NH2025-10

High Density Workgroup Switch

Installation and User Guide

Standards Compliance

UL 1950; CSA 22.2 No 950; VCCI; FCC Part 15 Class A; CE-89/336/EEC, 73/23/EEC

FCC Notice

WARNING: 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 and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

It is suggested that the user use only shielded and grounded cables when appropriate to ensure compliance with FCC Rules.

CE Mark

The CE mark symbolizes compliance with the EMC directive of the European Community. Such marking is indicative that the specified equipment meets or exceeds the following technical standards:

- EN 55022 – "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment"
- EN 50082-1 – "Electromagnetic compatibility – Generic immunity standard Part 1: Residential, commercial and light industry"
- IEC 1000-4-2 – "Electromagnetic compatibility for industrial-process measurement and control equipment Part 2: Electrostatic discharge requirements" – Severity level 3
- IEC 1000-4-3 – "Electromagnetic compatibility for industrial-process measurement and control equipment Part 3: Radiated electromagnetic field requirements" – Severity level 2
- IEC 1000-4-4 – "Electromagnetic compatibility for industrial-process measurement and control equipment Part 4: Electrical fast transient/burst requirements" – Severity level 2
- CISPR 22 – Radiated and Line-conducted Class A
- EN 60950 – ITE Safety

A "Declaration of Conformity", in accordance with the above standards, has been made and is on file at NBase-Xyplex Communications Ltd.

VCCI

This equipment is in the 2nd Class category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council For Interference by Information Technology Equipment aimed at preventing radio interference in such residential area.

When used near a radio or TV receiver, it may become the cause of radio interference. Read the instructions for correct handling.

Contents

Configuring, Modifying, and Monitoring the Unit

Overview

The NH2025-10 is a robust switch platform, representing the next generation in switching technology. It boasts a combination of cutting-edge hardware architecture, a rich set of Virtual LAN (VLAN) options and advanced network management features.
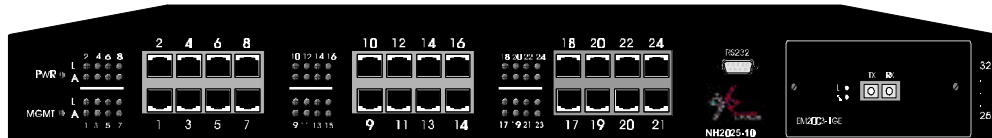
Figure 1 - General View

The NH2025-10 contains a built-in SNMP agent running on the SNMP Processor Board. This allows each unit to be managed from a centralized management station through any SNMP-compliant NMS.

The SNMP agent software complies with the following standards:

- **RFC 1155** – The Structure of Management Information (SMI) for TCP/IP Based Internets, May 1990

- **RFC 1212** – The Management Information Base I (MIB I)

- **RFC 1213** – The Management Information Base II (MIB II), March 1991.

- **RFC 1284** – The Ethernet MIB

- **RFC 1286** – The Bridge MIB

- **RFC 1757** – The RMON MIB

The NH2025-10 also supports two NBase-Xyplex private MIBs: switch.mib and gswitch.mib.

The SNMP agent utilizes UDP/IP (RFC 768, RFC950, RFC1071 and RFC791) as OSI layers 3 and 4 protocols, ICMP (RFC792) and ARP (RFC826) to complete the UDP/IP protocol suite.

The UDP/IP stack implementation conforms to:

- **RFC 1122** – Requirements for Internet hosts - communication layers.

- **RFC 1123** – Requirements for Internet hosts - application and support.

The NH2025-10 may be managed by any SNMP Manager that conforms to the above standards. It may be fully managed by MegaVision, NBase-Xyplex's multi-platform network management system. For more information on MegaVision, view our web site, or contact NBase-Xyplex for a data sheet.

The NH2025-10 implements an NBase-Xyplex Enterprise MIB and an NBase-Xyplex Product MIB that may be provided upon request.

Applications

A switch boosts network performance by segmenting a single large collision domain into smaller, separate collision domains. It also provides dedicated connections for heavily loaded networks using work stations and servers. In addition, the Full Duplex capability of Ethernet switches permits long distance connectivity for backbone applications or high throughput for high-performance dedicated servers. The NH2025-10 combines 10/100Mbps switched ports with a dport for accommodating an optional module.

The NH2025-10 switch can connect up to twenty-four 10/100Mbps ports and with a dport for accommodating an optional module Figure 2 illustrates various connection possibilities: Two NH2025-10 switches ,with Gigabit Ethernet uplink modules, located in different buildings can be connected via MM or SM fiber optic cable to a Gigabit Ethernet backbone. VLAN Tagging allows the creation of one logical VLAN across all switches. Additional connections include dedicated 10/100Mbps workgroup connections and 100Mbps dedicated servers.
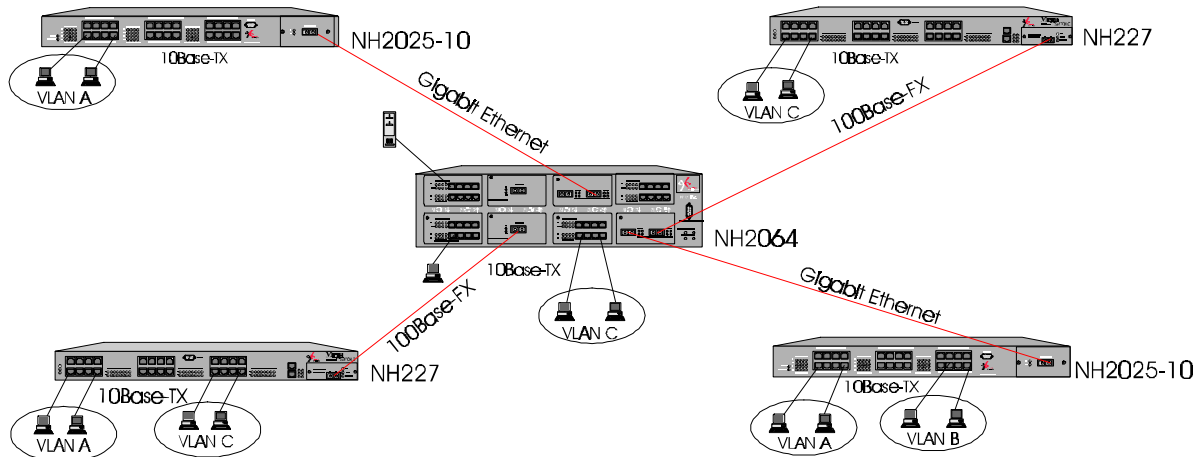
Figure 2 - Typical Application Example

NOTE: The NH2025-10 does not count as a repeater. Each of the segments connected to the switch can support a full Ethernet network; there can be up to four 10Base-T repeaters/hubs between any NH2025-10 port and any station.

Network Management Systems

Network management functions greatly assist in monitoring and controlling the network. The NH2025-10 can be monitored and controlled through MegaVision or through a generic SNMP-based NMS. The connection to the NH2025-10 may be achieved through Ethernet.

To enable management of an NH2025-10 device, you must define the device and provide specific parameters to establish communication. The Describe window is used to define a new device or to change the parameters of a previously defined device.

The NH2025-10 can also be configured and managed through the Command Line Interface.

Feature Summary

The following are the Performance/Configuration and Management features supported on the NH2025-10 switch.

Performance/Configuration

- 24 switched 10/100Mbps ports and a dport to accommodate one of the following uplink modules:

  – Single Gigabit Ethernet port (MM,SM)

  – Dual Gigabit Ethernet ports (MM,SM)*

  – 8 10/100 auto-negotiation ports module

  – 2 100Base-FX ports (MM,SM)

- The highest common port speed is automatically set when connecting any standard compliant (802.3u Auto-negotiation) network device or station.

- Each 10/100Base port operates in half duplex mode, for shared networks, or in a dedicated full duplex link, running at up to 200Mbps.

- All ports support auto-polarity detection and correction.

- Store-and-Forward switching.

- Flow Control (IEEE 802.3x) provides effective packet loss protection under heavy load conditions, minimizing delays and retransmission of data, thus improving network performance.

- Supports the creation of up to 64 Virtual LANs.

- Supports the Inter-Switch VLAN tagging standard which enables the creation of multiple groups across the network (IEEE 802.1q).

- MAC address table (up to 12K unicast entries).

- Maximum wire speed throughput on all ports simultaneously.

- Supports RMON (groups 1,2,3,9), Telnet for rapid fault detection and isolation.

- Port Mirroring.

- Spanning Tree Algorithm prevents broadcast loops

Management

- Fully managed through the comprehensive NBase-Xyplex MegaVision Network Management System, or any SNMP-based management platform.

- Extensive Command Line Interface (CLI) management provides out-of-band administration.

- Supports NBase-Xyplex's private MIB, Ethernet MIB and bridge MIB. The status of each port is displayed by an LED on the front panel. This LED indicates active and link status.

Installing and Setting Up the Unit

The NH2025-10 can operate as a stand-alone unit or in conjunction with any of NBase-Xyplex's other Ethernet offerings. Switch management is through NBase-Xyplex MegaVision software, any SNMP-compatible NMS, or through the Command Line Interface (CLI).

Installing the Unit

This section outlines the installation and operation of the NH2025-10.

The NH2025-10 comes as a 19" rack-mountable unit. However, it can be placed either in a rack mount, using the enclosed rack-mount brackets, or on a secure flat surface. Ensure that the unit is within reach of the necessary connections (i.e. power outlet, Ethernet connections, and if the NH2025-10 is monitored through the serial port, a PC, UNIX workstation, or modem). The unit is powered by a wide-range power supply for either 110 or 220 VAC operation.

> **WARNING**
> Free airflow must be maintained in order to permit adequate cooling of the unit. All FAN holes MUST be unobstructed.

Rack Mounting

If rack-mounted units are installed in a closed or multi-rack assembly, they may require further evaluation by certification agencies. The following items must be considered when rack mounting a unit:

1. The ambient temperature within the rack may be greater than room ambient temperature, however the amount of airflow required for safe operation should not be compromised. The maximum temperature for this equipment is 50°C (122F). Consideration should be given to the maximum rated ambient temperature.

2. The rack should be stable, verify that stability is not inadvertently compromised during and after installation.

Front Panel

The front panel of the NH2025-10 is illustrated below in Figure 3. The table below describes its various components, LED indications and their functions.
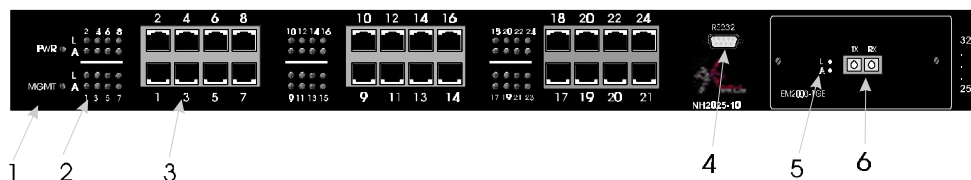
Figure 3 - Front Panel

1   Global LEDs

       PWR   **Green ON** indicates Power ON

       MGMT   **Blinking Green** indicates that the firmware is initializing

                     Solid Green indicates that firmware is installed and in proper operational mode

2   10/100 Port LEDs

       L   **Solid Green** indicates a valid connection. During LINK test, there is an intermittent flash on all the ports.

       A   **Solid Green** indicates network activity.

3   10/100 Base-T ports   One of three groups of switched Ethernet ports for 10/100Mbps connection

4   DB-9 Connector   RS-232 connection for NMS

5   Optional Module LEDs

6   Optional   Module Port/s

Rear Panel

The rear panel of the NH2025-10, which houses the power connection and ON/OFF switch, is illustrated in Figure 4. Two fan holes, which MUST be kept unobstructed, are located on the left side of the unit.

Figure 4 - Rear Panel

Installing Modules in the Unit

To insure proper installation, complete the following:

1. Power OFF the NH2025-10 switch.

2. Carefully slide an NH2025-10 module into a free dport and press firmly to insert.

3. Tighten the thumbscrews securely.

4. Power ON the NH2025-10 switch. If you have a flash version lower than 1.20 and you are installing F/O modules, you must download a new software version to the switch so that the firmware recognizes the new uplinks and the modules operate correctly.

Modules for NH 2025-10
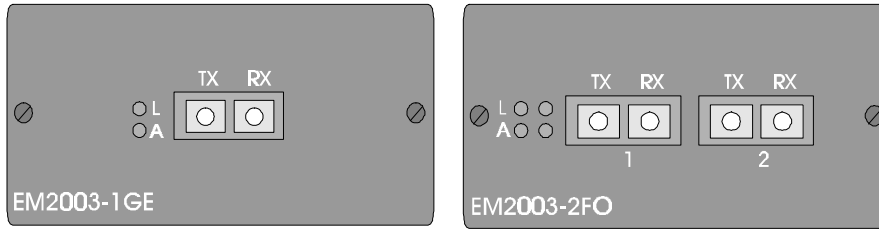
Figure 5 - Front Panels of the EM2003-1GE and EM2003-2FO Uplink Modules

EM2003-1GE

EM2003-1GE   One 1000BaseLX port (SM 1500nm, .0-60km)

> **LEDs**

L	Green	ON = Link, OFF = No Link
A	Green	ON = Activity, OFF = No Activity

Type	Connector	Wavelength	Budget	Estimated Range	Attenuation	Minimum Committed Power
SX/M	DSC	850nm	NA	0–350 km	3 dB/km	-9.5 dBm
LX/M	DSC	1310nm	NA	0–500 km	2 dB/km	-13 dBm
LX/S1	DSC	1310nm	NA	0–6 km	0.5 dB/km	-13 dBm
LX/S2	DSC	1550nm	8 dB	0–32 km	0.25 dB/km	-13 dBm
LX/S3	DSC	1550nm	15 dB	30–60 km	0.25 dB/km	-6 dBm

EM2003-2FO

EM2003-2FO   Two port 100Base-FX (MM, 1310nm, 0-2, DSC).

> **LEDs**

L	Green	ON = Link, OFF = No Link
A	Green	ON = Activity, OFF = No Activity

Type	Connector	Wavelength	Budget	Estimated Range	Attenuation	Minimum Committed Power
M	DSC	1310 nm	9 dB	0–2 km	2 dB/km	-16 dBm
MX	DSC	1310 nm	19 dB	2–7 km	2 dB/km	-6 dBm
S1	DSC	1310 nm	17 dB	0–25 km	0.5 dB/km	-13 dBm
S2	DSC	1310 nm	24 dB	25–50 km	0.5 dB/km	-8 dBm
S3	DSC	1550 nm	24 dB	50–100 km	0.25 dB/km	-8 dBm

7
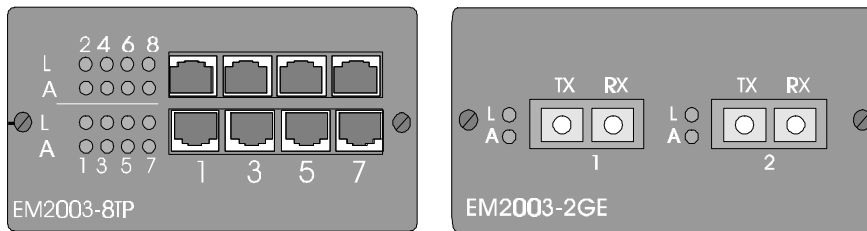
Figure 6 - Front Panels of the EM2003-8TP and EM2025-2GE* Modules

EM2003-8TP

EM2003-8TP	Eight port 10/100Base-TX switch module	
L	Green	ON = Link, OFF = No Link
A	Green	ON = Activity, OFF = No Activity

*Em2003-2GE**

EM2003-2GE*	Two port Gigabit 1000Base-SX (MM, 850nm, 0-350m)	
	*Future release	
L	Green	ON = Link, OFF = No Link
A	Green	ON = Activity, OFF = No Activity

Connecting Power to the Unit

The power cord should be plugged into an easily accessible outlet. A built-in power supply automatically adjusts to any outlet providing between 90 VAC and 264 VAC at 50/60 Hz.

For a 115 volt configuration, the power cord to be used is minimum type SJT (SVT) 18/3, rated 250 Volts AC, 10 Amps with a maximum length of 15 feet. One end is terminated in an IEC 320 attachment plug, the other in a NEMA 5-15P plug.

The power cord to be used with a 230 Volt configuration is minimum type SJT (SVT) 18/3, rated 250 Volts AC, 10 Amps with a maximum length of 15 feet. One end is terminated in an IEC 320 attachment plug. The other end is terminated as required by the country where the unit is installed.

Utilisez uniquement un câble secteur adapté à 230 volts, de type SJT (SVT) 18/3 minimum, 250 volts AC nominal, 10 Amps, et d'une longueur maximale de 4.5m. l'une des extrémités étant raccordée à un connecteur Type IEC320, tandis que l'autre extrémité correspondra aux spécifications du pays concerné.

Das Netzkabel ist das hauptsachliche Diskonnektionsmittel, es sollte in eine leicht erreichbare steckdos gesteckt werden. Das Netzkabel kann mit einer 230 Volts Konfiguration verwonder werden vom typ: Minimum VDE or HAR, 3 X 1.00 mm2, 250 VAC, 10 Amps, maximal 4.5m long. Ein Ende ontspriche dem Stecker IEC 320. Das andere Ende entspricht den Anfoderungen des entsprechenden Landes.

Input Supply

Check voltage ratings to assure there is no possibility of overloading the electrical circuits that could effect current overload protection and electrical wiring.

Grounding

Reliable grounding of this equipment must be maintained. Particular attention should be given to electrical connections when connecting to a power strip, rather than direct connections to the electrical outlet.

Connecting Ethernet Devices

For optimum performance, the Ethernet segments connected to the NH2025-10 must be configured carefully. Generally, the segments should be configured so that machines on a given port communicate primarily among themselves; that is, most traffic does not need to cross the switch. However, this is not the best configuration for certain situations.

Connecting Your Network

The cable connections to the 10/100BaseTX ports can be UTP or STP Category 3 and above, and cable length is limited to 100 meters on each port. STP cable carries a higher quality of signal and is less sensitive to environmental noise.

The RJ-45 ports of the switch are defined as MDI-X ports.

The 10/100BaseTX ports on the NH2025-10 are designed to be connected directly to a workstation, using a standard straight through patch cable. In order to cascade switches or connect a hub to the switch, a crossover cable must be used.

RJ-45 PIN	Function
1	TX +
2	TX -
3	RX +
6	RX -

SWITCH

RJ-45 PIN	Function
1	RX +
2	RX -
3	TX +
6	TX -

PC (NIC)
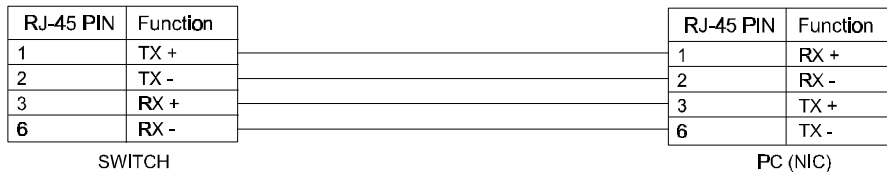
Figure 7 - Straight Cable Connection Between a NH2025-10 and a Workstation

RJ-45 PIN	Function
1	TX +
2	TX -
3	RX +
6	RX -

SWITCH

RJ-45 PIN	Function
1	RX +
2	RX -
3	TX +
6	TX -

HUB
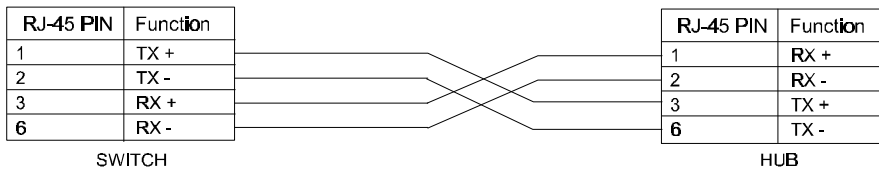
Figure 8 - Crossover Cable Connection Between an NH2025-10 and a Hub

Getting Started

This section describes how to connect to the management port, log into the Command Line Interface, and set the unit's IP Address.

Connecting to the Management Port

With the product we supply a management cable. You can use it to get access to the management port.

To configure the serial ports do the following items:

1. Connect the cable provided to the management port and communication interface (COM1 or COM2) of your PC.

2. Start Windows HyperTerminal and create a new connection with the property set to 9600 bit per second, 8 bits per character and no flow control.

3. Start HyperTerminal session and then type Enter to get the login prompt.

Logging Into the Command Line Interface

The Command Line Interface is protected with a login name and password.

To access the CLI the Network Administrator has to provide his name and a password.

Example

```
Please Login
username: don
password: (not echoed)
```

The factory default password is a null string. To log in just press the Enter key. Once you are logged into the CLI, you may change the password in order to avoid unauthorized access.

Setting the IP Address

To manage the MegaSwitch using an SNMP Network Management Application or to use the ping command to test the switch, it is necessary to assign an IP Address, a netmask and a broadcast address. The Network Administrator should assign the IP address in accordance with the existing IP addressing scheme.

Set the IP configuration using the set-ip-cfg command.

Example

```
SYS_console> set-ip-cfg 192.1.1.64 255.255.255.0 255.255.255.255
```

NOTE: If the switch has no IP Address, then the provided IP Configuration changes the running parameters as well as the NVRAM-based database. If the switch was already configured, the command only changes the NVRAM database. Therefore, to use the new parameters you should reset the Switch, using the `warm-reset` command.

You can also use the `set-ip` command to accomplish this. When you do, the mask and broadcast are automatically set to defaults according to the IP address class.

Example

```
SYS_console> set-ip 192.1.1.64
```

Verifying the Installation

After the installation is complete and the IP Address configured, use the Ping utility to test the connectivity.

The ping command sends an echo request to the host specified in the command line. For example, to test connectivity from the Switch to a workstation with an IP Address of 192.1.1.1, use the following command:

```
SYS_console> ping 192.1.1.1 100
```

Accessing the Command Line Interface Remotely

When the switch has an IP address, the administrative interface can be accessed remotely through Telnet. All commands work exactly as if the serial interface were being used. Please note that only one console session may be active at any given time. This means that after the first Telnet session is established, all other Telnet connections are refused until the current session is closed.

Using the Command Line Interface

This section describes how to use the Command Line Interface (CLI) to configure and manage the NH2025-10 switch.

Command Conventions

The following conventions are used within this guide to make understanding and using the CLI easier.

Command   Items appearing in this typeface are to be typed as shown.

Italics   Italicized items are variables and represent values. For example, *<IPaddress>* represents an IP address in dotted decimal notation as 123.1.2.3.

{ } | Items in { } and separated by | represent alternatives for the argument. For example:

```
get-comm  {read|write|*}
```

means you can type one of the following:

```
get-comm read
get-comm write
get-comm *
```

Command Line Help

The CLI provides command line help to ease in the entering of commands correctly. The following command line help is available:

- Command parameter Help
- Command group Help
- Command wildcard Help
- Command history

Getting Command Parameter Help

To get an explanation of a command's parameters add a question mark (?) after the command name. For example:

```
SYS_console> ping ?
```

The unit displays the available parameters for the `ping` command:

```
ping IP traffic generator
 [arg #0] destination IP address
 [arg #1] number of packets to send or 0 for endless ping
SYS_console> ping _
```

Note that the command is reprinted after the prompt. You can add the necessary parameters here. If a question mark is added after the first parameter, then the same explanation is provided, and the previous command, including the provided parameters, is redisplayed.

Example

```
SYS_console> ping 129.1.1.7 ?
```

The unit displays the next level of parameters:

```
ping IP traffic generator
 [arg #0] destination IP address
 [arg #1] number of packets to send or 0 for endless ping
SYS_console> ping 129.1.1.7
```

Getting Command Group Help

To find out the command groups that are available within the unit, enter a question mark at the CLI prompt. The CLI displays a list of all of the available command groups and a short explanation of each.

Example

```
SYS_telnet>?


             Commands groups are:
             ----------------------
 console        Console related commands
 system         System related commands
 ip             IP related commands
 snmp           SNMP related commands
 switch-db      Switching Database related commands
 vlan           Virtual LANS related commands
 echannel       EtherChannel Commands
 port-cfg       Port Configuration related commands
 statistics     Switching Statistics related commands
 sp-tree        Spanning Tree related commands
 ----------------------------------------------------------------
 use ! for previous cmd, ^U to clear line, ^W to clear previous word
 ----------------------------------------------------------------
```

Entering a group name from this list displays a list of the commands under that group.

Using Command Wildcards

The CLI allows you to use the question mark <?> as a wildcard when you are unsure of a command. To use the wildcard, place the question mark immediately after the command you are looking for.

NOTE: You can type all or just a portion of the command followed by the question mark and the CLI returns all commands that start with that string.

14

Example

```
SYS_console>get-c?
command 'get-c' not found
        Commands matching <get-c>
 get-comm    show current read or/and write community
 get-con-matrix  retrieves the VLAN connectivity matrix
 get-colls-cnt   gets the collision distribution counters per port
SYS_console>get-co
```

Retrieving Command History

The CLI allows you to retrieve a history of the last commands you have issued. Use the following keys to retrieve commands:

<!> or Ctrl/P	Retrieves the last command in the command history.
Ctrl/W	Deletes the previous word.
Ctrl/U	Erases the entire current line.
<Tab>	Completes the command when a partial unique command is provided.

NOTE: If after entering a key sequence, more than one screen-full of text is to be printed, you can continue to scroll through the text by hitting any key or you can stop the process by hitting the Esc key.

```
SYS_console>system
System related commands
-------------------------------------------------------
 sys-stat                show system status
 get-stst-level          show the selftest level
 set-stst-level          change the selftest level
 warm-reset              warm reset of the device
 cold-reset              cold reset of the device
 get-last-err            displays information about the last fatal error
 init-nvram              initialize NVRAM to default values
 get-sw-file             retrieves the SNMP Agent Software file name
 set-sw-file             sets the SNMP Agent Software file name - for  download
 get-tftp-srvr           retrieves the TFTP download server IP address
 set-tftp-srvr           sets the TFTP download server IP address
 set-tftp-mode           sets the TFTP download mode
 get-tftp-mode           retrieves the TFTP download mode
 sw-dnld                 software download BY TFTP
 set-fg-param            sets the Ethernet frame generator parameters
 start-fg                starts the Ethernet frame generator
 stop-fg                 stop the Ethernet frame generator
```

15

Command Line Errors

The CLI displays messages when you enter a command incorrectly. The following command line error messages are used:

- Nonexistent command
- Incorrect number of parameters

Nonexistent Command

If you enter a command incorrectly or if the command does not exist, the CLI returns an error message indicating the type of error that occurred.

Example

```
SYS_console> pin
command 'pin' not found
```

Incorrect Number of Parameters

If you enter a command correctly but the number of parameters is incorrect, the following message is displayed:

```
SYS_console> ping
too few arguments
```

Configuring, Modifying, and Monitoring the Unit

You can configure, modify, and monitor the unit using the following categories of commands:

- Console
- System
- IP configuration
- SNMP Agent
- Switching database and database entry management
- Virtual LAN
- EtherChannel
- Port Configuration
- Switching Statistics
- Spanning Tree

Refer to Appendix A for a quick reference of the available commands.

Console Commands

Console commands allow you to configure the CLI parameters and user interface. To view the console commands, enter `console` at the CLI prompt. The following are the available console commands.

help-kbd

This command lists the console function keys.

Example

```
SYS_console>help-kbd
  ---------------------------------------------------------
 Ctrl/U (or Escape)    clears the current line.
 Ctrl/W                clears the previous word.
 ! or Ctrl/P           presents the previous command.
 TAB                   completes command.
 ? or help             presents help. Depending on position:
in 1st column, list of the   categories.
in command, list of completed commands that start with the presented
string.
in parameters, lists of the    parameters.
 # - with line number  Repeats command from history,
For example: #26  Presents help for  line 26.
    Without line number  Shows entire history list.
  ---------------------------------------------------------
```

banner

The banner command displays the Nbase-Xyplex CLI logo.

clear

The clear command clears the screen and displays the CLI prompt.

login

The login command exits the CLI, but does not disconnect a Telnet session. This allows you to test a password (or other activity) without reconnecting.

logout

The logout command ends the actual CLI Session. To use the CLI, you must login again.

set-page

The set-page command sets the console page size (in lines per page). Valid values in lines are 5 to 127. The value of 0 means no paging. The default value is 21.

set-prompt

The set-prompt command allows you to set a new command line prompt for the CLI. This can be a more meaningful prompt, such as the location of a switch, or the name of a workgroup. The default prompt is SYS_console>. To change the prompt, use the following command:

```
set-prompt <new_prompt>
```

Example

```
SYS_console> set-prompt R&D_grp>
R&D_grp> _
```

set-attr-prompt

The set-attr-prompt command sets the prompt attributes. To set the prompt attributes, use the following command:

```
set-attr-prompt <number of option>
  [arg #0] options: 0-normal, 1-bold, 2-underline, 4-blink, 8-reverse
```

set-attr-msg

The set-attr-msg command allows you to define how the display message appears. To define how messages appear, use the following command:

```
set-attr-msg <number of option>
  [arg #0] options: 0-normal, 1-bold, 2-underline, 4-blink, 8-reverse
```

set-attr-text

The set-attr-text command sets the text display attributes. To define how text appears, use the following command:

```
set-attr-text <number of option>
  [arg #0] options: 0-normal,1-bold,2-underline,4-blink,8-reverse
```

set-passwd

The console requires you enter a password to log in. The set-passwd command allows you to change the console password. To change the console password:

1. Enter the set-passwd command at the CLI prompt. The system prompts you for the old password.
2. Enter the old password. The system prompts you for a new password.
3. Enter your new password. Note that the password is not echoed back to you. The system prompts you to reenter the new password.
4. Reenter the new password.

The following examples show an unsuccessful and successful password change.

```
SYS_console>set-passwd

Enter old password:

    Enter new password:

    Enter new password again:

    Error: different new passwords
```

If the password change succeeds, the system responds as follows:

```
SYS_console>set-passwd

     Enter old password:

     Enter new password:

     Enter new password again:

CLI running password changed

CLI password change in the NVRAM OK
```

System Commands

System Commands allow you to display and set the system-related parameters. To view the system commands, enter `system` at the CLI prompt. The following are the available system commands.

sys-stat

The sys-stat command displays general status information about the Ethernet Switch, and its SNMP Agent Hardware and Software.

Example

```
SYS_console>sys-stat
   NBase-Xyplex Nh2025-10 Version 1.08
   Mon Apr 26 16:09:47 1999
   SNMP Object ID is : <  1.3.6.1.4.1.629.16.2.1 >
  System MAC Address      :   00-20-1a-00-a7-5a
   Switching Data Base Size: 12288 entries
   Number of ports         : 25
   Total uptime(hundredths of seconds ):       700
   Total uptime(days, hh:mm:ss format): 0 days, 0:00:07.00

i/f   1 : description  [Port 1 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   2 : description  [Port 2 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   3 : description  [Port 3 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   4 : description  [Port 4 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   5 : description  [Port 5 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   6 : description  [Port 6 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   7 : description  [Port 7 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   8 : description  [Port 8 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   9 : description  [Port 9 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   10 : description [Port 10 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   11 : description [Port 11 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   12 : description [Port 12 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   13 : description [Port 13 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   14 : description [Port 14 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   15 : description [Port 15 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   16 : description [Port 16 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   17 : description [Port 17 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   18 : description [Port 18 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   19 : description [Port 19 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   20 : description [Port 20 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   21 : description [Port 21 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   22 : description [Port 22 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   23 : description [Port 23 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   24 : description [Port 24 – 10/100 BaseTx ETHERNET Port] : status [UP]
i/f   25 : description [Port 25 – 1000   BaseFx ETHERNET Port] : status [UP]
SYS_console>
```

This screen displays the following information:

- Device name and type
- SNMP Agent software version and release date
- Device SNMP object ID
- Device MAC address
- Switching database size
- Number of ports
- System uptime in 1/100 sec as well as in days, hours, minutes, seconds
- Interfaces description and status

get-stst-level

The `get-stst-level` command displays the self-test level (Disable or Enable) of the device. The default value is Enable.

set-stst-level

The `set-stst-level` command sets the self-test level of the device. There are two levels of self-test: Disable and Enable. The self-test level is stored in NVRAM. To set the self-test level, use the following command:

```
set-stst-level <level>
```

warm-reset

The `warm-reset` command resets the SNMP Agent software. The Switch configuration is changed according to the values stored in the NVRAM. This command permits you to refresh the Switch configuration after a change of the NVRAM parameters. The statistics counters are also reset by the warm-reset command.

cold-reset

The `cold-reset` command causes the switch to cold-reset. Cold reset is equivalent to power cycling the switch.

get-last-err

The `get-last-err` command retrieves the most recent system failure information.

Example

```
SYS_console>get-last-err
 System information since the last hardware reset
 -----------------------------------------------
 Software resets number : 0
 Fatal error text       :
 Fatal error uptime     : 0 days, 0:15:36.00
SYS_console>
```

NOTE: The "Software resets number" value is the number of executed "warm resets" commands issued after the last "cold reset."

init-nvram

The `init-nvram` command resets the non-volatile RAM on the SNMP Agent to default values. The reset takes effect after you reboot (warm or cold reset) the unit.

get-sw-file

The `get-sw-file` command retrieves the SNMP Agent Software file name.

set-sw-file

The `set-sw-file` command sets the name of the file downloaded by TFTP. This name must match the name of the agent software file on the TFTP server. To set the software file, use the following command:

```
set-sw-file <filename>
```

get-tftp-srvr

The `get-tftp-srvr` command retrieves the IP address of the TFTP server that the Agent uses to download software. Refer to the sw-dnld command for further information.

set-tftp-srvr

The `set-tftp-srvr` command sets the IP address of the TFTP server used for downloading. To set the IP address of the TFTP server, use the following command:

    set-tftp-srvr <IP address>

set-tftp-mode

The `set-tftp-mode` command sets the TFTP download mode. To set the TFTP download mode, use the following command:

    set-tftp-mode {client|server}

Upgrading the product's software can be done in two different ways,

1. Download from computer to the unit initiated from the unit itself with the appropriate command (sw-dnld),

   The unit acts as a client consuming from the computer, so a TFTP daemon should be started into the computer, and TFTP mode should be set to **client** in the unit.

2. Upload from the computer to the unit initiated from the computer itself,

   The units acts as a server offering a TFTP service to the computer, so the computer should use a TFTP client to upload the software into the unit that should be set to **server** mode.

get-tftp-mode

The `get-tftp-mode` command retrieves the TFTP download mode. This command requires no argument.

sw-dnld

The `sw-dnld` command starts the software download process from the remote TFTP server specified by the set-tftp-srvr command, retrieving the file specified by the set-sw-file command. The progress of the process appears under the form of a dot displayed at regular interval. Once the download is finished the software is copied into the non-volatile RAM then the equipment reboots.

IP Commands

This section lists the IP Configuration commands available at the CLI. It is separated into the following command sections:

- IP configuration
- Address Resolution Protocol (ARP)
- Bootp
- Ping

To view the IP commands, enter IP at the CLI prompt. The following are the available IP commands.

IP Configuration

get-ip

The get-ip command shows the device's current IP address, if any. The following are examples with no IP configuration and an IP configuration defined.

- No IP Configuration defined:

```
SYS_console> get-ip
 The device has no IP Address defined
SYS_console>
```

- IP Configuration defined:

```
SYS_console> get-ip
 The device IP address is: 194.090.136.187
SYS_console>
```

get-ip-cfg

The get-ip-cfg command shows the complete current IP configuration, that is, the address, network mask and broadcast address. The following are examples with no IP configuration and an IP configuration defined.

- No address defined:

```
SYS_console> get-ip-cfg
 The device has no IP Address defined
SYS_console>
```

- IP Configuration defined:

```
SYS_console> get-ip-cfg
 The device IP address, netmask and broadcast are:
            IP address   : 194.090.136.187
            IP netmask   : 255.255.255.000
            IP broadcast : 255.255.255.255
```

23

Setting an IP address

set-ip

The set-ip command sets the IP address of the SNMP Agent. If no IP address was previously set (as is the factory default configuration), the new value is used immediately and saved into NVRAM. Otherwise the new value is only stored in the NVRAM, and the user must execute a warm-reset to effect the change.

    set-ip <*IP address*>

set-ip-cfg

The set-ip-cfg command sets the IP address, network IP mask, and broadcast IP address. If no IP configuration was previously set (as is the default factory configuration), the new values are used immediately and saved into NVRAM. If a previous IP configuration was being used, the new configuration is saved in NVRAM. In order to use the newly defined values immediately, reset the system using the **warm-reset** command.

    set-ip-cfg <*IP address*> <*netmask*> <*broadcast*>

NOTE: If the IP configuration is not specified, the agent does not respond to any in-band requests, including ping messages. The following are examples with no IP configuration and an IP configuration defined.

- No IP Configuration defined:

```
SYS_console>set-ip-cfg 194.90.136.187 255 255.255.0 255.255.255.255
 Device IP Address set for this session
 Device IP Address change in the NVRAM OK
 The device NVRAM IP configuration will be:
           IP address   : 194.090.136.187
           IP netmask   : 255.255.255.000
           IP broadcast : 255.255.255.255
SYS_console>
```

- IP Configuration defined:

```
SYS_console>set-ip-cfg 194.90.136.187 255.255.255.0 255.255.255.255
 Device IP address unchanged for this session
 Device IP Address change in the NVRAM OK

 The device NVRAM IP configuration will be:
           IP address   : 194.090.136.187
           IP netmask   : 255.255.255.000
           IP broadcast : 255.255.255.255
SYS_console>
```

Perform a warm-reset to use the newly defined parameters.

Erasing an IP Configuration

clear-ip-cfg

The clear-ip-cfg command clears the NVRAM IP configuration.

Example

```
SYS_console>clear-ip-cfg
 Device IP Configuration cleared
SYS_console>
```

Configuring a Gateway

get-gatew

The get-gatew command shows the default gateway address.

Example

```
SYS_console>get-gatew
 The default gateway address is : 194.001.001.001
SYS_console>
```

set-gatew

The get-gatew command sets the default gateway IP Address. This command lets you specify the address of the router used to access a different IP network. The default value for the default gateway IP address is 0.0.0.0

```
    set-gatew <IP address>
```
Example

```
SYS_console>set-gatew 194.90.136.254
 Device Default Gateway change in the NVRAM OK
 Device Default Gateway changed to : 194.90.136.254
SYS_console>
```

Bootp Configuration

The bootp feature allows the unit to get its IP address from a bootp server that is properly configured. Bootp options supported include:

- Software filename (bf parameter)

- Unit IP address (ip parameter)

- TFTP server IP address (the IP address of the bootp server itself)

NOTE: Bootp is not part of the boot PROM in version 1.08 of the boot program, therefor NBase-Xyplex recommends you disable the bootp feature and manually set an IP address with the related commands before updating the image file.

To activate/deactivate bootp use the following commands:

`set-bootp` — Enables or disables the bootp process activation.
`get-bootp` — Retrieves the state of the bootp process.

Address Resolution Protocol (ARP)

To view the ARP commands, enter ARP at the CLI prompt. The following are the available ARP commands.

get-arp-tbl

The `get-arp-tbl` command displays the ARP table. The ARP table contains information relating IP addresses to MAC addresses and interface numbers. It also shows the TTL (Time-To-Live) value for each entry.

Example

```
SYS_console>get-arp-tbl
If  Ip                MAC                 TTL
============================================
01  194.090.136.254  08-00-87-1d-9b-32   1200
01  194.090.136.010  00-20-1a-01-3f-18   1200
01  194.090.136.028  08-00-09-9d-5e-30    900
SYS_console>
```

del-arp-entry

The `del-arp-entry` command deletes entries from the ARP table. If an IP address is specified, the matching arp entry is deleted. If * is specified, the entire ARP table is flushed. This command should be used if the network topology has physically changed, e.g. if a management station has been moved from one segment to another, thus changing its interface number.

   del-arp-entry {<*IP address*>|*}

add-arp-entry

The `add-arp-entry` command adds an entry to the ARP table.

   add-arp-entry <*IP address*> <*mac_address*> <*Interface*>

Example

```
SYS_console>add-arp-entry 194.90.136.133 00-11-22-33-44-55 1
 ARP Table Entry successfully added
SYS_console>
```

get-arp-stats

The get-arp-stats command gets ARP statistics.

Example

```
SYS_console>get-arp-stats
InMsgs:        : 0
InErrors       : 0
InIllegals     : 0
InBadOpcode    : 0
InRequests     : 0
InReplies      : 0
InReqNotForMe  : 0
OutMsgs        : 0
OutErrors      : 0
OutRequests    : 0
OutReplies     : 0
ResolveReqs    : 0
SYS_console>
```

Port configuration

This section contains commands for configuring and displaying the ports' parameters with the Administrative Interface. To view the port commands, enter port-cfg at the CLI prompt. The following are the available port commands.

Displaying the Port Configuration

To view the current port configuration, enter the following command:

get-port-cfg {<*dport*> pipe all}

Example

```
SYS_console>get-port-cfg
 PORT_ID  LAN_TYPE   LINK  IF_TYPE  SPEED_SEL  LAN_SPEED  FDPLX  FCNTRL    ENABLE
 ======================================================================================
    1      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
    2      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
    3      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
    4      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
                                        .
                                        .
                                        .
   22      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
   23      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
   24      ETH10/100  OFF   TP       AUTO       Not Set    N/A    DISABLED  ON
   25      ETH1000    OFF   FO       FORC1000   1000Mbps   ON     DISABLED  ON
SYS_console>
```

27

- PORT_ID: An interface number specified in the form of 1-25 (dport).
- LAN_TYPE:
  - ETH-10/100
  - ETH1000 indicates Gigabit Ethernet
- LINK: ON/OFF if ON a device is connected to the port and the link is UP
- IF TYPE: TP (twisted pair)/FO (fiber optic)
- SPEED_SEL: AUTO/FORC10/100/1000
- LAN_SPEED: The actual speed that has been negotiated between the entities.
- FDPLX: OFF = Standard Ethernet (default), ON = Full Duplex
- FCNTRL: DISABLED/ENABLED
- ENABLE: ON = port is enabled (default), OFF = port is disabled

Setting the port configuration

set-port-cfg

The `set-port-cfg` command selects the speed (10/100/auto-neg) and duplex mode (half/full).

```
set-port-cfg <port-number> <speed> <mode>
[arg #0] port index in format <dport>
[arg #1] enter either {auto|100|10}
opt.[arg #2] enter either {half|full}; default : half
```

Example

```
SYS_console>set-port-cfg 100 half
```

set-port-state

The `set-port-state` command is used to enable or disable a port when the Spanning Tree algorithm is not running.

```
set-port-state<port number > {enable|disable}
opt. [arg #0] port index in format <dport>; default:all
opt. [arg #1] enter either {enable|disable}; default:enable
```

Example

```
sys_console>set-port-state 2 enable
```

Setting the flow control

Ports are compliant to flow control specifications 802.3x or back-pressure.

You can set a port to perform flow control only if this port is in full duplex mode otherwise back-pressure is applied to control the incoming flow of data.

When the port is configured to do 802.3z flow control the switching engine sends a continuous flow of idle frames to avoid dead locks.

If the port applies back-pressure the mechanism is slightly different in the sense that instead of sending idle frames the switching engine sends a collision signal.

get-fctrl

The `get-fctrl` command displays the status of the flow control function.

```
get-fctrl <database> <port-number>
opt.[arg #0] database type - either {run|nvram|all}; default : run
opt.[arg #1] port index in format <dport>;default: all
get-fctrl nvram
SYS_console>get-fctrl ?
```

Example

```
get-fctrl     gets the port flow control request: enable or disable
opt.[arg #0] database type - either {run|nvram|all}; default : run
opt.[arg #1] port number  - 1..25; default : all
SYS_console>
```

set-fctrl

The `set-fctrl` command sets a port's flow control mode.

```
SYS_console>set-fctrl ?
set-fctrl     sets the port flow control: enable or disable
    [arg #0] database type - either {run|nvram|all}
    [arg #1] port number  - 1..25
opt.[arg #2] enter either {enable|disable}; default : enable
```

EtherChannel

The EtherChannel feature is also known under the name of Port Trunking. It allows equipment to pass data through multiple physical links. Providing an extended bandwidth and redundancy.

NOTE: If you want to use this feature in conjunction with VLAN be aware that you must set exactly the same VLAN configuration for each physical link that belongs to the EtherChannel group.

Also, before proceeding to the configuration of trunking ports you should be aware of the following considerations:

1. You cannot mix different media types (for example, optical and copper) in the same group.

2. You cannot declare more than 8 ports in a group.

3. You should declare groups with ports belonging to the same switching engine. You may declare a group using ports 1 to 8, or port 9 to 17 or port 18 to 24 or port 25 and 26.

NOTE: The EM2025-2GE module does not support EtherChannel groups.

Getting the EtherChannel Configuration

get-ec-tbl

The `get-ec-tbl` command retrieves the EtherChannel configuration.

```
get-ec-tbl {run|nvram|all}
```

Example

```
SYS_telnet>get-ec-tbl run
Ethernet Channel Table from RUN database
==========================================
 Ether-Channel-ID    Ports
==========================================
   1              23 24
```

Setting the EtherChannel Configuration

new-ec

The `new-ec` command sets the EtherChannel port configuration. EtherChannel allows the switch to split the traffic between two or more links.

```
new-ec     Create a new EtherChannel
    [arg #0] database type - either {run|nvram|all}
    [arg #1] Ports - ports list in format: d1-...-dn
```

Example

```
SYS_telnet>new-ec run 23-24
 RUN:OK
Ethernet Channel Table from RUN database
==========================================
 Ether-Channel-ID    Ports
==========================================
   1              23 24
```

Deleting the EtherChannel Configuration

del-ec

The del-ec command deletes the trunk port configuration.

```
del-ec      Remove an EtherChannel
    [arg #0] database type - either {run|nvram}
    [arg #1] EtherChannel index (from get-ec-tbl)
```

Port Priority

Consider the following when setting the Port Priority:

- Internal Use – The priority is used internally, the switch accepts frames coming from the port with the highest priority.

- External Use – Port Priority conforms to IEEE 802.1P standard and provides a priority scale from 1 to 8. The higher the value, the higher priority applied to the frame.

  This priority is embedded into the tag header, as defined in the IEEE 802.1Q standard. This can be set on a port or to a VLAN. To do this, you need to set the vlan-mode to tagged and then specify the ports connecting the switch to the others to trunk with the command set-tag-outbound-mode. Refer to the VLAN and Port Configuration sections of this guide for further information.

Set Port Priority

The set-port-priority command is used when a specific machine, or group of systems connected to a particular port, need to have their frames sent at a different level of priority than the other.

```
set-priority-port-cfg     sets the priority of a port
    [arg #0] database type - either {run|nvram|all}
opt.[arg #1] port number  - 1..25; default : all
opt.[arg #2] port priority 1..8 (1..4 - low, 5..8 - high); default : 1
```
Example

```
SYS_telnet>set-priority-port-cfg run 1 8
 The Port Priority was changed for port  1
```

31

Get Port Priority

get-priority-port-cfg

The get-priority-port-cfg command retrieves the port priority configuration.

Example

```
SYS_telnet>get-priority-port-cfg
Ports Priority Configuration :
   1- 8    2- 1    3- 1    4- 1    5- 1    6- 1    7- 1    8- 1
   9- 1   10- 1   11- 1   12- 1   13- 1   14- 1   15- 1   16- 1
  17- 1   18- 1   19- 1   20- 1   21- 1   22- 1   23- 1   24- 1
```

VLAN Priority

The vlan-prio-modify command applies to the components of that VLAN. This is a means to provide priority to a specific VLAN.

```
vlan-prio-modify {run|nvram}
    [arg #1] VLAN index (from get-vlan-tbl
    [arg #2] VLAN priority 1..8 (1..4 - low, 5..8 - high)
```

Example

```
SYS_console>vlan-prio-modify  run 1 8
 Set Runtime VLAN Tag Domain entry Ports 8 -
```

Modifying the Switch Policy

The switch policy determines the default behavior of the switch when no priority is declared. The set-priority-policy command is useful when there is not a real need to set a particular port or VLAN to a different priority level. The default policy value is 2, which corresponds to a low priority.

If you want this switch to have a higher policy you can define a different level from 1 to 4.

```
set-priority-policy {run|nvram|all}
opt.[arg #1] priority policy 1..4, default: 2
```

Example

```
SYS_console>set-priority-policy run 1
 Set Runtime Priority Policy 1 -
OK
SYS_console>get-priority-policy run
 Runtime Priority Policy is 1
SYS_console>
```

Spanning Tree Protocol (STP)

The switch software supports IEEE 802.1D Spanning Tree Protocol (STP) which ensures the existence of a loop-free topology in networks that contain any arrangement of devices.

STP produces a logical tree topology to ensure that a single path exists between any two end stations on an interconnected network. STP also provides a high degree of fault tolerance. It allows the network to automatically reconfigure the spanning tree topology if there is a bridge or data-path failure.

Multiple paths to a destination can be good, as in the case of using secondary paths to provide redundant links in the event of problems with the primary link. It can also lead to bad network performance when problems arise from having more than one path. STP allows for redundancy without the performance problems.

How the STP Topology Stabilizes

The switch software incorporates the IEEE 802.1D Spanning Tree Protocol (STP) to prevent the duplication of paths in an interconnected network.

1. When a switch, with STP enabled, starts up, it assumes that it is the Root Bridge and puts all of its external ports into "listening" mode. The switch then sends a configuration BPDU listing its bridge ID as being the Root Bridge ID (MAC address and priority) on all its external ports.

2. As each switch port receives a configuration BPDU, the switch compares the Root Bridge information in the BPDU to its current Root Bridge information. If the bridge priority or MAC address Root Bridge information in the BPDU supersedes the switch's current Root Bridge information, the switch sets the new Root Bridge ID and configuration information as current and sets the root interface. The switch then adds it own pathcost to the Root Bridge pathcost and resends this information on its external ports.

   If the root information received by the port does not supersede the current bridge information, the port compares the bridge ID in the message to its own bridge ID. If the root information received by the port supersedes the current bridge information, the port makes the received bridge ID as the designated bridge.

3. When the forwarding delay time expires, the switch checks the status of each interface. If the switch interface is either the root interface or a designated bridge for the interface, the port is set to forwarding. Otherwise it is blocked.

4. Periodically, the Root Bridge sends a Hello BPDU out on all of its external ports. If a switch does not receive a Hello BPDU from the Root Bridge, within the period of time specified by the Maximum Age Timer, the switch assumes that the network is reconfiguring and STP starts again.

33

Spanning Tree Parameters

Normally, each switch or bridge in a network participates in STP. The units work together as peers to determine which links are to forward packets between LANs, and which links are to be blocked. Links that forward packets are chosen based on which link has the lowest pathcost and priority. Redundant paths are blocked, unless another link which is a forwarding link is deactivated, at which the blocked link will then go into a forwarding state.

NOTE: NBase-Xyplex switches are compatible with STP software that conforms to the IEEE 802.1D specification. They are not compatible with other STP versions that do not conform to this specification (for example, the DEC STP implementation). If you install a NH2025-10 switch in a network where other devices are using non-conforming (i.e., not 802.1D) STP, you must make sure that no loops exist in the network topology.

Root Bridge

Units that participate in STP compete to be the Root Bridge of the switched network. At start-up, each unit broadcasts an STP message called a Configuration Bridge Protocol Data Unit (Configuration BPDU) through each of its interfaces, announcing its bridge ID, including its priority value and MAC address. The unit with the lowest priority value is recognized as the Root Bridge. In the event of a tie, the unit with the lowest MAC address becomes the Root. After the STP topology stabilizes, Hello BPDUs are periodically sent by the Root bridge and are propagated down the Spanning Tree by other bridges in the switched network. Each bridge adds its own pathcost before forwarding.

Manually Designating a Root Bridge

By assigning priority values to the switches in your network, you can designate which unit is to be the Root Bridge, which is to be the 1st backup Root Bridge, 2nd backup Root Bridge, etc. There are no rules for selecting a Root Bridge. However, most commonly the Root is located in the middle of the network or at the corporate data center. For instructions on assigning Priority values, refer to the Spanning Tree Commands section.

Selecting a Designated Switch/Bridge

When a LAN has multiple switches connecting it to a remote LAN, the units compete to determine which can provide the best service to the LAN. The units that can provide the best service is recognized as the Designated Switch/Bridge for the LAN. Other units provide standby connections.

Topology Change Notification BPDU

A non-Root interface sends a Topology Change Notification BPDU (TCN BPDU) over its Root interface any time it believes that the network topology has changed.

The following circumstances can cause this to happen:

- A Root interface gives up its Root status and the topology state is changing.

- A switch receives a TCN BPDU from another unit via a non-Root interface.

- An interface's state changes (it enters the Forwarding state). When a Root interface receives a TCN BPDU, it sets a Topology Changing flag in its Hello BPDU for an interval that is twice the length of the Forward Timer. When a non-Root interface receives a Hello BPDU with this flag set, it quickly ages its dynamic filter s so that it can relearn its filters based on the new topology.

Using STP to Manage Redundant Links

Multiple switches can be connected to form a larger switched network, without using STP the connections between the switches would form a loop. STP should be used to block one of the connections. If the primary connection fails for some reason, STP reconfigures the topology and direct all inter-switches traffic on the redundant link.

Spanning Tree and VLAN restrictions

If you want to use STP and VLAN you should know how the implementation of STP in our products operates. One instance of STP runs in the management VLAN. So the consequence is that STP does not resolve loop in VLAN to which it does not belong. If you want to use the redundancy facility you should use Trunking/EtherChannel feature instead.

Spanning Tree Commands

To view the Spanning Tree commands, enter sp-tree at the CLI prompt. The following are the available port commands.

Enabling/Disabling STP

`set-stp enable`

Enabling or disabling Spanning Tree does not take effect until the SNMP agent is reset, via `warm-reset`, `cold-reset` or a power cycle. The default is disabled.

`get-stp`

The `get-stp` command retrieves the current state of Spanning Tree.

`Example`

```
SYS_console> get-stp
Running spanning tree engine is disable
Next session of the Spanning Tree engine will be disabled.
SYS_console>
```

Viewing Bridge Parameters

get-st-bcfg

For determining Root in a spanning tree network, the MAC address is a tie breaker when priority values for devices are equal. In this case, the unit with the lowest MAC address becomes the root. For NH 2025-10 products, the lowest numbered switch has the lowest MAC address.

Example

```
SYS_console>get-st-bcfg
 802.1D SPANNING TREE BRIDGE INFO
 =================================
 Designated Root      : 0100-0800-870e-0742
 Bridge Priority      : 32768 ( 0x00008000 )
 Root Cost            :    10
 Root Port            :  1.02
 Max  Age             :    20
 Hello Time           :     2
 Hold  Time           :     1
 Forward Delay        :    15
 Bridge Max Age       :    20
 Bridge Hello Time    :     2
 Bridge Forward Delay :    15
 ------ The time units are seconds
SYS_console>
```

Configuring the Bridge

Modifying the designated root: set-br-prio

By modifying the bridge priority you are able to choose which component becomes the Root Bridge in your network. Decrease the priority to a value below the lowest priority you can see in the other switches if you want this bridge to be the Root Bridge.

    set-br-prio <*priority*>

The *priority* value is an integer in the range 0..65535. The default value is 32768.

Example

```
SYS_telnet>set-br-prio 32768
 The Bridge Priority was changed
SYS_console>
```

Max Age: set-br-maxage

The set-br-maxage command sets amount of time between Spanning Tree configuration messages.

    set-br-maxage <*maxage*>

The *maxage* value is displayed in seconds with the range of 6..40. The default value is 20.

Hello Time: `set-br-hellot`

The `set-br-hellot` command sets the Spanning Tree bridge's *hello time*.

    set-br-hellot <hello_time>

The *hello_time* is an integer in the range 1..10, displayed in seconds. The default value is 2.

Forward delay: `set-br-fwdel`

The `set-br-fwdel` command sets the Spanning Tree Bridge Forward Delay, which controls the amount of time between the listening and forwarding states of a port.

    set-br-fwdel <forward_delay>

The *forward_delay* value is an integer displayed in seconds in the range 4..30. The default value is 15.

Viewing the Port Configuration

`get-st-pcfg`

The `set-br-pcfg` command retrieves Spanning Tree port parameter table. If Spanning Tree is disabled, no parameters are retrieved.

    get-st-pcfg {<port-number>|all}
    opt. [arg#0] port index in format <dport>; default:all

Example

```
SYS_console>get-st-pcfg
 STP PORT TABLE
================
ID Prior State PathCost    DesigRoot        DesigCost   DesigBridge   DesigPort
-----------------------------------------------------------------------------
1  128   FWD     10     8000-0020-1a00-8ca2  20  8000-0020-1a00-a75a 8001 D
2  128   FWD     10     8000-0020-1a00-8ca2  20  8000-0020-1a00-a75a 8002 D
3  128   FWD     10     8000-0020-1a00-8ca2  20  8000-0020-1a00-a75a 8003 D
4  128   FWD     10     8000-0020-1a00-8ca2  20  8000-0020-1a00-a75a 8004 D
5  128   FWD     10     8000-0020-1a00-8ca2  20  8000-0020-1a00-a75a 8005 D
```

Setting Port Configuration

Port priority: `set-prt-prio`

The `set-prt-prio` command sets the Spanning Tree port priority, and gives ports priorities for blocking.

    set-prt-prio <dport>

The *dport* is the decimal port number, **port_priority** is an integer in the range 1..255. The default value is 128.

Example

```
set-prt-prio 4 128
Priority was changed for port 4
SYS_console>
```

Enabling/disabling a port: `set-prt-enb`

To enable or disable spanning tree on a port. The default value is disabled.

```
set-prt-enb <port-number> {enable|disable}
```

Example

```
SYS_console>set-prt-enb 4 enable
 The Port State was changed to <enable> for port    4
SYS_console>
```

Changing the path cost: `set-prt-pcost`

```
set-prt-pcost <dport> <path_cost>
```

The parameter *dport* is the integer port number, and the *path_cost* parameter is an integer path cost in the range 1..65535. Using 0 as path_cost causes the switch to calculate the path cost automatically according to the port speed. The default values are 4, 10, and 100.

Example

```
set-prt-pcost 4 20
 The Port Path Cost was changed for port 4
SYS_console>
```

Switching Commands

This section contains instructions for managing the Switching Database with the Command Line Interface. To view the available switch commands, enter switch-db at the CLI prompt.

The Switching Database consists of 12K entries. Each active entry contains the information relevant to a workstation, characterized by its Ethernet MAC Address.

Learning Table

The following section lists commands relevant to the Learning table and Aging mechanism of the switch. The *index* contained in the following commands is an integer number between one and the maximum size of the Switching Database Table (12K).

Aging Configuration

get-lt-age

The get-lt-age command displays the Switching Database Aging Time in seconds. The default value for the Aging Time is 300 seconds. The Aging Time is the time-out period for dynamically learned forwarding entries. An entry whose MAC address does not appear in the source field of an incoming packet for a period equal to the Aging Time is discarded.

Example

```
SYS_console> get-lt-age
Running aging period:  300 seconds
CURRENT aging period:  300 seconds
NVRAM aging period:    300 seconds
SYS_console>
```

set-lt-age

The set-lt-age command allows you to modify the Switching Database Aging Time. The change may be made:

- In the running database so that the new value is used immediately.

- In the NVRAM, meaning that the change occurs only in the next session.

- In both the running and the NVRAM databases.

  set-lt-age {run|nvram|all} <*aging_time*>

The *aging_time* value is in seconds. The default value is 300 seconds. Use a lower value if the number of active workstations at a given moment is larger than the size of the Switching Database. The aging time can be anywhere between 10 and 11,000 seconds. 0 is used for aging OFF.

Example

```
SYS_console> set-lt-age run 400
Aging Period update – OK
SYS_console>
```

get-lt-entry

The get-lt-entry command displays the entry at *index* in the Switching Database.

```
get-lt-entry <index>
```

The *index* value is the entry number in decimal, between 1 and 12288.

Example

```
SYS_console>get-lt-entry 1
 Entry  ---- MAC Address ----  LOCK  DPORT    SELF  Vid   T
================================================================
    1     00-20-1a-00-8c-3f     +    -NONE-    +   0000  –
SYS_console>
```

- **Entry –** Signifies the index in the Switching Database Table.

- **MAC Address –** contained in an entry or given as a parameter is printed as a 6-byte hexadecimal sequence separated by the "-" sign. For example:

  ```
  00-20-1A-00-01-29
  ```

- **LOCK –** If on (denoted as a +), the entry is not deleted by the switch aging process (static entry). If off (denoted as a -), this is a dynamic entry that may be automatically deleted by the switch aging process if the MAC address is not active during the aging time period.

- **DPORT –** The destination port to which frames with the stated address are forwarded.

- **SELF** (not user configurable) **–** If on (denoted as a +), the entry is a system address. These addresses are the switch's individual and group addresses, as well as other addresses added by the management system. If off (denoted as a -), the entry contains the MAC address of a station connected to the switch.

- **VID –** The VLAN Identifier (tag) (appears only when features are enabled).

- **T –** Tag flag (appears only when features are enabled).

get-lt-16

The get-lt-16 command displays 16 learning table entries starting at *index*, or * to continue from the last displayed index. The format of the display is similar to the previous command format. If the end of the Learning table is reached, the * parameter starts the list over from the beginning.

```
get-lt-16 {<index>|*}
```

Example

```
SYS_console>get-lt-16 *
number of entries:124
 Entry  ---- MAC Address ----  LOCK  DPORT     SELF
 ===================================================
    1      00-20-1a-00-a7-c7     +     -NONE-     +
    2      00-20-1a-01-a7-c7     +     -NONE-     +
    3      00-20-1a-02-a7-c7     +     -NONE-     +
    4      00-20-1a-03-a7-c7     +     -NONE-     +
    5      00-20-1a-04-a7-c7     +     -NONE-     +
    6      00-20-1a-05-a7-c7     +     -NONE-     +
    7      00-20-1a-06-a7-c7     +     -NONE-     +
    8      00-20-1a-07-a7-c7     +     -NONE-     +
    9      00-20-1a-08-a7-c7     +     -NONE-     +
   10      00-20-1a-09-a7-c7     +     -NONE-     +
   11      00-20-1a-0a-a7-c7     +     -NONE-     +
   12      00-20-1a-0b-a7-c7     +     -NONE-     +
   13      00-20-1a-0c-a7-c7     +     -NONE-     +
   14      00-20-1a-0d-a7-c7     +     -NONE-     +
   15      00-20-1a-0e-a7-c7     +     -NONE-     +
   16      00-20-1a-0f-a7-c7     +     -NONE-     +
SYS_console>
```

The first displayed entries belong to the system. These entries contain information related to the SNMP Agent and should never be modified or removed. These entries are locked, (a (+) in the LOCK and SELF columns).

MAC addresses, noted with a (-) in the LOCK and SELF columns were learned from the port stated in the DPORT field.

find-lt-addr

The find-lt-addr command searches for a MAC address in the Learning table. If the *mac_address* is found in the Switching Database, the entry is displayed:

```
find-lt-addr <mac_address> <VID>
[arg #0]  MAC address in hex format xx-xx-xx-xx-xx-xx
[arg #1]  VLAN ID
```

Example

```
SYS_console>find-lt-addr 00-20-1a-00-8c-4d 1
 Entry  ---- MAC Address ----  LOCK  DPORT     SELF  Vid   T
 ==============================================================
   15      00-20-1a-00-8c-4d     +     -NONE-     +   0000  -
SYS_console>
```

If the requested MAC address is not in the table, an error message is displayed.

41

Deleting Entries

del-lt-entry

The del-lt-entry command deletes the Learning table entry at *index*.

    del-lt-entry <*index*>

Deleting entries with the SELF field set (+) is prohibited since they are system addresses.

<table>
<tr><td align="center">CAUTION</td></tr>
<tr><td>Use the del-lt-entry command with caution, as it allows you to change the Switching Database.</td></tr>
</table>

del-lt-port

The del-lt-port command deletes the learning table entries for a particular port.

    del-lt-port <*port*>

```
sys_console> del-lt-port 3
```

del-lt-addr

The del-lt-addr command deletes the Learning table entry that matches the *mac_address*.

The command fails if the *mac_address* is not found in the Learning table. Again, as in the previous command, use caution when deleting system entries with a (+) in LOCK column.

    del-lt-addr <*mac_address*> <*Vid*>

Example

```
SYS_console>del-lt-addr 00-11-22-33-44-55
 MAC Address - 00-11-22-33-44-55 - not in LT
SYS_console>
```

Adding Static Entries

add-lt-entry

The add-lt-entry adds a Learning table entry to the Switching Database. The command parameters are described at the beginning of this chapter.

```
add-lt-entry adds an LT entry
    [arg #0] MAC address in hex format xx-xx-xx-xx-xx-xx
    [arg #1] port number - 1..25
    [arg #2] S- static (lock on) or D- aging out (lock off)
    [arg #3] VLAN Tag {2..4095}
    [arg #4] T- tagged or N- untagged
```

Example

```
SYS_console>add-lt-entry 1-2-3-4-9-10-11
 Add LT entry – OK
SYS_console>
```

Virtual Broadcast Domain

Virtual broadcasts domain is a concept that tends to confine broadcasts in a physical domain, it allows to diminish the bandwidth used by broadcasts, giving more room to the unicast traffic, it also prevent the phenomenon called broadcasts storms to affect the entire network. VBC are not made for a security purposes but to improve the efficiency of the communications in a network. VBC disconnect entities belonging to different domain by avoiding the service traffic (broadcasts) to go through. For instance, an ARP broadcast request sent by a machine which belongs to VBC 1 to a machine belonging to VBC 2 will not have an answer, thus the initiating entity cannot resolve the layer 3 address to a MAC address and consequently cannot communicate with the VBC 2 machine.

Viewing the VBC Mode

get-vlan-mode

```
get-vlan-mode {run|nvram}
```

Example

```
SYS_console>get-vlan-mode run
 Runtime VLAN mode is disabled
SYS_console>
```

Setting the VBC mode

set-vlan-mode

There are three modes available: vbc, tag, or none. The modes are mutually exclusive (i.e. only one mode can be defined for running session). The default value mode is none.

```
set-vlan-mode <database><VLAN state>
   [arg #0]  database type - either {run|nvram|all}
   [arg #1]  VLAN state: either {vbc|tag|none}
```
Example

```
SYS_telnet>set-vlan-mode run vbc
 Set run VLAN mode vbc- OK
```

Creating VBC Domains

set-vbc-domain

The set-vbc-domain command is applicable only after enabling the "vbc mode," using the set-vlan-mode command. It establishes a Virtual broadcast domain. The *port_list* value is a dash-separated list of ports to group into a broadcast domain.

```
set-vbc-domain {run|nvram|all}  <port_list>
```

For example, to create a virtual broadcast domain of ports 2, 5, and 6, use the following command:

```
sys_console>set-vbc-domain all 2-5-6
```

Viewing VBC Matrix

get-vbc-tbl

```
get-vbc-tbl {run|nvram}
```

Example

```
SYS_console>get-vbc-tbl run
 Runtime VLAN mode is VBC Domain
  RUNTIME    VIRTUAL BROADCAST DOMAIN TABLE
==========================================
     Ports
     00000000 01111111 11122222 2
VBC 12345678 90123456 78901234 5
 1: -+--++-- -------- -------- -
SYS_console>
```

NOTE: VBC are materialized with the sign "+" so the ports 1.1 to 1.4 belongs to VBC 1, port 1.5 to 1.6 belongs to VBC 2. The other ports 1.7 and 1.8 are in the default VBC. Broadcasts from VBC 1 cannot flood VBC 2 or even the default VBC.

get-vbc-matrix

The get-vbc-matrix command retrieves the current broadcast Domain matrix. The first column is the source port list. The other columns are broadcast destination ports to which frames from a given source port may be forwarded.

```
get-vbc-matrix <dport>
```

Example

```
SYS_console>get-vbc-matrix
   VBC CONNECTIVITY MATRIX
  ===============================
           0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
SRC to :   1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
    1 :    - - - - - - - - - - - - - - - - - - - - - - - - -
    2 :    - - - - + + - - - - - - - - - - - - - - - - - - -
    3 :    - - - - - - - - - - - - - - - - - - - - - - - - -
    4 :    - - - - - - - - - - - - - - - - - - - - - - - - -
    5 :    - + - - - + - - - - - - - - - - - - - - - - - - -
    6 :    - + - - + - - - - - - - - - - - - - - - - - - - -
    7 :    - - - - - - - - - - - - - - - - - - - - - - - - -
    8 :    - - - - - - - - - - - - - - - - - - - - - - - - -
                         .
                         .
                         .
   24 :    - - - - - - - - - - - - - - - - - - - - - - - - -
   25 :    - - - - - - - - - - - - - - - - - - - - - - - - -
SYS_console>
```

NOTE: In this example the sign "+" at the intersection of rows and columns mean that a connection is established. The sign "-" indicates that there is no connectivity.

Deleting a VBC

del-vbc-domain

```
del-vbc-domain {run|nvram}  <domain_id>
```

The `domain_id` parameter is the vbc id number as identified by `get-vbc-tbl`.

Example

```
SYS_telnet>del-vbc-domain run 1
 Delete Runtime Virtual Broadcast Domain entry - OK
 Runtime VLAN mode is VBC Domain
 RUNTIME    VIRTUAL BROADCAST DOMAIN TABLE
==========================================
    Ports
    11111111 7
VBC 12345678 1
 2: ----+++- -
```

NOTE: When you use the set-vbc-domain command with the all parameter, both the runtime and nvram databases are changed. In case you need to delete the mentioned vbc entries, you should run the del-vbc-domain command twice with run and nvram parameters.

Virtual Networking

Virtual Networking provides the capability to view user communities as a large set of disconnected, yet potentially connectable stations. This allows you to develop and apply your own criteria for grouping users within isolated work groups.

After such groups are created considering these criteria, the groups are actually implemented via hardware and software that, in effect, provide a Virtual Bridging function between all the member stations in a particular group. This collection of stations, referred to as a Virtual LAN, shares a common multicast domain. Members of different Virtual LANs can only communicate via Routers.

In the Figure, most stations are members of a particular Virtual LAN and have a particular Virtual LAN Number (VLN 2, 3, 4, etc.). Those stations not in a particular Virtual LAN are automatically members of the "Default Virtual LAN". MAC-layer unicast and multicast traffic propagating within this virtual topology can be separated into two groups: traffic passing between stations within the same Virtual LAN, and traffic passing across Virtual LAN boundaries.

Unicast traffic moving within a Virtual LAN is propagated from its source, directly to its destination. Other stations are not exposed to this traffic (in contrast to repeated environments) unless they ultimately share physical segments with either the source or destination specified in a particular dialog. Multicast traffic is passed to all stations in the Virtual LAN, as if all stations were connected to a single multi-port switch. Traffic cannot pass between Virtual LANs without the aid of a Router. These internetworking devices must be physically connected to the network with a separate physical interface for each Virtual LAN.

Important Considerations

Before configuring your VLAN you must strictly follow the scenario:

1. Set the VLAN mode to tagged.

2. Set the server ports (see Server Port chapter in this manual).

3. Set the tagging ports (see ISVLAN chapter in this manual).

4. Configure the new VLAN.

5. Configure the management VLAN.

Virtual LANs can be used to limit the broadcast domain and to establish secure virtual workgroups. The following parameters are used within the VLAN commands.

- **run** – indicates that only the currently running configuration is changed. Changes are not restored after a reset.

- **nvram** – indicates that only the configuration stored in non-volatile memory is changed. Changes do not take effect until a warm or cold reset.

- **all** – indicates that both the currently running configuration and the non-volatile configuration is changed. The changes take effect immediately and are restored after a reset.

Viewing the VLAN Mode

get-vlan-mode

```
get-vlan-mode {run|nvram}
```

Example

```
SYS_console>get-vlan-mode run
 Runtime VLAN mode is disabled
SYS_console>
```

Setting the VLAN Mode

set-vlan-mode

Three modes are available: vbc, tag or none. The modes are mutually exclusive (i.e. only one mode can be defined for running session). The default mode is none.

```
set-vlan-mode <database> <VLAN state>
    [arg #0]  database type - either {run|nvram|all}
    [arg #1]  VLAN state: either {vbc|tag|none}
```
Example

```
SYS_console>set-vlan-mode run tag
 Set run VLAN mode tag – OK
SYS_console>
```

Inter-Switch VLAN or ISVLAN

The inter-switch VLAN conforms to the standard IEEE 802.1q, which describe the method of passing tagged frames through a physical link. To satisfy the need, the frame format should be changed and 4 more bytes are added to the frame header between the end of address field and the frame type.

Tag Field Format

This is a 4 bytes long field divided into two sub-fields of 2 bytes respectively named TPID and TCI.

- TPID is the Tag Protocol Identifier which identifies the tag type of the frame.

- TCI contains the user priority bits and the VID (VLAN Identifier).

Principles of ISVLAN

To configure a tagged port that could carry specific tagged frames you need the necessary information about how our ISVLAN works.

- The port declared as tagged port should belong to all the VLAN's you are willing to interconnect between multiple switches with the command *set-tag-outbound-mode.*

- Once you have declared the tagged port you can create the specific VLAN's using the command set provided in this section.

Viewing the ISVLAN Mode

get-tag-outbound-mode

The get-tag-outbound-mode command shows the VLAN Tagging ports' state. A "T" indicates that the Tagging mode off the port is on, "A" indicates that the Tagging is off.

```
get-tag-outbound-mode {run|nvram}
```
Example

```
SYS_telnet>get-tag-outbound-mode
   1    2    3    4    5    6    7    8    9   10   11   12
===============================================
   T    A    A    A    A    A    A    A    A    A    A    A


  13   14   15   16   17   18   19   20   21   22   23   24
===============================================
   A    A    A    A    A    A    A    A    A    A    A    A


  25
====
   A
```

NOTE: The letter T means the port is set to tag mode. The letter A means the port is set to access.

Setting a Tagged Port

set-tag-outbound-mode

The set-tag-outbound-mode command can be used to enable or disable VLAN tagging to port/s on a network on which all nodes support the IEEE 802.1Q standard or a comparably capable network. Do not enable a port connected to a network on which there are any nodes that do not support the IEEE 802.1q standard.

```
set-tag-outbound-mode {run|nvram|all} <port-list> {enable|disable}
[arg #0]  database type - either {run|nvram|all}
[arg #1] ports - ports list in format: <dport>
[arg #2]  VLAN state: either {disable|enable}
```

Example

```
SYS_console>set-tag-outbound-mode run 5 enable
 Set run VLAN Tag awareness – OK
SYS_console>
```

Removing a Tagged Port

To remove a previously declared tagged port you have to use the same command.

```
set-tag-outbound-mode {run|nvram |all}<port-list>{enable|disable}
[arg #0]  database type - either {run|nvram|all}
[arg #1] ports - ports list in format: S1.D1-S2.D2-...-Sn.Dn
[arg #2]  VLAN state: either {disable|enable}
```

Example

```
SYS_console>set-tag-outbound-mode run 5.8 disable
 Set run VLAN Tag awareness – OK
SYS_console>
```

Server Port

A server port is a shared port among VLANs. This port is seen from every VLAN it belongs to, VLANS can see it but they cannot use it as a third party to communicate.

Creating a Server Port

new-srvr-port

The new-srvr-port command defines a "server port" as a VLAN with one port (server) and a dedicated tag. The user then defines the "server port" as a member of all the tag-based VLANs from which access is desired. Access to the "server port" is available only to ports of VLANs in which the "server port" is a member. This is done in order to share a common resource, such as a network server, over the defined tag VLANs.

48

NOTE: You must issue the `new-srvr-port` command before the `new-vlan` commands for those VLANs to which it will be made available.

```
new-srvr-port    Set a Vlan Server port(s)
    [arg #0] database type - either {run|nvram|all}
    [arg #1] server ports - ports list in format: d1-...-dn
    [arg #2] VLAN Tag { 2..4095 }
opt.[arg #3] VLAN priority 1..8 (1..4 - low, 5..8 - high); default : 1
```

Removing a Server Port

del-srvr-port

The `del-srvr-port` command deletes a defined server port.

```
del-srvr-port <database><port-list>
[arg#0] database type – either {run|nvram}
[arg#1] server ports – ports list in format: <dport>
```

VLAN

Creating a VLAN

new-vlan

The `new-vlan` command creates a new VLAN (`tag` based).

```
new-vlan    Make a new VLAN
    [arg #0] database type - either {run|nvram|all}
    [arg #1] Name of new vlan
    [arg #2] VLAN Domain - ports list in format: d1-...-dn
    [arg #3] VLAN Tag { 2..4095 }
opt.[arg #4] VLAN priority 1..8 (1..4 - low, 5..8 - high); default : 1
```
Example

```
SYS_console>new-vlan all v1 9-10-11-12 10
 Set run Port VLAN Domain entry – OK
SYS_console>
```

NOTE: If you plan to define a server port, then you must configure that before you define the VLANs.

Viewing VLAN Configuration

get-vlan-tbl
```
    Get-vlan-tbl {run|nvram}
```

Example

```
SYS_console>get-vlan-tbl run
 Runtime VLAN mode is VLAN Tagging
VLAN Table from RUN database (Mgmt tag: 1)
 RUNTIME    VLAN TAG DOMAIN TABLE
=========================================
 VID          NAME   PRIO  Ports
=========================================
  1 S     SRVR_30    1    1 2 3 4 9 10 11 12 5S
  2           RND    1    9 10 11 12 5S
  3       FINANCE    1    1 2 3 4 5S
SYS_console>
```

get-vlan-entry

```
get-vlan-entry <database> <VID>
    [arg #0]  database type - either {run|nvram} default : run
    [arg #1] VLAN index (from get-vlan-tbl; default : 1
```

Example

```
SYS_telnet>get-vlan-entry run 3
RUNTIME:
 =========================================
 VID          NAME   TAG  Prio Ports
=========================================
  3       FINANCE       20  1  1 2 3 4 5
SYS_console>get-vlan-entry run 3
```

Deleting a VLAN

del-vlan

NOTE: You cannot delete both Server and Management VLANs.

```
del-vlan <database> <VID>
    [arg #0]  database type - either {run|nvram}
    [arg #1]  VLAN id (from get-vlan-tbl
```

Example

```
SYS_console>del-vlan run 1
 Delete Runtime VLAN Tag Domain entry - OK
Runtime VLAN mode is VLAN Tagging
VLAN Table from RUN database (Mgmt tag: 1)
```

WARNING

If the Management VLAN is deleted, connections to the CPU are lost (management port).

VLAN Management

The processor that manages the product (SNMP responses and traps, remote telnet connections) does not belong to a VLAN that you have declared previously, so to get access to the processor through the network it is recommended to make the processor a part of a chosen VLAN with the following set of commands.

Viewing the Management Tag

get-mgmt-vlan-tag

By default the Management processor belongs to (CPU) VLAN tag 1.

```
get-mgmt-vlan-tag {run|nvram}
```
Example

```
SYS_console>get-mgmt-vlan-tag run
Management VLAN tag: 1
SYS_console>
```

Modifying the Management Tag

add-mgmt-to-vlan

The add-mgmt-to-vlan command adds management (CPU) to an existing VLAN.

```
add-mgmt-to-vlan <database> <VTAG>
   [arg #0]  database type - either {run|nvram}
   [arg #1]  VLAN Tag { 2 .. 4095 }
```
Example

```
SYS_console>add-mgmt-to-vlan run 10
Set Management VLAN TAG 10 -OK
SYS_console>
```

Deleting the Management from a VLAN

del-mgmt-from-vlan

The del-mgmt-from-vlan command returns the management VLAN tag to default value (1).

Example

```
SYS_console>del-mgmt-from-vlan run
Del Management VLAN - OK
SYS_console>
```

Creating a VLAN with Port Management

set-mgmt-vlan

The set-mgmt-vlan command creates a new VLAN, which automatically includes the CPU (management port).

```
set-mgmt-vlan    Set Management VLAN
    [arg #0] database type - either {run|nvram|all}
    [arg #1] Name of Management vlan
    [arg #2] Management VLAN Domain - ports list in format: d1-...-dn
    [arg #3] VLAN Tag { 2..4095 }
opt.[arg #4] VLAN priority 1..8 (1..4 - low, 5..8 - high); default : 1
```

Example

```
SYS_console>set-mgmt-vlan run v2 17-18-19-20
 Set run Management VLAN Domain – OK
SYS_console>
```

VLAN, Server-port, Example of Configuration

In the examples below, a new VLAN server is set to port 5 on VLAN tag number 30. The PAYROLL VLAN (tag 10) is set to ports 1 to 4, and the FINANCE VLAN (tag 20) is set to ports 11 to 15. Both of them are given access to the server on port 5.

Physical configuration schema

VLAN Server Port Configu[...]

```
new-srvr-port run 5 30
Set VLAN Server Ports – OK
```
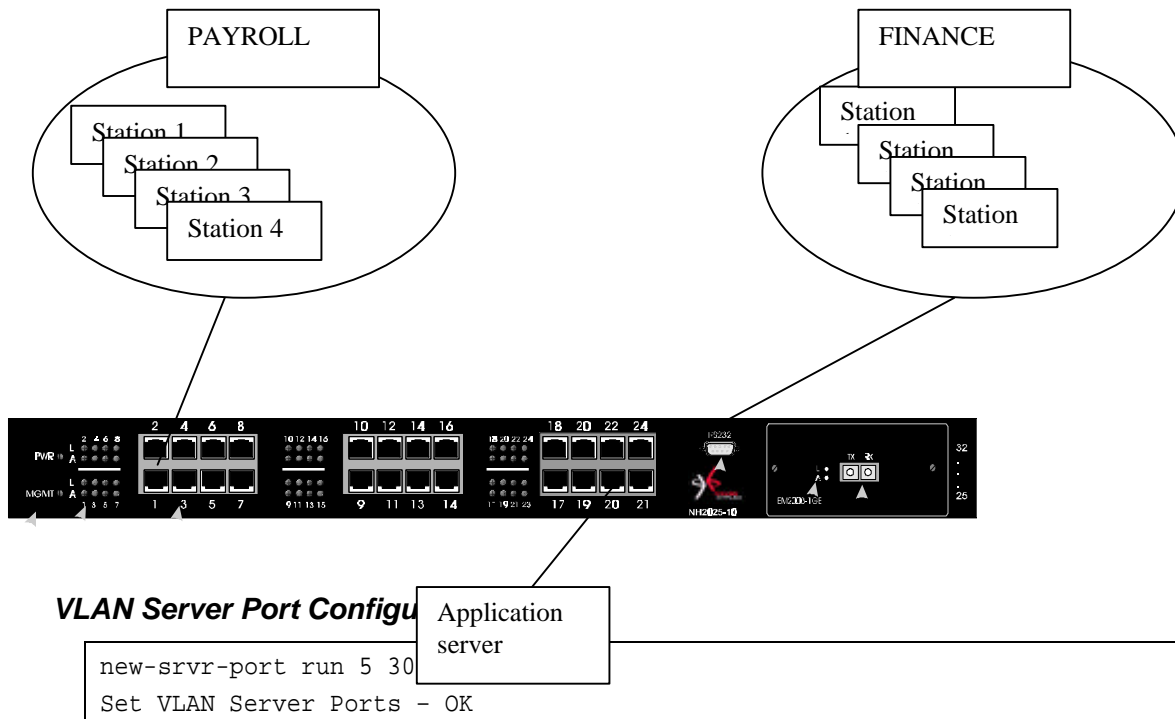
VLAN Configuration

Payroll VLAN Configuration:

```
sys-console>new-vlan run PAYROLL 1-2-3-5-9 10
Set run VLAN Domain entry - OK
SYS_console>
```

Finance VLAN Configuration:

```
sys-console>new-vlan run FINANCE 5-11-12-13-14-15 20
Set run VLAN Domain entry - OK
SYS_console>
```

Checking the Configuration:

```
SYS_console>get-vlan-tbl run
 Runtime VLAN mode is VLAN Tagging
VLAN Table from RUN database (Mgmt tag: 1)
 RUNTIME    VLAN TAG DOMAIN TABLE
==========================================
 VID   NAME        TAG PRIO      Ports
==========================================
  1 S     SRVR_30    30   1    1 2 3 4 9 10 11 12 13 14 15 5S
  2       PAYROLL    10   1    1 2 3 4 9 5S
  3       FINANCE    20   1    11 12 13 14 15 5S
SYS_console>
```

Utilities Commands

Ping Commands

The ping command is intended for testing the connectivity between the switch and other IP network devices. It is not intended as a traffic generator. Thus, using the endless ping option is not recommended.

ping

The `Ping` command pings the `Ipaddress specified number` of times or `0` for endless ping. The ping process starts sending one datagram per second until the `number` of datagrams are sent. It prints one line of output for each response that it receives. The ping command does not return any output if there is no response. Normal response time is 1 to 10 seconds.

    ping <*IP address*> {<*number*>|0}

Example

```
SYS_console>ping 194.90.136.20 4
SYS_console>194.90.136.20 Alive. echo reply: id 4643, seq 1, echo-data-len 0
194.90.136.20 Alive. echo reply: id 4643, seq 2, echo-data-len 0
194.90.136.20 Alive. echo reply: id 4643, seq 3, echo-data-len 0
194.90.136.20 Alive. echo reply: id 4643, seq 4, echo-data-len 0
 PING process stopped - statistics :
  ICMP echo requests   :          4
  ICMP echo responses  :          4
 PING process - press <CR> for prompt
SYS_console>
```

If a host does not respond, only statistics are printed. Failure to get an echo response from a host may be due to:

- A bad physical connection

- A non-existent or inactive host

- Network Unreachable: no corresponding entry in the routing table

- Destination Unreachable: the default gateway failed to route the datagram

- Outdated ARP table information - flush the ARP table with the del-arp-entry command.

ping-stop

If you started a long ping, use this command, or CTRL-C to stop the active ping process.

Port mirroring

The port mirroring feature allows you to copy selected frames to a probe port for diagnostic and troubleshooting purposes.

Port mirroring allows you to attach a network protocol analyzer to a probe port to view the types of traffic passing through a particular switch port or ports.

This analysis can help troubleshoot network problems on a port-by-port basis.

Setting the Monitoring Port

set-mon-port

```
set-mon-port <port>
```

Example

```
SYS_telnet>set-mon-port 1
 Set of the Monitor Port - OK
```

Monitoring with: monitor

To set the port to be monitored and start the monitoring process decimal port. All traffic from this port is duplicated on the monitoring port specified by the set-mon-port command.

```
monitor <dport>
```

Example

```
SYS_telnet>monitor 1
Start monitoring port 1 - OK
```

The monitoring device must be connected to the monitoring port before monitoring is activated.

Saving the Configuration

save-mon

The save-mon command saves the current port-monitoring configuration to the NVRAM.

Example

```
SYS_telnet>save-mon
 Save monitoring configuration to NVRAM - OK
```

Stopping Monitoring

stop-mon

Example

```
SYS_telnet>stop-mon
 Stop monitoring - OK
```

Viewing the NVRAM Configuration

get-nv-mon

The get-nv-mon command retrieves the port monitoring information stored with the save-mon command in the NVRAM.

Example

```
SYS_telnet>get-nv-mon
 The NVRAM based monitoring configuration is :
     Monitored port: 4
     Monitor   port: 2
     Monitor ACTIVE
```

Erasing the NVRAM configuration

clear-nv-mon

Example

```
SYS_telnet>clear-nv-mon
 Clear NVRAM  monitoring configuration - OK
```

Frame Generator

Setting the Frame Generator

set-fg-param

The set-fg-parm command sets the frame generator parameters. The *dest* and *source* parameters are dash-separated hardware addresses in hex. The fill_byte parameter is a single byte used to fill the entire packet except for the first 12 bytes. The length is the total length of the packet excluding CRC.

```
set-fg-param <dest> <source> <fill_byte> <length>
```

Example

```
SYS_console>set-fg-param 00-0E-DE-02-80-01 00-0D-01-32-11-22 aa 100
SYS_console>
```

Starting the Frame Generation

start-fg

The start-fg command starts frame generation. The *dport* parameter is a dash-separated list of ports on which to generate traffic. For example, a *dport* send frames to another *dport*. The *count* parameter specifies the number of frames to send on each interface. A *count* of 0 specifies an infinite number of packets. The *rate* parameter specifies the number of packets per second to generate.

```
start-fg <dport> <count> <rate>
```

Example

```
SYS_console>start-fg  1 9 0 10
SYS_console>
```

Stopping the Frame Generation

stop-fg

This command stops the Ethernet frame generator.

SNMP

This section explains how to use the Simple Network Management Protocol (SNMP) to manage LAN Switch Processors. It assumes that you are using an SNMP-based network management software application such as NBase-Xyplex MegaVision ™ to manage the switches. Hereafter, this section refers to your network management application as a Network Operations Center (NOC). Additionally, this section describes the RMON (Remote Monitoring) application and the type of network management applications that enable you to use RMON.

NBase-Xyplex SNMP Support

SNMP is an Internet standard protocol, defined by the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157, which specifies how network management information is carried through a network. NBase-Xyplex switches support SNMP by implementing an SNMP agent. The agent stores Management Information Base (MIB) data and makes it available when requested through SNMP Set, Get, and Get_Next requests.

In addition, NBase-Xyplex switches generate SNMP Trap messages. Traps are notices that the switch sends to an SNMP manager indicating that a specific event has occurred, or that the condition of a unit has changed significantly.

SNMP basic configuration

To enable your NOC to communicate with a NBase-Xyplex switch, you must assign it an IP address. Use the following command to do this:

set-ip-cfg ip-address ip-mask ip-broadcast

The address you assign must be valid for the network connected to the switch. In a routed network, depending on the switch location, you also need to assign a subnet mask and gateway, as follows:

set-gatew ip-gateway-address

To make sure that your NOC can exchange information with the switch, Ping the switch from the NOC.

SNMP Community String Commands

```
------------------------------------------------------------
get-comm        show current read or/and write community
set-comm        change the read or write community
```

SNMP Community strings authenticate access to the MIB (Management Information Base). Community strings function as "passwords" embedded in every SNMP packet. The community string must match one of the two community strings configured in the switch for the message to be processed. There are two community strings, one for each of the following types of accesses:

- **read** – mode gives read access to all the objects in the MIB, but does not allow write access.

- **write** – mode gives write access to all objects in the MIB.

Viewing the Community String

get-comm

The get-comm command displays the SNMP community string for a given access mode (read or write). If the access mode is specified as *, both the read and the write community strings are displayed.

```
get-comm {read|write|*}
```

Example

```
SYS_console> get-comm *
 Current read  community is: < public >
 Current write community is: < private >
SYS_console>
```

Setting the Read or Write Community

set-comm

The set-comm command lets you specify the SNMP community string for each of the two access modes: read and write.

```
set-comm {read|write}  <community-string>
```

Example

```
SYS_console>set-comm write password
 New write community is: < password >
SYS_console>
```

SNMP Traps

Traps are notices that the switch sends to an SNMP manager indicating that a specific event has occurred, or that the condition of a unit has changed significantly. SNMP Traps are disabled by default.

NOTE: Trap messages do not provide an entirely reliable event notification mechanism; they can get dropped, and are not acknowledged or retransmitted once dropped.

When the Switch detects an extraordinary event, it generates a trap. A trap is a notification message that may be sent to predefine Network Management Stations. A trap event may be a reset (cold or warm), detection of an interface link status change, an SNMP authentication failure due to an incorrect community string, and so.

The SNMP trap commands let you manage whether or not the device issues an authentication trap to the list of selected SNMP Management Stations. The list has a maximum of five entries.

```
get-auth        shows the traps authentication mode
set-auth        modifies the traps authentication mode
get-traps       show destination stations in the trap list
add-trap        add a destination station to the trap list
del-trap        delete a destination station from the trap list
```

Setting Authentication Traps

Authentication Failures – This trap is generated whenever a login attempt fails during the authentication process on a management port.

Viewing the Authentication Trap Status

get-auth

Example

```
SYS_console>get-auth
The authentication trap messages are enabled
SYS_console>
```

Setting the Authentication Trap

```
set-auth {enable|disable}
```

Example

```
SYS_telnet>set-auth disable
 The authentication trap message mode change OK
 The authentication trap messages are DISABLED
```

Configuring the Trap Stations

Viewing the stations list:

get-traps

Example

```
SYS_console>get-traps
            SNMP TRAP TABLE
            ==============
    IPADDR                       COMMUNITY
 ---------------------------------------------------
  194.090.136.126   -----------    public
SYS_console>
```

Adding a station to the list:

add-trap

The add-trap command enters the IP Address of the SNMP Management Station and the trap community string that appears in the trap message.

```
    add-trap <IP address> <trap-community>
```

Example

```
SYS_console>add-trap 194.90.136.20 rnd
 Entry 194.90.136.20 - rnd added
            SNMP TRAP TABLE
            ==============
    IPADDR                       COMMUNITY
 ---------------------------------------------------
  194.090.136.126   -----------    public
  194.090.136.020   -----------    rnd
 ---------------------------------------------------
SYS_console>
```

Deleting a station from the list:

```
    del-trap <IP address>
```

The station's *IP address* must be given as shown in the list provided with get-trap command.

Example

```
SYS_console>del-trap 194.90.136.20
 Entry 194.90.136.20 – deleted
SYS_console>
```

Statistics

This section contains instructions for displaying the switching statistics. Type `statistics` at the CLI to view all the related commands.

Clearing the Switch Counters

clr-cnt

The `clr-cnt` command clears the Ethernet and bridging counters.

Getting Statistics on a Particular Port

get-eth-cnt

    get-eth-cnt <*dport*>

Example

```
get-eth-cnt <dport>
SYS_console>get-eth-cnt 7
 Ethernet Statistics for port 7
 ====================================================
 Good Bytes Received                     :      2840
 Good Bytes Sent                         :       964
 Good Frames Receive                     :        22
 Good Multicast Frames Receive           :         7
 Good BroadCast Frames Receive           :         9
 Frames Sent                             :         6
 Multicast Frames Sent                   :         1
 BroadCastFrames Sent                    :         0
 Receive and Transmit Collisions         :         0
 Receive and Transmit Late Collisions    :         0
 Receive CRC or Alignment Error          :         0
 Receive Frame > 1518 bytes with Bad CRC :         0
 Receive Fragments                       :         0
 Receive Frame > 1518 bytes with Good CRC :        0
 ====================================================
SYS_console>
```

Getting Collisions on a Port

    get-colls-cnt <*dport*>

Example

```
SYS_console>get-colls-cnt 7
 Ethernet Collision Counters for port 7
 =======================================
 Collision Count          :      128
 Single Collision Count   :        0
 Multiple Collision Count :        0
 Excessive Collision Count :       0
 Late Collision Count     :        0
 =======================================
SYS_console>
```

61

Rmon Statistics

Getting Rmon Statistics Group for a Port

```
get-rmon-cnt  <dport>
```

Example

```
SYS_console>get-rmon-cnt 3
 Ethernet RMON Counters for port 3
 ================================
 etherStatsOctets      :     11971
 etherStatsPkts        :       116
 etherStatsBcastPkts   :        52
 etherStatsMcastPkts   :        56
 etherStatsCRCAllignPkts:        0
 etherStatsUndersizePkts:        0
 etherStatsOversizePkts :        0
 etherStatsRuntPkts     :        0
 etherStatsJabberPkts   :        0
 etherStatsCollisions   :        0
SYS_console>
```

Getting the Packet Size Distribution

```
get-sdist-cnt  <dport>
```

The get-sdist-cnt command is available for Fast Ethernet ports only.

Example

```
SYS_console>get-sdist-cnt 3
 RMON Packet Size Distribution Counters for port 3
 ============================================================
 etherStatsPkts64Octets         :       16
 etherStatsPkts65to127Octets    :       109
 etherStatsPkts128to255Octets   :       23
 etherStatsPkts256to511Octets   :        7
 etherStatsPkts512to1023Octets  :        0
 etherStatsPkts1024to1518Octets :        0
SYS_console>
```

Getting the Management Counters

```
get-mgm-brcnt
```

The get-mgm-brcnt command retrieves the counters for the management interface.

Example

```
SYS_console>get-mgm-brcnt
 Management Port Counters
 ==========================================
 Frm   Received    :     23756
 Bytes Received    :   2319627
 Frm Received Ucast:         0
 Frm Received Bcast:     12683
 Frm Received Mcast:     11073
 Frm Transmited    :         0
 Bytes Transmited  :         0
 Frm Transmit Ucast:         0
 Frm Transmit Bcast:         0
 Frm Transmit Mcast:         0
 ---------------------------------------------------------
 port :    Received frames     :    Transmited frames  :
 number: UCAST : BCAST : MCAST : UCAST : BCAST : MCAST :
    1       0       0       0       0       0       0
    2       0       0       0       0       0       0
    3       0       0       0       0       0       0
    4       0       0       0       0       0       0
    5       0       0       0       0       0       0
    6       0       0       0       0       0       0
    7       0       0       0       0       0       0
    8       0     454      38       0       0       0
    9       0       0       0       0       0       0
   10       0       0       0       0       0       0
   11       0       0       0       0       0       0
   12       0   12229   11037       0       0       0
   13       0       0       0       0       0       0
   14       0       0       0       0       0       0
   15       0       0       0       0       0       0
   16       0       0       0       0       0       0
   17       0       0       0       0       0       0
   18       0       0       0       0       0       0
   19       0       0       0       0       0       0
   20       0       0       0       0       0       0
   21       0       0       0       0       0       0
   22       0       0       0       0       0       0
   23       0       0       0       0       0       0
   24       0       0       0       0       0       0
   25       0       0       0       0       0       0
SYS_console>
```

Trouble Shooting

The NH2025-10 is a highly reliable unit. If you encounter an operating problem, follow the troubleshooting steps below. If the problem persists, contact your local NBase-Xyplex representative.

1. Ensure that the unit is plugged into a grounded, functioning AC outlet providing between 90 VAC and 264 VAC at 50/60 Hz. Check the power fuse and replace if blown.

CAUTION
For continued protection against fire, replace with same type and rating fuse.

2. Review all link LEDs to ensure that those ports you believe should be functioning are properly attached to a cable.

3. Verify that your cables are wired correctly.

    Problem: LINK LED is ON but data is not being forwarded through switch.

    Cause: Cables are too long.

    Solution: Make sure that cables are as defined in the installation section of this guide. Check that cables meet the 10Base-T/100Base-TX standards and that they do not exceed 100m.

4. Review all link LEDs to ensure that those ports you believe should be functioning are properly configured, and not disabled or partitioned.

    Problem: Port disabled due to a defective device on segment.

    Cause: When a defective NIC card causes a permanent jam on the network, the port will be disabled by the NH2025-10.

    Solution: a) Locate the defective device and disconnect it from the network.

                b) The disabled port can be enabled through management or by shutting off the unit and powering up again.

5. Ensure that the equipment attached to the switch is properly configured.

If you encounter any situations or problems you cannot solve, obtain, if possible, the following information:

The serial number of your switch and its hardware address

-   If the NMS option is installed, the firmware revision number displayed in the terminal console banner message.

-   The configuration of the equipment being interfaced with the switch.

-   The sequence of events leading up to your problem.

-   Troubleshooting procedures you have already followed.

After compiling the above information, contact your local MRV communications representative or a Customer Service Representative. In addition, if you have specific questions about your network configuration, or have a particularly difficult network, please call our technical support.

Tel (US): 1-800-435-7997
Tel (Int.): +1+978-952-4888
Fax: (978) 952-4880
E-mail: service@mrv.com

Commands Quick Reference

Console Commands

help-kbd	Lists the console functional keys.
banner	Displays banner.
clear	Clears the screen (no argument is required with this command).
login	Exits Admin Interface; but does not disconnect a Telnet session.
logout	Exits Admin Interface; Telnet session will be disconnected.
set-page	Sets console page.
set-prompt	Changes console prompt.
set-attr-prompt	Sets the prompt attributes.
set-attr-msg	Sets the message attributes.
set-attr-text	Sets the text attributes.
set-passwd	Changes the console password.

System Commands

sys-stat	Shows system status.
get-stst-level	Shows the hardware selftest level.
set-stst-level	Changes the hardware selftest level.
warm-reset	Restarts the device without resetting the log.
cold-reset	Restarts the device the same way as a power cycle.
get-last-err	Retrieves the number of warm resets since the last hardware reset. It also displays the last Fatal error message and the time since that error happened.
init-nvram	Resets the non-volatile RAM on the SNMP Agent to default values.
get-sw-file	Retrieves SNMP agent software file name.
set-sw-file	Sets the SNMP Agent Software file name - for download.
get-tftp-mode	Retrieves the TFTP download mode.
set-tftp-mode	Sets the TFTP download mode.
get-tftp-srvr	Retrieves the TFTP server address.
set-tftp-srvr	Sets the TFTP server IP address.
sw-dnld	Begins software download from TFTP server.
set-fg-param	Sets the Ethernet frame generator parameters.
start-fg	Starts the Ethernet frame generator
stop-fg	Stops the frame generator.

IP Commands

get-ip	Shows current IP address.
set-ip	Sets IP address.
get-ip-cfg	Shows current IP configuration.
set-ip-cfg	Sets IP address, netmask and broadcast.
clear-ip-cfg	Clears IP configuration in NVRAM.
get-gatew	Shows default gateway.
set-gatew	Defines default gateway.
get-bootp	retrieves the state of the BOOTP process
set-bootp	enables or disables the BOOTP process activation

Ping Commands

ping	ICMP utility.
ping-stop	Stops the ping process.

ARP Commands

get-arp-tbl	Displays the ARP Table.
del-arp-entry	Deletes an entry/all entries (*) of the ARP table.
add-arp-entry	Adds an entry to the ARP table.
get-arp-stats	Gets ARP statistics.

EtherChannel Commands

new-ec	Creates a new EtherChannel.
get-ec-tbl	Shows EtherChannel Table.
get-ec-entry	Show EtherChannel entry.
del-ec	Removes an EtherChannel.

SNMP Commands

get-comm	Shows current read and /or write community.
set-comm	Changes the read or write community.
get-auth	Shows the traps authentication mode.
set-auth	Sets the trap authentication mode.
get-traps	Shows destination stations in the trap list.
add-trap	Adds destination station to trap list.
del-trap	Deletes a destination station from trap list.

Switching Database Commands

get-lt-entry	Gets a Learning Table entry at index.
get-lt-16	Gets 16 Learning Table entries starting at a given index.
find-lt-addr	Searches for an address in the Learning Table.
del-lt-entry	Removes a Learning Table entry at index.
del-lt-port	Deletes the Learning Table entries for a port.
del-lt-addr	Removes a Learning Table with a given address.
add-lt-entry	Adds a Learning Table entry.
get-lt-age	Displays the Learning Table aging period.
set-lt-age	Modifies the Learning Table aging period.

Virtual LAN Commands

set-vbc-domain	Defines a Virtual Broadcast domain.
del-vbc-domain	Deletes a Virtual Broadcast domain.
get-vbc-tbl	Displays the Virtual Broadcast domain table.
get-vbc-matrix	Retrieves the VBC connectivity matrix monitor.
get-vlan-mode	Displays the current VLAN operational mode.
set-vlan-mode	Selects the desired VLAN definition mode.
new-vlan	Creates a new VLAN.
new-srvr-port	Sets a VLAN Server's port(s).
del-srvr-port	Deletes a defined "server port".
get-vlan-entry	Displays a specific VLAN's table, by entering its VLAN id.
get-vlan-tbl	Displays the VLAN Table.
add-mgmt-to-vlan	Adds management (CPU) to an existing VLAN.
del-mgmt-from-vlan	Returns the management (CPU) VLAN tag to default value (1).
set-mgmt-vlan	Sets management (CPU) for VLAN (Default =1).
get-mgmt-vlan-tag	Retrieves the Management (CPU) VLAN tag.
del-vlan	Deletes a VLAN.
set-priority-policy	Sets a policy for switch priority.
get-priority-policy	Gets a policy for switch priority.
vlan-prio-modify	Modifies the VLAN priority.

Port Monitoring

set-mon-port	Sets the monitoring port on which the sniffer is connected.
monitor	Sets the port to be monitored and also starts the monitoring process.
stop-mon	Ends port monitoring.
get-nv-mon	Retrieves port monitoring information stored in NVRAM.
save-mon	Saves current port monitoring information into NVRAM.
clear-nv-mon	Clears port monitoring information in NVRAM.

Port Configuration Commands

get-port-cfg	Displays the configuration of all ports.
set-port-cfg	Sets the port speed, port duplex, or auto.d: auto, 100, 10, or 1000
set-port-state	Enables or disables a port when Spanning Tree algorithm is not running.
get- fctrl	Displays the status of the port flow control function..
set- fctrl	Sets the mode of operation of the port flow control function..
set-priority-port-cfg	sets the priority of a port
get-priority-port-cfg	displays the port priority configuration
get-tag-outbound-mode	Shows the VLAN Tagging ports' state.
set-tag-outbound-mode	Enables or disables VLAN tagging to a port and should be set to ports on a network on which all nodes support the IEEE 802.1q. Disable any port connected to a network on which there are any nodes that do not support the IEEE 802.1q.

Switching Statistics Commands

clr-cnt	Clears switch Ethernet and bridging counters
get-eth-cnt	Gets Ethernet counters per port
get-colls-cnt	Gets collision distribution counters per port
get-rmon-cnt	Gets Ethernet RMON counters per port
get-sdist-cnt	Gets packet size distribution counters per port
get-mgm-brcnt	Gets switching counters of the mgmt port

Spanning Tree Commands

get-stp	Displays Spanning Tree session state
set-stp	Enables/Disables Spanning Tree - for the next session
get-st-bcfg	Retrieves Spanning Tree Bridge parameters
get-st-pcfg	Retrieves Spanning Tree port parameter table
set-br-prio	Sets Spanning Tree bridge priority
set-br-maxage	Sets Spanning Tree bridge MaxAge
set-br-hello	Sets Spanning Tree bridge HelloTime
set-br-fwdel	Sets Spanning Tree bridge Forward Delay
set-prt-prio	Sets Spanning Tree port priority
set-prt-enb	Sets Spanning Tree port to enable or disable mode
set-br-pcost	Sets Spanning Tree port path cost

Appendix A
System Default Values

console

Password	NONE
Prompt	SYS_console>

system

SW file name	changes according to revision (flash.hex)
tftp mode	Server

snmp

Read Community:	public
Write Community:	private
Authentication Mode:	Enable
Traps Managers:	NONE

switch-db

Aging Time	300

port configuration

port duplex	HALFAUTO
port select	AUTO

spanning tree

Spanning Tree	disable	
Bridge Priority	32768	0-65535
Bridge Max Age	20	6.0 - 40.0 sec
Bridge Hello Time	2	1.0 - 10.0 sec
Bridge Forward Delay	15	4.0 - 30.0
Port Priority	128	0-255
Port Cost	4/10/100 (depending on switch/port module speed/LAN speed (Mbps).)	0-65535

Appendix B
Firmware Download Using TFTP

The switch can be updated with new firmware using TFTP applications. The update can be done with the switch defined as either a TFTP client or a TFTP server.

NOTE: Bootp should be set to disable with the command `set-bootp` disable before proceeding to the software update.

Download Procedure - "Client Mode"

A remote TFTP server station is required.

1. Configure the following switch parameters:

    - set-tftp-mode client

    - set-tftp-srvr IP address of the TFTP server station

    - set-sw-file file name of the firmware to be loaded ("name".hex)

2. Operate the remote TFTP server, with the path defined for the location of the "name" hex file.

3. Start the download procedure using the sw-dnld command in the switch.

NOTE: After successful completion of the download, the switch reboots and operates the new firmware.

- Once the switch is rebooted it is possible to set bootp to enable with the command set-bootp enable.

- NBase-Xyplex strongly recommends erasing the NVRAM with the command init-nvram, and then proceeding to an entire reconfiguration of the switch. This will allow the new firmware to operate normally.

Download Procedure - "Server mode"

A remote TFTP station operated in client mode is required.

1. Configure the switch with the following parameters:

    - set-tftp-mode server

    - set-sw-file - file name of firmware to be loaded ("name".hex)

2. Operate the remote TFTP program in client mode and configure:

    - Path of the file to be loaded ("name".hex)

    - IP address of the remote server (the switch)

3. Start the download procedure with the "sw-dnld" command in the switch and "send" in the TFTP client.

TFTP Recovery - Breaking into the BootROM

Unsuccessful downloading as a result of a corrupted file, premature time-out, etc., may cause the switch to enter a reboot "loop". If this happens, do the following:

1. Stop the loop situation and break into the BootROM menu by pressing the Enter key during the boot process. This stops the loop.

2. login and use the set of commands provided by the BootROM.

3. Use the set of commands provided by the BootROM to set or check the TFTP setting. You can check with the following commands:

    - **`get-sw-file`** gives you the software name,

    - **`get-tftp-srvr`** displays the tftp server IP address

    - **`get-tftp-mode`** provides you with the mode (client or server)

    To set the configuration use the commands below:

    - **`set-sw-file Filename`** (the name of the software located into the tftp server)

    - **`set-tftp-srvr`** (the tftp server's IP address)

    - **`set-tftp-mode client`**

4. At this point, you can use the previously entered TFTP parameters, and a new download session started with the **`sw-dnld`** command.

NOTE: After successful completion of the download, the switch reboots and operates the new firmware, but keeps the old parameters.

Appendix C
Technical Specifications

Compatibility

The 2025-10 is compatible with the following: IEEE 802.3; IEEE 802.3u (Fast Ethernet); 802.1q; IEEE 802.1d (Bridge/Spanning Tree), Ethernet MIB, BRIDGE MIB, RMON (Groups 1,2,3,9), IEEE 802.3x (Flow Control)

Electrical

Voltage	100 - 240 VAC
Frequency	50 - 60 Hz
Power Consumption	40W

Connectors

STP	RJ-45 shielded
RS-232	DB-9

Optical

1000Base-FX (SX, LX)

SX/M	850nm;	0-300 m	MM, DSC
LX/M	1310nm;	0-500 m	MM, DSC
LX/S1	1310nm;	0-6 km	SM, DSC
LX/S2	(DFB)1550nm;	0-20 km	SM, DSC
LX/S3	(DFB)1550nm;	0-50 km	SM, DSC

Learning Table

12K MAC addresses

Boot and Configuration

NVRAM configuration loaded on power up.

Physical

H x W x D	6.55 x 44.06 x 33.0 cm	2.6" (1.5U) x 17.3" x 13"
Weight	3.6 kg	8 lb.

Environment

Operating Temperature	0°C to 50°C	32°F to 122°F
Storage Temperature	-10°C to 50°C	14°F to 122°F
Humidity	85% maximum, non-condensing	

Standards Compliance

UL-1950; CSA 22.2 No 950; VCCI; FCC Part 15 Class A; CE - 89/336/EEC, 73/23/EEC

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com