Release Notes for the BayStack 202/203/204/205 100 Mb/s Ethernet Hubs

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Part No. 896-00190-C
July 1998

Bay Networks

896-00190-C

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

Trademarks

Statement of Conditions

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

Bay 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.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

Introduction

These release notes contain information about the BayStack™ 200-series hubs that was not available when *Using the BayStack 202/203 100 Mb/s Ethernet Managed Hub* (Bay Networks® part number 893-01036-A), *Using the BayStack 204/205 100 Mb/s Ethernet Hub* (Bay Networks part number 893-01035-A), and *BayStack 202/203/204/205 100 Mb/s Ethernet Hubs* (Bay Networks part number 893-01037-A) were published.

These notes contain information about the following topics:

New Features in Release 3.1

Software release 3.1 provides BaySecure LAN Access™ security for the BayStack 200-series hubs. Eavesdrop Protection and Hardware Intrusion Control are hardware-based features that operate at the hub port to prevent unauthorized network access or network monitoring. The Software Intrusion control (Allowed Nodes) feature enables you to specify a list of network nodes that are allowed to access the network or prohibited from accessing the network.

Security features are set up for clusters of four ports; that is, you enable or disable the features for four ports at a time. However, when security is enabled, the protection and security actions apply to individual ports. Security features are set up through the console port menus, either at the console port or using the Telnet Protocol application.

BaySecure LAN Access

BaySecure LAN Access is fully compatible with IEEE 802.3, 10BASE-T, and 100BASE-T standards. It is interoperable with common 10BASE-T and 100BASE-T network interface cards (NICs) and transceivers. Because BaySecure LAN Access is completely compatible with IEEE 802.3 standards, it is transparent to encryption and authentication applications, physical and password security, and internetworking.

BaySecure LAN Access consists of the following three components that can, depending on the hardware platform, be used together or separately:

- Hardware consisting of BayStack 200-series hubs, managed and unmanaged
- Agent software residing in a managed hub in the stack
- Optivity LAN network management software residing at the network management station (for Software Intrusion Control only)

Hardware Functionality

BayStack 200-series hubs support the following real-time, hardware-based BaySecure functions:

- Eavesdrop Protection
- Hardware Intrusion Control
- Address learning, either one-shot AutoLearn™ or single MAC entry

Eavesdrop Protection prevents an end station from receiving confidential data that is not explicitly addressed to that specific station. Eavesdrop Protection is based on the idea that confidential data should be received by specified authorized stations only and relies on the association of a single authorized source address (ASA) for each port on the host module. The host module uses this ASA to filter packets transmitted from the module to the end station.

Eavesdrop Protection works after BaySecure LAN Access security options are fully configured and the hub shifts operation from the broadcast nature of standard 100BASE-T Ethernet to point-to-point secured 100BASE-T transmissions. The hub uses the authorized source address (ASA) to filter data frames going from the module to the end station. The destination address of each frame is checked, in real time, at each port.

If the destination address of the frame does not match the source address of the attached device on that port, a jam signal is substituted for the remainder of the frame on the receive path. Similar to the jam signal transmissions sent immediately following a collision, the BaySecure LAN Access jam signal consists of a meaningless string of ones and zeros inserted seamlessly into the frame stream. The Eavesdrop Protection jam signal prevents the data frame from reaching an unintended end station, while maintaining the collision domain of the Ethernet segment. The end result is that only the intended destination address can read the frame. All other stations hear a busy signal, which allows carrier sense multiple access/collision detection (CSMA/CD) to function normally. Compatibility with IEEE 802.3 specifications is maintained.

Multicast and broadcast data frames normally contain polling or control messages rather than confidential data. These frames are not filtered but are transmitted through every port.

Hardware-based Intrusion Control provides fast, real-time filtering of one or two MAC addresses per port; prevents unauthorized Data Terminal Equipment (DTE) from accessing the network; and allows network administrators to monitor and restrict network moves and changes.

Hardware Intrusion Control detects DTE transmissions in a manner similar to Eavesdrop Protection filtering. On the transmit path from the port to the network, BaySecure LAN Access compares the MAC source address of an incoming frame with the authorized source address of the host module port. A nonmatch signals a violation, and the port is immediately, but temporarily, jammed under control of the hub. This action effectively scrambles the frame's data field contents. The frame reaches the network, but the data field contents are invalidated. This activity is carried out automatically, on a frame-by-frame basis, and lasts only for the duration of the frame transmission. After the ASA is received, the port recovers from a jammed state within a recovery period of less than one second. Network connectivity is maintained during the recovery period.

The third hardware-based functional area is address learning (one-shot AutoLearn), which simplifies the assignment and administration of authorized source addresses. The hub automatically captures the MAC source address for the first two frames to be received at the port. One-shot AutoLearn permits quick capture of an address and reduces configuration requirements.

Agent Functionality

A Simple Network Management Protocol (SNMP) agent is intelligent software that monitors managed SNMP network devices and gathers statistical data in management information base (MIB) format. A central network management entity, such as Optivity® network management software, regularly polls the SNMP agents and downloads the contents of their MIBs. The agents may also act on requests from the network management system.

BaySecure LAN Access agents allow for *software*-based Intrusion Control, which provides multiple MAC addresses filtering based on the Allowed Nodes or Allowed Nodes Plus (both Allowed Nodes and Not-allowed Nodes) configuration tables.

Security Modes

Six different BaySecure LAN Access security modes define who can access the network, the access rights and privileges they can exercise, and what actions will be taken against unauthorized users. Each mode is configured through specific settings applied either individually or simultaneously to agents or hardware modules. Most of the security modes offer multiple options logically grouped to provide a specific type of Eavesdrop Protection or Intrusion Control action.

The configured BaySecure LAN Access security modes allow you to implement a network security policy that provides either or both of the following protections:

- Prevents unauthorized users from accessing network data not addressed directly to their station (Eavesdrop Protection)
- Deters unauthorized hardware transmissions to the network (Intrusion Control)

The following six security modes are available:

- Security Disabled
- Eavesdrop Protection
- Software Intrusion Control
- Software Intrusion Control with Eavesdrop Protection
- Hardware Intrusion Control
- Hardware Intrusion Control with Eavesdrop Protection

Security Disabled

Security Disabled mode disables all security features. If a port, hub, or network is configured with this security mode, any user can access, send, and/or receive data through any available port. Use this security mode only if you have decided that unrestricted network access is appropriate and/or if all data traversing the network is considered to be nonconfidential.

Eavesdrop Protection

Eavesdrop Protection mode permits anyone to access the port, one user at a time. The user receives traffic destined for that specific MAC address, as well as any broadcast and multicast frames. This mode is a hardware-only mode and does not provide notification of any intruder violations. Use this security mode if you want unrestricted user access to a port, yet want to ensure that each user receives only data addressed to that ASA, as well as broadcast and multicast frames.

Software Intrusion Control

Software Intrusion Control permits any user identified from an approved list to access the port. Approved users can access this port to send and receive data on that segment. This mode is an agent-only mode, with software-based Intrusion Control enabled. There is no Eavesdrop Protection in this mode; all users on the Allowed Nodes list are permitted access to all data. Use this security mode when you want only clearly identified individuals or functional entities who match the ASA to access the network, but you do not care what data they have access to after they are on the network.

Software Intrusion Control with Eavesdrop Protection

This mode combines hardware-based Eavesdrop Protection and software-based Intrusion Control. Any user identified from an approved list can access the port and can send data on that segment. However, each user receives only traffic destined for that specific MAC address, as well as all broadcast and multicast frames. Use this mode when you want only clearly identified individuals or functional entities that match the authorized source address to have access to the network and want to provide them with unrestricted access privileges to send data over the network, yet want to restrict their access to certain data only.

Hardware Intrusion Control

Hardware Intrusion Control permits only one user to access the port. This user may be determined individually or selected on a connectivity "snap shot" first-come-first-served basis (also known as one-shot AutoLearn). The approved user can send and receive anything on that segment. This mode is a hardware and agent mode, with hardware-handled violations. Eavesdrop Protection is disabled; Intrusion Control is enabled. Use this mode when you want only clearly identified individuals or functional entities to have access to the network through a particular connection point and want to provide them with unrestricted access privileges to send and receive data over the network from this connection point.

Hardware Intrusion Control with Eavesdrop Protection

This mode is a hardware and agent mode, with hardware-handled violations. Both Eavesdrop Protection and Intrusion Control are enabled. Only one user can access the port. This user may be determined individually or selected on a connectivity "snap shot" first-come-first-served basis (also known as one-shot AutoLearn). The approved user receives only traffic destined for that port, as well as all broadcast and multicast frames. Use this mode when you want only clearly identified individuals or functional entities to have access to the network through a particular connection point and want to provide them with unrestricted access privileges to send data over the network from this connection point, yet want to restrict their access to certain data only.

Note: This is the most secure setting of the BaySecure LAN Access security modes.

BaySecure LAN Access Configuration

Table 1 shows which of the management interfaces for the switch you can use to set up the BaySecure features.

Table 1. User Interfaces for Setting Up BaySecure Features

Feature	How to Set It Up			
	Web Management Interface	**Console Menus**	**Telnet Connection**	**Optivity**
Software Intrusion Control		x	x	
Hardware Intrusion Control		x	x	
Eavesdrop Protection		x	x	
Address Learning		x	x	

Table 2 provides a matrix that details who may access the network, what access limits are set for authorized users, and what happens to unauthorized users under each BaySecure LAN Access security mode. Table 3 provides details of the security mode configuration settings. Shaded areas are hardware configurations or actions.

Table 2. Security Mode "Who" and "What" Matrix

Mode	Who is Authorized to Access Network	Access Limits for Authorized Users	Hardware Action	Software Action
1: Disabled	Anyone	None	None	None
2: Eavesdrop Protection	Anyone, one user at a time	Receive only ASA, broadcast and multicast frames	None	None Trap
3: Software Intrusion control	User from Allowed Nodes list		None	None
	User from Allowed Nodes list		None	Trap
	User from Allowed Nodes list		None	Partition
	User from Allowed Nodes list		None	Trap & Partition
4: Software Intrusion Control with Eavesdrop Protection	User from Allowed Nodes list	Receive only ASA, broadcast and multicast frames	None	None
	User from Allowed Nodes list	Receive only ASA, broadcast and multicast frames	None	Trap
	User from Allowed Nodes list	Receive only ASA, broadcast and multicast frames	None	Partition
	User from Allowed Nodes list	Receive only ASA, broadcast and multicast frames	None	Trap & Partition
5: Hardware Intrusion Control	One AutoLearn user only	None	Jam	None
	One AutoLearn user only	None	Jam	Trap
	One preassigned user only	None	Jam	None
	One preassigned user only	None	Jam	Trap
6: Hardware Intrusion Control with Eavesdrop Protection	One AutoLearn user only	Receive only ASA, broadcast and multicast frames	Jam	None
	One AutoLearn user only	Receive only ASA, broadcast and multicast frames	Jam	Trap
	One preassigned user only	Receive only ASA, broadcast and multicast frames	Jam	None
	One preassigned user only	Receive only ASA, broadcast and multicast frames	Jam	Trap

Table 3. BaySecure LAN Access Security Mode Settings

Mode	Address Learning Setting	Allowed Nodes Setting	Eavesdrop Protection Setting	Hardware Intrusion Control Setting	Hardware Action	Software Action
1: Disabled	Off	Off	Off	Off	None	None
2: Eavesdrop Protection	One Shot or Single MAC	Off	On	Off	None	None Trap
3: Software Intrusion Control	Off	On	Off	Off	None	None
	Off	On	Off	Off	None	Trap
	Off	On	Off	Off	None	Partition
	Off	On	Off	Off	None	Trap & Partition
4: Software Intrusion Control with Eavesdrop Protection	One Shot or Single MAC	On	On	Off	None	None
	One Shot or Single MAC	On	On	Off	None	Trap
	One Shot or Single MAC	On	On	Off	None	Partition
	One Shot or Single MAC	On	On	Off	None	Trap & Partition
5: Hardware Intrusion Control	One Shot	Off	Off	On	Jam	None
	One Shot	Off	Off	On	Jam	Trap
	Single MAC	Off	Off	On	Jam	None
	Single MAC	Off	Off	On	Jam	Trap
6: Hardware Intrusion Control with Eavesdrop Protection	One Shot	Off	On	On	Jam	None
	One Shot	Off	On	On	Jam	Trap
	Single MAC	Off	On	On	Jam	None
	Single MAC	Off	On	On	Jam	Trap

New Console Menus for BaySecure

This section describes the new console port menus used for setting up BaySecure security for the BayStack 200-series 100 Mb/s Ethernet hubs. A new command on the Main Menu provides the entry point for these menus.

BaySecure Configuration Menu

When you press a from the Main Menu, the BaySecure Configuration Menu is displayed (Figure 1).

```
BaySecure Configuration Menu                BayStack 200 100BASE_T NMM
Unit:  1









p - Port Security Configuration Menu
n - Allowed Nodes Configuration Menu
t - Time Partition Setting
[Esc] - Return to previous menu

Enter command:
```

Figure 1. BaySecure Configuration Menu

The BaySecure Configuration Menu allows you to perform the following tasks:

- Set up port security
- Set up the Allowed Nodes feature
- Set the security partition interval for ports

Table 4 describes the commands on the BaySecure Configuration Menu.

Table 4. Commands on the BaySecure Configuration Menu

Command	Meaning
p	**[Port Security Configuration Menu]** Use the p command to display the Port Security Menu, which allows you to set Eavesdrop Protection and Intrusion Control for groups of four ports on the hub. For a description of the Port Security Configuration Menu, see page 12.
n	**[Allowed Nodes Configuration Menu]** Use the n command to display the Allowed Nodes Configuration Menu, which allows you to set Allowed Nodes protection for individual ports on the hub. For a description of the Allowed Nodes Configuration Menu, see page 17.
t	**[Time Partition Setting]** Use the t command to specify a partition interval in minutes for a port that has been partitioned by the BaySecure security features. **Note:** If you set the time partition interval to 0 (zero), the port remains partitioned until you manually unpartition it from the Main Menu or through SNMP management.
[Esc]	**[Return to previous menu]** Use this command to return to the Main Menu.

Port Security Configuration Menu

When you press p from the BaySecure Configuration Menu, the Port Security Configuration Menu is displayed (Figure 2).

```
Port Security Configuration Menu                    BayStack 200 100BASE_T NMM
Unit:  1

s - Show Security Configuration
a - Add/Modify Security Configuration
d - Delete Security Configuration
w - Save values to FLASH
[Esc] - Return to previous menu

Enter command:
```

Figure 2. Port Security Configuration Menu

The Port Security Configuration Menu allows you to perform the following tasks:

- Check the current security configuration settings
- Set up Eavesdrop Protection and Intrusion Control for port groups, as well as changing existing settings for these features
- Delete the security settings for a port group
- Save the configuration settings

Table 5 describes the commands on the Port Security Configuration Menu.

Table 5. Commands on the Port Security Configuration Menu

Command	Meaning
s	**[Show Security Configuration]** Use this command to display the Show Security Configuration screen, which shows learned MAC addresses (up to 2), security mode, AutoLearn mode, and software action for each port.
a	**[Add/Modify Security Configuration]** Use this command to display the Add/Modify Security Configuration Menu, which allows you to specify the security settings for ports. For more information about the Add/Modify Security Configuration menu, see page 14.
d	**[Delete Security Configuration]** Use this command to delete the security settings for a port group. When you press d, you are prompted to enter a unit number and group number. (Ports are grouped into sets of four.)
w	**[Save values to FLASH]** Use the w command to save the security settings to nonvolatile memory. If you do not save the configuration settings, they are not preserved during a power cycle.
[Esc]	**[Return to previous menu]** Press the Esc key to return to the BaySecure Configuration Menu.

Add/Modify Security Configuration Menu

When you press a from the Port Security Menu, the Add/Modify Security Configuration Menu is displayed (Figure 3).

```
Add/Modify Security Configuration Menu      BayStack 200 100BASE_T NMM
Unit:  1

***** Unit < 0 >, Group < 0 > Security Settings *****

Security Mode:  NoSecurity
Auto Address Learning Mode:   NotApplicable
Number of Source Addresses:   1
Software Action: NotApplicable



u - Unit Number Selection          |  l - Auto Learning Mode Selection
g - Group Number Selection         |  n - Number of Source Address
s - Security Mode Selection        |  m - MAC Address Selection
a - Software Action Selection      |  d - Apply Configuration Settings
[Esc] - Exit Security Configuration

Enter command:
```

Figure 3. Add/Modify Security Configuration Menu

This menu allows you to set up security for port groups in the hub stack. The upper part of the menu shows current settings for the security parameters. When you specify a unit (hub) number and port group number, the display scrolls to show the current settings for the specified group. Likewise, each time you set one of the security parameters on the menu, the display scrolls to reflect the new setting.

Table 6 describes the commands on the Add/Modify Security Configuration Menu.

Table 6. Commands on the Add/Modify Security Configuration Menu

Command	Meaning
u	**[Unit Number Selection]** When you press u, you are prompted to enter the unit number of the hub you are configuring.
g	**[Group Number Selection]** When you press g, you are prompted to enter the number of the port group you are configuring.
s	**[Security Mode Selection]** When you press s, you are prompted to enter the security mode. Possible choices are: • 1 - Security disabled • 2 - Eavesdrop Protection • 3 - Software Intrusion Control* • 4 - Software Intrusion Control with Eavesdrop Protection • 5 - Hardware Intrusion Control • 6 - Hardware Intrusion Control with Eavesdrop Protection
a	**[Software Action Selection]** When you press a, you are prompted to enter the software action to be used in case of a security violation. Possible choices are: • 1 - No action • 2 - Send trap • 3 - Partition port (valid only for Software Intrusion Control modes) • 4 - Partition port and send trap (valid only for Software Intrusion Control modes)
l	**[Auto Learning Mode Selection]** When you press l, you are prompted to enter the AutoLearn mode for the hub. Possible choices are: • 1- Single MAC User Entry—You must manually enter one or two MAC addresses that are allowed to access this port group. • 2 - One Shot Auto Learn—The hub automatically learns the first two MAC addresses that access this port group.
n	**[Number of Source Addresses]** When you press n, you are prompted to specify either 1 or 2 as the number of source addresses that can access this port group.
m	**[MAC Address Selection]** When you press m, you are prompted to specify one or two MAC addresses for a port group and to indicate whether these are allowed or not allowed to access the ports.

Table 6. Commands on the Add/Modify Security Configuration Menu (continued)

Command	Meaning
d	**[Apply Configuration Settings]** When you press d, the security configuration settings you have entered become active. The screen displays the current settings, and a message asks you to confirm that they are correct. **NOTE:** You must save the settings to nonvolatile memory using the w command on the Port Security Configuration Menu to preserve them through a system power cycle.
[Esc]	**[Exit Security Configuration]** Press the Esc key to return to the Port Security Configuration Menu.

* If you select Software Intrusion Control, with or without Eavesdrop Protection, you must use the Allowed Nodes Configuration Menu to set up the list of allowed and not-allowed nodes.

Allowed Nodes Configuration Menu

When you press n from the BaySecure Configuration Menu, the Allowed Nodes Configuration Menu is displayed (Figure 4).

```
Allowed Nodes Configuration Menu             BayStack 200 100BASE_T NMM
Unit:  1


The current numbers of allowed nodes:        0
The maximum numbers of allowed nodes:      300
The current numbers of not-allowed nodes:    0
The maximum numbers of not-allowed nodes:  100







s - Show Node Access Configuration
a - Add Allowed Node
d - Delete Allowed Node
m - Modify Allowed Node
w - Save values to FLASH
[Esc] - Return to previous menu

Enter command:
```

Figure 4. Allowed Nodes Configuration Menu

The Allowed Nodes Configuration Menu shows the current number of allowed and non-allowed nodes that have been set up and enables you to perform the following tasks:

- Check the current allowed nodes configuration
- Add or delete a MAC address to be allowed or not allowed to access the hub
- Modify an existing allowed or not-allowed node
- Save the allowed nodes settings to nonvolatile memory

Table 7 describes the commands on the Allowed Nodes Configuration Menu.

Table 7. Commands on the Allowed Nodes Configuration Menu

Command	Meaning
s	**[Show Node Access Configuration]** When you press s, you are prompted to enter a unit number. Then the Node Access Configuration screen shows which ports have allowed and not-allowed nodes assigned to them. **Note:** If you used a zero (0) with the a command to specify all units, you must also use a zero with this command to show the node access configuration.
a	**[Add Allowed Node]** When you press a, you are prompted to enter a unit number, port number, and segment number, and then to choose whether this will be an entry for an allowed or not-allowed node. Then you are prompted to enter a MAC address. **Note:** You can specify all units or all ports by entering a zero at the prompt.
d	**[Delete Allowed Node]** When you press d, you are prompted to enter a unit number, port number, and segment number, followed by the MAC address you are deleting.
m	**[Modify Allowed Node**] Use this command to change a current entry for an allowed or not-allowed node. When you press m, you are prompted to enter a unit number, port number, segment number, and MAC address. Then you are prompted to choose Allowed or Not Allowed for this entry.
w	**[Save values to FLASH**] Use the w command to save the security settings to nonvolatile memory. If you do not save the configuration settings, they are not preserved during a power cycle.
[Esc]	**[Return to previous menu]** Press the Esc key to return to the BaySecure Configuration Menu.

Setting Up Security

As shown in Tables 2 and 3 on pages page 8 and page 9, respectively, the BaySecure security modes and options offer a wide variety of possibilities for security configurations. This section provides basic instructions for setting up one security configuration. Use the same general principles to set the configuration that is appropriate for your network.

Review Tables 2 and 3 and decide the type or types of security to set up. You can specify different combinations of features for each group of four ports. Hardware Intrusion Control acts more quickly than Software Intrusion Control, but it limits the number of allowed MAC addresses to two addresses per port. Software Intrusion Control allows up to 300 MAC addresses per port.

Before you start, have a list of MAC addresses for your network.

Setting Up Hardware Intrusion Control with Eavesdrop Protection

The most secure security mode is Hardware Intrusion Control with Eavesdrop Protection.

To set up this security mode:

1. **Go to the Add/Modify Security Configuration Menu:**
   a. **From the Main Menu, press a to display the BaySecure Configuration Menu.**
   b. **Press p to display the Port Security Configuration Menu.**
   c. **Press a to display the Add/Modify Security Configuration Menu.**

      The upper part of the Add/Modify Security Configuration Menu shows the current security settings.
2. **Use the u and g commands to specify the unit and port group to set up.**
3. **Set the security parameters for the specified group:**
   a. **Use the s command to select the Security Mode, and then select 6 - Hardware Intrusion Control with Eavesdrop Protection.**

      The display scrolls, and the upper part of the menu shows recommended settings for Auto Address Learning Mode (One-shot), Number of Source Addresses (1), and Software Action (No Action).

   b. **To change one of the other security settings, use the a, l, or n command and respond to the screen prompt.**

   c. **If you changed the AutoLearn mode to Single MAC User Entry, use the m command to specify one or two MAC addresses that are allowed to access the port.**

4. **When you have set up all the security parameters for this port group, press d to apply the configuration settings.**
5. **Repeat steps 2 through 4 for each remaining port group you are setting up.**
6. **Press [Esc] to return to the Port Security Configuration Menu.**
7. **Press w to save the configuration settings to flash memory.**

Setting Up Software Intrusion Control

Software Intrusion Control allows you to enter up to 300 allowed or 100 not-allowed MAC addresses for each port group.

To set up Software Intrusion Control:

1. **Go to the Add/Modify Security Configuration Menu:**

   a. **From the Main Menu, press a to display the BaySecure Configuration Menu.**

   b. **Press p to display the Port Security Configuration Menu.**

   c. **Press a to display the Add/Modify Security Configuration Menu.**

   The upper part of the Add/Modify Security Configuration Menu shows the current security settings.

2. **Use the u and g commands to specify the unit and port group to set up.**
3. **Set the security parameters for the specified group:**

   a. **Use the s command to select the Security Mode, and then select either 3 - Software Intrusion Control or 4 - Software Intrusion Control with Eavesdrop Protection.**

b. **If you selected Software Intrusion Control with Eavesdrop Protection, you must set up the software action and AutoLearn Mode parameters for Eavesdrop Protection.**

Note: When Software Intrusion Control is selected, the possible software actions for a security violation include partitioning the port. If a port is partitioned as a result of the BaySecure security action and you have set the time partition interval to zero, you must manually unpartition the port from the Main Menu or through SNMP management. If the time partition interval is set to a number other than zero, the port automatically unpartitions at the end of the specified time.

c. **If you selected Single MAC User Entry for the AutoLearn mode, use the m command to specify one or two MAC addresses that are allowed to access the port.**

Caution: When you select Single MAC User Entry, the upper part of the display shows all zeroes for the specified MAC addresses. You must enter valid addresses for these ports, or else no network nodes will be able to access the ports.

4. **When you have set up all the parameters for this port group, press d to apply the configuration settings.**
5. **Repeat steps 2 through 4 for each remaining port group you are setting up.**
6. **Press [Esc] to return to the Port Security Configuration Menu.**
7. **Press w to save the configuration settings to flash memory.**
8. **Press [Esc] to return to the BaySecure Configuration Menu.**
9. **Set up the Allowed Nodes List.**
   a. **Press n to display the Allowed Nodes Configuration Menu.**
   b. **Use the a, d, and m commands to specify the nodes that are allowed or not allowed to access this port group.**
   c. **Press w to save the Allowed Nodes settings to flash memory.**

BaySecure Configuration File

This section provides a portion of a sample BaySecure LAN Access NMM configuration file. To save space, file parameters unrelated to BaySecure LAN Access are not listed here. Refer to the documents shipped with your product for a complete listing of all configuration parameters.

```
############ BAYSECURE SECURITY FEATURE ############################
# RULES : There are 2 separate settings for users to configure.
#  1) timePartion (optional) - see description below.
#  2) BaySecure Node Access Software Control Configuration Table.
#
# NOTE: The Rule #2 must be set according to the table definition
#in your User Guide.
#-----------------------------------------------------------------
#
# 1) Global Variable : timePartition.
#
# In BaySecure Port Security Configuration Table, the SoftwareAction
# Mode can be either partitionPort or sendTrapPart. There are two
# types of partition that a user can choose from:
# permanent-partition or timed-partition partition_interval
# where partition_interval is an optional.
# The timed-partition will be done if the partition_interval
# is greater than zero.  If the user chooses to omit the
# timed-partition, the default value is zero, i.e no timed-partion.
# The value indicates the duration of time for port partitioning
# in minutes.
#
#
#Example: time partition for 2 minutes.
#s5time-partition 2

#-----------------------------------------------
# 2) BaySecure Node Access Software Control Configuration Table
# Setting
#
# In BaySecure Node Access Software Control Configuration Table,
# the following variables have to be set accordingly:
#
#Key Word    : s5baysecure-node.
#
#      Segment Type : 1) Backplane Segment Type.
#         2) Local Segment Type.
#         3) All Segment Type (i.e. the Segment number will apply
#       both Segment types).
#
```

```
#    Segment Number : the segment number of the specified segment
#    type.
#         The segment number 0 is referred to ALL segments
#         of the specified segment type.
#
#Comp Number : the index of the comp containing the board on which
#         the port is located. Comp 0 is referred to ALL comp
#         in the chasis.
#
#Port Number : the index of the port on the board.
# Port 0 is referred to ALL ports in the board.
#
#MAC Address : MAC address can be referred to allowed station or
#         not-allowed station which is indicated by the Node
#         Access Controlled Type.
#
# NodeAccessCtrlType: 1) node Allow.
#         2) node NOT Allow.
#
#    Execution Type : 1) not Applicable.
#         2) create
#
#
#-----------------------------------------------------------------
# EXAMPLE #1 : BaySecure Node Access Software Control Configuration
# Table
#
# key word:  s5baysecure-node
# segment type:(1);
# segment number:(1);
# comp number: (5);
# port number: (5);
# MAC Address:0800201A5890
# NodeAccessCtrlType:(1);
# Execution Type:(2);
#
#
#---------------------------------------------


#-----------------------------------------------------------------
# EXAMPLE #2 : BaySecure Node Access Software Control Configuration
# Table
#
# key word:  s5baysecure-node
# segment type:(1);
# segment number:(1);
# comp number: (5);
```

```
# port number: (6);
# MAC Address:0800201A5890
# NodeAccessCtrlType:(2);
# Execution Type:(2);
#
#
#-----------------------------------------------------------------
# Total Node Address = 256



s5baysecure-node 1 1 5 1 0800201A5890 1 2
s5baysecure-node 1 1 5 2 0800201A5890 1 2
s5baysecure-node 1 1 5 3 0800201A5890 1 2
s5baysecure-node 1 1 5 4 0800201A5890 1 2
s5baysecure-node 1 1 5 5 0800201A5890 1 2
s5baysecure-node 1 1 5 6 0800201A5890 1 2
s5baysecure-node 1 1 5 7 0800201A5890 1 2
s5baysecure-node 1 1 5 8 0800201A5890 1 2
s5baysecure-node 1 1 5 9 0800201A5890 1 2
s5baysecure-node 1 1 5 10 0800201A5890 1 2
s5baysecure-node 1 1 5 11 0800201A5890 1 2
s5baysecure-node 1 1 5 12 0800201A5890 1 2
```

MIBs Supported by this Release

Software release 3.1 supports the following RFCs and MIBs:

- RFC 1213
- RFC1215
- RFC1271
- S5000—Agent MIB
- S5000—Chassis MIB
- S5000—Chassis Trap MIB
- S5000—Ethernet Common MIB
- S5000—Ethernet Trap MIB
- S5000—Ethernet Redundant Links MIB
- S5000—Ethernet Multisegment Topology MIB
- S5000—Common Statistics MIB
- S5000—Ethernet MIB
- Subset of S5000—Common BaySecure MIB

Bug Fixes

The content area of each Web page displays the system uptime (time since the most recent power cycle or system reset) in the upper left corner. The counter for this display would reset to zero every five days. This problem has been fixed. (53718)

Known Problems

The Web management interface for the BayStack 200-series hubs is not fully supported by Microsoft® Internet Explorer. The following problems exist:

- Using Internet Explorer 3.x, the Traffic and Error functions for the Statistics page are not supported. When you click on these links, the system displays a Java script error message. (80492)
- Using Internet Explorer 3.x or 4.x, the folder titles in the navigation bar are displayed as screen text instead of as active links. The page titles listed under the folders provide active links to all the management pages. (79341)
- Using Internet Explorer 4.0 or later, the Statistics page opens, but the delta function for displaying values is not supported.

If you resize the window when you are using Netscape Navigator to access the Web management interface, the display of the content area reverts to the Device Configuration page and all folders in the navigation bar close. (79343)

If you click on the Reload or Refresh button in the Web management interface, the display of the content area reverts to the Device Information page. (79340)

With access control for the management functions enabled, Telnet sessions from a console terminal sometimes appear to “hang” when you try to enter a login name. This phenomenon happens only when users repeatedly log in and out. If you wait for the access control timeout period, you can attempt the login process again. You can also press [Ctrl]+[B] from the local console to terminate the Telnet session and then log in again. (53701)

Unavailable Statistics Counters

Some statistics counters are not fully supported in the hardware for communication with Optivity network management software and the Web management interface. Table 8 lists the counters and where they are supported.

Table 8. Statistics Counters

Counter	Interface	Port	Cluster	Segment
Good Octets	Yes	Yes	Yes	Yes
Good Frames	Yes	Yes	Yes	Yes
Broadcast Frames	Yes	No	No	Yes
Multicast Frames	Yes	No	No	Yes
Alignment Errors	Yes	Yes	Yes	No
Runts	No	Yes	Yes	No
Too Long Frames	No	Yes	Yes	Yes
Fragments	No	Yes	Yes	No
Very Long Events	No	Yes	Yes	No

For those counters that are not supported, a get request always returns a value of 0 (zero).

Mounting Options

The original versions of *Using the BayStack 202/203 100 Mb/s Ethernet Managed Hub* (Bay Networks part number 893-01036-A), *Using the BayStack 204/205 100 Mb/s Ethernet Hub* (Bay Networks part number 893-01035-A), and *BayStack 202/203/204/205 100 Mb/s Ethernet Hubs* (Bay Networks part number 893-01037-A) contain instructions for mounting the BayStack 200-series hubs on a wall. These instructions are in error; the BayStack 200-series hubs cannot be mounted on a wall. The BayStack 200-series hubs can be installed only in an equipment rack or on a table or shelf.