Release Notes for the Model 281xSA and 331xSA NMM Version 1.5.2 Agent

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Part No. 896-075-E
June 1996

Bay Networks

896-075-E

Trademarks

SynOptics and Optivity are registered trademarks of Bay Networks, Inc. Autotopology, Bay Networks, Bay Networks Press, Optivity LAN, Optivity Campus, System 3000, Expanded View, OmniView and LattisWorks 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 Ethernet agent version 1.5.2 for Model 281xSA hubs and Model 331xSA Network Management Modules (NMMs). Thy highlight the additions and changes from the version 1.3.x agent. For more information about these products, refer to the documentation shipped with them. To obtain the agent software, refer to your Bay Networks™ Support Services Plan and then contact your local sales office.

These release notes cover the following topics:

- Product enhancements
- Compatible firmware versions
- Previous features
- Supported MIBs
- Bug fixes
- Known problems
- New configuration file
- Operational notes
- Out-of-band connection
- Related publications and ordering information

Version 1.5.2 Product Enhancements

Version 1.5.2 of the agent software is compatible with the System 3000™ Fast Ethernet (100BASE-T) backplane. To manage the System 3000 Fast Ethernet host modules, you must purchase Model 3410 NMM agent software version 1.1.0. For more information about the System 3000 Fast Ethernet products, refer to the documentation shipped with the products.

Compatible Firmware Versions

Ethernet agent version 1.5.2 for Model 281xSA and 331xSA NMMs requires the following compatible firmware versions:

- Model 281xSA version 1.5.2 requires version B or C firmware.
- Model 331xSA version 1.5.2 requires version A or B firmware.

Previous Features

This section lists the new features that appear in version 1.5.0 and 1.5.1 agents.

Event Action Support

The RMON Event Action extensions of the version 1.5.0 and later agents provide a powerful mechanism unavailable with standard RMON probes. Standard RMON Events are only able to send a Simple Network Management Protocol (SNMP) trap and/or log the event to the NMM. The Event Actions tables allow a variety of actions to be taken. The supported event actions are:

- no action
- trap
- log
- trap and log
- partition
- unpartition

Expression Threshold Support

An important new feature of the version 1.5.0 and later agents is that they allow you to create thresholds that are based on the evaluation of mathematical expressions. These expressions can include one or more integer-based MIB variables. You can create these expressions using the Custom Threshold window of Optivity® Threshold Manager. Combined with the event action capabilities, expression thresholds provide an extremely useful tool for proactive network management.

Furthermore, new statistics collection features allow the agent to compute such statistics as the average, minimum, and maximum of a sample over a user-defined period of time. The statistics computation can be performed for expressions as well as for standard RMON alarms set on RMON, proprietary, or other standard MIB objects.

On the 281xSA and 331xSA NMMs, the 1.5.0 and later agents allow a choice of thresholding methods while migrating to standard RMON Alarms and Event based thresholds. Proprietary (BNET) thresholds are still set and maintained with Optivity, or through a NMM's configuration file; standards-based RMON Alarms and Events are set with the redesigned RMON threshold GUI available in Optivity LAN™ 7.0. Expression thresholds are set using the new Custom Threshold features of Optivity LAN 7.0.

Threshold NVRAM Storage

The version 1.5.0 and later agents allow you to save RMON thresholds and expression thresholds into nonvolatile RMA (NVRAM), so that the user-defined threshold configuration of the NMM can be restored after a system reset or reboot.

RMON Threshold Storage

Up to 19 RMON alarms, and their associated 38 events and 38 event actions, can be saved to NVRAM.

Expression Threshold Storage

Like RMON thresholds, expression thresholds can also be stored in NVRAM. The number of expression thresholds that can be stored depends on the size and complexity of the expression. For example:

- For the largest allowable expressions (295 bytes each; includes 5 to 7 MIB objects), up to 6 entries can be saved.
- For medium-sized expressions (130 bytes each; includes 3 to 4 MIB objects), up to 15 entries can be saved.
- For small expressions (70 bytes each; includes 2 to 3 MIB objects), up to 28 entries can be saved.

In addition to saving expression thresholds to NVRAM, you can also use the Optivity network management software to create a profile of the entire threshold configuration. By restoring this profile to the NMM after a reboot, you can easily restore any thresholds that are not saved to NVRAM.

Saving Thresholds to NVRAM

There are four ways to write RMON and expression thresholds to NVRAM:

- Using Threshold Manager—from the Threshold Summary Table window, go to the Tools menu and choose Save to NVRAM. See your Optivity documentation for more information.
- Using the Expanded View™ application—click the right mouse button on the NMM; a menu appears. Click the right mouse button on Configuration; a submenu appears. Choose save configuration to save the thresholds.
- Using a MIB Browser—set the MIB object s3AgentWriteEeprom to writeEeprom(2).
- Using the service port—use the "-w" selection of the service port's main menu to save the thresholds to NVRAM.

Saving BNET Proprietary Thresholds

Because of the NVRAM requirements of the new RMON and expression threshold storage features, the older BNET proprietary thresholds cannot be saved to NVRAM with version 1.5.0 and later agents. However, you can still continue to create and use the BNET proprietary thresholds without saving them to NVRAM. These thresholds will be restored after each reboot of the NMM if they are defined in the NMM configuration file, and the configuration load mode is set to remote.

Supported MIBs

The following MIBs are supported in version 1.5.2 and later agents:

- 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)
- RMON Trap MIB
- IPX MIB, version 1.1.0
- SynOptics® Root MIB, version 1.4.1
- SynOptics Common MIB, version 4.7.4
- SynOptics Ethernet MIB, version 4.6.0
- SynOptics Common Trap MIB, version 1.4.0
- SynOptics Ethernet Trap MIB, version 1.4.0
- SynOptics RMON Extensions MIB, version 1.0.6 (snpxEventActTable supported)

Bug Fixes

This section contains bug fixes that have been incorporated in recent releases of the Model 281xSA and 331xSA Ethernet agents.

Version 1.5.2

The following bugs were fixed in version 1.5.2:

- Creating an entry on the snpxExprTable no longer creates a second (zero value) entry on the snpxAlarm StatsTable [Bug ID 20537].
- Entering an expression with a divide by zero on the snpxExprTable no longer generates the message “snpxExpr: Attempt to divide by zero! returning dummy result zero” on the console.

Version 1.5.1

Version 1.5.1 fixes a bug found in version 1.5.0 that caused problems in the Expanded View Optivity application. Expanded view would not work when attempted on a Model 281xSA or 331xSA NMM. The problem was that an SNMP get request would fail on the MIB objects that retrieve the Default Gateway, Secondary Default Gateway, and Boot Router:

- s3AgentDefaultGateway
- s3AgentSecDefaultGateway
- s3AgentBootRouter

This problem was also reflected in Optivity Campus™ by the inability to display the Configuration-->Show Boot Profile menu from the NMM Slot menu options. No other Optivity Campus applications appear to have been affected. [Bug ID 17742]

Version 1.5.0

The following problems were corrected in the version 1.5.0 agent:

- The version 1.3 agent would not send the correct threshold exceeded trap. This is fixed in version 1.5.0 and later. [Bug ID 8393]
- When its router was downed, the version 1.3 agent would spend so much time ARPing the downed router that it would respond slowly to SNMP requests. This would cause OmniView™ to perform poorly while updating its information. Versions 1.5.0 and later fix this bug by changing the default interval between ARP requests. Previously, the NMM would ARP the router 5 times every 10 seconds; in versions 1.5.0 and later the NMM ARPs the router 3 times every 60 seconds. [Part 1 of bug ID 2981]
- With previous agent versions, board LED failure traps were sent regarding boards on other segments within the chassis. This was caused by the NMMs not being downloaded in the other segments. This problem is fixed in versions 1.5.0 and later, which only send board failure traps regarding boards on the same segment within the NMM that have legitimately failed. [Part 2 of bug ID 2981]
- With previous agent versions, collision counters for the dot3Stats table were always zero, even when there had been collisions. This problem is fixed in versions 1.5.0 and later, which correctly updates the dot3Stats table when collisions occur. [Bug ID 2980]
- With previous agent versions, the utilization rate displayed on the LEDs on the front panel of the NMM would not match the value of etherHistoryUtilization. The reason for this was a slight difference between the ways the two utilization rates were calculated. This problem is fixed in versions 1.5.0 and later, which calculate both utilization rates with the formula specified in RFC 1757. [Bug ID 2978]
- With previous agent versions, there were no checks or warnings issued when saving a configuration that places the boot router or default gateway on a different subnet than the NMM's IP addresses. This problem can give the impression that the unit is malfunctioning when it fails to boot or does not respond properly to requests. Changes incorporated in versions 1.5.0 and later reduce the chances of such improper configuration. [Bug ID 2041]

When configuring the default router (Router IP Address), the secondary default router (Secondary Router IP Address) or the boot router (Boot Router IP Address) with a subnet address (except 0) that is inconsistent with the NMM's IP subnet value, the version 1.5.0 and later agents respond as follows:

– When configuring the unit with the configuration file, the agent rejects the entry and posts the following message on the service screen:

```
ERROR: Address contains subnet value that is inconsistent with
NMM's IP Subnet value
```

– When configuring the unit with the service port, the agent accepts the entry and displays the following message:

```
WARNING:
Address contains subnet value that is inconsistent with NMM's
IP Subnet value. Check addresses and subnet masks for
consistency.
Press <sp> to continue
```

– When configuring the unit using an SNMP set command, the agent rejects the entry and returns "badValue" for the following MIB objects:

  • S3Agent DefaultGateway

  • s3AgentSecDefaultGateway

  • s3AgentBootRouter

• With previous agent versions, a 331xSA managing a 3301 would not send out an autoPartition trap if one of the ports on the 3301 autopartitioned. This problem is fixed in versions 1.5.0 and later, which correctly send an autopartition trap. [Bug ID 4477]

• Version 1.5.0 and later capture error packet status properly when the RMON filter group is set up to filter error packet status (that is, jabbers or runts).

- With previous agent versions, certain traps would report incorrect values for some of their variables. This problem is fixed in versions 1.5.0 and later. Table 1 lists trap variables that have been corrected to report properly when sent with their associated traps

Table 1. Trap Variable Corrections in Version 1.5.0 and later

Trap	Corrected Trap Variable
enetAuthViolationA	s3EnetCommonPortPartStatus s3EnetAuthNodeStatus
remoteBridgePortOperationChanged	s3EnetRemBridgePortOpSts
enetThreshExceeded	s3EnetThreshObject s3EnetThreshSlot s3EnetThreshPort s3EnetThreshType s3EnetThreshCondition s3EnetThreshSetValue s3EnetThreshActualValue s3EnetThreshAction s3EnetThreshExceedCount s3EnetThreshDuration
flashUpdateFailure	s3AgentFlashStatus
portAutoPartition	s3EnetPortPartStatus s3EnetPortJabberStatus
portDTEJabbering	s3EnetPortJabberStatus
enetAuthViolation	s3EnetPortPartStatus s3EnetAuthNodeStatus

Known Problems

This section describes the known problems affecting the version 1.5.2 release of the agent software for the Model 281xSA and 331xSA Ethernet NMMs.

- A polling interval of less than five seconds on etherHistoryUtilization in the RMON history table causes erratic results at higher traffic rates. It is recommended that polling intervals be set no less than five seconds [Bug ID 2976].
- The front panel utilization display of the NMM does not update if more than 50 percent of network traffic is 64-byte packets [Bug ID 2975].
- When the service port is updating, the agent will not respond to ping or SNMP requests. This is caused by the higher priority placed upon service port tasks. The solution for this problem is to minimize the amount of time spent using the service port [Bug ID 2971].
- s3EnetPortShortEvents are not counted properly. This is because the hardware has difficulty tagging short events (packets smaller than 64 bytes having invalid CRC) [Bug ID 2969].
- In Optivity LAN 7.0, the Autotopology™ discovery process is sometimes disrupted by incompatibilities between certain devices that transmit multisegment topology hellos and those that do not. A workaround is documented in the release notes for Optivity LAN 7.0. This problem does not appear in Optivity LAN versions prior to 7.0. Refer to Table 2 to determine the circumstances under which this problem appears.

Autotopology is only disrupted in segments where Group A devices are mixed with Group B devices that have agent versions listed in the Affected Agent Version column. Where this problem occurs, it can be eliminated by upgrading the Group B devices to the agent versions listed in the Remedied Agent Version column.

Table 2. Autotopology Compatibility

Group	Device	Affected Agent Version	Remedied Agent Version
A	281x/331x		All versions
	331xA/S		All versions
	281xSA, 331xSA		All versions
	5310-06		All versions
B	5310A/SA	1.2.2 through 1.4.2	1.5.0
	5DN310	1.3	1.5
	BayStack 10MB	1.3	1.4
	BayStack 100MB	1.1.0	1.1.1
	BayStack WGS 6-port	3.0.3	
	BayStack WGS 7-port	3.2.1	
	28200		1.4
	28115, 28104	1.1, 1.2, 1.3	1.4
	58000		1.4.1

New Configuration File

This section contains a sample NMM configuration file for the version 1.5.1 agent. Use any ASCII text editor, such as vi, to modify the sample file or create a new configuration file.

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:
#281sa152.img
#331sa152.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
# writable 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 hexadecimal 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
#
# 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
#
#
#-------- 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 -
#
```

Operational Notes

This section covers general operational notes regarding the version 1.5.2 agents for Model 281xSA and 331xSA NMMs.

Network Layer Addresses

Model 281xSA and 331xSA NMMs learn network layer addresses only for packets sent directly to them. Additional ARP requests on the network are not currently added to tables, but they will be in future releases.

Using Expression Thresholds

Thresholds have long been a desirable feature in providing proactive network management techniques. However, with conventional thresholds, users must often choose threshold parameters without proper baselining, or they must spend considerable time selecting specific parameters to indicate network health. Often, what is actually needed is a comparison between one statistic and another or a ratio between parameters. The expression thresholds of the version 1.5.2 agent provide this capability.

Expression thresholds allow users to create alarms on any well-formed, integer-based mathematical expression. This greatly optimizes the flexibility of standard threshold capabilities and provides a new level of threshold customization far beyond today's existing methods. Because NMM agent polling and action mechanisms are local to the chassis, this new enhancement extends Bay Network's embedded capabilities while continuing to eliminate the need for NMS intervention and event-action execution.

Encompassed within the expression threshold features are mechanisms providing trend-analysis capabilities. Agents now have the capability to save a minimum, maximum, and average of an expression. These averages can be calculated for user-defined windows of "X" sample cycles.

For example, the following expression can be created to calculate the ratio of overhead traffic on a given segment:

((broadcast frames+multicast frames)/total frames) * 100

While users may want to take action on a threshold exceeded in a 15-second interval, they may also want to know what the average value was from that expression calculation for the last 10 sample intervals. By defining a window size of 10, the agent keeps a sliding tally of minimum, maximum, and average values for the last ten 15-second intervals.

On the 281xSA and 331xSA NMMs, the 1.5.0 agent allows a choice of thresholding methods while migrating to standard RMON Alarms and Event-based thresholds. Proprietary (legacy) thresholds can still be set and maintained by setting them through Optivity or a NMM's configuration file. RMON Alarms and Events can be set with the redesigned RMON threshold GUI available in Optivity LAN 7.0.

Out-of-band Connection

This section describes the general procedure for establishing a telephone line connection between an NMM and a network management station (NMS). This procedure is useful for those times when the NMM cannot otherwise communicate with the NMS.

The Out-of-Band Connect feature allows you to establish a telephone line connection with a hub using the RS-232 port on an NMM installed in the hub and a modem on your PC management station. You can then communicate with the network management module and continue to manage and monitor it if in-band network communications are disrupted.

This section includes the following procedures:

- Preparing for out-of-band connection
- Establishing an out-of-band connection
- Terminating an out-of-band connection

NOTE: *Operations performed using an out-of-band connection are significantly slower than operations performed using an in-band connection.*

Preparing for an Out-of-band Connection

Before you can successfully establish an out-of-band connection to a hub, you must configure your modems, network management station, and the receiving hub. The following sections provide instructions for making the appropriate configurations.

Configuring the Modems

Out-of-band connections require two modems: the calling modem and the receiving modem. The following sections describe cabling and configuration considerations for each modem.

NOTE: *Bay Networks recommends using 9600-baud Hayes-compatible modems. Baud rates as low as 1200 are supported but may result in slower response times. Do not use baud rates lower than 1200.*

Calling Modem

The calling modem is located at your PC management station. It can have either a DB-9 or DB-25 COM port. For DB-25 COM ports, use a straight-through male DB-25 to female DB-25 RS-232 cable. For DB-9 COM ports, use a standard DB-9 to DB-25 RS-232 cable.

Using Windows Terminal or an equivalent terminal emulation package, configure the modem software as shown. The examples in this section apply to Hayes-compatible modems; the settings for your modem may differ:

- Set the modem to the factory default settings.

  Enter the following:
  ```
  AT&F&W
  ```

- Set the modem to perform hardware (RTS/CTS) flow control.

  Enter the following:
  ```
  AT&K3&W
  ```

- Set the modem to “hang up” when on-to-off transition of DTR occurs.

  Enter the following:
  ```
  AT&D2&W
  ```

- Set the modem for carrier detection.

  Enter the following:
  ```
  ATX4&W
  ```

Refer to the documentation included with the modem for details on making the configurations.

Receiving Modem

The receiving modem is located at the hub. Use a straight-through RS-232 male DB-25 to female DB-25 cable to connect the RS-232 port on the NMM to the modem.

Using Windows Terminal or an equivalent terminal emulation package, configure the modem software as shown below. The examples in this section apply to Hayes-compatible modems; the settings for your modem may differ):

- Set the modem to the factory default settings.

  Enter the following:
  ```
  AT&F&W
  ```

- Set the modem to perform hardware (RTS/CTS) flow control.

  Enter the following:
  ```
  AT&K3&W
  ```

- Set the modem to AUTO-ANSWER.

  Enter the following:
  ```
  ATS0=1&W
  ```

- Set the modem to “hang up” when on-to-off transition of DTR occurs.

  Enter the following:
  ```
  AT&D2&W
  ```

- Set the modem for carrier detection.

  Enter the following:
  ```
  ATX4&W
  ```

Refer to the documentation included with the modem for details on making the configurations.

Configuring the Receiving Hub

The following NMM out-of-band parameters must be set correctly:

- The baud rate setting for the NMM must match the baud rate setting specified in the Out-of-Band Manager configuration list for the selected NMM, and the baud rate setting on the modem.
- The initialization string must contain the correct telephone number for the management station to call the NMM.

For instructions on establishing an out-of-band connection, see "Configuring the Management Station" next in this section.

Configuring the Management Station

The management station configuration is set using the Out-of-Band Manager application. This application can be started from any of the Optivity views and runs independently of the current view. Out-of-Band Manager is used to configure, establish, and terminate out-of-band connections.

To configure an out-of-band connection, follow these steps:

1. **Start the Out-of-Band Manager using one of the following procedures:**
   - From Campus Command Center, select a hub from the Contents panel for which you want to start the Out-of-Band Manager. Choose Out-of-Band Manager from the Applications menu.
   - From HP OpenView, select a hub for which you want to start the Out-of-Band Manager. Choose Out-of-Band Manager from the Applications menu.
   - From ManageWise, select a hub for which you want to start the Out-of-Band Manager. Choose Optivity Tools and then Out-of-Band Manager from the Tools menu.

The Out-of-Band Configuration dialog box is displayed similar to Figure 1.

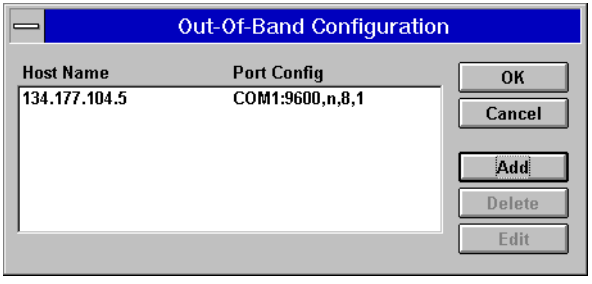

Figure 1. Out-of-Band Configuration dialog box

2. Click the Add button to add new COM ports to the management station configuration.

To edit an existing port configuration, select the port; then click the Edit button. The Serial Port Configuration dialog box is displayed similar to Figure 2.

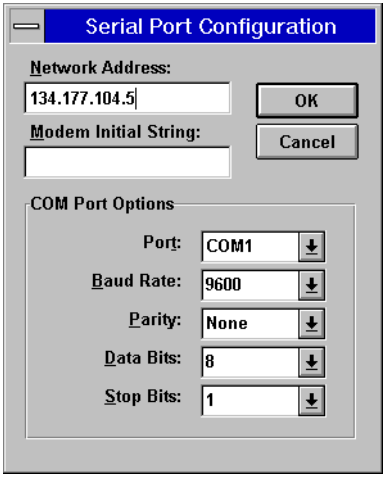

Figure 2. Serial Port Configuration dialog box

3. **Enter the following configuration information:**
   - Network Address (IP or IPX address)
   - Modem Initial String (for example - ATDT, 7075551234)
   - COM port name, Com1
   - Baud rate, 9600 baud
   - Parity, none
   - Data Bits, 8
   - Stop Bits, 1
4. **Click the OK button after you have entered all of the port configuration information.**

   The Out-of-Band Configuration dialog box is displayed.
5. **Click the OK button when you finish configuring your ports.**

Changing Out-of-band Time Outs

The out-of-band time out can be changed to accommodate a lower-speed link.

To change the time out, follow these steps:

1. **Use a text editor to open the SYNOPT.INI file.**
2. **Change the value of the AsyncDefaultTimeout parameter in the Optivity section of the file.**

   The default is 25 tics, 400 ms, or 10 seconds. A larger time out setting may be helpful for low-speed links.

Establishing an Out-of-band Connection

After you have made all of the appropriate configurations described in the previous sections, you can establish an out-of-band connection.

To establish an out-of-band connection, follow these steps:

1. **Start the Out-of-Band Manager by selecting Out-of-Band Manager from the HP OpenView or ManageWise Applications menu.**

   The Out-of-Band Connection dialog box is displayed, similar to Figure 3.

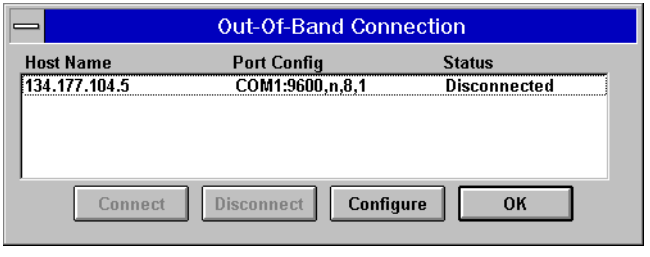

Figure 3. Out-of-Band Connection dialog box

NOTE: *If the initialization string has not been configured or is not yet in the database, a dialog box appears, allowing you to specify the string. Because control characters (including Backspace) are valid initialization string characters, use [Shift+Backspace] to make corrections.*

2. **Select the address of the hub you want to connect; then click the Connect button.**

   The status of the connection is displayed in the Status column of the Out-of-Band Connection dialog box.

3. **After the out-of-band connection is made, you can continue using Optivity to monitor and manage the hub even if network communications are disrupted.**

NOTE: *Operations performed using an out-of-band connection are significantly slower than operations performed using an in-band connection.*

Terminating an Out-of-band Connection

To terminate an out-of-band connection and reestablish an in-band connection from the Out-of-Band Connection Manager, select the desired port and click the Disconnect button. In-band communications resume.

Related Publications and Ordering Information

For more information about using the Model 281xSA Ethernet Hub and Model 331xSA Ethernet Network Mangement Module, 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)

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: 1-800-845-9523
- FAX:—U.S./Canada: 1-800-582-8000
- FAX—International: 1-916-939-1010

You can also use these numbers to request a free Bay Networks Press catalog.