction

This release note addendum for Accelar™ software release 2.0.5.6 describes the enhancements and bug fixes to the Accelar software that have been implemented in release 2.0.5.6. 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*).

Software release 2.0.5.6 includes updates to the run-time software only. The latest software components are:

- Run-Time Software Version 2.0.5.6 (ac1a2056.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: 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 2.0.5. Configurations with boot monitor software versions prior to 2.0.1 must upgrade to Boot Monitor Software Version 2.0.5.

Note: Before upgrading your software from either version 2.0.4 or earlier, back up your current configuration file. Version 2.0.5.6 configuration files contain configuration options that are not compatible with version 2.0.4 or earlier run-time options. It is important to back up the current configuration file before upgrading, in case you must revert to a previous version of the run-time image.

For the latest information about software issues, always refer to the Accelar 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 2.0.5.6 requires 32 MB of DRAM. If you do not have 32 MB of DRAM, an error message appears when you boot up the Accelar switch.
The memory upgrade kit (AA0011017) is available for the XLR1297SF module and increases DRAM to 32 MB. If your Accelar 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 2.0.5.6

Note the following recommendations and miscellaneous information about Accelar software release 2.0.5.6:

- Accelar software release 2.0.5.6 does not support global filters. Configuration information relating to global filters is ignored on boot-up when you use software release 2.0.5.6. Upon booting up with software version 2.0.5.6, 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 2.0.5.6, 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 2.0.5.6 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 enforced operational configuration (eoc) mode (refer to the Accelar 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 as 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)

Multicast Limitations in Release 2.0.5.6

DVMRP in the 2.0.5.6 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 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 range is 225-239.0.0.x and 224-239.128.0.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 an Accelar 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 (Spanning Tree Groups) > Configuration. To configure STP on a port with Device Manager, choose the port and the Spanning Tree tab.

High-Priority Switching

The Accelar 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.

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 sets flags highpriomode true
```

Bugs Fixed in Release 2.0.5.6

The following sections list bugs that were fixed in Accelar software release 2.0.5.6:

- Enforce operational configuration (eoc) mode for ARU2 also supports ARU2/QUID2 hardware combinations. (107667)
- The Accelar routing switch properly handles situations where IP traffic from the same IP source address is received on two different ports and one of those ports goes down. (117515)
- IP packets that are received on two different ports with the VRRP MAC address as destination are properly handled and do not go to the CPU unnecessarily. (117777)

Known Issues

The following sections list known issues in Accelar software release 2.0.5.6.

General

The following known general issues are in Accelar software release 2.0.5.6:

- Some resources are reserved when using software release 2.0.x in QUID5/ARU3 mode. As a consequence, this configuration will support 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 1.3.1, the maximum VLAN number is further reduced by the number of IGMP-snoop groups (1 per group).
- SNMP may fail after receiving an invalid SNMP get request. (111019) Once this failure occurs, SNMP does not recover.
- The ipForwDatagrams counter returns invalid data (decrementing number) when queried on a switch with IP forwarding disabled. (111336)
- 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 you use more than a single destination filter to a host address, destination filters added after the first one fail; only the first applied filter functions correctly.
- When heavily oversubscribed, the 2-port Accelar Gigabit Ethernet module may experience intermittent connectivity loss.

  To avoid this issue, distribute traffic over multiple Accelar Gigabit Ethernet modules.

Multicast

The following known multicast issues are in Accelar software release 2.0.5.6:

- 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)
- Software currently limits the combined number of multicast senders and receivers to a total of 400. (109932, 108438)
- When using 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)
- Deleting a VLAN does not remove IGMP access filters. (97500)

IPX

The following known IPX issue is in Accelar software release 2.0.5.6:

- When multiple encapsulation types are configured on links between Accelar routing switches with IPX routing enabled, CPU intervention may be required to forward traffic, depending on the encapsulation type through which the routes are learned. (112681) This situation can cause high CPU utilization and affect performance.

  The workaround is not to configure multiple encapsulation types on those links.

Related Publications

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