

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

## **Software Release 2.0.4**

4401 Great America Parkway  
Santa Clara, CA 95054

8 Federal Street  
Billerica, MA 01821

Part No. 206494-D  
August 1999

**NORTEL**  
NETWORKS™



\* 2 0 6 4 9 4 - D \*

## **Copyright © 1999 Nortel Networks**

All rights reserved. Printed in the USA. August 1999.

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.

Bay Networks is a registered trademark, and Accelar, BayStack, LinkSafe, and Nortel Networks are 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 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 Accelar™ software release 2.0.4 describes the enhancements and bug fixes to the Accelar software that have been implemented in release 2.0.4. This document is an addendum to the *Release Notes for the Accelar 1000 Series Products Software Release 2.0* (Bay Networks® 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 2.0.4 includes updates to the run-time software only. The latest software components are:

- Run-Time Software Version 2.0.4 (acc2.0.4)
- Boot Monitor Software Version 2.0.1 (accboot2.0.1) supplied as a Boot Monitor Updater
- Device Manager Version 2.0.2 (for Microsoft® Windows® 95 or Windows 98 and Windows NT®: dm\_202.exe; for UNIX: dm\_2.0.2.tar.Z)
- VLAN Manager Version 2.0.2 (for Windows 95 or Windows 98 and Windows NT: dm\_202.exe; for UNIX: dm\_2.0.2.tar.Z)



**Note:** Before upgrading your software from either version 2.0.3 or earlier, back up your current configuration file. Version 2.0.4 configuration files contain configuration options that are not compatible with version 2.0.3 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 instructions to download the software, refer to *Upgrading to Accelar 2.0 Software* (Bay Networks part number 206077-A) found on the documentation CD and on the Nortel Networks Customer Service Documentation Web page.

---



**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. For details, refer to Accelar 2.0 documentation.

---

For the latest information about software issues, always refer to the Accelar Products site from the Nortel Networks™ Web page ([www.nortelnetworks.com](http://www.nortelnetworks.com)) or contact Nortel Networks Customer Support at 1-800-2LANWAN.

This addendum includes the following sections:

- [Recommendations and Information About Release 2.0.4](#) (this page)
- [Hardware Multicast Limitations in Release 2.0.4](#) (page 3)
- [New Features in Release 2.0.4](#) (page 3)
- [Bugs Fixed in Release 2.0.4](#) (page 18)
- [Known Issues in Release 2.0.4](#) (page 20)
- [Related Publications](#) (page 21)

## Recommendations and Information About Release 2.0.4

Note the following recommendations and miscellaneous information about Accelar software release 2.0.4:

- The new XLR1298SF SSF module has 32 megabytes (MB) of dynamic random access memory (DRAM). Although release 2.0.4 does not require 32 MB of DRAM, if you will be using RMON or are in a large OSPF routing environment and your switch SSF module is an XLR1297SF module with only 16 MB of DRAM, you should upgrade your SSF module to increase memory size to improve performance. A memory upgrade kit (AA0011017) is available for the XLR1297SF module to increase DRAM to 32 MB.
- When loaded on an XLR1297SF module with 16 MB of DRAM, IPX maximum RIP routes and maximum SAP entries are set to minimum values (RIP 128; SAP 64) to conserve memory. If you are using IPX and require more IPX RIP routes or SAP entries, the values for IPX maximum RIP routes and maximum SAP entries can be reset by using the following CLI commands:
  - **config ipx set max-route <value>**
  - **config ipx set max-sap <value>**

After resetting the parameters, save the configuration and reboot the switch.

- 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.

## Hardware Multicast Limitations in Release 2.0.4

The ARU3 ASICs (-B version modules and chassis) introduced the capability 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.

This 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.

## New Features in Release 2.0.4

The following section explains the new features and provides configuration information. Release 2.0.4 of the Accelar Management Software includes the following new features:

- [Unknown MAC Discard \(page 4\)](#)
- [Broadcast SNMP Trap Receiver \(page 17\)](#)
- [OSPF Passive Ports \(page 17\)](#)
- [Disabling IPX NetBIOS Propagation \(page 18\)](#)

## Unknown MAC Discard

Accelar software release 2.0.4 enhances the Unknown MAC Discard feature introduced in version 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 Accelar routing switch. This feature is enabled per port. The idea of Unknown MAC Discard is that any frame originating from or destined to a MAC address that is not known by the Accelar routing switch on that port is a security violation and can be dropped.

Using Accelar software version 2.0.4, you can create a table of MAC addresses that are allowed access to the specified port. So a MAC address is “known” and is forwarded normally if it has been defined in the allowed MAC table or if there is a static VLAN Forwarding Database (fdb) entry for the MAC address.

An allowed MAC table is created for each port and applies to all VLANs associated with the port. The table defines which MAC addresses are allowed on the port, in addition to any static MAC entries; this is a separate table than the VLAN forwarding databases. Because each port has an allowed MAC table, the same MAC address can be allowed on multiple ports. This situation contrasts to a VLAN fdb, in which a given MAC address can exist on only one port for a given VLAN.

Entries are added to the allowed MAC table either manually or using AutoLearn, which is in either One-Shot AutoLearn mode or Continuous AutoLearn mode. An additional feature is the Lock AutoLearn MACs setting. These settings are described as follows:

- **Manual**—A user can manually enter a MAC address into the allowed MAC table for a given port. Manual entries in the allowed MAC table are saved in the configuration file; thus all manual entries are saved and restored across system reboots.

- 
- One-Shot AutoLearn—In this mode, the user specifies the number of first-learned MAC addresses to allow access on that port, and the switch adds addresses into the allowed MAC table. The allowed MAC table continues to grow because entries are never aged out; in this mode, the entries remain until the user clears the table. To clear the autolearned entries, refer to the configuration instructions following this section.



**Note:** When in One-Shot AutoLearn mode, the MAC addresses in the allowed MAC table are not saved and restored across resets unless both Unknown MAC Discard and the Lock AutoLearn mode parameters are enabled.

---

- Continuous AutoLearn—In this mode, the routing switch adds new MAC addresses into the allowed MAC table. Using Continuous AutoLearn, the user specifies the number of most recently learned MACs to allow access on that port. However, the entries in the allowed MAC table are aged out as the entries in the underlying VLAN fdb's age out. To manually clear the autolearned entries, refer to the configuration instructions following this section.



**Note:** When in Continuous AutoLearn mode, the MAC addresses in the allowed MAC table are not saved and restored across resets unless both Unknown MAC Discard and the Lock AutoLearn mode parameters are enabled.

---

- Lock AutoLearn MACs—The Lock AutoLearn MACs setting fixes the allowed MAC table to its current state for the port. No new MAC addresses will be allowed even if an AutoLearn mode (either One-Shot AutoLearn or Continuous AutoLearn) is enabled.



**Note:** The Lock AutoLearn MACs feature should be enabled after the allowed MAC table reaches a steady state of one or more MAC addresses. When enforced, no new MAC addresses are allowed.

---

When Lock AutoLearn MACs is enabled, the allowed MAC table can be saved in the configuration file; thus all entries using AutoLearn are saved and restored across system reboots. (Refer to the [“Routing and Unknown MAC Discard Feature”](#) section for a discussion of the feature limitations.)

Unknown MAC Discard is fundamentally a security feature. If a MAC address other than an allowed MAC address attempts to send traffic through the routing switch, that is considered a violation.

The three configurable actions that the switch performs when triggered by a MAC violation on a port are to log the violation, to send a trap, and to administratively down the port:

- **MAC violation logging**—When there is a MAC violation, the switch can be configured to create a system log entry.

A MAC violation log entry looks like the following:

```
24: [07/22/1999 20:08:29] WARNING: Code=0x0 Task=tCppRxTask: An intrusion MAC address:00:00:6f:21:00:00 at port 3/2
26: [07/22/1999 20:08:30] INFO: Code=0x0 Task=tCppRxTask: Link Down(3/2)
27: [07/22/1999 20:08:30] WARNING: Code=0x0 Task=tCppRxTask: An intrusion MAC address:00:00:6f:21:00:01 at port 3/2
29: [07/22/1999 20:08:31] WARNING: Code=0x0 Task=tCppRxTask: An intrusion MAC address:00:00:6f:21:00:02 at port 3/2
31: [07/22/1999 20:08:32] WARNING: Code=0x0 Task=tCppRxTask: An intrusion MAC address:00:00:6f:21:00:03 at port 3/2
```

The log entry includes the date and time of the violation, the port at which the violation occurred, and the disallowed MAC address.

- **MAC violation SNMP trap**—When there is a MAC violation, the switch can be configured to send an SNMP trap. The trap sent by the switch is the Nortel Networks enterprise trap rcMacViolation.

- Administratively downing the port—When there is a MAC violation, the switch can be configured to administratively down (AdminDown) the port. By downing the port, *all* devices including the offending device will be denied access on that port. This action is particularly useful in high-security environments where intrusions from unknown machines cannot be tolerated. The port will remain in the AdminDown state until it is manually brought into an AdminUp state by the administrator or during a system reboot.



**Note:** The maximum number of allowed MAC addresses the system can track is 1000. The maximum number of entries that can be saved in the binary configuration is 100. If more than 100 MAC entries must be stored in a configuration, an ASCII configuration file can be used.

If you exceed 1000 MAC addresses while using Continuous AutoLearn, you receive the nonstop log and console note: “WARNING: All Mac Address table is full. Can’t learn Mac xx:xx:xx:xx:xx:xx!” This may impact SNMP and CPU performance and overflow the log file on flash memory.

---

## Routing and Unknown MAC Discard Feature

For IP routed traffic, the Accelar routing switch is always effective in blocking traffic destined to an unknown MAC address and can generally block traffic sent from an unknown MAC address.

The routing switch can always block traffic destined to a MAC address for which there is:

- No static ARP entry
- No entry in the allowed MAC table
- and*
- No static entry in the VLAN fdb

When the routing switch needs to route a frame to an unknown MAC address, it will send an ARP request for the MAC address of the end station. If the MAC address that replies to the ARP request meets *all* of these three criteria (no static ARP entry, no entry in the allowed MAC table, *and* no static entry in the VLAN fdb), the router ignores the ARP reply and sends an ICMP unreachable message back to the originating device.

To block routed traffic from an unknown MAC address, the routing switch ignores ARP requests originating from unknown MAC addresses. In general, this procedure prevents the station from effectively sending routed traffic. Note that any return traffic will be effectively blocked given that the above condition is true.



**Note:** If security is a primary concern, Nortel Networks recommends that Unknown MAC Discard be configured to administratively down the port on any routed VLANs when a MAC violation occurs.

---

## Configuring Using Device Manager

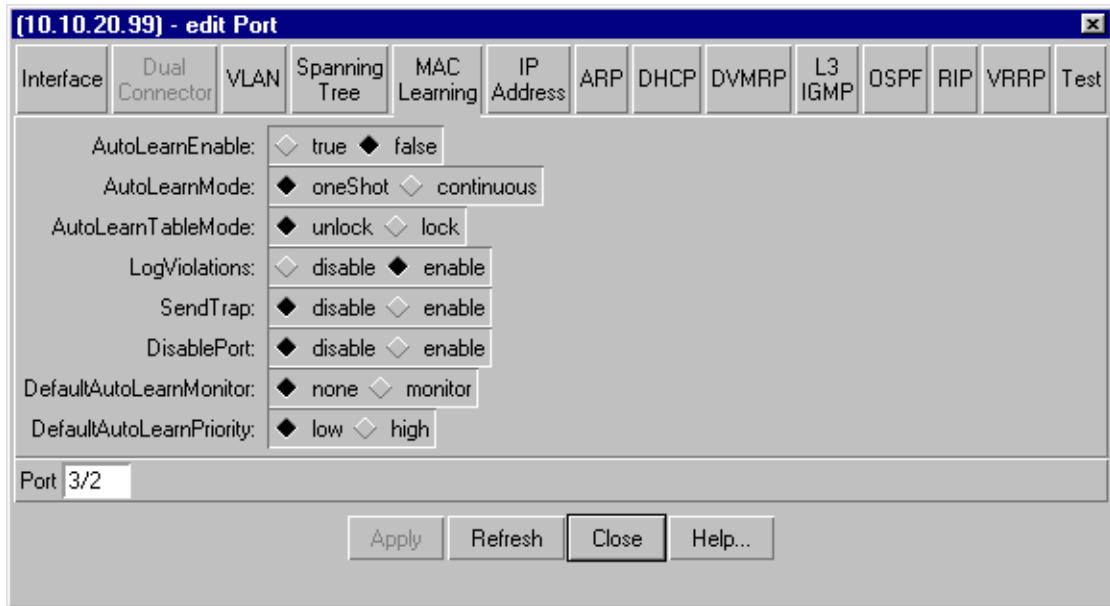
You use several Device Manager windows to configure and view the allowed MAC table.



**Note:** You must enable the Unknown MAC Discard feature on the Port Interface window to implement the allowed MAC table features discussed in this section. You can configure the allowed MAC table parameters with the Unknown MAC Discard feature disabled, but you must enable the Unknown MAC Discard feature to activate the allowed MAC table feature.

---

Using Device Manager, open the edit Port window and choose the MAC Learning tab ([Figure 1](#)).



**Figure 1. MAC Learning Window**

The fields in the MAC Learning window are shown in [Table 1](#).

**Table 1. MAC Learning Window Fields**

Field	Description
AutoLearnEnable	Sets the port to autolearn addresses for the allowed MAC table.
AutoLearnMode	Sets the autolearn mode on the port for populating the allowed MAC table to either: <ul style="list-style-type: none"> <li>oneShot</li> <li>continuous</li> </ul>
AutoLearnTableMode	Sets the allowed MAC table to current state. When locked, no new MAC addresses will be learned: <ul style="list-style-type: none"> <li>unlock</li> <li>lock</li> </ul>
LogViolations	Enables the system to create a system log entry when a disallowed MAC address attempts to send traffic through the selected port.

**Table 1. MAC Learning Window Fields (continued)**

Field	Description
SendTrap	Enables the system to send an SNMP trap (rcMacViolation) when a disallowed MAC address attempts to send traffic through the selected port.
DisablePort	Enables the system to administratively down the port when a disallowed MAC address attempts to send traffic. To bring the port back up, the administrator must manually enable the selected port or reboot the system. Choosing enable in this field automatically disables the selected port when an intrusion occurs.
DefaultAutoLearnMonitor	This field contains: <ul style="list-style-type: none"> <li>• none</li> <li>• monitor</li> </ul> When this field is set to monitor, the MAC address is set to be monitored. The port where this MAC address is learned must be configured to mirror traffic to another port where it can be monitored. For more information, refer to Port Mirroring in the Accelar 2.0 documentation.
DefaultAutoLearnPriority	Sets the priority of the traffic for the learned MAC address: <ul style="list-style-type: none"> <li>• low</li> <li>• high</li> </ul>

The buttons at the bottom of the MAC Learning window are:

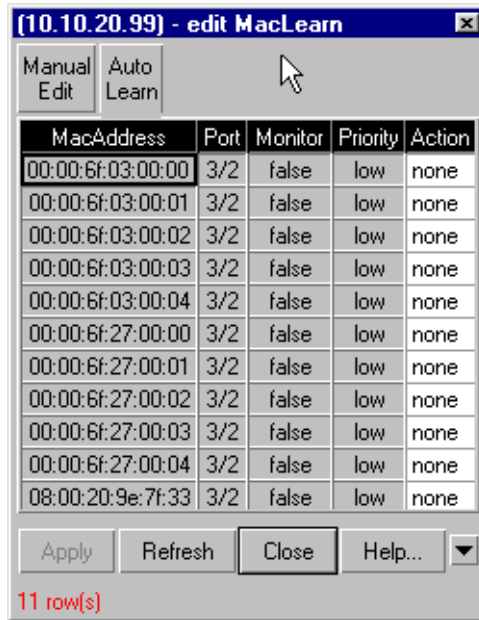
- **Apply**—Use this button to apply the changes.
- **Refresh**—Use this button to refresh the information in the window. Every time you click Refresh, new information is polled from the switch and displayed.
- **Close**—Use this button to close the MAC Learning window.
- **Help**—Use this button to launch the online Help.



**Note:** To lock the allowed MAC table, click lock in the AutoLearnTableMode field.

---

To view the autolearned addresses in the allowed MAC table, choose VLANs, and MacLearning..., AutoLearn ([Figure 2](#)). To set the parameters for the autolearned entries into the allowed MAC table, use the MAC Learning window ([Figure 1](#)), which you access by choosing Edit > Port > MAC Learning.



**Figure 2. AutoLearn Window**

The fields in the AutoLearn window are shown in [Table 2](#).

**Table 2. AutoLearn Window Fields**

Field	Description
MacAddress	Lists all the autolearned MAC addresses for the allowed MAC table.
Port	Shows the port.
Monitor	Shows one of two values: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> When this field shows true, the MAC address is set to be monitored. For more information, refer to Port Mirroring in the Accelar 2.0 documentation

**Table 2. AutoLearn Window Fields (continued)**

Field	Description
Priority	Shows whether traffic for a listed MAC address is designated low or high priority.
Action	Use this field to move a MAC address to the Manual Edit table of the allowed MAC table. When you select this box, a pull-down menu appears. Select convertToManualEdit, and click the Apply button at the bottom of the AutoLearn window.

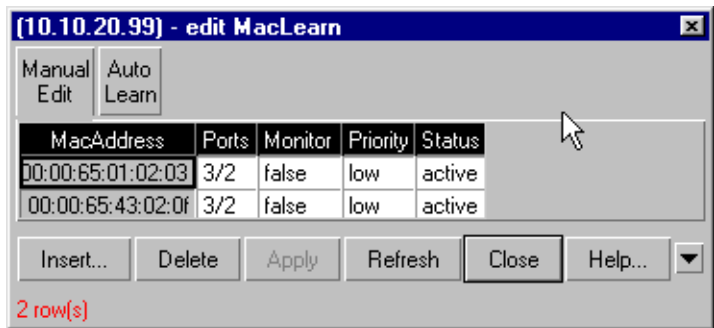
The buttons at the bottom of the AutoLearn window are:

- Apply—Use this button to apply the changes.
- Refresh—Use this button to refresh the information in the window. Every time you click Refresh, new information is polled from the switch and displayed.
- Close—Use this button to close the MAC Learning window.
- Help—Use this button to launch the online Help.



**Note:** To delete an individual autolearned MAC address, move it to the Manual Edit table and delete from there.

To manually add an allowed MAC address, choose VLANs, and MacLearning..., Manual Edit ([Figure 3](#)).



**Figure 3. Manual Edit Window**

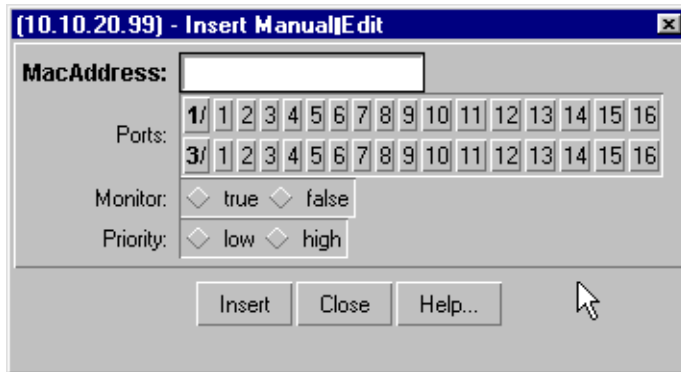
The fields in the Manual Edit window are shown in [Table 3](#).

**Table 3. Manual Edit Window Fields**

Field	Description
MacAddress	Lists all the manually entered MAC addresses for the allowed MAC table.
Ports	Shows the port.
Monitor	Shows one of two values: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> When this field shows true, the MAC address is set to be monitored. For more information, refer to Port Mirroring in the Accelar 2.0 documentation.
Priority	Shows whether traffic for a listed MAC address is designated low or high priority.
Status	Shows whether the MAC address is active or inactive. If you change this field to invalid, you delete the selected MAC address from the allowed MAC table.

The buttons at the bottom of the Manual Edit window are:

- **Insert**—Use this button to specify the MAC address you want to add to the allowed MAC table.
  - When you click this button, the Insert Manual Edit window ([Figure 4](#)) opens.
- **Delete**—Use this button to delete a MAC address from the allowed MAC table.
  - Highlight the MAC address you want to delete in the table.
  - Click the Delete button.
- **Apply**—Use this button to apply the changes.
- **Refresh**—Use this button to refresh the information in the window. Every time you click Refresh, new information is polled from the switch and displayed.
- **Close**—Use this button to close the MAC Learning window.
- **Help**—Use this button to launch the online Help.



**Figure 4. Insert Manual Edit Window**

The fields in the Insert Manual window are shown in [Table 4](#).

**Table 4. Insert Manual Window Fields**

Field	Description
MacAddress	Enter the MAC address into this field.
Ports	Select which port you want to allow traffic from entered MAC to enter and exit.
Monitor	Select one of two values: <ul style="list-style-type: none"> <li>• true</li> <li>• false</li> </ul> When you select true, the MAC address is set to be monitored. For more information, refer to Port Mirroring in the Accelar 2.0 documentation.
Priority	Designate traffic for the listed MAC address as low or high priority.

The buttons at the bottom of the Insert Manual window are:

- **Insert**—Use this button to add the new MAC address to the allowed MAC table shown in the Manual Edit window ([Figure 3](#)).
- **Close**—Use this button to close the MAC Learning window.
- **Help**—Use this button to launch the online Help.



**Note:** To clear AutoLearn entries (either One-Shot or Continuous) from the allowed MAC table using Device Manager, choose Edit > Port > Interface > Action <flushAll/flushMacfdb>.

## Configuring Using the CLI

Use the CLI commands to configure the Unknown MAC Discard feature as follows:

---

```
config ethernet <ports> unknown-mac-discard
followed by:
```

---

<code>activation &lt;enable disable&gt;</code>	Enables the Unknown MAC Discard feature. Although you can configure the feature with it disabled, the Unknown MAC Discard feature <i>must</i> be enabled to be implemented.
<code>add-allow-mac &lt;mac&gt; &lt;none monitor&gt; &lt;low high&gt;</code>	Manually enters MAC address into the allowed MAC table. Sets monitor and priority for specified MAC address (see below in table for explanations of monitor and priority).
<code>autolearn &lt;enable disable&gt;</code>	Enables the autolearn mode on the port for populating the allowed MAC table.
<code>autolearn-mode &lt;one-shot continuous&gt;</code>	Sets the autolearn mode on the port for populating the allowed MAC table to either: <ul style="list-style-type: none"> <li>• one-shot</li> <li>• continuous</li> </ul>
<code>default-autolearn-monitor &lt;none monitor&gt;</code>	Sets the MAC address to be monitored. The port where this MAC address is learned must be configured to mirror traffic to another port where it can be monitored. For more information, refer to Port Mirroring in the Accelar 2.0 documentation.
<code>default-autolearn-priority &lt;low high&gt;</code>	Sets the priority of the traffic for the learned MAC: <ul style="list-style-type: none"> <li>• low</li> <li>• high</li> </ul>
<code>info</code>	Displays the current configuration for the Unknown MAC Discard feature.

---

**config ethernet <ports> unknown-mac-discard**

followed by:

---

lock-autoload-mac <enable disable>	Enables the lock feature on the autoload MAC addresses. When enabled, no new MAC addresses will be learned (either one-shot or continuous); it sets the allowed MAC table to current state.
remove-allow-mac <mac>	Removes manually entered MAC address from allowed MAC table.
violation-downport <enable disable>	Enables the system to administratively down the port when a disallowed MAC address attempts to send traffic. To bring the port back up, the administrator must manually enable the selected port or reboot the system. Choosing enable in this field automatically disables the selected port when an intrusion occurs.
violation-logging <enable disable>	Enables the system to create a system log entry when a disallowed MAC address attempts to send traffic through the selected port.
violation-sendtrap <enable disable>	Enables the system to send an SNMP trap (rcMacViolation) when a disallowed MAC address attempts to send traffic through the selected port.

---

The following CLI commands display information about Unknown MAC settings:

---

show ports info unknown-mac-discard [<ports>]	Displays configuration for the Unknown MAC Discard feature for each port or for the specified port.
show vlan info manual-edit-mac	Displays entries that were manually entered into the allowed MAC table.
show vlan info autoload-mac	Displays entries that were autolearned by the switch (either one-shot or continuous) for the allowed MAC table.

---



**Note:** To clear AutoLearn entries (either One-Shot or Continuous) from the allowed MAC table use the command **config ethernet <ports> unknown-mac-discard lock-autolearn-mac disable**.

---

## Broadcast SNMP Trap Receiver

In this release (2.0.4), users can specify a directed broadcast address (for example, 10.10.40.255) as a trap receiver. When a device sends a trap to this directed broadcast address, any host listening on the local subnet will be able to receive a copy of the trap.

### Configuring

In Device Manager, choose Edit > Chassis > TrapReceiver > Insert; enter the destination address of the trap. This IP address can now be a broadcast address.

In the CLI, use **config sys set snmp trap-recv <ipaddress>**.

## OSPF Passive Ports

Within a VLAN, users can enable or disable reception of OSPF traffic on a per port basis; this configuration will apply to all VLANs on the configured port. The port will continue to generate Hello packets.



**Note:** This behavior applies only to a port in a VLAN. If the port is an isolated routing port; this behavior will disable OSPF on that port.

---

### Configuring

In Device Manager, choose Edit > Port > OSPF > Enable <true/false>. This parameter can now be configured for individual ports.

In the CLI, use **config ethernet <port> ip ospf <enable/disable>**.

## Disabling IPX NetBIOS Propagation

With the release of Accelar software version 2.0.4, 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**.

## Bugs Fixed in Release 2.0.4

The following sections list bugs that were fixed in Accelar software release 2.0.4.

### General

The following general bugs have been fixed in release 2.0.4:

- Accelar routing switch ports connected to a BayStack™ 450 switch using MLT will no longer remain in a blocking state after toggling the spanning tree state from fast to normal learning on the BayStack 450 switch. (99413)
- Configuration problems with spanning tree groups, VLANs, and MLT groups after resetting the Accelar switch have been resolved. (105190, 105195, 105273)
- User-defined PIDs for protocol-based VLANs are now properly saved in NVRAM. (105202)
- Initialization issues with the Model 1216FX and 1216TF modules in Accelar 1200 chassis with particular slot configurations have been resolved. (105975)
- ASCII-based configuration file problems related to OSPF router-id, MLT, and VLAN configuration have been corrected.

### CLI

The following CLI bugs have been fixed in release 2.0.4:

- The **show tech info** command now executes correctly. It will no longer interrupt execution and return the error message “invalid vlan id.” (104930)
- The trap receiver version can now be set from the CLI. (105580, 94343)
- The **show config** command now displays protocol type for RARP VLANs. (105387)
- The limitation of configuring max 500 static routes through the CLI has been removed. (106120)



**Caution:** You can create configurations larger than the maximum size binary configuration file that can be saved in NVRAM. If this happens, you get an error message when attempting to save to NVRAM. These larger configurations can be saved in ASCII-based configuration files. Refer to Accelar 2.0 documentation for information about how to use ASCII-based configuration files.

---

## MLT

The following MLT bugs have been fixed in release 2.0.4:

- Brouter ports are not allowed to join an MLT group; this is not a supported configuration. (96180, 97193)
- ARP table update problems in certain MLT configurations have been corrected. (104872, 105647)

## IP

The following IP bugs have been fixed in release 2.0.4:

- A static route will maintain precedence over a learned route with the same cost after its next hop goes down and comes back. (102602)
- ARP entries no longer age out at twice the aging time configured. (104132)
- RouteSource settings in RIP/OSPF announce policies can now be properly saved in the configuration file (105053), and the CLI command syntax is now consistent between RIP and OSPF. (106406)

## OSPF

The following OSPF bug was fixed in release 2.0.4:

- Accelar routing switches connected over virtual links will now properly advertise Summary LSAs. (105558)

## Known Issues in Release 2.0.4

### IP Multicast

The following IP multicast issues exist in the software version 2.0.4 release:

- IP multicast traffic does not route properly over tagged Gigabit links. (106116)
- IP unicast forwarding can be affected when streaming IP multicast traffic over a tagged Gigabit link.

### VRRP and MLT

The following VRRP and MLT issue exists in the software version 2.0.4 release:

- In an unlikely configuration where you have more than two Accelar units connected with Multi-Link Trunking (MLT) in a serial configuration running VRRP, it is possible that if an MLT link goes down, then back up, the VRRP advertisement messages will not be seen by all Accelar units. (99150)

### Unknown MAC Discard

The following Unknown MAC Discard issues exist in the software version 2.0.4 release:

- 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.

## Related Publications

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

