WDM4/G

FIBER OPTIC 4 GIGABIT WAVELENGTH DIVISION MULTIPLEXER

User's Manual

TABLE OF CONTENTS

1 INTRODUCTION

1.1 About this manual

This manual is a guide to the installation and operation of the WDM4 Fiber Optic Wavelength Division Multiplexer, hardware and software.

Product description helps you to understand how the WDM4 works.

Installation guides you through the set up and connection of the WDM4 to your network and power sources.

Operation provides instruction for using your WDM4 Fiber Optic Wavelength Division Multiplexer, the functions preformed, and the network management software.

Customer support provides information on WDM4 return policy and customer support information.

1.2 Equipment Description

The WDM Gigabit Ethernet product line is designed to convert 4 multimode or singlemode port signals to two singlemode trunk output fibers, at distances of up to 35km. The WDM4 provides solutions to both distance and fiber limited connections. By multiplexing different optical wavelengths on the same fiber, four full duplex channels can be operated over just two fiber lines instead of eight. The WDM4/G is protocol dependent and supports up to 4-Gigabit Ethernet input ports, every port uses a dedicated PLL (Phase Lock Loop) to insure minimum jitter and to maximize the BER (bit error rate). The WDM Fiber Optic components are tested to pass BER of 10^{-12}.

System Overview

The WDM is designed to enable greater bandwidth and distance transmission over a pair of singlemode (SM) fibers. The input transceivers for each port can be MM 850nm or any of LX options as per customer's request.
The trunk transceivers for the WDM link operate at the 1500nm window. The receivers are designed to provide over 50dB of suppression between ports.

The signals from input ports 1 and 3 are transmitted and received over SM link 1; the signals from input ports 2 and 4 are transmitted and received over trunk link 2. The trunk links are labeled LNK1 and LNK2 respectively. This aggregation of data provides some degree of redundancy in the event of a fiber cut. Unlike competing systems which send all four transmits or receives over a single fiber, a fiber cut with the WDM will still allow send and receive half the bandwidth, instead of zero.

Features

- Four fiber optic ports for Gigabit inputs
- Distance of up to 35km for singlemode fiber
- 1U 19" rack mount
- Dual fully redundant and hotswappable power supplies
- SNMP fully managed
- SX or LX Gigabit input

1.3 Fiber optic cable

The WDM4 in different versions is compatible on the port connectors with all popular sizes of multimode and singlemode fiber optic cable 50/125, 62/125, 9/125, while the trunk connector is only compatible with singlemode.

1.4 Fiber Optic connectors

The WDM4 is utilizing a bi-directional full-duplex link therefore it is sensitive to reflection, in order to reduce the potential reflection in the WDM link it is recommended to use special connectors.
The WDM4 uses a dual SC connector with UPC polish on every port, and a Dual SC connector with APC polish on the 4-Gigabit Trunk.

- Angled PC (APC) connector provides low back reflection characteristics. The standard APC provides a <-60db back reflection, and are polished to a 8° angle and minimize back reflection by forcing the reflected rays into the cladding.

- Ultra PC (UPC) provides <-50db optical return loss which is required in high end optical networks.

2 HARDWARE INSTALLATION

2.1 Unpacking the unit

Verify that no visible damage has been caused to the outer box. Remove all material from the packing box and confirm receipt of the following:

- WDM/4 Multiplexer
- RS232 Serial cable for network management
- 2x Rack mounting brackets
- 6x Screws to attach Mounting brackets to the WDM4 unit
- 2x AC Power cord
- User's manual
- Warranty card

In the unlikely event that anything is missing, contact your authorized dealer or representative. If it becomes necessary to return the unit, repackage the unit in its original box.

2.2 General Installation

Make sure there is enough space to pull and connect both the electrical and optical cables without stressing them beyond the manufacturer's limitation (bend radius minimums).

2.3 AC Power connection

Each WDM unit comes with two hot swappable redundant AC power supplies. Power connections are made by connecting the power inlets of the power supplies at the back end of the unit to the wall socket. It is recommended to connect each power cord to a different AC Circuit breaker, to provide max redundancy in case of power failure.
On the front left side of the unit are the Power supply status LEDs, each Power supply has two LEDs, PWR indicates Power supply present, PG indicates Output power good. Power supply 2 (PS2) is located on the rear, behind the LEDs, and Power supply 1 (PS1) is located beside Power supply 2.

> Note: the management controls the Power Supply display, therefore, a slight delay may appear when inserting and removing power cords.

2.4 Fiber optic cable connection

Most cable manufacturers identify the individual fibers in the cable. Select to appropriately terminated fibers and mark both ends with unique identification labels (e.g. CMG02 of cable #03, Fiber #08) to ensure that the fiber connected to the near-end are the same ones that are connected to the far-end.

Use the following steps to connect the WDM4 unit:

1. Proper Optical fiber connection on the WDM ports is to cross from transmit (XMT) port to receive (RCV) port.
2. The WDM4 link is a Full Duplex by directional link therefore the same trunk fiber must be connected to LNK1 of the WDM4 unit and to LNK1 trunk of the remote WDM4. The same applies to LNK2 on both units.

3. Take the following steps to make DSC type connection:

    - Clean the port; first remove and save the dust caps from the optical port. Blow the connector dry with compressed air. Visually inspect the connector.
    - Clean the connector; Use lint-free cloth dampened with alcohol to thoroughly wipe the side and end of the ferrule. Blow the ferrule dry with compressed air. Visually inspect the ferrule for lint.
    - Insert connector; Holding the connector by the strain relief boot, insert the connector ferrule into the port, until the “key” engages in the slot of the coupling.

2.5 Port connection

Proper Optical fiber connection on the WDM ports is to cross from transmit (XMT) port to receive (RCV) port.

Every port on the WDM4/G can be connected to data communication equipment (DCE) or to an Edge device PC or server. Distance to the port is recommended not to exceed 100m. Follow instructions on **2.4**, step 3, and verify that the optical power inserted into every one of the ports is not less than –19dbm and no more than –6dbm.
On each side of the Port Fiber connectors two LED’s exist:

- The bottom Right LED marked **SD** indicate Signal Detect by the port on the Port receive fiber.
- The Top Right LED indicate “PLL Lock” on the Port receive fiber.
- The bottom Left LED, marked **SD,** indicate Signal Detect from the Trunk in the demuxed wavelength.
- The Top Left LED indicate “PLL Lock” from the Trunk in the demuxed wavelength.

2.6 Trunk connection

The WDM4 Trunk uses a proprietary protocol and can therefore be connected only to a similar protocol on the remote side.

The WDM4 trunk consists of two Bi-directional links; each of which carrying two ports LNK1 carries ports 1, and 3, and LNK2 carries ports 2, and 4. The fiber connected to LNK1 of the local WDM4 unit must be connected to LNK1 trunk of the remote WDM4. The same applies to LNK2 on both units.

Follow instructions on **2.4**, step 3, and verify that the optical power inserted into LNK1 and LNK2 is not less than –15dbm and no more than –6dbm.

3 HARDWARE OPERATION

3.1 Turn on procedure

The following steps are to be taken in order to insure proper operation of the WDM4/G

1 Verify that the Power LED's and Power Good LED's are ON.

Verify fan operation (verify airflow on the left side of the unit.)

2 Connect the link Fibers as described in section 2.6 to both units.

3 Connect Port no 1 as described in section 2.5 to both units.

4 Verify, on both side of the link that all LED's next to the connected port as well as the active link (LNK1 for ports 1& 3 LNK2 for ports 2&4) are ON.

5 Verify that the port Gigabit traffic is passing through the WDM4/G.

6 Repeat steps 3,4,5 for ports 2,3 and 4.

4 MANAGEMENT SOFTWARE

4.1 Device specifics

4.1.1 WDM4 Network Management Module

The WDM4 management is designed to be used with the NC316 and the WDM4 series of network converters. The WDM4 management can be used with WDM4 chassis. Both in- and out-of-band management is supported.

4.1.2 LEDs

- PWR: illuminates when unit is powered
- FLT: illuminates when there is a problem with the unit
- RX: flashes when in-band management frames are received (not yet supported by current Megavision version)
- TX: flashes when in-band management frames are transmitted (not yet supported by current Megavision version)
- COL: flashes when in-band management data frames collide
- LNK: illuminates when in-band management link is detected (not yet supported by current Megavision version)

4.2 Operation

4.2.1 Administrative Interface

Overview

This section describes some useful system concepts for dealing with the on-board SNMP agent, and administrative interface of the device.
The Administrative Interface provides the following:
a. Configuration of system parameters, including the serial line and/or the console's parameters
b. Configuration of the Switch's SNMP Agent parameters
c. Configuration of the port's physical and bridging parameters
d. Network performance monitoring
e. A fail-safe backup for in-band management

The RS232 Interface

The device has an RS232 interface, which may be used for a serial connection to the Administrative Interface, to run SLIP, or to download firmware in the event of Flash corruption (using Z-modem or Y-modem).
The serial parameters for the RS232 interface are: 8 data bits, 1 stop bit, no parity, and no flow control, at 9600 baud.

Command Line Interface

Access to the Administrative Interface is via a command-line-interface, meaning that in order to ask the device to perform some operation, simply type the appropriate command.
To execute a command, simply type the command, followed by the parameters that the command requires (see the Reference Guide, or online help), and press <return>. You must type the correct number of parameters. If you do not, then the

Administrative Interface will inform you whether you have typed too many or too few arguments, and will repeat the command as it was previously typed. If you entered too many parameters, the Administrative Interface will delete the extra parameters when re-displaying the line. Simply hit <return> if the new command is as desired, or change the command line as necessary.
Of course, the backspace (<^h> or <del>) keys work on the command line. You may not, however, use the arrow keys. There are several additional keys that are useful:

Key function
Ctrl-h Backspace
Delete Backspace
Return Enter the command
? On-line help (displays the parameters for the entered command)
! Repeat previous command
Ctrl-p Repeat previous command
Ctrl-w Delete previous word
Ctrl-n Repeat next command (if you have already used Ctrl-p or !)
Ctrl-u Erase line
Tab Command completion (see below)
Quotation Enclose an argument containing spaces in quotation marks to include the spaces in the argument

The <Tab> key has a special purpose. If you type some text and then press the <Tab> key, the Administrative Interface searches for commands that begin with the text entered. If it finds a single match, then that command will be automatically displayed. If more than one command matches the entered text, then the system will display as much text as is shared by all the commands which share the already entered text, and will beep. After this, you may type the rest of the desired command name, or you may press <Tab> again. If you press <Tab> again, then the list of commands that match the text entered will be displayed.
For example, suppose that the command line interface consisted only of the commands get-lt-filter, and get-lt-16. Then, if you typed “ge<Tab>”, the system would respond by filling in “get-lt-“. If you pressed <Tab> again, then the two commands would be listed. If you continued by typing “f<Tab>”, then the system would finish the command “get-lt-filter”.
The Administrative Interface assumes that any space between text is to separate parameters. When a parameter is a text string, and you want to include a space inside the text string, enclose the entire parameter in quotation marks, as follows:
Set-prompt “My Prompt:”
The system maintains a history list of up to 20 commands, which have been typed in by the user. To move backwards through this list, use <Ctrl-p> or <!>. To move forwards, use <Ctrl-n>.
If you enter a command incorrectly, a message is displayed indicating the type of error that occurred. For example, typing a nonexistent command gives the following message:

```
SYS_console> pin
command <pin> not found
```

If the command exists but the number of parameters is incorrect, the following message is displayed:

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

The Administrative Interface provides a history of the last commands. In order to obtain the last command in the command history, press <!> or Ctrl-P at the prompt.

If you forget the commands in a section, you may type <?> to bring up a list of command categories. You may then type that category at the prompt to bring up a list of commands in that section. For example, type <ip> at the prompt to bring up the following list:

SUPER> ip

IP related commands
---
ip-clear-nv reset IP config to default values
get-ip-cfg show current Private Port IP Config
get-ip show current Private Port IP address
set-ip set current Private Port IP address
set-ip-cfg set current Private Port IP address
get-bootp retrieves the state of the BOOTP process
set-bootp enables or disables the BOOTP process activation
set-gatew define default gateway
get-gatew show default gateway
get-arp-tbl display the ARP table
del-arp-entry deletes an entry/all entries(*) of the ARP table
add-arp-entry add an entry to the ARP table
get-def-ttl Retrieves the running default TTL value
set-def-ttl Modifies the running default TTL value
ping IP traffic generator
ping-stop stop the ping process
get-ping-info gets the ping database

Finally, the user may press <Tab> to see the list of commands which start with the text he has already typed, e.g.:

```
SYS_console> get-c
 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 dist. counters per port
SYS_console>
```

Users, access rights, and Logging in and Out

The Administrative Interface allows up to ten different users. Each user has a username, a password, a prompt, and a user access level. When the device is shipped from the factory (or the cli-clr-nvram command is used), there are two users, name superuser (the supervisor) and user (a default user).

Access rights define what commands are available to the user. There are three access levels:

Limited	Read-only access to non-sensitive commands
Normal	Read/Write access to non-sensitive commands
Supervisor	Full access to all commands

The term “Non-Sensitive commands” refers to those commands that cannot have a fatal impact on managing the system if entered incorrectly. For example, only the supervisor is allowed to set the IP configuration of the device.

The supervisor can add or remove users and change the access level of the users on the system. However, users cannot be promoted to supervisor status, and the supervisor cannot reduce his access rights.

To change users, simply log out of the current session, using the login or logout command, and enter the new username and password. Any user can change his password with the set-passwd command. Note that the supervisor does not need to know the password of a user to delete the account. Thus if a normal user forgets his password, the supervisor can simply delete and re-add the user to the system.

The supervisor password when the device is shipped is “super”, just like the username. Use the set-passwd command the first time you log in as supervisor to change this password. Do not forget the supervisor password.

First Time Login

The following parameters should be set up the first time you log in. (Log in with username “super” and password “super”):
Change the supervisor password, using the set-passwd command
Set up the IP configuration, using the set-ip, set-prv-ip, and set-gatew commands
Set the SNMP Community strings, using the set-comm command
Enable or disable BOOTP, as desired, and set the TFTP server IP address (set-bootp, set-tftp-srvr)

Telnet

Once an IP address is set, the Administrative Agent can be contacted using the Telnet protocol (a TCP/IP terminal interface protocol). The interface looks and operates exactly the same whether using the RS232 interface or Telnet.
The telnet protocol can be run through the switching ports, the private interface, or the RS232 serial interface via SLIP.
To exit the Administrative Interface without closing the Telnet session (for instance, to change users), use the login command. To exit the Administrative Interface and close the Telnet connection, use the logout command.
Up to 5 Telnet sessions can be active at any one time, either with the same users or with different users. There is no restriction on how many times a particular user can log in.

Boot Sequence, and Restarting the System

The bootup sequence of the device is as follows:

1. BOOTROM initializes the CPU, and displays the version number.
2. BOOTROM loads the Operating System from the Flash. If this fails, then the BOOTROM will attempt to execute Z-modem, or Y-modem to get the firmware across the serial line.
3. Operating System executes the self-test.
4. Self-test loads the hardware, and executes if the self-test level is not “none”
5. Operating System executes the BOOTP process if enabled
6. Operating System executes the SNMP Agent software.

To restart the device, there are two options, cold-reset and warm-reset. Cold resetting the device will cause a full re-initialization from step 1. Warm resetting the device will simply exit the SNMP Agent and resume from step 6.

BOOTP and TFTP

TFTP, or Trivial File Transfer Protocol, is a method to read or write data from or to an embedded system. TFTP works by sending IP/UDP frames between a client and server, passing the data as needed. The SNMP agent contains both a TFTP client and TFTP server. When the device is acting as a TFTP server, a remote client (UNIX, or a windows-based application, usually) must send or get a file. If the agent is acting as a client, there must be a server configured to send or receive the data. The system supports both netascii and binary transfer modes. To configure the SNMP agent to act as a TFTP client, use the set-tftp-srvr, set-rsw-

file, and sw-dnld commands. To act as a server, only the set-sw-file command is needed.

When a TFTP request is received which matches the filename shown by get-sw-file, the system will record the contents of the file, and upon successful completion, reboot the device. After sw-dnld has successfully completed, the device will also be restarted. In addition to these mechanisms, there is a third way to use TFTP, via the BOOTP process.

BOOTP is a protocol for initializing a device's IP and other configuration, and perhaps for initiating a firmware download. A BOOTP server must be present on the network, connected to the private interface, and BOOTP must be enabled on the device for the protocol to operate. The BOOTP client (the device) sends a broadcast frame about once every second for 30 seconds unless a response from a server is received. If no response is received, then the previous IP configuration (if any) will be installed when the SNMP agent is loaded.

If a response is received, then the IP configuration of the system will be set from the BOOTP response, and the new configuration saved. In addition, the BOOTP response can tell the system to upgrade the device firmware using the TFTP protocol. To do this, the BOOTP server must specify a TFTP server IP address and a filename. In addition, the feature must be enabled from the system (set-bootp-swdnld), and the filename must match the system firmware filename (CMMC.rev). For BOOTP/TFTP operation, this filename is permanent, that is, it cannot be changed by any user. Any firmware upgrades released will have this filename.

After the TFTP process is finished, when started from BOOTP, the new SNMP agent will be loaded immediately.

Upgrading the system software

When the system software is working properly, and a simple upgrade is desired, the easiest way to proceed is with a TFTP client on a PC. Simply check that the filename on the device matches the filename on the PC, and use TFTP send (either binary or netascii). After the process is finished, the system will automatically reboot and the new software will be loaded.

If the system software somehow gets corrupted, there are two possibilities. First, if only the SNMP agent or self-test are corrupted, then the Operating System can be used as either a TFTP client or server to load new software via the private interface. Connect a terminal to the serial port, and follow the stated instructions.

If the Operating System itself is corrupted, then the BOOTROM will force the user to select between Z-modem and Y-modem. Simply answer the question, and connect a host using the appropriate software transfer protocol to the serial line. Send the file (CMMC.rev) using the stated protocol. After the process is complete, the device will boot automatically.

Message Logging

The SNMP Agent software has a message logging feature to record, display, or send SNMP Traps in response to certain conditions detected by the system. The default parameters for this message logging system are sufficient for normal operation.

There are four different ‘databases’ in the message logging system. The display database simply refers to displaying messages in the Administrative Interface. This display is typically left off except for serious errors. Fatal errors will also cause the device to reboot. The running log database is a log of those messages that have occurred during the current running session of the SNMP Agent (i.e., since the last boot). This log is cleared every time the switch is rebooted. Typically only severe errors are logged in this database. The NVRAM database is a log in the NVRAM, which contains the 30 most recent messages including one each time the device boots. The purpose of this database is to record fatal errors to be reported to Technical Support. To access the list of messages in either log, use the disp-msg-log or disp-msg command.

The fourth database, the Traps database, issues an SNMP Trap instead of logging the message. This allows a network administrator to get an immediate notification of errors.

If necessary, you can change the threshold of any of these databases. If the severity of a message is higher than the threshold of any given database, then that database will get a copy of the message. By default, all thresholds are set at the error level. In addition, there are three security levels: informational, warning, and fatal levels.

NVRAM

The device has a Non-Volatile RAM (NVRAM) to store configuration parameters. This NVRAM is split into several sections, including data for IP, the system, Spanning Tree, port configuration, VLANs, and the CLI. Each of these sections can be cleared individually, or all together with the init-nvram command. When new firmware is loaded into the device, an attempt is made to upgrade each section to the most recent version. In the case where this operation is not successful, only the affected section will be reset to the default values. The other sections will be unaffected.

In addition, there is a section devoted to the Operating System, which shares some information with the system and IP sections (for use in the BOOTP/TFTP process by the OS). The values in this special “power-up” section override any values in the corresponding SNMP Agent section. When an adjustment is made to a parameter from the SNMP Agent (either via SNMP or the Administrative Interface), the corresponding entry in the power-up block is also set. The information in the power-up block includes the private IP address, gateway, TFTP server, self-test level, BOOTP enable, and some few other parameters.

Ping

In order to check the IP connectivity between the SNMP Agent and any external device, the system provides a ping capability. Ping is an ICMP/IP protocol, which sends an echo request from one host and expects a reply from the other. After a 1-second timeout, a new request will be sent. If the device receives a response before the timeout, then it will wait about 1 second before sending another request. If there is a logical and physical connection between the device and the destination, then all of the requests will be answered, and only responses will be seen. If there are no responses at all, this implies that either the IP configuration is

not correct on the device or destination, or there is no connection (check link, etc.). If there are some responses and some timeouts, then there is likely an intermittent cabling problem – check the error statistics.
To start pinging a host, use the ping command. Simply type the destination IP address (in dotted decimal notation, e.g. 192.168.1.1), and the number of requests to send. SNMP can also be used to ping a remote host while watching from an NMS.
You can ping up to 5 hosts simultaneously. To view the status of the various ping sessions, use the get-ping-info command.
If the Administrative Interface ping command is used, then the results of the ping are displayed on the console as they are received (either responses or timeouts).
To stop a ping session, use the ping-stop command. To stop all ping sessions registered for the current Administrative Interface session, use <Ctrl-c>.

The Private Interface

The device control board is equipped with a private management interface. This is a 10Base-T with an MDI-X (to connect directly to an end-station). This interface is specifically designed to allow a connection to the device when you do not want to use any of the bridging ports to connect. For example, if you have a 4 port switch module installed in the 316 Chassis and want to connect a laptop directly to the device, you can use a 10Base-T connection directly from the laptop to the control board, instead of connecting both the WDM4 and the laptop to the 4 port switch. Note that this may be desirable for remote administration, but this configuration is not necessary for local administration.
The private interface fully supports SNMP, Telnet, and TFTP as needed. In addition, this interface is used for BOOTP purposes.
The private interface is basically a Network Interface Card attached directly to the CPU of the device. It has no interaction whatsoever with the bridging ports. The device maintains a separate (if desired) IP address for the private interface. This IP address is also used by the Operating System when the SNMP Agent is not running. In that case, the bridging ports are disabled completely and only the private interface is functional.
To look at management statistics for the private interface, it fully supports the Interfaces MIB, and has interface ID 1.

SLIP

SLIP stands for Serial Line Internet Protocol (or Serial Line IP). It is a protocol to run IP over a serial (RS232 for example) physical connection. The SNMP Agent allows the RS232 port to be configured to run SLIP. In this case, a separate IP address must be installed for the SLIP interface (set-slip-cfg). To connect to this port, a standard null-modem serial cable must be used, and the PC must be configured to run SLIP.
Any IP protocol can be run across the SLIP interface, including Telnet, TFTP, and SNMP. The purpose of this feature is to connect a laptop or other device to send data (TFTP) or manage the device using SNMP (most often under a graphical NMS), when an Ethernet connection is unavailable.

Parameter Upload/Download

The WDM4 has the capability of easily storing and reproducing its configuration details; in this fashion it is possible to duplicate the functions of a “master” WDM4 system in another location with minimal operator effort. Storing the configuration of a WDM4 is done using the par-upld and par-dnld commands, described later in this manual.

4.2.2 Command Line Interface

Console Commands

Command console
Description displays the commands in this section

Command help-kbd
Description lists the console functional keys
A handy reference guide if you forget the shortcut keys listed in the beginning of this manual

Command banner
Description displays the opening login banner

Command clear
Description clears the screen

Command login
Description exits the Administrative Interface

Command logout
Description exit the Admin Interface and any active Telnet session

Command set-passwd [arg #0]
Description ANY USER - sets the password for the current user
[arg #0]: current password

Command set-prompt [arg #0]
Description changes the console prompt
[arg #0]: new prompt

Command add-user [arg #0]
Description SUPERVISOR ONLY - add user name
[arg #0]: user name

Command delete-user [arg #0]
Description SUPERVISOR ONLY - delete user name and password
[arg #0]: user name

Command list-users
Description SUPERVISOR ONLY - lists user names

Command cli-clear-nv
Description SUPERVISOR ONLY - clears CLI NVRAM

Command set-access [arg #0] [arg #1]
Description SUPERVISOR ONLY - set access rights
[arg #0]: user name
[arg #1]: access rights { limited | normal }

Command set-full-sec [arg #0]
Description enables/disables the backdoor passwords.
[arg #0]: { enable | disable }

Chassis Commands

Command get-temp [arg #0]
Description display temperature
[arg #0]: chassis number {1}

Command get-min-temp-limit [arg #0]
Description display minimum temp alarm limit
[arg #0]: chassis number {1}

Command set-min-temp-limit [arg #0] [arg #1]
Description define minimum temp alarm limit
[arg #0]: chassis number {1}
[arg #1]: minimum temperature limit (celsius)

Command get-max-temp-limit [arg #0]
Description display maximum temp alarm limit
[arg #0]: chassis number {1}

Command set-max-temp-limit [arg #0] [arg #1]
Description define maximum temp alarm limit
[arg #0]: chassis number {1}
[arg #1]: minimum temperature limit (celsius)

Command get-module-list [arg #0]
Description list modules in slots
[arg #0]: chassis number {1}

Command set-module-reset [arg #0] [arg #1] [arg #2]
Description reset card
[arg #0]: chassis number {1}
[arg #1]: slot number
[arg #2]: setting {phy|queue|switch}

Command get-chassis-info [arg #0]
Description display chassis information
[arg #0]: chassis number {1}

Command get-module-info [arg #0] [arg #1]
Description display module information
[arg #0]: chassis number {1}
[arg #1]: slot number

System

Command system
Description displays the commands in this section

Command sys-clr-nv
Description clears system NVRAM to default values

Command sys-stat
Description show system status, such as Agent software version number, MAC address, fan and power supply status, uptime, and the number of cold and warm boots.

Command cold-reset
Description cold restarts the system, any values in n-vram are loaded

Command warm-reset
Description soft reset, any values in n-vram are loaded

Command get-sw-file
Description retrieves the SNMP Agent Software file name

Command set-sw-file [arg #0]
Description sets the SNMP Agent Software file name. It is recommended you leave this to the default value unless instructed otherwise by NBASE.
[arg #0]: file name

Command get-rsw-file
Description retrieves the SNMP Agent Software remote file name

Command set-rsw-file [arg #0]
Description sets the SNMP Agent Software remote file name
[arg #0]: file name

Command get-par-file
Description gets the Configuration Parameters file name

Command set-par-file
Description sets the Configuration Parameters file name
[arg #0]: file name

Command get-rpar-file
Description gets the Configuration Parameters remote file name

Command set-rpar-file [arg #0]
Description sets the Configuration Parameters remote file name
[arg #0]: file name

Command get-tftp-srvr
Description retrieves the TFTP download server IP address

Command set-tftp-srvr [arg #0]
Description sets the TFTP download server IP address
[arg #0]: TFTP server IP address

Command sw-dnld
Description starts the SNMP software download from the pre-defined server

Command init-nvram
Description initialize NVRAM

Command get-stst-level [arg #0]
Description displays the selftest level

Command set-stst-level [arg #0]
Description sets the selftest level. Do not change this setting unless instructed to by an NBASE technician.
[arg #0]: { none | short | long }

Command disp-msg-log [arg #0]
Description displays the message log
[arg #0]: database type - either { run | nvram }

Command del-msg-log [arg #0]
Description clears the message log
[arg #0]: database type - either {run|nvram}

Command disp-msg [arg #0] [arg #1]
Description displays the message entry
[arg #0]: database type - either { run | nvram }
[arg #1]: message index(decimal): 1 - MAX SIZE

Command set-rmon-tx [arg #0]
Description sets Enable/Disable RMON count of TX'ed frames
[arg #0]: New mode: { enable | disable }

Command get-rmon-tx

Description shows whether RMON counts of TX'ed frames are enabled or disabled

Command set-bc-thresh [arg #0]
Description sets the Broadcast Rx Threshold
[arg #0]: New Threshold: (frames per seconds)

Command get-bc-thresh
Description gets the Broadcast Rx Threshold

Command set-mg-thresh [arg #0]
Description sets the Management Traffic Rx Threshold
[arg #0]: New Threshold: (frames per seconds)

Command get-mg-thresh
Description gets the Management Traffic Rx Threshold

Command get-mac-address
Description display mac address for management card

Command get-msg-lvl [arg #0]
Description gets the message log security level
[arg #0] type – either {disp|run|nvram|trap}

Command set-msg-lvl [arg #0] [arg #1]
Description sets the message log security level
[arg #0]: type- either {disp|run|nvram|trap|all}
[arg #1]: security level – either {fatal|error|warning|info|memo}

IP

Command ip
Description displays the commands in this section

Command ip-clear-nv
Description resets the IP configuration to default values

Command get-ip-cfg
Description shows the current Private Port IP configuration

Command get-ip
Description shows the current Private Port IP address

Command set-ip [arg #0]

Description set current Private Port IP address
[arg #0]: IP Address

Command set-ip-cfg [arg #0] [arg #1] [arg #2]
Description sets current Private Port IP address configuration
[arg #0]: IP Address
[arg #1]: Netmask
[arg #2]: Broadcast address

Command get-bootp
Description retrieves the state of the BOOTP process

Command set-bootp [arg #0]
Description enables or disables the BOOTP process activation (requires reset)
[arg #0]: { enable | disable }

Command set-gatew [arg #0]
Description define default gateway
[arg #0]: IP Address

Command get-gatew
Description show default gateway

Command get-arp-tbl
Description displays the ARP table

Command del-arp-entry [arg #0]
Description deletes an entry or all entries(*) in the ARP table
[arg #0]: {IP address | *}

Command add-arp-entry [arg #0]
Description add an entry to the ARP table
[arg #0]: IP address

Command get-def-ttl
Description retrieves the running default TTL value

Command set-def-ttl [arg #0]
Description modifies the running default TTL value
[arg #0]: default TTL value : 1-255 (seconds)

Command ping [arg #0] [arg #1]
Description IP traffic generator
[arg #0]: destination IP address
[arg #1]: number of packets to send or 0 for endless ping

Command ping-stop [arg #0]
Description stop the ping process
[arg #0]: destination IP address

Command get-ping-info
Description gets the ping database

SNMP

Command snmp
Description displays the commands in this section

Command get-traps
Description show destination stations in the trap list

Command add-trap [arg #0] [arg #1]
Description add a destination station to the trap list
[arg #0]: IP address
[arg #1]: community

Command del-trap [arg #0]
Description delete a destination station from the trap list
[arg #0]: IP address

Command get-comm [arg #0]
Description show current read or/and write snmp community string
[arg #0]: { read | write | * }

Command set-comm
Description change the read or write snmp community string
[arg #0] either {read|write}
[arg #1] new comm

Port Configuration

Command Get-port-info <chassis number> <slot number> <port number>
Description display port information
Parameters chassis number - {1-2}, slot number - {1-16}, port number - { port number }

Command Set-port-loopback <chassis number> <slot number> <port> <state>
Description sets the port loopback mode
Parameters chassis number - {1-2}, slot number - {1-16}, port number - { 1 | 2 | 3 | 4 }, state {10|100}

Command Set-port-disable <chassis number> <slot number> <port> <state>
Description sets the port enabled or disabled
Parameters chassis number - {1-2}, slot number - {1-16}, port number - {1|2|3|4}, state {on|off}

Command Set-port-enable <chassis number> <slot number> <port> <state>
Description sets the port enabled or disabled
Parameters chassis number - {1-2}, slot number - {1-16}, port number - {1|2|3|4}, state {on|off}

Command Set-port-dplex <chassis number> <slot number> <port number> <state>
Description sets the port duplex mode
Parameters chassis number - {1-2}, slot number - {1-16}, port number - { port number }, state - { half | full }
Note: If Link Configuration is enabled, then the command changes the advertised state of Set-port-dplex. Otherwise, the current state is changed.

Command Set-port-speed <port number> <speed>
Description sets the port speed (also refer to set-port-lcfg)
Parameters port number - { port number }, speed - { auto | 10 | 100 | 1000 }
Note: If Link Configuration is enabled, then the command changes the advertised state of Set-port-speed. Otherwise, the current state is changed.

Command Set-port-lcfg <chassis number> <slot number> <port> <state>
Description sets the port auto-negotiation mode
Parameters chassis number - {1-2}, slot number - {1-16}, port number - {1|2|3|4}, state {on|off}
Note: If Link Configuration is enabled, then the command changes the advertised state of Set-port-lcfg. Otherwise, the current state is changed.

4.2.3 Using the WDM4 with a SNMP manager

This section contains instructions regarding the configuration and management of the WDM4 with an SNMP Management System (e.g. MegaVision).

Configuring the WDM4 with an SNMP Agent:
The WDM4 with a SNMP Agent board installed is a plug and play device. Once connected to the network and powered ON, the WDM4 starts operating according to factory set default values. However, to ensure proper operation and maximum performance specific to your network configuration and to provide SNMP access, some environment-specific parameters must be configured through the Administrative Interface.

The following steps should be taken:
Global Setup
Connect a terminal to the Administrative Interface Port.

Log in to the Administrative Interface - see Chapter 2.

3.Initialize all the WDM4 parameters to their default values. Use the following command sequence:
init-nvram
warm-reset

4. Wait until you see the LOGIN prompt again. Log in to the Administrative Interface. Now all system parameters have been initialized to their default values.

IP Setup

Modify the system IP configuration to match your IP network. Use the set–ip-conf command in order to provide an IP address, a netmask and a broadcast address. For example:

set-ip-cfg 129.1.1.64 255.255.255.0 129.1.1.255

Check that the actual IP configuration matches the desired one:

SYS_console> get-ip-cfg

The device IP address, netmask and broadcast are:

IP address : 129.001.001.064
IP netmask : 255.255.255.000
IP broadcast : 129.001.001.255

Set the default gateway address using the set-gatew command (for more details see Chapter 3 - IP Commands). This should be a station that can route IP packets to non-local IP networks. For example:

SYS_console> set-gatew 129.1.1.1

Confirm that the default gateway IP address was properly accepted:

SYS_console> get-gatew

Device default gateway address is : 129.001.001.001

SNMP Setup

1. Set up the SNMP communities strings for the two access modes: read and write. Confirm that the read and write communities were properly accepted:

SYS_console> set-comm read public
New read community is: < public >
SYS_console> set-comm write private
New read community is: < private >
SYS_console> get-comm *
Current read community is: < public >
Current write community is: < private >
SYS_console> _

2. Setup the trap receiver table: add the Network Manager Station(s) that are to receive system generated traps:

SYS_console> add-trap 129.1.1.76 public
Entry 129.1.1.76 - public added
SNMP TRAP TABLE
==========

IPADDR	COMMUNITY
129.001.001.065	public
129.001.001.076	public

Troubleshooting

This section provides troubleshooting hints for problems you may encounter when trying to manage the WDM4 using an SNMP Management System.

If your SNMP Manager has trouble communicating with the SNMP Agent in the switch, check your SNMP configuration parameters.
Your Network Administrator can help determine if your IP configuration (IP Address. netmask, and broadcast address) is correct. If the SNMP management workstation is on a different network, be sure that you defined an appropriate Default Gateway IP Address (see Chapter 3 - IP Commands).
Check the community string configuration by using the get-comm * command.
If you are not receiving any traps, check that you entered the Network Management Workstation address in the trap receiver table correctly. Display the table using the get-trap-tbl command. Check that both the IP Address and the community string are correct.
If the network management station does not receive authentication failure traps, check for the Authentication Mode using the get-auth command.
Check that you have a correct physical connection to the switch. Test that the switch port is configured with the desired speed.
Test the connection to the Network Management Station by pinging it.
If the network's physical topology has changed recently (e.g. a Network Management Station has been moved from one segment to another), the ARP cache may be out of date. You can use the del-arp-entry command to flush the cache.

SPECIFICATIONS

Technical specifications

Electrical
Dual AC power supply.
95-240VAC 47-63Hz
Fuse 2A
Hot Swappable Fully redundant
Power cord per power supply
Indication: Green LED = Power supply 1 inserted (PS1)
Green LED = Power supply 1 Good (PG)
Green LED = Power supply 2 inserted (PS2)
Green LED = Power supply 2 Good (PG)

Operating Temperature Range
0°- 40°c

Storage temp
-40° - 95°c

Humidity
85% maximum non-condensing

Standard Compliance
UL1950, cUL, FCC PART 15-1, CE.

PORT

Protocol Gigabit Ethernet
Sensitivity: -19dbm minimum
Optical power:-10dbm minimum
Indication: Green LED = signal detect (SD)
(Per port) Green LED = PLL lock

TRUNK

4-Gigabit full duplex proprietary protocol. 1550nm window.
Sensitivity: -17dbm minimum
Optical power: -6dbm minimum
Indication: Green LED = Link 1
Green LED = Link 2
(Per Demux port) Green LED = signal detect (SD)
(Per Demux port) Green LED = PLL lock

NMS

SNMP	Out of band and in band.
RS232	DB9 Connector
10-Base T	RJ45 Connector

Indication:

TX	Green LED =	NMS Transmit
RX	Green LED =	NMS receive
FLT	Green LED =	NMS fault
COL	Green LED =	Collision on 10 Base T port
LNK	Green LED =	Link on 10 Base T Port

Dimensions

H,L,W

1.75”x17”x18

5 CUSTOMER SUPPORT

5.1 Return policy and Technical Support

Return Policy

For your convenience NBase Communications offers a toll free number (800)-435-7997 to facilitate technical support and obtaining RMA (Request Merchandise Authorization) numbers.
Please have the following information ready when calling for an RMA request.

P.O. or Invoice Number		Model Number	Serial Number
Requester's Name	Requester's Phone #	Company Name of Requester	END-USER Company Name
Reason for RMA request……detail problem description			

All products have a **ONE – YEAR FACTORY WARRANTY** and a 30 day turn around time for repair or replacement of product solely at the discretion of NBase Communications. The issued RMA numbers is valid for 30 days from the issued date.

RETURN for CREDIT

Must be requested within the first 30 days of factory ship date in order to avoid restocking fees. The return shipping must be prepaid.
If unit will be returned 31 to 60 days from factory ship date a 20% of invoice restocking fee will be apply.

- All products must be in the original and reusable factory box with all original packing materials.
- All miscellaneous accessories such as cables, manuals, diskettes and mounting hardware must be included.
- The product can not have been altered or modified in any way.

RETURNS for REPAIR / REPLACEMENT

- Must be requested within the ONE – YEAR period starting from the factory ship date.
- Advance overnight (24-hour turn around) replacements are offered only within the first 30 days of factory ship date or with the purchase of an Extended Warranty.
- If products are not found to be defective, there is a 10% of invoice handling charge plus return shipping cost.
- **Charges for Out of warranty repair as follow: Min 12% of purchased price or Maximum of current unit price.**

EVALUATION RETURNS

Evaluation must clearly be the intent at the time of ordering and so notated on the P.O. All products must be returned within the requested time period stated on the P.O. for testing.

SHIPPING INSTRUCTIONS

Please ship the return products (PREPAID) to NBase Communications, 8928 Fullbright Ave.

Chatsworth, CA 91311.

Handling charges and credits will be based on the condition of the merchandise as received at our factory. **RMA #** must be clearly visible on outside of shipping carton.

A Return Material Authorization number (RMA) must be obtained for all defective Products and the (RMA) must be used within 40 days of the issue date. Sending a product without RMA number, or after more than 40 days will cause package to be sent back and handling fee of $85 will be issued.