Release Notes for the Model 281xSA and 331xSA Ethernet NMM Software Version 2.0

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Part No. 201406-A
February 1998

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Trademarks

Bay Networks, Optivity, and SynOptics are registered trademarks of Bay Networks, Inc.

Autotopology, BayStack, DesignMan, System 2000, and System 3000 are trademarks of Bay Networks, Inc.

Other brand and product names are registered trademarks or trademarks of their respective holders.

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.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR52.227-19 or subparagraph (c)(1)(a) of the Rights in Technical Data and Computer Software clause of DFARS 52.227-7013, and any successor rules or regulations, whichever is applicable.

Introduction

These release notes contain information about the Model 281xSA and Model 331xSA Network Management Module (NMM) Ethernet Agent version 2.0. For more information about these products, refer to the documentation shipped with the product.

These release notes cover the following topics:

New Features

The Model 281xSA and Model 331xSA Ethernet NMM Agent version 2.0 supports the following new features:

- User access control
- Telnet support
- RMON2 support
- Trap Filtering Support
- OpenBay module support

User Access Control

Version 2.0 enables you to control access to the hub service port menus by setting up a password. Authorized users can then access the user interface from the service port or from a remote terminal using the Telnet Protocol. For information about Telnet support, refer to “Telnet Support” on page 11.

Note: The menus shown in this section illustrate service port menus from the Model 331xSA NMM. The same options are available on the Model 281xSA NMM service port menus.

Accessing the Service Security Menu

Choose command e from the NMM Main Menu to display the Service Security Menu as shown in Figure 1. The Service Security Menu provides commands for displaying other menus and for directly executing actions.

```
Enter command: Service Security Menu


Authentication & Access Control: <on>


u - Username/Password management menu
s - Source IP Address access control menu
t - Telnet Access management menu
c - Toggle Authentication & Access Control Checking
w - Save values to EEPROM




[ESC] - Return to previous Menu

Enter command:
```

Figure 1. Service Security Menu

The following commands can be selected from the Service Security Menu:

u **[Username/Password management menu]** Use the u command to display the Username/Password Management Menu. Refer to page 5 for details about the Username/Password Management Menu.

s **[Source IP Address access control menu]** Use the s command to display the Source IP Addr. Access Control Menu. Refer to page 7 for details about the Source IP Addr. Access Control Menu.

t **[Telnet Access management menu]** Use the t command to display the Telnet Access Management Menu. Refer to page 9 for details about the Telnet Access Management Menu.

c **[Toggle Authentication & Access Control Checking]** Use the c command to toggle the authentication and access control checking feature on or off. When the feature is toggled on, a user is required to enter a user name and its associated password to access the service port menus. When the feature is toggled off, a user does not need to enter any information to access the service port menus. When you modify this option, a message appears and indicates that the status has been modified but not saved to electrically erasable programmable read-only memory (EEPROM).

For more information about authentication and access control to the console port menus, refer to “Using the Authentication and Access Control Checking Option” on page 10.

w **[Save values to EEPROM]** Use the w command to save changes to EEPROM.

Managing the NMM Service Port Login Passwords

The service port password controls access to all read and write functions for the NMM. The NMM supports three general-purpose user name and password pairs: Manager, Operator, and User.

Note: In version 2.0 of the agent, all three user names have equal unlimited access privileges.

The NMM does not have passwords associated with the user names when it is shipped from the factory. Bay Networks® strongly recommends that you configure the necessary passwords when you set up the NMM. You can assign a different password to each user name. If there is no password configured for a user name, the user is prompted only for a login user name.

The user names are case sensitive. You cannot modify these user names or add new ones.

Logging Out

To end the user interface session, use the e command [Exit] from the Main Menu.

The session remains active until you exit the session. A Telnet session cannot be initiated until the service port session has ended and the Access Control Checking option (command c on the Service Security Menu) is toggled off.

Accessing the Username/Password Management Menu

The Username/Password Management Menu (see Figure 2) is a submenu of the Service Security Menu. Use this menu to manage the NMM service port login passwords.

```
Username/Password Management Menu


Entry    Username                Password
1        Manager                 <present>
2        Operator                <empty>
3        User                    <present>

p - Modify a Password
c - Clear all Passwords
k - Clear a Password
w - Save values to EEPROM
[ESC] - Return to previous Menu




Enter command:
```

Figure 2. Username/Password Management Menu

The following commands can be selected from the Username/Password Management Menu:

p **[Modify a Password]** Use the p command to change an existing password. After you choose the p command, a screen displays and prompts you to specify the user name for which you want to modify the password. When you successfully enter and verify the new password, a message appears and indicates that the password has been modified but not saved to EEPROM.

c **[Clear all Passwords]** Use the c command to remove the passwords for all three user names.

k **[Clear a Password]** Use the k command to clear an individual password for the Manager, Operator, or User user names.

w **[Save values to EEPROM]** Use the w command to save the changes to EEPROM.

Managing Source IP Addresses

The Source IP Addr. Access Control Menu (see Figure 3) is a submenu of the Service Security Menu. Use this menu to manage the NMM service port login IP addresses that use the Telnet Protocol. The NMM uses the source IP addresses in this list only to verify Telnet access.

If no IP addresses are specified in the Source IP Addr Access Control Menu, the version 2.0 agent permits any host IP address to establish a Telnet session with the NMM.

```
Source IP Addr. Access Control Menu


          Source IP Addr
Entry     Match Value                    Addr Mask
1         134.177.32.42                  255.255.255.255
2         121.110.10.0                   255.255.255.0
3         105.166.15.0                   255.255.0.0
4         126.0.0.0                      255.0.0.0
5         <empty>                        <empty>


m - Modify an Entry
c - Clear all Source IP Address
k - Clear a Source IP Address
w - Save values to EEPROM
[ESC] - Return to previous Menu

Enter command:
```

Figure 3. Source IP Addr Access Control Menu

The following commands can be selected from the Source IP Addr Access Control Menu:

m **[Modify an Entry]** Use the m command to change an existing source IP address and its associated mask. After you choose the m command, a screen displays and prompts you to specify the source IP entry for which you want to modify the address. When you successfully enter the new address and mask, a message appears and indicates that the information has been modified but not saved to EEPROM.

c **[Clear all Source IP Address]** Use the c command to remove all source IP addresses and masks from the list.

k **[Clear a Source IP Address]** Use the k command to remove an individual source IP address entry from the list.

w **[Save values to EEPROM]** Use the w command to save the changes to EEPROM.

Managing Telnet Access

The Telnet Access Management Menu (see Figure 4) is a submenu of the Service Security Menu. Use this menu to disable or enable Telnet support and to modify the inactivity timeout interval.

```
Telnet Access Management Menu



Telnet Service Menu Access:         <permitted>
Telnet Inactivity Timeout:          xxxxx (seconds)


t - Toggle Telnet Service Menu Access
i - Set Telnet Inactivity Timeout
w - Save values to EEPROM
[ESC] - Return to previous Menu









Enter command:
```

Figure 4. Telnet Access Management Menu

The following commands can be selected from the Telnet Access Management Menu:

t **[Toggle Telnet Service Menu Access]** Use the t command to enable or disable Telnet access to the service port. The Telnet Service Menu Access field displays <permitted> when Telnet is enabled or displays <disabled> when Telnet is disabled. When you change the status, a message appears and indicates that the information has been modified but not saved to EEPROM.

i **[Set Telnet Inactivity Timeout]** Use the i command to change the Telnet inactivity timeout value. The Telnet Inactivity Timeout field displays the timeout value in seconds when the timer is enabled, or the field displays <disabled> when the timer is disabled. To disable the timer, enter a value of 0 (zero). When you successfully enter a new value, a message appears and indicates that the information has been modified but not saved to EEPROM.

w **[Save values to EEPROM]** Use the w command to save changes to EEPROM.

Using the Authentication and Access Control Checking Option

The Toggle Authentication & Access Control Checking option on the Service Security Menu (see Figure 1 on page 2) allows you to control which IP addresses have access to the service port menus.

When the Toggle Authentication & Access Control Checking option (command c) is toggled off and Telnet is enabled, it is possible for any IP address to establish a Telnet session with the NMM. Under this scenario, the Telnet session has priority over the service port and the following message is displayed at the service port:

```
Local access blocked by remote Telnet session. Enter CTRL ^B to abort the
remote session.
```

Enter Ctrl+B to disconnect the Telnet session and to reestablish an active session at the console. You can prevent a Telnet session from interrupting an active session at the console by toggling on the Toggle Authentication & Access Control Checking option (command c) from the Service Security Menu.

When the Toggle Authentication & Access Control Checking option is toggled on, only the IP addresses that are specified on the Source IP Addr Access Control Menu can establish a Telnet session with the NMM. An authorized IP address can also establish a Telnet session with the NMM after the console user has physically

logged out of a session or the console logs out itself when it reaches the value of the inactivity timer. If an attempt is made to initiate a Telnet session while the console session is still active, the following message is displayed at the service port:

```
Telnet (<remote IP>) session is rejected-local console busy
```

If an attempt is made to initiate a Telnet session from an unauthorized user, the following message is displayed at the console port:

```
Telnet (<remote IP>) is terminated due to non-allowed source IP address
```

To prevent an unwanted Telnet user from accessing the console port menus, Bay Networks recommends that you specify the IP addresses that can access the console port menus in the Source IP Addr Access Control Menu. Otherwise, if the IP addresses are not specified and the authentication and access control checking feature is on and Telnet is enabled, it is possible for any Telnet user who knows the passwords associated with the Manager, Operator, or User user names to connect to the service port.

Telnet Support

This feature enables a remote user to log in to the service port menus of the NMM from a remote terminal using a standard Telnet interface. Telnet, the Internet standard protocol for remote terminal connection service, allows you to access all service port functionality from a remote client. The remote terminal connects to the well-known port for Telnet (UDP 23) on the NMM. When a Telnet session is established, the local service port on the NMM is temporarily disabled until the Telnet session is disconnected.

Logging In to Telnet

By default, access through Telnet is enabled at the factory. A successful Telnet login or a failed Telnet login results in an informational message displayed at the service port screen.

Starting Telnet

To use Telnet, you must have a Telnet application on your workstation. Refer to your Telnet documentation for information about how to start a Telnet session. Only one Telnet session can be active at a time.

Note: To avoid having a remote Telnet session log in and take control over the console port session, Bay Networks recommends that you toggle on the Toggle Authentication & Access Control Checking feature (command c) from the Service Security Menu.

To start a Telnet session from a UNIX or PC Telnet-capable workstation, type the "Telnet <NMM IP>" command at the pound sign (#) or percentage symbol (%). For example:

```
# telnet 10.160.2.102
```

Logging Out of Telnet

If you do not manually exit the user interface session, it will end automatically after 10 minutes of idle time; then the following message will appear at the console port:

```
Telnet (<remote IP>) is terminated due to inactivity
```

Beginning with the version 2.0 agent, you can change the inactivity timeout value using the i command [Set Telnet Inactivity Timeout] from the Telnet Access Management Menu.

RMON2 Support

The version 2.0 NMM agent supports the Internet Engineering Task Force (IETF) standard for remote network monitoring version 2 (RMON2) as defined in RFC 2021.

Model 281xSA and 331xSA Ethernet NMM Agent version 2.0 with 4 megabytes (MB) or more of dynamic random access memory (DRAM) support the following RMON2 groups:

- protocolDir
- protocolDist
- addressMap
- nlHost
- nlMatrix
- probeCapability

Accessing the RMON Support Menu

Choose command d from the NMM Main Menu to display the RMON Support Menu. This menu appears and indicates the amount of DRAM installed. It also indicates which RMON level is enabled or disabled.

Note: To enable the RMON2 features in the version 2.0 NMM agent, Bay Networks recommends that you use 4 or 8 MB of memory DRAM to support RMON2; otherwise, RMON2 features are disabled.

Bay Networks has qualified the following SIMM modules and recommends their use with Bay Networks NMMs (see Table 1).

Table 1. Recommended SIMM Modules

Part Description	Mfg. Part Number	Manufacturer
IC DRAM 1Mx32 70ns AU SIMM32 4MB	MH1M32ADJ-7	Mitsubishi
	MCM32130SHG70	Motorola
	MT8D132G-7	Micron
	TM124BBK32-70	TI

Table 1. Recommended SIMM Modules (continued)

Part Description	Mfg. Part Number	Manufacturer
IC DRAM 2Mx32 70ns AU SIMM32 8MB	HB56D232BS-7A	Hitachi
	MH2M32EJ-7	Mitsubishi
	MCM32230SHG70	TI
	TM248CBK32B-70	Motorola
	MT16D232G-7	Micron

Compatible Firmware Versions

The Model 281xSA and 331xSA Ethernet NMM Agent version 2.0 requires the following compatible firmware versions:

- Model 281xSA version 2.0 requires version B firmware.
- Model 331xSA version 2.0 requires version A or later firmware.

Trap Filtering Support

This feature allows you to enable or disable the generation of Simple Network Management Protocol (SNMP) trap protocol data units (PDUs). You can enable or disable a trap individually or as a group. To access the Main Trap Management Menu, choose command m from the Main Menu.

From the Main Trap Management Menu (as shown in Figure 5), you can access a submenu for each of the following trap groups:

- Lattis Secure traps
- Chassis traps
- Chassis - Power Supply traps
- Ethernet traps
- Bridge traps
- Router traps
- SNMP Generic traps
- RMON traps

```
Main Trap Management Menu




l - Lattis Secure             traps menu
c - Chassis                   traps menu
d - Chassis - Power Supply    traps menu
e - Ethernet                  traps menu
b - Bridge                    traps menu
o - Router                    traps menu
s - SNMP Generic              traps menu
r - RMON                      traps menu
[Esc] - Return to previous Menu

Enter command:
```

Figure 5. Main Trap Management Menu

The following commands can be selected from the Main Trap Management Menu:

l **[Lattis Secure traps menu]** Use the l command to enable or disable Authorization Violation Traps and Lattis Secure Init Required Traps.

c **[Chassis traps menu]** Use the c command to enable or disable the following traps:

- Board Hot - Swap Traps
- Board Led Failure Traps
- Flash Upgrade Failure Traps

d **[Chassis - Power Supply traps menu]** Use the d command to enable or disable the following traps:

- Redn PS Summ Diode Failure Traps
- Board PS Failure Traps
- Chassis PS Failure Traps
- Chassis Fan Failure Traps
- Redn PS + 5v Current Exceed Traps

- Redn PS + 12v Current Exceed Traps
- Redn PS Ambien Temp Stat Chg Traps

e **[Ethernet traps menu]** Use the e command to enable or disable the following traps:

- Port Auto - Partitioned Traps
- Port DTE Jabbering Traps
- Repeater Health Traps
- Repeater Group Change Traps
- Ethernet Threshold Exceeded Traps
- NMM SaturationA Traps
- Redundant Bad Remote Config Detected Traps
- Ethernet Channel Change Traps
- Redundant Port Switchover Traps

b **[Bridge traps menu]** Use the b command to enable or disable the following traps:

- Local Brdg Diag Traps
- Local Brdg Op Chg Traps
- Remote Brdg Port Op Diag Traps
- Remote Brdg Diag Traps
- Remote Brdg Op Chg Traps

o **[Router traps menu]** Use the o command to enable or disable Router Operation Changed Traps and Router Diag Traps.

s **[SNMP Generic traps menu]** Use the s command to enable or disable the following traps:

- Cold-Start Traps
- Authentication Failure Traps

r **[RMON traps menu]** Use the r command to enable or disable the following traps:

- Rising Alarm Event Traps
- Falling Alarm Event Traps

You also can selectively enable and disable individual traps from the configuration file. The following is an example of the Trap Filtering section that has been added to the configuration file:

```
################ TRAP ENABLE/DISABLE ##########################
#
# To selectively enable or disable individual trap PDUs generated
# by the platform, uncomment out the line and indicate
# "enable" or "disable" for the indicated traps.
#
# Example:
# Trap_Snmp_coldStart            enable   #enable SNMP cold start traps
# Trap_Snmp_coldStart           disable  # disable SNMP cold start traps
#
#
# Trap_Chassis_boardSwap                                enable
# Trap_Chassis_boardLEDFailure                          enable
# Trap_Chassis_flashUpdateFailure                       enable
# Trap_Chassis_chassisPowerSupplyFailure                enable
# Trap_Chassis_chassisFanFailure                        enable
# Trap_Chassis_boardPowerSupplyFailure                  enable
# Trap_Chassis_redPsPlus5vCurrentExceed                 enable
# Trap_Chassis_redPsPlus12vCurrentExceed                enable
# Trap_Chassis_redPsAmbientTempStatChg                  enable
# Trap_Chassis_redPsSummingDiodeFailure                 enable
# Trap_Snmp_coldStart                                   enable
# Trap_Snmp_authenticatedFailure                        enable
# Trap_Rmon_risingAlarm                                 enable
# Trap_Rmon_fallingAlarm                                enable
# Trap_Enet_portAutoPartition                           enable
# Trap_Enet_portDTEJabbering                            enable
# Trap_Enet_rptrHealth                                  enable
# Trap_Enet_rptrGroupChange                             enable
# Trap_Enet_enetThreshExceeded                          enable
# Trap_Enet_nmmSaturationA                              enable
# Trap_Enet_redunBadRemCfgDetected                      enable
# Trap_Enet_enetChannelChange                           enable
# Trap_Enet_redundPortSwitchover                        enable
# Trap_Enet_remoteBrigdePortOperationDiagnostic         enable
# Trap_Enet_remoteBrigdeDiagnostic                      enable
# Trap_Enet_remoteBrigdeOperationChanged                enable
```

```
# Trap_Enet_localBrigdeOperationChanged              enable
# Trap_Enet_localBrigdeDiagnostic                    enable
######## 2k/3k Ethernet Router Traps
# Trap_Enet_routerOperationChanged                   enable
# Trap_Enet_routerDiagnostic                         enable
######## 2k/3k Ethernet Platform Trap
# Trap_Enet_AuthorizationViolation                   enable
# Trap_Enet_LattisSecureInitRequired                 enable
#
```

OpenBay Module Support

The Model 331xSA Ethernet NMM software version 2.0 supports the OpenBay System 3000 module Application Server Model (AMS) by detecting the presence of the ASM in the same chassis and reporting it to Optivity.

Supported MIBs

The following MIBs are supported in the version 2.0 agent:

- RFC 1213 (MIB II)
- RFC 1215 (SNMP Generic Trap MIB)
- RFC 1516 (SNMP Repeater MIB)
- RFC 1757 (RMON MIB)
- RFC 1398 (EtherLike MIB)
- RFC 1515 (MAU MIB)
- RFC 2021 (RMON 2 MIB)
- RMON Trap MIB
- IPX MIB
- SynOptics® Root MIB
- SynOptics Common MIB
- SynOptics Ethernet MIB
- SynOptics Common Trap MIB
- SynOptics Ethernet Trap MIB
- SynOptics RMON Extensions MIB

Known Problems

The following problems are known to exist in version 2.0 of the agent:

- A polling interval of less than 5 seconds on etherHistoryUtilization in the RMON history table causes erratic results at higher traffic rates. Bay Networks recommends that polling intervals be set no less than 5 seconds.
- The front panel utilization display of the NMM does not update if more than 50 percent of network traffic is 64-byte packets.
- When the service port is updating, the agent will not respond to ping or SNMP requests. The solution for this problem is to minimize the amount of time spent using the service port.
- The s3EnetPortShortEvents are not counted properly because the hardware has difficulty tagging short events (packets smaller than 64 bytes having invalid CRC).
- An SNMP cold start trap cannot be disabled.
- Sometimes when the console disconnects a Telnet session, it will report that the remote Telnet session timed out after the Telnet idle timeout.
- Autotopology™ can sometimes be disrupted with older agents on the same network. To ensure that the Autotopology feature works properly, be sure that all agents are upgraded to the levels listed (see Table 2).

Table 2. Autotopology compatibility

Device	Agent versions
5310A/SA	1.5.0 or later
5DN310	1.5.0
BayStack™ 10 MB	1.4.0
BayStack 100 MB	1.1.1
28200	1.4.0
28115, 28104	1.4.0
58000	1.4.1

- When doing a reset on a Model 281xSA or Model 331xSA Ethernet NMM from Optivity® Network Management Software an SNMP response to reset is never returned from the hub even though the reset took place.

- When a Model 3410 Ethernet NMM is installed in a chassis containing a Model 3314SA Ethernet NMM running a version 1.5.2 software agent, the Model 3314SA Ethernet NMM will repeatedly send out power supply fail traps.
- DesignMan™ causes the Model 331xSA Ethernet NMM to lose connectivity with the network.
- Subnet masks are not being saved properly to NVRAM on Model 281xSA and 331xSA Ethernet NMMs during bootup.
- After restarting a Model 281xSA or 331xSA Ethernet NMM with threshold settings in the configuration file, the threshold values do not function until a period of time had passed.
- After the download of a Model 281xSA or 331xSA Ethernet NMM agent the following error message might appear: “ERROR Address contains subnet value that is inconsistent with NMM’s IP subnet value.” This problem happens when the configuration file contains a subnet mask that is different from the stored subnet mask.

New Configuration File

This section contains a sample NMM configuration file for the version 2.0 agent. Use any ASCII text editor, such as vi, to modify the sample file or to create a new configuration file. This file is used for both the Model 281xSA and 331xSA NMM.

Blank lines are ignored, and lines beginning with the pound sign character (#) are considered comments. You can modify the file by inserting new lines according to the examples shown in the file or by removing the comment character from an appropriate line and editing the line.

Caution: Always make a backup copy of the NMM configuration file to use as a reference before editing the NMM configuration file.

```
# Specify file name for the NMM image file.  NOTE this has to be
# the first un-commented line in this file for the NMM to load properly.
# For example:
331sa200.img
281sa200.img
# Assign local subnet mask for this NMM.
# Default for Class A NMM IP Address is 255.0.0.0.
# Default for Class B NMM IP Address is 255.255.0.0.
# Default for Class C NMM IP Address is 255.255.255.0.
# For example:
#netmask 255.255.255.0
#
# Specify the primary default router for this NMM.
#default-router xxx.xxx.xxx.xxx
# For example:
#default-router 0.0.0.0
#
# Specify the secondary default router for this NMM.
#secondary-default-router xxx.xxx.xxx.xxx
#
# Specify the router address for this NMM's TFTP request.
#boot-router xxx.xxx.xxx.xxx
#
# Enable or disable the automatic discovery of available default
# router(s).  Valid entries are on and off.  Default is on.
# For example:
#ping-router on
#
# Specify the time interval of pinging router(s) in seconds.
```

```
# Maximum number is 42,949,672 seconds. (approximate 497 days)
# Default/ minimum time is:
#ping-time 60
#
# Specify the Novell network number for this NMM. Must be exactly
# eight hexadecimal digits.
#network-number 00000000
#
# Indicate baud rate used for the RS-232 out-of-band port. Valid entries
are
# 300, 1200, 2400, 4800 and 9600 baud.
# Default is:
#baud-rate 9600
#
# Enter the NMM's initialization string used for out-of-band
communication.
# For example:
#initialization-string ATDT,9,1,415-555-1212
#
# Specify the concentrator's location (64 characters max.).
# For example:
#location Building A
#
# Specify the concentrator's name (64 characters max.).
# The default string is SYNOPTxxyyzz, where xxyyzz represents the
# last 3 bytes of this NMM's hexadecimal MAC address.
# For example:
#sysname concA.abcCompany.com
#
# Specify the name & phone number of the concentrator's administrator
# or contact person (64 characters max.).
# For example:
#syscontact John Smith - Network Administrator - ext 5555
#
# Specify the community string used for read only operations. Specifying
# no community string will default to public for read only objects.
# For example:
#read-community public
#
# Specify the community string used for read and write operations.
# Specifying no community string will default to private for read and
# writeable objects.
# For example:
#write-community private
#
# Enter the list of IP trap receivers along with their community strings
# and ageout times, in seconds. The maximum number is 42,949,672 seconds
```

```
# (approx 497 days). Specifying no ageout time defaults to indefinite
time.
# Specify only one entry pair per line, up to a maximum of 10 entries.
# For example:
#ip-trap-receiver xxx.xxx.xxx.xxx trap-community public 9000
#
# Enter the list of IPX trap receivers along with their community strings
# and ageout times, in seconds. The maximum number is 42,949,672 seconds
# (approx 497 days). Specifying no ageout time defaults to indefinite
time.
# Specify only one entry pair per line, up to a maximum of 10 entries.
# Entry format is:
# <Novell network #>:<Novell Host #> trap-community <community string>
<ageout time>
# Note that <Novell network #> contains 8 hexadecimal numbers and <Novell
Host #>
# contains 12 hexadecimal numbers.
# For example:
#ipx-trap-receiver abcdefab:123456789012 trap-community public 9000
#
# Enable or disable the use of authentication traps. Valid entries are
# on and off. Default is on.
# For example:
#authentication-traps on
#
# Enable or disable concentrator retiming.
# Valid entries are on and off. Default is on.
# The 281xSA NMM does not have this keyword.
# For example:
#retiming on
#
# Specify the image load mode for this NMM. Valid choices are
# remote-only, local-only or remote-with-local-backup.
# For example:
#image-load-mode remote-only
#
# Specify the config load mode for this NMM. Valid choices are
# remote-only, local-only or remote-with-local-backup.
# For example:
#config-load-mode remote-only
#
# Specify the boot mode for this NMM. network configures the
# NMM to use the network for remote loading of the NMM's
# configuration information. eeprom configures the NMM to use
# data stored in NVRAM for local loading. Default is eeprom.
# For example:
#boot-mode eeprom
#
```

```
# Specify the management protocol for this NMM. Valid choices are
# IP_IPX, IP, and IPX. Default is IP_IPX.
# For example:
#management-protocol IP_IPX
#
# Specify the boot protocol for this NMM. Valid choices are
# AUTO, IP, IPX, and IP_IPX. Default is AUTO.
# For example:
#boot-protocol AUTO
#
# Save configuration data to NVRAM.
#save-to-eeprom
#
# Specify time interval of traps sent out for existing predefined
# conditions. The valid range is 10 to 3600 seconds, in 10 second
# increments. Default is 10 seconds.
# for example:
#trap-interval 10
#
# Specify the lifetime of a node list entry in seconds.
# Maximum number is 42,949,672 seconds (approximate 497 days).
# Default is 900 seconds.
# For example:
#portlife 900
#
# Specify the lifetime of a traffic matrix entry in seconds.
# Maximum number is 42,949,672 seconds (approximate 497 days).
# Default is 1200 seconds.
# For example:
#trflife 1200
#
# Specify how many nodes are allowed to associate with a particular port.
# Default is 800 for 281xSA and 331xSA.
# For example:
#max-nodes-per-port 800
#
# Specify allowed nodes for this NMM. Specify only one entry per line.
# The format is:
#node AABBCCDDEEFF slot# port#
# Where AABBCCDDEEFF is the hexidecimal MAC address with 12 hex digits.
# slot# and port# are decimal numbers.
# For example:
#node 013489ABCDEF 1 6
#node abcdef987654 2 5
#node 000081111111 2 6
#node 000082222222 2 7
#node 000083333333 2 8
#
```

```
# "Wild card" notation:
# If slot# or port# is either 0 or blank, that entry will be treated
# as a wild card.
# For example, this wild card entry specifies all ports associated
# with the concentrator:
#node 1234567890ab
# This wild card entry also specifies all ports associated
# with the concentrator:
#node 1234567890ab 0 0
# This wild card entry specifies all ports associated with slot 5
# in this concentrator:
#node 234567890abc 5 0
#
# Enable allowed nodes and set the security level to be used
# when the system is up. Security can be set at either concentrator,
# slot, or port level. System default is OFF for allowed nodes
# features; to enable allowed nodes, uncomment the appropriate line.
# For example:
#allow-on conc
#allow-on slot
#allow-on port
#
# Specify the action to be taken when a node security violation occurs.
# Actions can be specified for violations at the port, slot, or
concentrator
# level. Format are
#         port slot# port# action#
#         slot slot# action#
#         conc action#
# Where slot#, port#, action# are all decimal numbers.
# For action#, valid choices are 2, 3, 4, or 5.
# 2 = no_action;
# 3 = send_trap_only;
# 4 = partition_port_only;
# 5 = send_trap_and_partition_port;
#
# This port-level example is used to check slot 5, port 11.
# If address violation occurs, send trap only.
#port 5 11 3
# This port-level example is used to check slot 4, port 12.
# If address violation occurs, do nothing.
#port 4 12 2
# This port-level example is used to check slot 2, port 3.
# If address violation occurs, send trap and partition port.
#port 2 3 5
#
# This slot-level example is used to check slot 5 and
# partition that port if address violation occurs.
```

```
#slot 5 4
# This slot-level example is used to check slot 3 and
# send trap and partition that port if address violation occurs.
#slot 3 5
#
# This concentrator-level example is used to check
# entire concentrator. If address violation occurs,
# send a trap and partition the port to which the concentrator
# is connected.
#conc 5
#
# Specify MAC address auto-learn mode for a LattisSecure port.
# one-shot-auto-learn configures the LattisSecure port to learn
# the first MAC address pass through this port. continuous-auto-learn
# configures the LattisSecure port to continuously learn the MAC
# address pass through this port.
# LattisSecure is not supported by 281xSA.
# The format is:
#    learn-mode slot# port# auto-learn-mode
# Where slot# and port# are decimal numbers.
# Default is no auto-learn for all ports in LattisSecure module.
# For example:
#learn-mode 6 1 one-shot-auto-learn
#
# Enable or disable eavesdropping protection for a LattisSecure port.
# Format of the command:
#      eavesdropping-protection slot# port# <on | off>
# Where slot# and port# are decimal numbers.
# Default is off for all ports in LattisSecure module.
# LattisSecure is not supported by 281xSA.
# For example:
#eavesdropping-protection 6 12 off
#
# Lock/Unlock security configuration. Valid entries are on and off.
# Default is off.
# For example:
#security-config-lock off
#
# Add an entry to the threshold table.
# Format of the command:
# threshold IN OB SL PO TY CN SV AC DU
# IN = index, for 331xSA from 1 to 288, inclusive
#             for 281xSA from 1 to 160, inclusive
# OB = object, which is one of the following:
#    conc     Threshold is set for a concentrator
#    slot     Threshold is set for a slot
#    port     Threshold is set for a port
# SL = slot number, for 3000 concentrator from 1 to 12, inclusive
```

```
#                   for 3030 concentrator from 1 to 4, inclusive
#                   for 281xSA concentrator from 1 to 5, inclusive
# PO = port number, for 3000/3030 concentrator from 1 to 24, inclusive
#                   for 281xSA concentrator from 1 to 17, inclusive
# TY = type, which is one of the following:
#    good-bytes
#    good-packets
#    bad-packets
#    crc-error-packets
#    misaligned-packets
#    runt-packets
#    fragments
#    too-long-packets
#    collisions
#    late-collisions
#    link-status
#    multicast-packets
#    broadcast-packets
#    short-events
#    source-address-changes
#    data-rate-mismatches
#    network-errors
#    backoff-errors
#    bad-to-good-packets-ratio
#    network-errors-to-good-packets-ratio
#    collisions-to-good-packets-ratio
# CN = condition, which is one of the following, depending on TY:
#    cross       Trigger alarm when actual-value crosses set-value
#    over        Trigger alarm when actual-value is greater than
set-value
#    over-rate   Trigger alarm when actual-value/second is greater than
#                set-value/second
#    link-on     Trigger alarm when port link status is on
#    link-off    Trigger alarm when port link status is off
#    over-ratio  Trigger alarm when actual-value (ratio type only) is
#                greater than set-value
# SV = set value, which can be an absolute number or a rate per second
# AC = action, which is one of the following:
#    trap-only            Send trap only
#    partition-slot       Partition a slot, specified by SL
#    partition-port       Partition a port, specified by SL and PO
#   trap-partition-slot  Send trap and partition a slot, specified by SL
#  trap-partition-port  Send trap and partition a port, specified by SL
#                        and PO
# DU = Duration in seconds of period during which threshold is monitored
#
# Sample threshold table entries:
# This sample threshold table entry is number 6 in the table.
```

```
# It counts CRC error packets for a concentrator. When the number
# of CRC errors in 10 second goes over 1000, it sends a trap.
#threshold 6 conc 0 0 crc-error-packets over 1000 trap-only 10
#
# This sample threshold entry is number 2 in the table.
# It checks slot 3 for 200 good bytes in 10 seconds. When the counter
# crosses 200, it sends a trap and partitions the slot.
#threshold 2 slot 3 0 good-bytes cross 200 trap-partition-slot 10
#
# Enable or disable automatic network topology build-up.
# Valid entries are on and off. Default is on.
# For example:
#hello-message on
#
################ TRAP ENABLE/DISABLE ##########################
#
# To selectively enable or disable individual trap PDUs generated
# by the platform, uncomment out the line and indicate
# "enable" or "disable" for the indicated traps.
#
# Example:
# Trap_Snmp_coldStart            enable   #enable SNMP cold start traps
# Trap_Snmp_coldStart           disable  # disable SNMP cold start traps
#
#
# Trap_Chassis_boardSwap                                enable
# Trap_Chassis_boardLEDFailure                          enable
# Trap_Chassis_flashUpdateFailure                       enable
# Trap_Chassis_chassisPowerSupplyFailure                enable
# Trap_Chassis_chassisFanFailure                        enable
# Trap_Chassis_boardPowerSupplyFailure                  enable
# Trap_Chassis_redPsPlus5vCurrentExceed                 enable
# Trap_Chassis_redPsPlus12vCurrentExceed                enable
# Trap_Chassis_redPsAmbientTempStatChg                  enable
# Trap_Chassis_redPsSummingDiodeFailure                 enable
# Trap_Snmp_coldStart                                   enable
# Trap_Snmp_authenticatedFailure                        enable
# Trap_Rmon_risingAlarm                                 enable
# Trap_Rmon_fallingAlarm                                enable
# Trap_Enet_portAutoPartition                           enable
# Trap_Enet_portDTEJabbering                            enable
# Trap_Enet_rptrHealth                                  enable
# Trap_Enet_rptrGroupChange                             enable
# Trap_Enet_enetThreshExceeded                          enable
# Trap_Enet_nmmSaturationA                              enable
# Trap_Enet_redunBadRemCfgDetected                      enable
# Trap_Enet_enetChannelChange                           enable
# Trap_Enet_redundPortSwitchover                        enable
```

```
# Trap_Enet_remoteBrigdePortOperationDiagnostic       enable
# Trap_Enet_remoteBrigdeDiagnostic                    enable
# Trap_Enet_remoteBrigdeOperationChanged              enable
# Trap_Enet_localBrigdeOperationChanged               enable
# Trap_Enet_localBrigdeDiagnostic                     enable
######## 2k/3k Ethernet Router Traps
# Trap_Enet_routerOperationChanged                    enable
# Trap_Enet_routerDiagnostic                          enable
######## 2k/3k Ethernet Platform Trap
# Trap_Enet_AuthorizationViolation                    enable
# Trap_Enet_LattisSecureInitRequired                  enable
#
# Specify the maximum number of hosts will be collected on an interface
# on behalf of each RMON hostControlEntry. The valid range is
# [100, 2048]. Default is 100.
# For example:
#rmon-max-host 100
#
# If this keyword is present, the agent will automatically setup RMON
host
# control entries for all interface(s) present on the NMM at system
startup
# time. This keyword does not require any parameter. Default is off.
rmon-dflt-host
#
# If this keyword is present, the agent will automatically setup RMON
matrix
# control entries for all interface(s) present on the NMM at system
startup
# time. This keyword does not require any parameter. Default is off.
rmon-dflt-matrix
RMONMaxHost 500
RMON2_MaxConversations   1000
RMON2_MaxHosts   1000
RMON1_MaxConversations   100
RMON1_MaxHosts 100
RMON1_CreateHostAtStartup
RMON1_CreateMatrixAtStartup
RMON2_CreateMatrixAtStartup
RMON2_CreateHostAtStartup

#------------ The following Section is for 281xSA only ---------
#
# Configure the Software Redundant Links
#
# Basic format is
#
# 2k-sw-red ActiveSlot ActivePort StandbySlot StandbyPort
```

```
#
# Maximum number of Software Redundant Links that may be set up is 4
#
# When link-based redundant links are specified in this config file, it
may
# be done in one or multiple lines. However, if multiple lines are used,
# every new line must start with the key word "2k-sw-red". A redundant
# pair may also not be split into different lines; it must be defined
# completely in the same line.
#
# Legal examples are:
# 2k-sw-red 1 2 3 4-one pair in one line
# 2k-sw-red 1 2 3 4 2 1 4 3             - two pairs in one line
# 2k-sw-red 1 2 3 4 2 1 4 3 5 1 5 6 4 4 4 17- four pairs in one line
#
# 2k-sw-red 1 2 3 4- three pairs in two lines
# 2k-sw-red 1 2 3 4 2 1 4 3
#
# 2k-sw-red 1 2 3 4 -
# 2k-sw-red 2 1 4 3 - three pairs in 3 lines
# 2k-sw-red 5 1 5 6
```

Related Publications

For more information about using the Model 281xSA or Model 331xSA Ethernet NMM, refer to the following documentation:

- *Using the Model 281xSA Ethernet Hub* (Bay Networks part number 893-743-A)
- *Using the Model 331xSA Ethernet Network Management Module* (Bay Networks part number 893-744-A)

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone -- U.S./Canada: 888-422-9773
- Phone -- International: 510-490-4752
- Fax -- U.S./Canada and International: 510-498-2609

This document is also available in PDF format on the World Wide Web at *support.baynetworks.com/library/tpubs*. Click on the Hubs category, and choose either the System 2000™ Documentation or System 3000™ Documentation category. From either category menu, choose the Release Notes and Upgrade Instructions sub category.