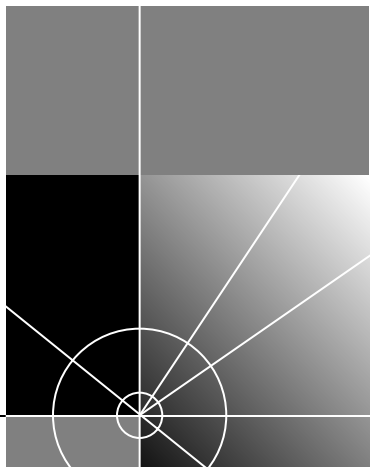
CoreBuilder® 5000
Distributed Management Module Commands Guide

Software Version v6.0



http://www.3com.com/

Part No. 10012823
Published November 1999

3Com Corporation
5400 Bayfront Plaza Santa Clara, California 95052-8145

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided for you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.277-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.277-7015 (Nov 1995) or FAR 52.277-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Federal Communications Commission Notice

This equipment was 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 you must correct the interference at your own expense.

Canadian Emissions Requirements

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

EMC Directive Compliance

This equipment was tested and conforms to the Council Directive 89/336/EEC for electromagnetic compatibility. Conformity with this directive is based upon compliance with the following harmonized standards:

EN 55022 – Limits and Methods of Measurement of Radio Interference

EN 50082-1 – Electromagnetic Compatibility Generic Immunity Standard: Residential, Commercial, and Light Industry

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case you may be required to take adequate measures.

Compliance with this directive depends on the use of shielded cables.

Low Voltage Directive Compliance

This equipment was tested and conforms to the Council Directive 72/23/EEC for safety of electrical equipment. Conformity with this directive is based upon compliance with the following harmonized standard:

EN 60950 – Safety of Information Technology Equipment

VCCI Class A Compliance

この装置は，第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）基準に適合しております。
従って，住宅地域またはその隣接した地域で使用すると，ラジオ，テレビジョン受信機等に受信障害を与えることがあります。
取扱説明書に従って正しい取り扱いをして下さい。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise When such trouble occurs, the user may be required to take corrective actions.

Trademarks

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, CoreBuilder, LANsentry, ONsemble, PACE, and Transcend are registered trademarks of 3Com Corporation. ONline and TriChannel are trademarks of 3Com Corporation. 3Com Facts is a service mark of 3Com Corporation.

Sun is a registered trademark of Sun Microsystems, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

DEC and DEC net are registered trademarks of Compaq Computer Corporation.

IPX and Novell are registered trademarks of Novell, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

CONTENTS

TECHNICAL SUPPORT

3COM CORPORATION LIMITED WARRANTY

About This Guide

Introduction

This guide describes the commands used to manage 3Com devices in the 3Com CoreBuilder® 5000 Integrated System Hub, using the CoreBuilder 5000 Distributed Management Module (DMM) interface. Use this guide to find specific information about hub management commands available from the DMM command-line parser. Refer to the *CoreBuilder 5000 Distributed Management Module User Guide* for instructions on installing, configuring, and using the module.

If the information in the release notes shipped with your product differs from the information in this guide, follow the release note instructions.

Audience

This guide is intended for the following people at your site:

- Network manager or administrator
- Trained hardware installer or service personnel

How to Use This Guide

Table 1 shows the location of specific information.

Table 1 How to Use This Guide

If you are looking for	Turn to
An overview of the DMM command line parser	Chapter 1
A comprehensive list of commands available for managing hubs using the DMM command line interface	Chapter 2
Instructions for contacting the 3Com technical support organization and for accessing other product support services	Appendix A

Conventions

Table 2 and Table 3 list conventions used throughout this guide.

Table 2 Graphic Conventions

Icon	Notice Type	Alerts you to
	Information note	Important features or instructions
	Caution	Risk of personal safety, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 3 Text Conventions

Convention	Description
"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your terminal screen. For example: `NetLogin:`
Text represented as **`commands`**	**`This typeface`** is used to represent commands that you enter. For example: **`SETDefault !0 -IP NETaddr = 0.0.0.0`**
Italics	*Italics* are used to denote *new terms* or *emphasis*. In command "Format" sections, italics denote variables for which you provide one of the allowed values.

Related Documents

This section provides information on supporting documentation, including:

- 3Com Documents
- Reference Documents

3Com Documents

The following document provide additional information on 3Com products:

- *CoreBuilder 5000 Quick Start and Reference Guide* — Provides information on the installation, operation, and configuration of the CoreBuilder 5000 hub. This guide also describes the principle features of the CoreBuilder 5000 Fault-Tolerant Controller Module.
- *CoreBuilder 5000 Distributed Management Module User Guide* — Provides information on the CoreBuilder 5000 Distributed Management Module's operation, installation, and configuration. This guide also describes the software commands associated with the Distributed Management Module.

For a complete list of 3Com documents, contact your 3Com representative.

Reference Documents

The following documents supply related background information:

Case, J., Fedor, M., Scoffstall, M., and J. Davin, *The Simple Network Management Protocol*, RFC 1157, University of Tennessee at Knoxville, Performance Systems International and the MIT Laboratory for Computer Science, May 1990.

Rose, M., and K. McCloghrie, *Structure and Identification of Management Information for TCP/IP-based Internets*, RFC 1155, Performance Systems International and Hughes LAN Systems, May 1990.

1 INTRODUCTION

This chapter contains the following sections:

- Management Command Conventions
- Management Commands

Management Command Conventions

Table 4 describes the command conventions used in this document.

Table 4 Command Conventions

Convention	Definition and Example
System Output	`Courier` typeface
Terminal Prompt	System prompt is shown as `CB5000>`
User Defined Input	Indicated by **`bold courier text`**

Understanding Command Conventions

You manage the CoreBuilder® 5000 Distributed Management Module (DMM) by entering commands at the management prompt on the terminal console, or remotely using TELNET. Commands are not case-sensitive (that is, you can use uppercase and lowercase characters with equal effect), with the exception of the SET COMMUNITY command.

Using Terminal Keystrokes

In addition to alphanumeric characters, terminal input for the DMM includes basic keyboard functions and control sequences. For example, you can correct typing mistakes by pressing the Delete key or the Backspace key. Pressing Enter in the middle of a command entry when an argument is expected causes the DMM to prompt you for additional information. Terminal keystrokes and their functions are outlined in Table 5.

Table 5 Keystroke Functions

Keystroke	Function
Backspace	Moves the cursor back one character and deletes that character.
Ctrl+C	Terminates the current command and returns to a blank command line at any time.
Ctrl+D	Closes a TELNET session.
Ctrl+R	Retypes the previous command string on the command line.
Delete	Same as Backspace.
Enter	Enters the command.
spacebar	Completes a command through *command completion* (refer to next section).
?	Displays the available command options.

Using the Command Completion Feature

Command completion allows the DMM interface to accept abbreviated command input. When using command completion, you need only enter a minimum number of characters to distinguish the command from other acceptable choices and press Space to complete the command. For example, if you type:

```
sa
```

Press the spacebar and the command is completed as follows:

```
save
```

If the characters entered are not sufficient to determine a unique command, the DMM waits for more characters to be entered. For example, entering the letter s and pressing the spacebar is not sufficient for the DMM to determine which command to issue because commands other than SAVE start with the letter s (for example, SET, SHOW).

Management Commands

Chapter 2 provides an alphabetized list of Distributed Management Module (DMM) commands.

Each description includes:

- One or more examples outlining the proper syntax for the command
- Parameter options
- Corresponding terminal responses

Entering Management Commands

Enter management commands at the management prompt. By default, the management prompt is `CB5000>`. Refer to the SET TERMINAL PROMPT command in Chapter 2 for information about customizing the default management prompt.

Entering Parameters

The DMM management software has an intelligent parser that recognizes modules.

- If you enter an invalid parameter for a module type:
  - The parser backspaces over the invalid parameter.
  - The DMM waits for you to complete the command line with a valid parameter.
- If you attempt to set a parameter to the same setting it is currently configured for:
  - A message is displayed that reiterates the setting.
  - The parser sends a `Command aborted` message.

2 MANAGEMENT COMMANDS

This section provides an alphabetized list of CoreBuilder® 5000 Distributed Management Module (DMM) commands.

Each description includes:

- Format for the command, including parameter options
- Examples, including corresponding terminal responses
- Related commands

For information on CoreBuilder 5000 Switched FastModules, refer to the CoreBuilder 5000 FastModule User Guide.

For information on CoreBuilder 5000 SwitchModules, refer to the CoreBuilder 5000 SwitchModule User Guide.

?

Use the ? command to list available command choices and parameter options.

Format

any command ——— **?**

Example

To view the available management commands, use the following command after you log in using the administrator password:

```
CB5000> ?

Possible completions:
     bootp
     clear
     copy
     download
     logout
     maintain
     monitor
     ping
     reset
     revert
     run
     save
     set
     show
     telnet
     upload
```

The ? character does not appear on the screen after you enter it.

BOOTP

Use the BOOTP command to download configuration information from the bootptab file on a BootP server to a DMM. BootP (Bootstrap Protocol) is a UDP/IP-based protocol (User Datagram Protocol/Internet Protocol) that allows a device to configure itself dynamically without user intervention.

Format

bootp

Example

The following command initiates the BootP function on the DMM:

```
CB5000> bootp
```

Related Commands

CLEAR BOOTP
SET BOOTP MODULE
SET BOOTP POWER_UP_MODE
SET BOOTP SERVER_IP_ADDRESS
SHOW BOOTP

CLEAR ATM

Use the CLEAR ATM command to clear the ATM's if_Name (interface name) for the ATM-layer interface.

Format

clear atm — *slot* — **if_name** — *name*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
name	Use up to 63 characters for the ifName.

Example

The following command clears the ATM if_name (Test) from the ATM module in slot 4.

```
CB5000> clear atm 4 if_name Test

Slot 04 parameter cleared.
```

Related Commands

SET ATM NEIGHBOR IF_NAME
SHOW ATM INTERFACE

CLEAR BOOTP

Use the CLEAR BOOTP command to clear current BootP settings.

Format

clear bootp — **module**
result

module	Clears any setting made using the SET BOOTP MODULE command.
result	Clears the result stored for the last BootP operation.

Example

The following command clears BootP configuration settings from the DMM:

```
CB5000> clear bootp module
BootP module configurations cleared.
```

Related Commands

BOOTP
SET BOOTP MODULE
SET BOOTP POWER_UP_MODE
SET BOOTP SERVER_IP_ADDRESS
SHOW BOOTP

CLEAR BPORT_LEC ELAN_NAME

Use the CLEAR BPORT_LEC ELAN_NAME command to clear the name of the configured LAN (ELAN) associated with the LAN Emulation Client (LEC).

The value of the ELAN name may or may not be taken into account by the LAN Emulation Configuration Server (LECS) and LAN Emulation Server (LES)*, depending on the policy configured on those servers.*

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

clear bport_lec — *slot.lec* — **elan_name** — *name*

slot.lec	Identifies the slot and lec for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
name	Specifies the name (up to 63 characters) of the LAN associated with the LEC.

Example

The following command clears the name of the LEC in slot 4, port 1 to Main:

```
CB5000> clear bport_lec 4.1 elan_name Main
Bridge Port 04.01 parameter cleared.
```

Related Commands

SET BPORT_LEC ELAN_NAME
SHOW BPORT_LEC CONFIGURATION

CLEAR BPORT_LEC LECS_ATM_ADDRESS

Use the CLEAR BPORT_LEC LECS_ATM_ADDRESS command to clear the configured ATM address of the LAN Emulation Configuration Server (LECS).

The ATM address is 20 hexadecimal numbers separated by periods. Each number can range from 0 to FF. However, the following addresses are illegal:

- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
- FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

clear bport_lec ——— *slot. lec* ——— **lecs_atm_address** ——— *ATM address*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
ATM address	Specifies the ATM address of the LAN Emulation Configuration Server (LECS).

Example

The following command clears the ATM address of the LECS in slot 4, port 1:

```
CB5000> clear bport_lec 4.1 lecs_atm_address
39.99.99.99.ac.00.00.00.
00.99.99.01.02.03.04.05.06.07.08.00
Bridge Port 04.01 parameter cleared.
```

Related Commands

SET BPORT_LEC LECS_ATM_ADDRESS
SHOW BPORT_LEC CONFIGURATION

CLEAR BPORT_LEC LES_ATM_ADDRESS

Use the CLEAR BPORT_LEC LES_ATM_ADDRESS command to clear the configured LAN Emulation Server (LES) ATM address.

The ATM address is 20 hexadecimal numbers separated by periods. Each number can range from 0 to FF. However, the following addresses are illegal:

- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
- FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

clear bport_lec — *slot.lec* — **les_atm_address** — *ATM address*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
ATM address	Specifies the ATM address of the LES.

Example

The following command clears the ATM address of the LES in slot 4, port 1:

```
CB5000> clear bport_lec 4.1 les_atm_address 39.00.99.99.99.99.ac.
00.99.99.99.99.99.99.99.99.99.99.99.99
Bridge Port 04.01 parameter cleared.
```

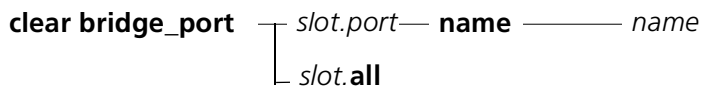
Related Commands

SET BPORT_LEC LES_ATM_ADDRESS
SHOW BPORT_LEC CONFIGURATION

CLEAR BRIDGE_PORT NAME

Use the CLEAR BRIDGE_PORT NAME command to clear a bridge port name. When you enter this command, you can specify one bridge port name or all bridge port names.

Format



slot.port	Identifies the port for this operation. *slot* is the slot number (1 through 17) and *port* is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Clears all bridge port names in a particular slot.
name	Specifies the name (up to 32 characters) you want to identify this port.

Example

The following command clears the name finance_1 to port 3 on the SwitchModule in slot 5:

```
CB5000> clear bridge_port 5.3 name finance_1
```

Related Command

SET BRIDGE_PORT NAME

CLEAR COMMUNITY

Use the CLEAR COMMUNITY command to delete an entry from the community table. Community tables establish groups of stations that can exchange information with the DMM agent.

Format

all	Clears all community table entries.
1...10	Clears just the entry you specify. For example, if you enter CLEAR COMMUNITY 2, the management hub clears community table entry #2. Use the SHOW COMMUNITY command to display a list of numbered entries.

Example

The following command clears community table entry #5:

```
CB5000> clear community 5
Community 5 cleared.
```

Related Commands

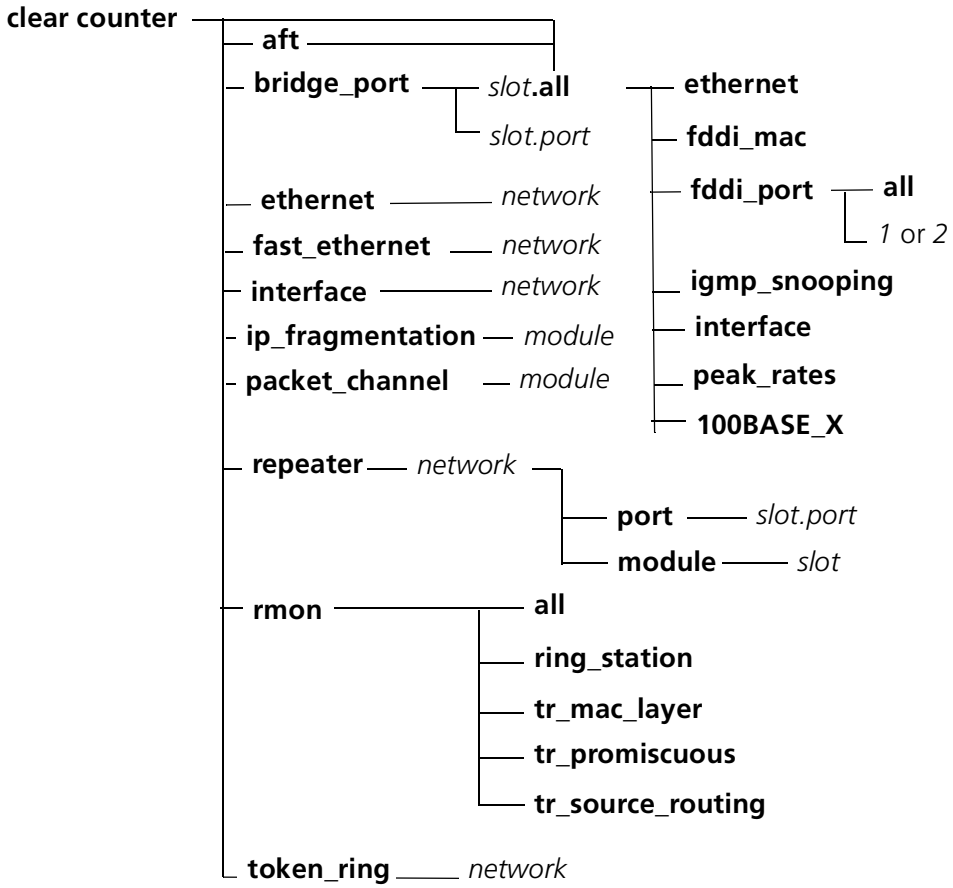
SET COMMUNITY
SHOW COMMUNITY

CLEAR COUNTER

Use the CLEAR COUNTER command to reset to zero DMM counters or a specific group of DMM counters.

The CLEAR COUNTER command does not affect counters reported by SNMP, which are always stored as absolute values, as specified in the SNMP standard.

Format



network	Any of the active available backplane or isolated Ethernet or Fast Ethernet or Token Ring networks.
slot.port	Selects a port to clear counters for. *slot* is the slot number (slot 1 through slot 17) and *port* is the port number (port 1 through port 4). For example, to specify port 4 on the module in slot 6, enter **6.4**
module.slot	Specifies the module and the slot number in the hub.

Example 1 The following command clears Ethernet counters on Ethernet network 1:

```
CB5000> clear counter ethernet ethernet_1
Ethernet Statistics for ETHERNET_1 cleared.
```

Example 2 The following command clears repeater counters on port 3, Fast Ethernet network 1:

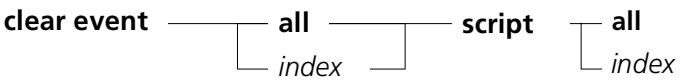
```
CB5000> clear counter repeater fast_ethernet_1 port 3.1
Repeater Statistics for Port 3.1 on FAST_ETHER_1 cleared.
```

Related Command SHOW COUNTER

CLEAR EVENT SCRIPT

Use the CLEAR EVENT SCRIPT command to clear assignments for scripts to run when a specified RMON event occurs.

Format



all	Clears all script-to-event assignments.
index	Specifies the index number of the RMON event that triggers the script. Use the SHOW RMON EVENT CONTROL command to view events listed by index number. Use the SHOW EVENT command to view script-to-event assignments listed by index number.

Example

The following command clears the assignment of script 1 to RMON event 3:

```
CB5000> clear event 3 script 1
Event Index 3 cleared.
```

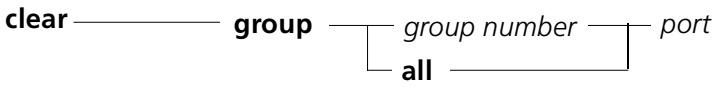
Related Commands

SET EVENT SCRIPT
SHOW EVENT
SHOW RMON EVENT CONTROL
SHOW SCRIPT

CLEAR GROUP

Use the CLEAR GROUP command to remove all groups or individual groups from the indicated port.

Format



group number	Removes the specified group from the port.
port	Removes all the groups from the specified port (1 through 40)

Example

The following command clears the group from port 1:

```
CB5000> clear group group1 1
```

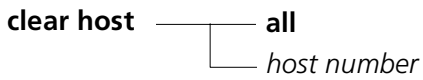
Related Command

CLEAR COUNTER BRIDGE_PORT IGMP_SNOOPING

CLEAR HOST

Use the CLEAR HOST command to clear a host entry name from the host table.

Format



all	Removes all host table entries.
host number	Removes just the entry you specify. For example, if you enter CLEAR HOST 2, the DMM removes host table entry #2. Use the SHOW HOST command to display a list of numbered entries. *host* = 1...20

Example

The following command clears the first host name from the host table:

```
CB5000> clear host 1
Host 1 name cleared.
```

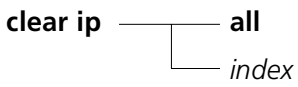
Related Commands

SET HOST
SHOW HOST

CLEAR IP

Use the CLEAR IP command to clear previously entered Internet Protocol (IP) information associated with one or all hub networks.

Format



all	Clears all IP information stored on the DMM.
index	Specifies the index number for the network whose IP information you are clearing.

Example The following command sequence clears the IP information for ETHERNET_2:

```
CB5000> show ip

Active Default Gateway : 151.104.25.1

Index Network         Slot IP Address         Subnet Mask        Default Gateway
----- ------------- ---- -----------       -----------       ---------------

  1     ETHERNET_2     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  2     ETHERNET_3     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  3     ETHERNET_4     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  4     ETHERNET_5     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  5     ETHERNET_6     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  6     ETHERNET_7     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  7     ETHERNET_8     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0
  8     TOKEN_RING_1   N/A    151.104.25.120    ff.ff.ff.00        151.104.25.1
  9     ISOLATED       1      127.0.0.1         ff.00.00.00        0.0.0.0
  10    ISOLATED       15     127.0.0.1         ff.00.00.00        0.0.0.0
  11    ETHERNET_1     N/A    151.104.25.120    ff.ff.ff.00        0.0.0.0

CB5000> clear ip 1

IP Address Table entry number 1 for network ETHERNET_2 cleared.
```

Related Commands SET IP
SHOW IP

CLEAR IP ARP_CACHE

Use the CLEAR IP ARP_CACHE command to clear the Address Resolution Protocol table when ring configuration changes are made. The ARP table entries time out if not updated within 20 minutes.

You should clear the ARP table if you either:

- Change a station's IP configuration (for example, interfaces, IP address)
- Experience difficulty in communicating with a station

After the table is cleared, the DMM relearns all stations' IP-to-MAC addresses when the next IP-based operation is established. The ARP table is then rebuilt with the new information.

Format

clear ip arp_cache

Example

The following command clears the DMM ARP cache:

```
CB5000> clear ip arp_cache
ARP Cache Flushed.
```

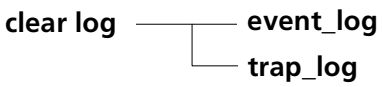
Related Commands

SET IP
SHOW IP

CLEAR LOG

Use the CLEAR LOG command to erase the information in the event or trap log.

Format



event_log	Clears the DMM log of fatal system errors.
trap_log	Clears the DMM log of system messages.

Example

The following command clears the fatal system error log:

```
CB5000> clear log event_log
Event log is cleared.
```

Related Commands

SHOW LOG EVENT_LOG
SHOW LOG TRAP_LOG

CLEAR LOG MODULE EVENT_LOG

Use the CLEAR LOG MODULE EVENT_LOG command to erase the event_log information from the SwitchModule NVRAM.

If you are running SwitchModule code Version v1.00, the following message is displayed: `Module's software version does not support this feature`. *This command supports only SwitchModule Version v1. 10 or later.*

Format

clear log ——— **module** — *slot* — **event_log**

slot	Specifies the slot number of the SwitchModule.

Example

The following command clears SwitchModule event log information from SwitchModule NVRAM:

```
CB5000> clear log module 2 event_log
Module 2 event log is cleared.
```

Related Command

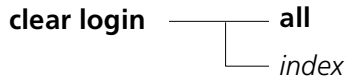
SHOW LOG MODULE EVENT_LOG

CLEAR LOGIN

Use the CLEAR LOGIN command to remove previously entered login names.

The DMM lets you store up to 10 user names and passwords. These provide access to the management software.

Format



all	Removes all login names.
index	Removes just the entry you specify. For example, if you enter CLEAR LOGIN 2, the removes login entry #2. Use the SHOW LOGIN command to display a list of numbered entries. *index* = 1...10

Example

The following command clears the first login entry:

```
CB5000> clear login 1
Login 1 cleared.
```

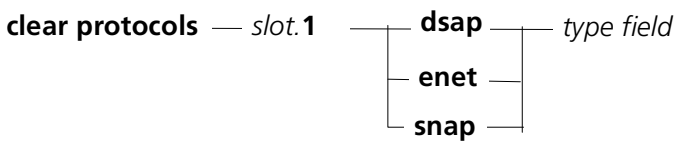
Related Commands

SET LOGIN
SHOW LOGIN

CLEAR PROTOCOLS

Use the CLEAR PROTOCOLS command to remove a protocol filter from an CoreBuilder 5000 SwitchModule.

Format



slot.**1**	Identifies the SwitchModule that is affected by this command.
dsap	Delete a filter for packets with the protocol type DSAP.
enet	Delete a filter for packets with the protocol type Ethernet.
snap	Delete a filter for packets with the protocol type SNAP (SubNetwork Access Protocol).
type field	Specifies the type field of the protocol filter you are deleting.

Example

The following command deletes the filter for Ethernet DECnet Phase IV packets from the protocol forwarding table:

```
CB5000> clear protocols 4.1 enet 60-03
Filter cleared.
```

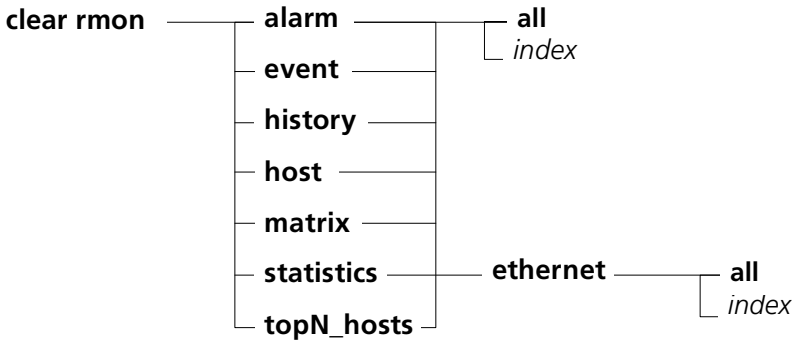
Related Commands

SET PROTOCOLS FORWARDING
SHOW PROTOCOLS

CLEAR RMON

Use the CLEAR RMON command to clear previously entered Ethernet RMON control tables.

Format



all	Clear all the RMON control table entries for the specified option (alarm, statistics).
index	Index number for the RMON control table entry for the specified option (alarm, statistics) you are clearing.

Example

The following command clears the first control table entry in the RMON alarm control table:

```
CB5000> clear rmon alarm 1
Alarm 1 cleared.
```

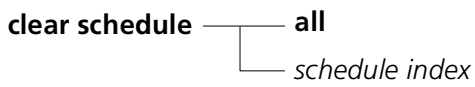
Related Commands

SET RMON
SHOW RMON CONTROL

CLEAR SCHEDULE

Use the CLEAR SCHEDULE command to remove a schedule entry from the schedule table.

Format



all	Removes all schedule entries from the schedule table.
schedule index	Removes the schedule entry you specify. For example, if you enter CLEAR SCHEDULE 2, the DMM removes schedule #2 from the schedule table. Use the SHOW SCHEDULE command to display the current schedule table. *index* = 1...10

Example

The following command clears schedule entry #3 from the schedule table:

```
CB5000> clear schedule 3
Schedule 3 cleared.
```

Related Commands

SET SCHEDULE
SHOW SCHEDULE

CLEAR SCRIPT

Use the CLEAR SCRIPT command to remove a script from the script table.

Format

all	Removes all scripts from the DMM.
number	Removes the specific script number you specify. For example, if you enter CLEAR SCRIPT 2, the DMM removes script #2 from the script table. Use the SHOW SCRIPT command to display the script table. *number* = 1... 8

Example

The following command removes the first script from the script table:

```
CB5000> clear script 1
Script 1 cleared.
```

Related Commands

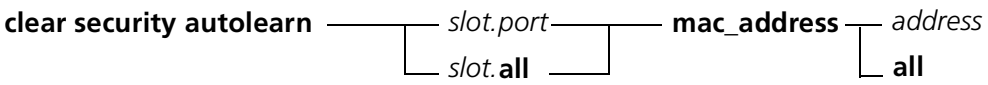
COPY SCRIPT
RUN SCRIPT
REVERT/SAVE SCRIPTS
SET ALERT SCRIPT
SET SCRIPT
SHOW SCRIPT

CLEAR SECURITY AUTOLEARN

Use the CLEAR SECURITY AUTOLEARN command to clear entries from the Autolearning database.

To remove all old MAC addresses from the Autolearning database, you must clear both the Autolearn Address table using the CLEAR SECURITY AUTOLEARN slot.ALL MAC_ADDRESS command and then clear the Security Address database using the CLEAR SECURITY PORT slot.ALL MAC_ADDRESS command.

Format



slot.port	Identifies the port for this operation. *slot* is the slot (1 through 17) and *port* is the port number (1 through 40). For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.
address	MAC address you are clearing using this command. The format for MAC addresses is nn-nn-nn-nn-nn-nn. The address 00-00-00-00-00-00 is invalid for this command.

Example

The following command clears the MAC address 08-00-87-01-a7-b2 from the Autolearning database, associated with port 3 on the module in slot 7:

```
CB5000> clear security autolearn 7.3 mac_address 08-00-87-01-a7-b2
Port 07.03 address 08-00-87-01-a7-b2 cleared from autolearning
area.
```

Related Commands

SET SECURITY AUTOLEARN
SHOW SECURITY AUTOLEARN

CLEAR SECURITY INTRUDER_LIST

Use the CLEAR SECURITY INTRUDER_LIST command to clear the list of port security intrusions.

Format

clear security intruder_list

Example The following command clears the intruder list:

```
CB5000> clear security intruder_list
Security Intruder List cleared.
```

Related Command SHOW SECURITY INTRUDER_LIST

CLEAR SECURITY PORT

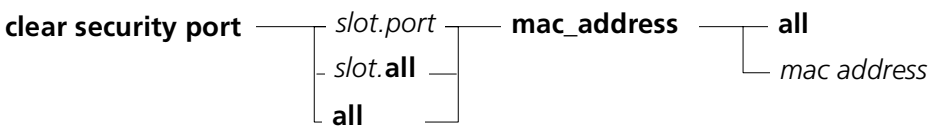
Use the CLEAR SECURITY PORT command to remove a MAC address from the security database for a port.

To remove all old MAC addresses from the Autolearning database, you must clear both the Autolearn Address table using the CLEAR SECURITY AUTOLEARN slot.ALL MAC_ADDRESS command and then clear the Security Address database using the CLEAR SECURITY PORT slot.ALL MAC_ADDRESS command.

Removing an authorized MAC address does not automatically disable Security Mode. If you remove the only authorized MAC addresses for a port but do not disable Security Mode, the DMM prevents any station from communicating through the port.

Use the SET SECURITY PORT MODE command to enable and disable Security Mode.

Format



slot.port	Removes the MAC address from the security database for the port identified by *slot.port*. *slot* is the slot number and *port* is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Removes the MAC address from the security database for all ports in the identified slot.
all	Removes all MAC addresses from the security database for the entire hub.
mac address	Removes the MAC address from the security database for the identified port. Enter the address as a series of six hexadecimal bytes separated by hyphens. For example, 10-00-f1-0f-0c-63.

Example

The following command clears the MAC address 07-34-24-02-0F-00 from the security database for all ports on the module in slot 7:

```
CB5000> clear security port 7.all mac_address 07-34-24-02-0F-00
Port 07.all security MAC address 07-34-24—02-0F-00 cleared.
```

Related Commands

REVERT/SAVE SECURITY
SET SECURITY PORT ACTION_ON_INTRUSION
SET SECURITY PORT MAC_ADDRESS
SET SECURITY PORT MODE
SHOW SECURITY PORT

CLEAR TFTP RESULT

Use the CLEAR TFTP RESULT command to clear the TFTP Result field in the SHOW TFTP command display.

The DMM uses TFTP (Trivial File Transfer Protocol) to download files. The DMM reports the status of the download in the TFTP Result field that is displayed when you use the SHOW TFTP command. The CLEAR TFTP RESULT command overwrites the value currently stored for TFTP Result with the value CLEAR.

Use the CLEAR TFTP RESULT command before you begin a download so you can check the status of the download after it has been completed.

Format

clear tftp result

Example The following command clears the current TFTP Result value:

```
CB5000> clear tftp result
Tftp result cleared.
```

Related Command SHOW TFTP

CLEAR TR_SURROGATE

Use the CLEAR TR_SURROGATE command to clear Token Ring surrogate information.

Format

clear tr_surrogate — *slot.***2** ——— *group*

slot	Identifies the slot where the specified TR-NMC for this operation resides.
group	Specifies the name of the Token Ring surrogate group you want to clear. The rem_soft_error group is the only group implemented currently.

Example

The following command clears the Token Ring surrogate REM soft error information on the TR-NMC in slot 11.2:

```
CB5000> clear tr_surrogate 11.2 rem_soft_error
```

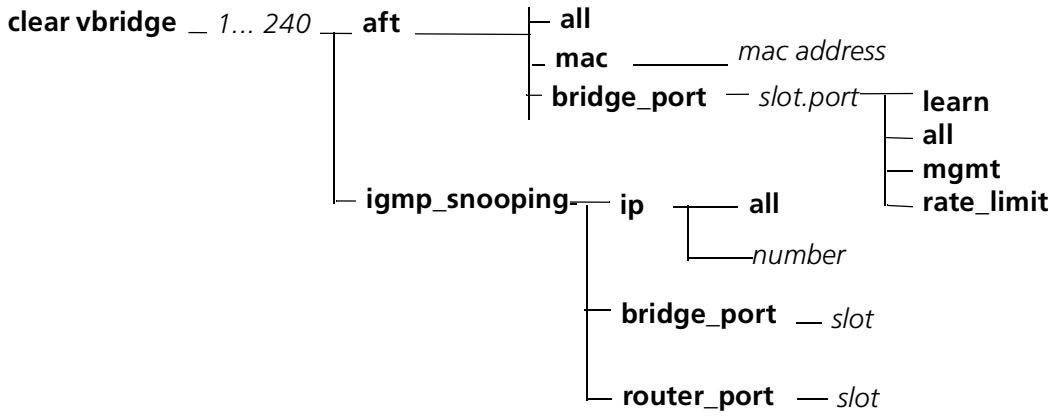
Related Command

SHOW TR_SURROGATE

CLEAR VBRIDGE

Use the CLEAR VBRIDGE command to delete specified Address Forwarding Table (AFT) or Internet Grouping Management Protocol (IGMP) snooping vbridges.

Format



1....240	Identifies the vbridge.
all	Deletes all user-created entries and learned addresses in the specified virtual bridge address table.
mac	Deletes entries related to a specific MAC address from the address table.
mac address	MAC address for the AFT vbridge to be deleted.
bridge_port	Deletes the user-created entries (mgmt) on a specified port.
slot.port	*slot* and *port* where the module with the vbridge to be deleted resides.
number	IP address for the IGMP snooping vbridge to be deleted.

Example

This command deletes AFT entries related to the MAC address 8f-59-43-63-35-68 from the AFT:

```
CB5000 > clear vbridge 2 aft mac 8f-59-43-63-35-68
Clear Vbridge 2 AFT Entry 8f-59-43-63-35-68 Deleted.
```

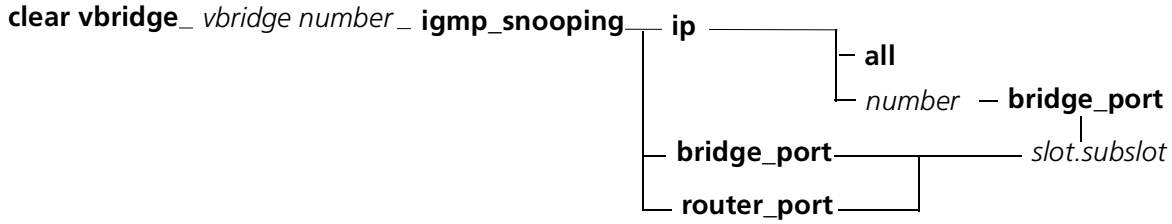
Related Command

SHOW VBRIDGE AFT

CLEAR VBRIDGE IGMP_SNOOPING

Use the CLEAR VBRIDGE IGMP_SNOOPING command to remove all IGMP Snooping knowledge on the indicated bridge port slot.port.

Format



vbridge number	Identifies the specific vbridge from which to clear the IGMP Snooping information.
number	IP address from which to clear the IGMP Snooping information.
slot.subslot	Identifies the specific bridge port or router port from which to clear the IGMP Snooping information.

Example

The following command clears the IGMP Snooping information from vbridge 10 on port 3 of the module in slot 8, subslot 1:

```
CB5000> clear vbridge 10 igmp_snooping bridge_port 8.1
```

Related Command

CLEAR COUNTER BRIDGE_PORT IGMP_SNOOPING

COPY SCRIPT

Use the COPY SCRIPT command to copy the contents of one script to another script.

Format

copy script — *source script index* — **to** — *target script index*

source script index	Identifies the source script. Use the SHOW SCRIPT command to display a list of scripts. *source script index* = 1...8
target script index	Identifies the target script. For example, the command COPY SCRIPT 1 to 6 copies the contents of script 1 through script 6. *target script index* = 1...8

Example

The following command copies script 1 to script 2:

```
CB5000> copy script 1 to 2
Script 1 copied to script 2.
```

Related Commands

RUN SCRIPT
REVERT/SAVE SCRIPTS
SET ALERT SCRIPT
SET SCRIPT
SHOW SCRIPT

DOWNLOAD FROM_DEVICE

Use the DOWNLOAD FROM_DEVICE command to download operational or boot code from the master DMM to a standby DMM in the same hub.

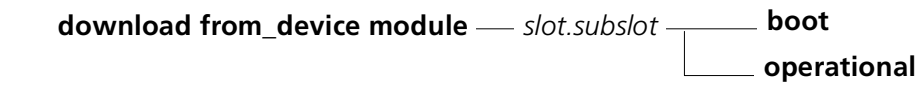
Refer to the CoreBuilder 5000 Distributed Management Module User Guide *for detailed download procedures.*

Use this command only when 3Com Corporation issues a new Update Distribution Kit (UDK) diskette. The download takes 15 to 30 seconds to complete. (Time frames from the operational code may take about 6 minutes for DMM code.) Each dot displayed during the procedure indicates a packet received.

If the DMM does not respond after a BOOT download, contact your 3Com representative for more information.

A short window of vulnerability exists during the download of boot code to the DMM, during which a loss of power can leave the DMM without BOOT code, and therefore not operational. If the DMM does not respond after a BOOT download, contact your 3Com representative for more information.

Format



slot.subslot	Selects the slot that you want to download DMM code to. The source is always the hub's master DMM. For DMM with carrier, use subslot 8 and for DMM (without carrier), use subslot 1.
boot	A small program that gets each module up and running. In the DMM, it also handles the self-download function.
operational	The code that provides module functionality. Operational updates are more common, because they may provide additional functionality.

Example

The following command initiates the download of boot code from the master DMM to the standby DMM in slot 6.1:

```
CB5000> download from_device module 6.1 boot
```

Related Commands

DOWNLOAD IN_BAND
DOWNLOAD OUT_OF_BAND

DOWNLOAD IN_BAND

Use the DOWNLOAD IN_BAND command to load new software into the DMM. An in-band download takes place over the network.

The DOWNLOAD IN_BAND command loads new software into the DMM. When you enter the command, the DMM requests the download from a TFTP (Trivial File Transfer Protocol) server on your network. The TFTP server transmits the new code to the DMM, and, if needed, the DMM then transmits the new code to the module.

Before you use the DOWNLOAD IN_BAND command:

- Use the SET TFTP FILE_NAME command to specify the name of the file to download.
- Use the SET TFTP SERVER_IP_ADDRESS command to specify the IP address of the TFTP server.

Save all parameters (including TFTP) before downloading DMM and RCTL code.

Traffic statistic collection and display features are disabled during a download. These features restart automatically after the download completes successfully.

Any network function (such as Ping and Telnet) that attempts to communicate with a DMM will not succeed until the download completes successfully and the DMM reinitializes.

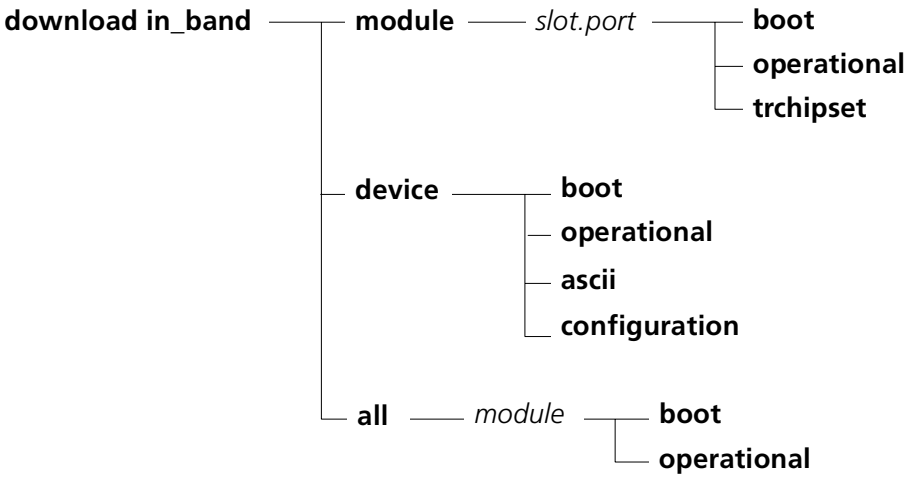
A short window of vulnerability exists during the download of boot code to the DMM, during which a loss of power can leave the DMM without BOOT code, and therefore not operational. If the DMM does not respond after a BOOT download, contact your 3Com representative for more information.

Part of the inband download procedure involves configuring TFTP parameters. Refer to the SET TFTP FILE_NAME and SET TFTP SERVER_IP_ADDRESS commands in this chapter for information on using TFTP.

Do not use the RESET MASTERSHIP command during download.

You cannot download modules using the SLIP interface.

Format



module	Specifies download to a particular module in the hub.
device	Specifies download to the DMM.
all	Specifies download to all modules of the selected type.
boot	Specifies a download of boot code.
operational	Specifies a download of operational code.
trchipset	Specifies a download of chipset code to the TR-NMC module.
ascii	Specifies a download of an ASCII script file.
configuration	Specifies a download of a binary configuration file. This command applies to the DMM only.
module	The module type that you want to download code to. Only certain 3Com CoreBuilder® 5000 modules support this operation.
slot.subslot	The location of the module where you want to download the new code.

Example The following command starts a download of operational code to the management hub:

```
CB5000> download in_band device operational

Please stand by for download:
(Target will reset upon successful download completion)

The 3Com Key Code can be obtained by completing the UDK
fax form and faxing it to 3Com at (508) 460-6195.

Enter Upgrade Distribution Kit Serial number: XXXXXXXX
Enter 3Com Key Code: XXXXXXXXX

Welcome to Boot Services version 3.0.
1024 kBytes flash memory installed.

Inband download in progress.

boot>

Opening file xmm.bin on 151.104.2.98...
Connected to 151.104.2.98.
Connection closed for flash erasure.

Erasing flash... done.

Opening file xmm.bin on 151.104.2.98...
Connected to 151.104.2.98.

Receiving TFTP Packets:

.........................................................
.........................................................
.....................................

727824 bytes received in 63.72 seconds.

Calculating CRC... done.
Updating checksum... done.
Download complete.
```

Related Commands

DOWNLOAD OUT_OF_BAND
SET TFTP FILE_NAME
SET TFTP SERVER_IP_ADDRESS
UPLOAD IN_BAND CONFIGURATION

DOWNLOAD OUT_OF_BAND

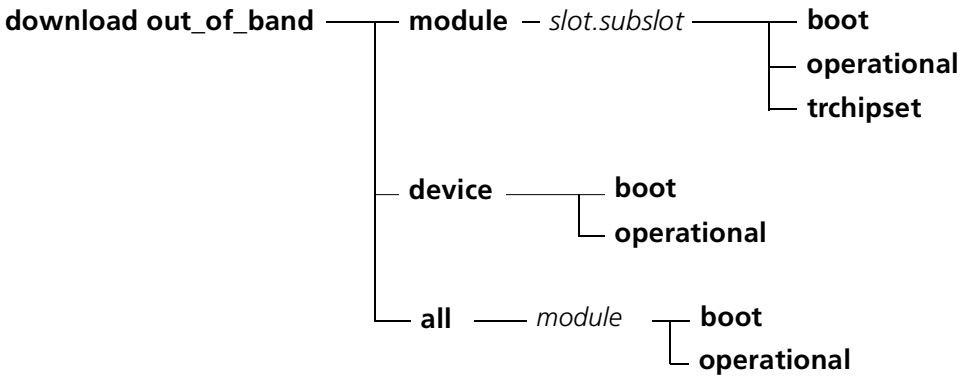
Use the DOWNLOAD OUT_OF_BAND command to load new software onto the DMM. An out-of-band download uses XMODEM and takes place over a serial connection between a personal computer and the console port on the DMM.

Traffic statistic collection and display features are disabled during a download. These features restart automatically after the download completes successfully.

Any network function (such as Ping and Telnet) that attempts to communicate with a DMM will not succeed until the download completes successfully and the DMM reinitializes.

Do not use the RESET MASTERSHIP command during a download.

Format



module	Specifies download to a particular module in the hub.
device	Specifies download to the DMM.
all	Specifies download to all modules of the selected type.
boot	Specifies a download of boot code.
operational	Specifies a download of operational code.
trchipset	Specifies a download of chipset code to the TR-NMC module.
ascii	Specifies a download of an ASCII script file.
configuration	Specifies a download of a binary configuration file. This command applies to the DMM only.
module	The module type that you want to download code to. Only certain 3Com CoreBuilder® 5000 modules support this operation.
slot.subslot	The location of the module where you want to download the new code.

Example The following command initiates a download of boot code to the DMM issuing the DOWNLOAD command (that is, a self-download):

```
CB5000> download out_of_band device boot

Please stand by for download:
(Target will reset upon successful download completion)


Welcome to Boot Services version v3.0.0.
1024 kBytes flash memory installed.

boot> download out_of_band device boot

Please initiate file transfer sequence.

CC

Calculating CRC... done.
Erasing flash... done.
Writing flash... done.
Updating checksum... done.
Download complete.

Booting device...
Login:
```

Enter the command once at the DMM "operational"

Enter the command a second time at the DMM boot > prompt.

The download process ends by rebooting the device.

Related Command DOWNLOAD IN_BAND

LOGOUT

Use the LOGOUT command to log out from either a remote or local DMM session.

If you are logged in to a local session (a session with the management hub to which the terminal is connected), entering the LOGOUT command ends the session.

If you are logged in to a remote DMM or other device, entering the LOGOUT command breaks the connection to the remote device and leaves you connected to the local device.

Format

logout

Example

The following command logs you out from a local session:

```
CB5000> logout
Good-Bye
```

Related Commands

SAVE
REVERT

MAINTAIN

Use the MAINTAIN command to enter maintenance mode. Certain inventory related commands are available only from maintenance mode. Maintenance mode allows you to enter information that is written permanently in a module's EEPROM. Maintenance mode gives you access to the BOOT, DOWNLOAD, SET INVENTORY POWER, and SHOW INVENTORY POWER commands. You must SAVE or REVERT all changes before entering maintenance mode.

Only logins with super-user access can enter maintenance mode.

You cannot enter the MAINTAIN command if you are connected to a remote DMM through the TELNET command. Enter the BOOT command to exit maintenance mode.

The DMM does not track network statistics when in maintenance mode.

Format

maintain

Example The following command allows a user with super-user privileges to enter maintenance mode:

```
CB5000> maintain
```

To enter maintenance mode, enter your current session password at the prompt as shown below:

```
Enter current session password for user "system":
```

The following information appears:

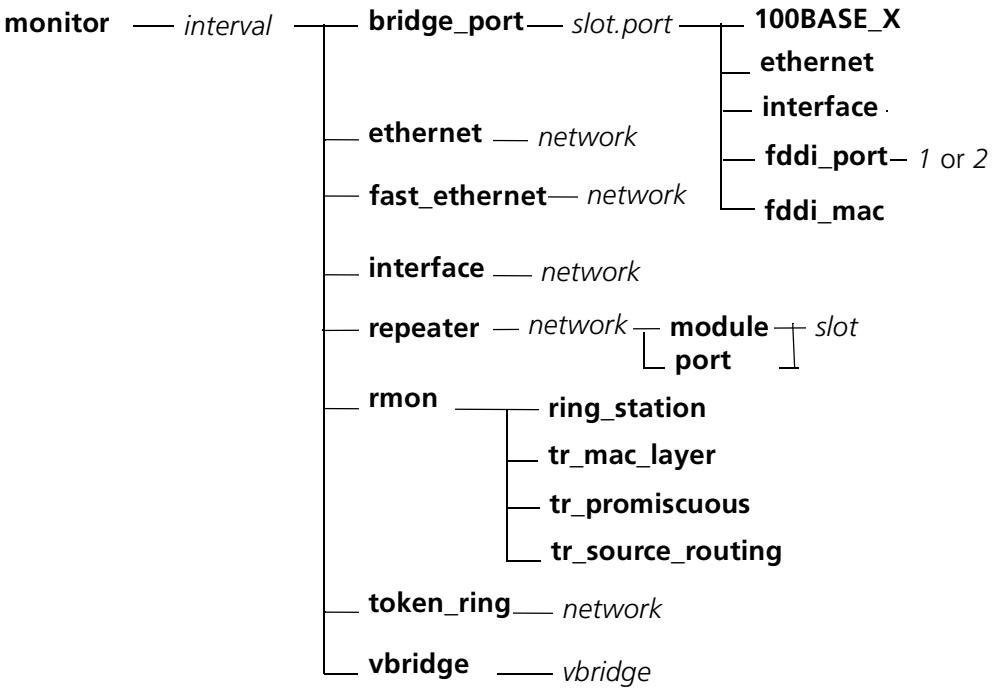
```
CB5000
Distributed Management Module (vx.xx)
Copyright 199x 3Com Corporation
>>
```

MONITOR

Use the MONITOR command to view ongoing network statistics. This command displays statistics for a device, network, or port. The display is updated periodically based on the number of minutes and seconds you assign. Press Ctrl+C to discontinue this process and return to the management prompt.

The MONITOR command reports information similar to the SHOW COUNTER command display except that the MONITOR command display captures events only at the time of request. The information displayed by the SHOW COUNTER command is current. Refer to the SHOW COUNTER commands for descriptions of the displays.

Format



interval	The system-specified range of time allotted for monitoring is 00 through 30 minutes (mm) and 05 through 59 seconds (ss). Use these ranges when specifying a length of time to monitor your network.
slot.port	Specifies the *slot* (1 through 17, 1 through 10, or 1 through 7) and *port* (1 through 40) you want to monitor.
network	Indicates the type and number of network to monitor: ■ ethernet_1 through ethernet_8 ■ fast_ethernet_1 through fast_ethernet_4 ■ isolated
vbridge	Specifies the SwitchModule virtual bridge (1 through 240) you want to monitor.

Example The following command displays statistics every 2 minutes for traffic on ethernet_1:

```
CB5000> monitor 2:00 ethernet ethernet_1

Ethernet Statistics for ETHERNET_1
------------------------------------------------------------------------------
                                      Cumulative        Last Time Interval
------------------------------------------------------------------------------
FCS Errors                           0                           0
SQE Test Errors                      0                           0
Alignment Errors                     0                           0
Carrier Sense Errors                 0                           0
Frame Too Longs                      0                           0
Deferred Transmissions               0                           0
Late Collisions                      0                           0
Excessive Collisions                 0                           0
Single Collision Frames              0                           0
Multiple Collision Frames            0                           0
Internal MAC Receive Errors          0                           0
Internal MAC Transmit Errors         0                           0

Display will refresh every 2 minutes 0 seconds.
Press CTRL-C to exit.
```

Related Command SHOW COUNTER

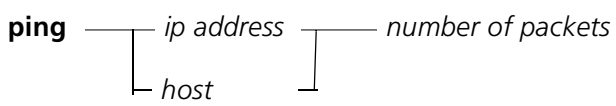
PING

Use the PING command to verify that a device is active on the network.

The PING command sends up to 255 ICMP (Internet Control Message Protocol) request packets to the specified device. If the device is alive, it responds to each request packet that it receives. If the device responds to less than 100 percent of the request packets, the network may be dropping packets.

If you are having trouble pinging to a remote device, make sure the device is on the same network (segment), or bridged or routed to that segment.

Format



ip address	Specifies the IP (Internet Protocol) address of the device to be tested. The format of the address is nnn.nnn.nnn.nnn.
host	Specifies the name of the host to be tested.
number of packets	Number of request packets to send. You can use any number in the range of 1 through 255. The default is 1 packet.

Example

The following command sends two ping requests to IP address 133.8.9.60:

```
CB5000> ping 133.8.9.60 2
```

The device responds to both request packets:

```
Starting ping, resolution of displayed time is 10 milli-sec
64 bytes from 133.8.9.60: icmp_seq=0. time=10. ms
64 bytes from 133.8.9.60: icmp_seq=1. time=20. ms

Number transmitted=2 Number received=2 Percent loss=0
Total time=30 Minimum time=10 Maximum time=20 Average time=20
```

RESET DEVICE

Use the RESET DEVICE command to reset the DMM you are connected to. You must save or revert unsaved changes before this command executes.

Format

reset device

Example

The following command resets the DMM you are connected to:

```
CB5000> reset device
Resetting device...
Distributed Management Module (vx.xx)
Copyright(c) 199x 3Com Corporation.
```

After the reset completes, the login prompt is displayed as follows:

```
Login: {enter login name}
Password: {enter password}
```

Related Commands

RESET MODULE
REVERT
SAVE

RESET HUB

Use the RESET HUB command to perform a hub reset.

Use this command only if a hub is not functioning properly. The hub is reset to its most recent saved configuration.

You must SAVE or REVERT any unsaved changes before you execute this command.

Format

reset hub

Example The following command resets all hardware and software in the hub:

```
CB5000> reset hub
Resetting hub.
```

Related Commands

RESET DEVICE
RESET MODULE
REVERT
SAVE

RESET MASTERSHIP

Use the RESET MASTERSHIP command to force an election to take place between all management modules in the hub. The result of this command is to elect a new master management module, based on the mastership priority setting. The DMM-elected master provides all command and control capabilities in the hub. The controller places all other DMMs in the hub in standby mode. CoreBuilder 5000 DMMs always take precedence over ONline™ management modules.

This command causes a master management module election in the hub in which it is installed. The management module with the highest mastership priority setting becomes master. You set a DMM's mastership priority using the SET MODULE MASTERSHIP_PRIORITY command. A DMM always assumes mastership over an ONline management module installed in a CoreBuilder 5000 hub.

You can only enter this command from a Master DMM and you must SAVE or REVERT any changes before you execute this command.

CAUTION: *Do not enter this command from a Telnet session. Slave DMMs do not have network connectivity. Resetting mastership from a Telnet session may cause you to lose the session without being able to reconnect.*

The time it takes to complete an election depends on a management module's mastership priority setting. A DMM with a mastership priority value of 10 completes a mastership election fastest. A DMM with a mastership of 1, however, takes about 90 seconds to complete a mastership election. Set the master DMM to 10 and the slave DMMs to mastership priority values of 7, 8, or 9 to facilitate the election process.

Format

reset mastership

Example The following command causes the DMM to initiate a mastership election:

```
CB5000> reset mastership
Resigning
```

Related Commands RESET HUB
SET MODULE MASTERSHIP_PRIORITY

RESET MODULE

Use the RESET MODULE command to perform a hardware reset of a module in the hub. Use this command only if a module is not functioning properly. If used for the main (.1) subslot, the command resets each submodule in the slot. The DMM resets the module in the specified slot to its last-saved configuration.

When you enter this command for the main board in a slot (.1):

1. The system prompts you to confirm that you want to reset all modules in the slot.
2. Press y to execute the reset.

You cannot reset either the DMM to which you are logged in or the Active Controller Module using this command. To reset the DMM, use the RESET DEVICE command. To reset the Active Controller Module, use the RESET HUB command. The RESET HUB command resets all modules, including the Controller Module.

Format

reset module ——— *slot.subslot*

slot	Indicates the slot to reset: 1 through 19.
subslot	Indicates the subslot to reset: 1 through 7.

Example

The following command resets the main board, and any boards in subslots, on the module in slot 6:

```
CB5000> reset module 6.1
Resetting this module will reset all of the modules in this slot.
Do you wish to continue ? (y/n) : y
Resetting module 6.1.
```

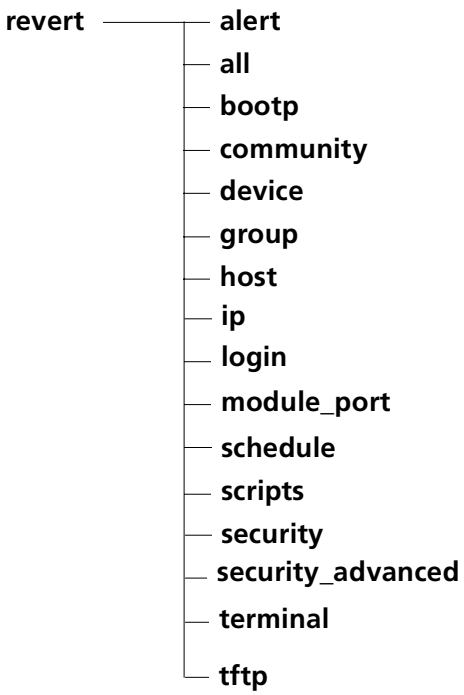
Related Commands

RESET HUB
SHOW MODULE ALL

REVERT

Use the REVERT command to return to the configuration settings that were in effect as of the last save. You can revert all settings or just the settings of a functionally related group of parameters. For example, if you enter the REVERT ALERT command, any SET ALERT changes you made (after the last SAVE) are abandoned. In addition, REVERT ALERT only affects the ALERT option (all other parameter groups are unchanged).

Format



Example 1 The following command reverts the DMM's terminal configuration:

```
CB5000> revert terminal
Reverting terminal parameters.
```

Example 2 The following command reverts all settings to the most recently saved DMM terminal configuration:

```
CB5000> revert all
Reverting all parameters.ed
```

Related Command SAVE

RUN SCRIPT

Use the RUN SCRIPT command to run a specified script file.

Format

run script ——— *index*

index	Identifies the script to be run. Use the SHOW SCRIPT command for a numbered list of scripts. The options are 1 through 8.

Example

The following command runs script 1:

```
CB5000> run script 1
```

[command output for script 1 is displayed]

Related Commands

SET SCRIPT
SHOW SCHEDULE

SAVE

Use the SAVE command to save the current configuration values established by the SET command.

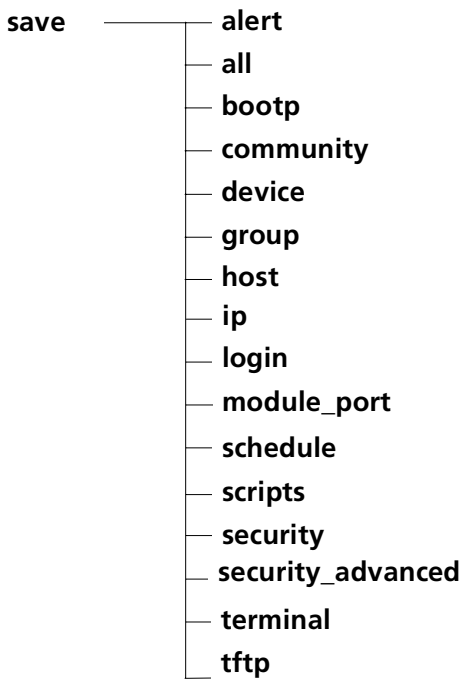
Parameter values established by the SET command are effective immediately but are not saved in non-volatile memory. Use the SAVE command to save these values in non-volatile memory. When the hub is reset, due to user command or power cycling, the hub reinitializes using the values in non-volatile memory.

The SAVE ALL command saves all of the configuration values made using the SET command.

You can save all settings or just the settings of a functionally related group of parameters. Entering a SAVE command with a specific option saves only the portion of the configuration that applies to the option. For example, SAVE TFTP saves only TFTP parameters.

When the SAVE command is executed on the master DMM in a hub that also has slave DMMs, the saved settings are also saved on the slave DMM. Do not execute any RESET DEVICE, HUB, or MASTERSHIP commands, or power down any management modules or the hub itself for at least 2 minutes after you enter the SAVE command. Also, if a SAVE command is executed on a slave DMM, the settings that are saved are only saved locally on the slave. If a subsequent save is issued on the master, the slave acquires those settings. If a SAVE command is executed on a slave, and it becomes master before any SAVE commands are executed on the current master, it then teaches its settings to the now slave DMMs.

Format



Example 1 The following command saves the DMM's current configuration settings:

```
CB5000> save all
Saving all parameters.
```

Example 2 The following command saves the current module and port configuration settings:

```
CB5000> save module_port
Saving module and port parameters.
```

Related Command REVERT

SET

Use the SET command to change configuration values. Parameter values established by the SET command are effective immediately but are not permanently saved. The SET command parameters have options of their own. The following pages describe these options in detail.

Format

set —— *command heading*

command heading	Chooses the parameter to set: alert atm bootp bport_lec bport_mau bridge_port clock community device group host inventory ip login module network port power protocols rmon schedule script security security_advanced sonet terminal tftp tr_surrogate trunk vbridge

Related Command

SHOW

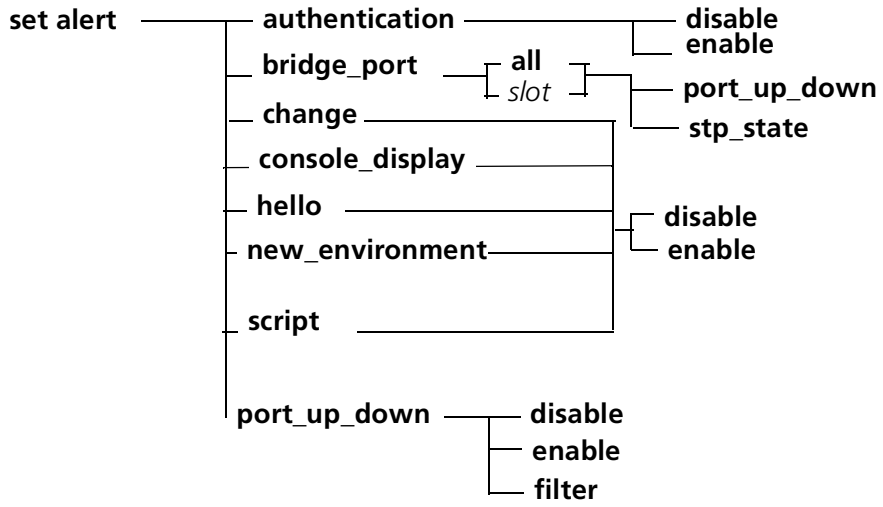
SET ALERT

Use the SET ALERT command to configure a DMM action when certain events (see parameter descriptions below) occur. DMM actions include:

- Sending alerts (traps) to a designated trap receiver (for example, a 3Com CoreBuilder 5000 SwitchModule)
- Displaying alert messages on the screen of a locally connected terminal

You must configure the trap receiver through the community table (SET COMMUNITY command) so the DMM knows where to send traps.

Format



authentication	Enables or disables authentication traps. The DMM issues an authentication trap when an SNMP manager tries to read from or write to the management hub and the user's community name is not valid for the attempted operation. The factory setting is authentication traps enabled.
bridge_port	Enables or disables bridge port port up and down and STP state aerts. The DMM issues a port_up_down trap for a bridge port if the bridge port starts or stops operating. This is independent of repeater port_up_down alerts. The DMM also issues an stp_state alert when the spanning tree instance for a bridge port has a topology change.
change	Enables or disables change traps. The DMM issues a change trap when a change to the management hub's configuration occurs. The factory setting is change traps enabled.
console_display	Enables or disables trap displays on the local terminal. The factory setting is console_display enabled. Hub up and hub down traps *are* displayed on the screen even if console_display is disabled.

hello	Enables or disables hello traps. The DMM issues a hello trap when the DMM is reset, and then once every minute until it receives a valid SNMP message. If the DMM has not received a valid SNMP message after 4 hours and 15 minutes, it stops sending hello traps. The factory setting is hello traps enabled.
new_environment	Enables or disables new formatting of environmental alerts. The DMM issues an environmental alert when there is a status change in fans, power supplies, hub temperature, voltage levels, or power reserve.
script	Displays a message on the locally connected terminal (screen) when the DMM executes a script. The DMM never transmits a script alert message. The factory setting is script messages disabled.
port_up_down	Enables, disables, or filters port_up_down traps. The DMM sends a port_up_down trap whenever a port on the stack starts operating (goes up) or stops operating (goes down). The table that follows shows how you can configure the port_up_down trap. The factory setting is port_up_down traps disabled.
disable	Disables the specified trap.
enable	Enables the specified trap.
filter	Applies to port_up_down traps only. Refer to the following table.

Port_Up_Down Setting	Result
enable	The DMM generates port up and port down alerts for all ports in the hub.
disable	The DMM generates no port up and port down alerts.
filter	The DMM generates port up and port down alerts according to the alert setting for each port. Use the SET PORT ALERT command to configure port up and port down alerts for specific ports.

Example 1 The following command disables the DMM from sending traps when it executes a script:

```
CB5000> set alert script disable
Alert SCRIPT set to DISABLE.
```

Example 2 The following command enables the DMM to send a trap whenever a user makes a configuration change to the DMM:

```
CB5000> set alert change enable
Alert CHANGE set to ENABLE.
```

Example 3 The following command disables the DMM from displaying trap messages on the terminal connected to the DMM:

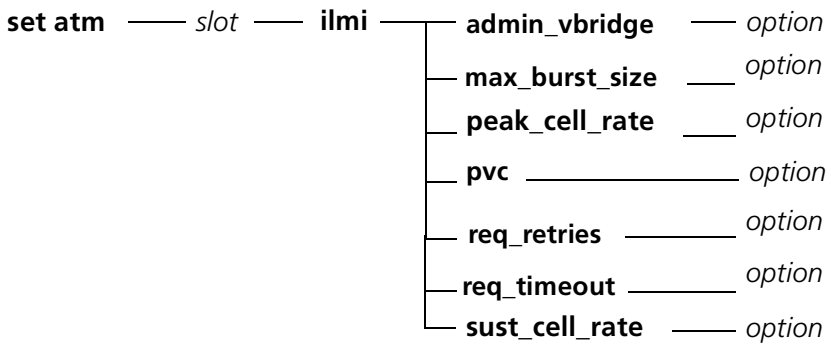
```
CB5000> set alert console_display disable
Alert CONSOLE_DISPLAY set to DISABLE.
```

Related Commands SET PORT ALERT
SHOW ALERT

SET ATM ILMI

Use the SET ATM ILMI command to configure the Interim Local Management Interface (ILMI) ATM attributes associated with the module.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
admin_vbridge	Specifies the vbridge to be used for administrative purposes.
option	Choose from a range of 1 through 240.
max_burst_size	Specifies the maximum burst size (in cells) for ILMI operations.
option	Choose from a range of 1 through 100. The default value is 11.
peak_cell_rate	Specifies the peak cell rate as a percentage of line rate for ILMI operations.
option	Choose from a range of 1 through 100. The default value is 5.
pvc	Specifies (in vpi/vci format) the PVC Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) to be used for ILMI operations.
option	The format for this option is value/value. The default value is 0/16.
req_retries	Specifies the number of retries associated with ILMI operations.
option	Choose from a range of 0 through 4. The default value is 2.
req_timeout	Specifies the timeout in seconds for ILMI operations.
option	Choose from a range of 5 through 60. The default value is 5.
sust_cell_rate	Specifies the sustained cell rate as a percentage of line rate for ILMI operations.
option	Choose from a range of 1 through 100. The default value is 1.

Example

The following command sets the ILMI maximum burst size at 20 cells for the module in slot 4:

```
CB5000> set atm 4 ilmi max_burst_size 20
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

Related Command

SHOW ATM ILMI CONFIGURATION

SET ATM LEARP_QUIET_TIME

Use the SET ATM LEARP_QUIET_TIME command to specify the LAN Emulation Address Resolution Protocol (LE-ARP) quiet time.

The LE-ARP quiet time is the period of time that the LAN Emulation Client (LEC), after failing to resolve a Media Access Control/Asynchronous Terminal Mode (MAC/ATM) address binding using LE-ARP, refrains from issuing further LE-ARP requests for the MAC address. Choose a value of 0 to disable this mode of operation.

Format

set atm — *slot* — **learp_quiet_time** — *option*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
option	Choose from a range of 0 through 60. The default value is 5.

Example

The following command sets the learp_quiet time to 20 seconds for the module in slot 4:

```
CB5000> set atm 4 learp_quiet_time 20
Slot 04 parameter set.
```

Related Command

SHOW ATM INTERFACE

SET ATM NEIGHBOR IF_NAME

Use the SET ATM NEIGHBOR IF_NAME command to specify the value of the ifName for the peer ATM device's ATM-layer interface.

Normally, this value is provided automatically by the peer through the Interim Local Management Interface (ILMI). However, if the peer's ILMI does not provide this value, you can use this command to configure the value for network management purposes.

The peer interface's ifName is advertised in the ATM Backbone SwitchModule's RFC1695 ATM MIB.

Format

set atm — *slot* — **neighbor** — **if_name** — *option*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
option	Use up to 63 characters for the ifName.

Example

The following command sets the neighbor if_name for the peer ATM device in slot 4 to Test:

```
CB5000> set atm 4 neighbor if_name Test
Slot 04 parameter set.
```

Related Command

SHOW ATM INTERFACE

SET ATM NEIGHBOR IP_ADDRESS

Use the SET ATM NEIGHBOR IP_ADDRESS command to specify an IP address for the peer ATM device to which SNMP requests on UDP port 161 may be directed.

Normally, this value is provided automatically by the peer through the Interim Local Management Interface (ILMI). However, if the peer's ILMI does not provide this value, you can use this command to configure the value for network management purposes.

The peer IP address is advertised in the ATM Backbone SwitchModule's RFC1695 ATM MIB.

The ATM NEIGHBOR IP address is four decimal numbers separated by periods. Each number can range from 0 to 255. However, the following addresses are illegal:

- 0.0.0.0
- 255.255.255.255

Format

set atm — *slot* — **neighbor** — **ip_address** — *option*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
option	Use 4 decimal numbers separated by periods for the IP address.

Example

The following command sets the neighbor ip_address for the peer ATM device in slot 4 to 02.04.80.20:

```
CB5000> set atm 4 neighbor ip_address 02.04.80.20
Slot 04 parameter set.
```

Related Command

SHOW ATM INTERFACE

SET ATM NUM_LECS

Use the SET ATM NUM_LECS command to specify the number of LAN Emulation Clients (LECs) you expect to support on this module. The system uses the value you select for resource allocation sizing during initialization. The value you select takes effect after module reset.

Format

set atm — *slot* — **num_lecs** — *option*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
option	Choose from a range of 1 through 64.

Example

The following command sets the num_lecs in slot 4 to 20:

```
CB5000> set atm 4 num_lecs 20
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

Related Command

SHOW ATM INTERFACE

SET ATM NUM_VCCS

Use the SET ATM NUM_VCCS command to specify the number of virtual circuits you expect to support on this module. The system uses the value you select for resource allocation sizing during initialization.

VCCS is an abbreviation for Virtual Channel Connections.

Format

set atm — *slot* — **num_vccs** — *option*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
option	Choose from a range of 128 through 512.

Example The following command configures the num_vccs in slot 4 to 128:

```
CB5000> set atm 4 num_vccs 128
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

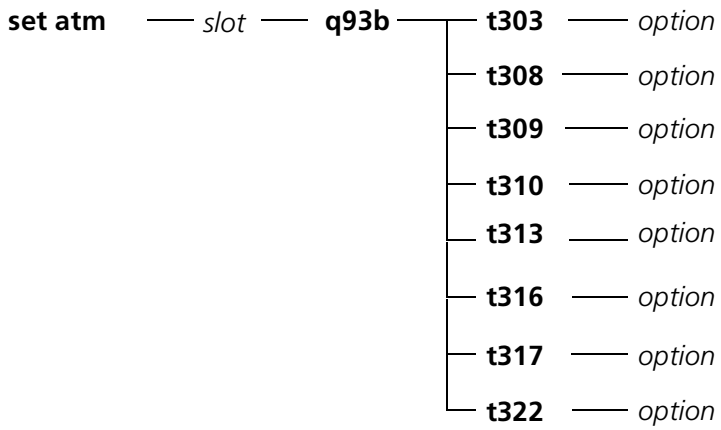
Related Command SHOW ATM INTERFACE

SET ATM Q93B

Use the SET ATM Q93B command to specify the values of Q93B timers.

CAUTION: *Do not change the default settings for this command. Any changes you make may cause interoperability problems with other ATM equipment.*

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
t303	Specifies (in seconds) the t303 value.
option	Choose from a range of 1 through 300. The default value for User Network Interface (UNI) version t3.0/3.1 is 4/4.
t308	Specifies (in seconds) the t308 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 30/30.
t309	Specifies (in seconds) the t309 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 90/10.
t310	Specifies (in seconds) the t310 value.
option	Version 3.0/3.1 is 10/10.
t313	Specifies (in seconds) the t313 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 4/4.
t316	Specifies (in seconds) the t316 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 120/120.
t317	Specifies (in seconds) the t317 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 60/60.
t322	Specifies (in seconds) the t322 value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 4/4.

Example The following command sets the ATM Q93b timer to 2 seconds:

```
CB5000> set atm 4 q93b t303 2
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

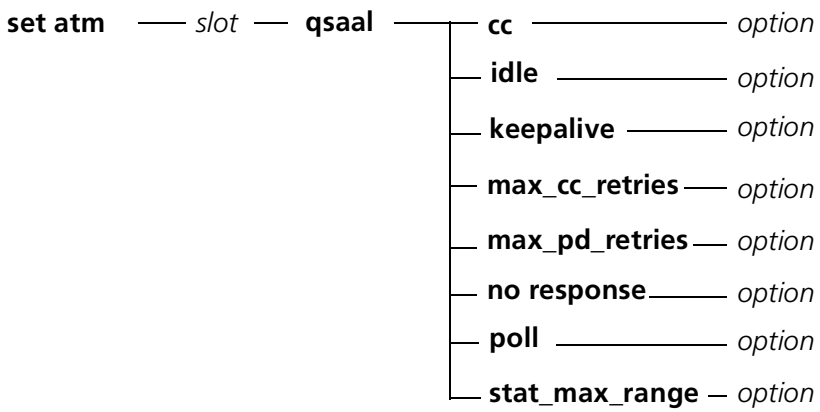
Related Command SHOW ATM Q93B

SET ATM QSAAL

Use the SET ATM QSAAL command to specify the values of QSAAL parameters.

3Com recommends that you do not change the default settings for this command. Any changes may cause interoperability problems with other ATM equipment.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
cc	Specifies (in seconds) the cc value.
option	Choose from a range of 1 through 300. The default value for User Network Interface (UNI) Version 3.0/3.1 is 2/1.
idle	Specifies (in seconds) the idle value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 15/15.
keepalive	Specifies (in seconds) the keepalive value.
option	Choose from a range of 1 through 300. The default value for UNI version 3.0/3.1 is 1/2.
max_cc_retries	Specifies (in seconds) the max_cc_retries value. Range is 1 through 4.
option	Choose from a range of 1 through 4. The default value is 4.
max_pd_retries	Specifies (in seconds) the max_pd_retries value. Range is 1 through 25.
option	Choose from a range of 1 through 25. The default value is 25.
no_response	Specifies (in seconds) the no_response value.
option	Choose from a range of 1 through 300. The default value for UNI Version 3.0/3.1 is 10/7.
poll	Specifies (in milliseconds) the poll value.
option	Choose from a range of 100 through 10000. The default value for UNI Version 3.0/3.1 is 100/750.
stat_max_ranges	Specifies (in seconds) the stat_max_ranges value. Range is 1 through 67.
option	Choose from a range of 1 through 67. The default value is 67.

Refer to the ATM Backbone SwitchModule User Guide *for definitions of parameters and additional information.*

Example The following command sets the ATM QSAAL idle value to 2:

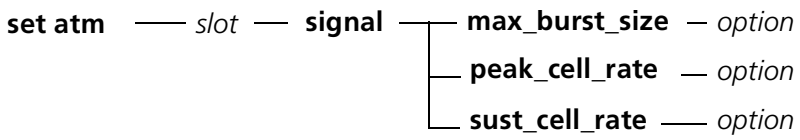
```
CB5000> set atm 4 qsaal idle 20
Slot 04 parameter set. Setting saved.
Warning: Change does not become operational until module is reset.
```

Related Command SHOW ATM QSAAL

SET ATM SIGNAL

Use the SET ATM SIGNAL command to specify parameters for the signalling Virtual Channel Connection (VCC). The parameters you set take effect at the next module reset.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
max_burst_size	Specifies the maximum burst size (in cells).
option	Choose from a range of 1 through 100. The default value is 7.
peak_cell_rate	Specifies the peak cell rate as a percentage of line rate.
option	Choose from a range of 1 through 100. The default value is 5.
sust_cell_rate	Specifies the sustained cell rate as a percentage of line rate.
option	Choose from a range of 1 through 100. The default value is 1.

Example

The following command sets the maximum ATM signal burst size in cells to 9:

```
CB5000> set atm 4 signal max_burst_size 9
Slot 04 parameter set.
```

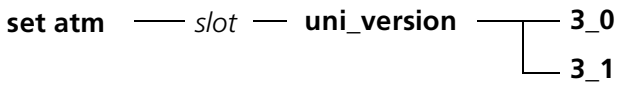
Related Command

SET ATM ILMI

SET ATM UNI_VERSION

Use the SET ATM UNI_VERSION command to specify the User Network Interface (UNI) version you want to use. The default setting is 3_1. The version you specify takes effect at the next module reset.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
3_0	Specifies UNI Version 3.0.
3_1	Specifies UNI Version 3.1.

Example

The following command sets the ATM version to 3.0:

```
CB5000> set atm 4 uni_version 3.0
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

Related Command

SHOW ATM ILMI CONFIGRATION

SET ATM VPI_VCI_BITS

Use the SET ATM VPI_VCI_BITS command to specify the number of valid bits for the Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) field. The total number of VPI and VCI bits must not exceed 9.

Format

set atm — *slot* — **vpi_vci_bits** — *vpi/vci*

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
vpi/vci	Choose the number of valid bits for the Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) field. You can choose from one of the following ranges: ■ 0 through 9 ■ 1 through 8 ■ 2 through 7 ■ 3 through 6 The default value is 0 for VPI and 9 for VCI.

Example

The following command sets the ATM VPI bits to 3 and the VCI bits to 8:

```
CB5000> set atm 4 vpi_vci_bits 3/8
Slot 04 parameter set.
Warning: Change does not take effect until module is reset.
```

Related Command

SHOW ATM ILMI CONFIGURATION

SET BOOTP MODULE

Use the SET BOOTP MODULE command to specify an NMC (or A-ENMC interface) to use as the BootP interface. BootP (Bootstrap Protocol) is a UDP/IP-based protocol (User Datagram Protocol/Internet Protocol) that allows a device to configure itself dynamically without user intervention. This command applies to the DMM and the Advanced DMM/Controller modules.

Format

set bootp module —— *slot.subslot*

slot.subslot	*slot* is the slot number in the hub. *subslot* is the subslot on the module in the specified slot. For example, to identify subslot 4 of slot 6, enter **6.4**

Example

The following command specifies slot 5, subslot 1 as the BootP interface:

```
CB5000> set bootp module 5.1
```

Related Commands

CLEAR BOOTP
SET BOOTP POWER_UP_MODE
SET BOOTP SERVER_IP_ADDRESS
SHOW BOOTP

SET BOOTP POWER_UP_MODE

Use the SET BOOTP POWER_UP_MODE command to define whether or not the DMM issues a BootP request upon power-up.

Format

disable	Configures the DMM to not issue a BootP request upon power-up.
enable	Configures the DMM to issue a BootP request upon power-up.

Example

The following command causes the DMM to issue a BootP request each time it powers up:

```
CB5000> set bootp power_up_mode enable
BootP power_up_mode set to ENABLED.
```

Related Commands

CLEAR BOOTP
SET BOOTP SERVER_IP_ADDRESS
SHOW BOOTP

SET BOOTP SERVER_IP_ADDRESS

Use the SET BOOTP SERVER_IP_ADDRESS command to define the BootP server IP address to which the DMM sends BootP requests. If you do not specify an IP address, the DMM sends the request to the broadcast address.

Format

set bootp server_ip_address —— *ip address*

ip address	IP address of the BootP server. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4. The factory setting is 255.255.255.255, which is a broadcast address.

Example

The following command specifies that the DMM send BootP requests to IP address 127.3.6.58:

```
CB5000> set bootp server_ip_address 127.3.6.58
BootP IP address set to 127.3.6.58.
```

Related Commands

CLEAR BOOTP
SET BOOTP POWER_UP_MODE
SHOW BOOTP

SET BPORT_LEC BUS_RATE_LIMIT

Use the SET BPORT_LEC BUS_RATE_LIMIT command to set the BUS rate from the DMM. BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec — *slot.lec* — **bus_rate_limit** — *option*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
option	Specifies the BUS rate limit in packets/seconds. Values range from 0 through 65535. Default value is 5000 packets/sec. A value of 0 (zero) means no limit.

Example The following command sets the LEC in slot 4, port 1 to a BUS rate limit of 5000:

```
CB5000> set bport_lec 4.1 bus_rate_limit 5000
Bridge Port 04.01 bud rate limit parameter set.
```

Related Command SHOW BPORT_LEC CONFIGURATION

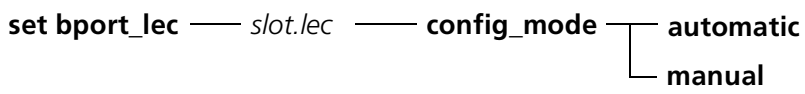
SET BPORT_LEC CONFIG_MODE

Use the SET BPORT_LEC CONFIG_MODE command to specify how the LAN Emulation Client (LEC) port acquires its LAN emulation configuration parameters – automatically or manually.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
automatic	Specifies that the LEC attempts to acquire its LAN emulation configuration parameters from a LAN Emulation Configuration Server (LECS).
manual	Specifies that the LEC's LAN emulation parameters are configured locally.

Example

The following command sets the LEC in slot 4, port 1 to automatically configure from a LECS:

```
CB5000> set bport_lec 4.1 config_mode automatic
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

SET BPORT_LEC ELAN_NAME

Use the SET BPORT_LEC ELAN_NAME command to supply the name of the emulated LAN (ELAN) associated with the LAN Emulation Client (LEC).

The value of the ELAN name may or may not be taken into account by the LAN Emulation Configuration Server (LECS) and LAN Emulation Server (LES)*, depending on the policy configured on those servers.*

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec — *slot.lec* — **elan_name** — *name*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
name	Specifies the name (up to 63 characters) of the LAN associated with the LEC.

Example

The following command sets the elan_name of the LEC in slot 4, port 1 to Main_lec:

```
CB5000> set bport_lec 4.1 elan_name
Enter bport_lec 4.1 elan_name:
Main_LEC
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

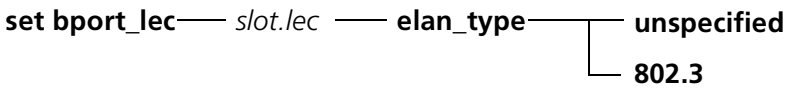
SET BPORT_LEC ELAN_TYPE

Use the SET BPORT_LEC ELAN_TYPE command to specify the emulated LAN (ELAN) type associated with the LAN Emulation Client (LEC).

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
unspecified	Allows the LEC to determine the type of emulated LAN when the LEC attempts to join the emulated LAN.
802.3	The IEEE 802.3 LAN is the only supported emulated LAN type.

Example

The following command sets the LEC in slot 4, port 1 to type 802.3:

```
CB5000> set bport_lec 4.1 elan_type 802.3
Bridge Port 04.01 parameter set. Setting saved.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

SET BPORT_LEC FRAME

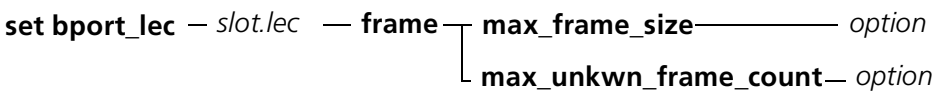
Use the SET BPORT_LEC FRAME command to specify two parameters for the emulated LAN:

- Maximum frame size
- Maximum unknown frame count

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
max_frame_size	Specifies the maximum frame size (in octets) for the emulated LAN.
option	You can choose from one of the following options: ■ 1516 ■ 4544 ■ unspecified Unspecified allows the LECs to determine the maximum frame size when the LEC tries to join the emulated LAN. You can create an FDDI-like LAN emulation by configuring the LAN type as IEEE 802.3 and then setting the maximum frame size to 4544.
max_unkwn_frame_count	Specifies the maximum number of frames sent by a LEC to the Broadcast and Unknown Server (BUS) for a given unicast LAN destination within a specified maximum unknown time period.
option	You can choose from a range of 1 through 10 frames.

Example

The following command sets the maximum frame size of the LEC in slot 4, port 1 to 1516:

```
CB5000> set bport_lec 4.1 frame max_frame_size 1516
Bridge Port 04.01 parameter set.
```

Related Commands

SHOW BPORT_LEC CONFIGURATION
SET BPORT_LEC TIME

SET BPORT_LEC LEC_DEFAULTS

Use the SET BPORT_LEC LEC_DEFAULTS command to restore the LAN Emulation attributes of a LAN Emulation Client (LEC) to the default values listed below.

This command is only effective when the LEC has been disabled by executing the SET BPORT_LEC MODE command.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec —— *slot.lec* —— **lec_defaults**

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
lec_defaults	The default settings for the LEC.

Attributes	Value
config_mode	automatic
elan_type	unspecified
max_frame_size	unspecified
elan_name	Zero-length string ("admin" for LEC 1)
les_atm_address	Zero-length ATM address
lecs_atm_address	Zero-length ATM address
num_elan_vccs	<max vccs on module>
control_timeout	120 sec
max_unknown_frame_count	1
max_unknown_frame_time	1 sec
vcc_timeout	1200 sec
max_retry_count	1
aging_time	300 sec
forward_delay_time	15 sec
expected_arp_resp_time	1 sec
flush_timeout	4 sec
path_switch_delay	6 sec
connect_complete_timer	4 sec

Example

The following command sets the default setting of the LEC in slot 4, port 1:

```
CB5000> set bport_lec 4.1 lec_defaults
Bridge Port 04.01 parameter set. Setting saved.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

SET BPORT_LEC LECS_ATM_ADDRESS

Use the SET BPORT_LEC LECS_ATM_ADDRESS command to specify the ATM address of the LAN Emulation Configuration Server (LECS) when configuration mode is set to automatic.

The ATM address is 20 hexadecimal numbers separated by periods. Each number can range from 0 to FF. However, the following addresses are illegal:

- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
- FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec —— *slot.lec* —— **lecs_atm_address** —— *ATM address*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
ATM address	Specifies the ATM address of the LAN Emulation Configuration Server (LECS).

Example

The following command sets the ATM address of the LECS in slot 4, port 1:

```
CB5000> set bport_lec 4.1 lecs_atm_address 39.99.99.99.ac.00.00.00.
00.99.99.01.02.03.04.05.06.07.08.00
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

SET BPORT_LEC LES_ATM_ADDRESS

Use the SET BPORT_LEC LES_ATM_ADDRESS command to specify the LAN Emulation Server (LES) ATM address when configuration mode is set to manual.

The ATM address is 20 hexadecimal numbers separated by periods. Each number can range from 0 to FF. However, the following addresses are illegal:

- 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
- FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec — *slot.lec* ——— **les_atm_address** —— *ATM address*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
ATM address	Specifies the ATM address of the LES.

Example

The following command sets the ATM address of the LES in slot 4, port 1:

```
CB5000> set bport_lec 4.1 les_atm_address 39.00.99.99.99.99.ac.
00.99.99.99.99.99.99.99.99.99.99.99.99.99
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

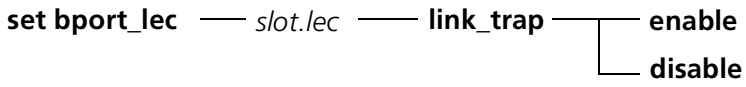
SET BPORT_LEC LINK_TRAP

Use the SET BPORT_LEC LINK_TRAP command to enable or disable link traps for a LAN Emulation Client (LEC) port.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
enable	Enables link traps for a LEC port.
disable	Disables link traps for a LEC port.

Example

The following command enables link traps for the LEC in slot 4, port 1:

```
CB5000> set bport_lec 4.1 link_trap enable
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC STATUS

SET BPORT_LEC MODE

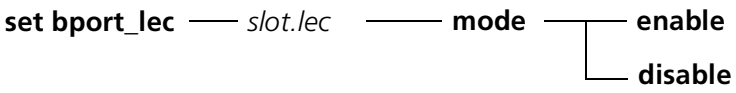
Use the SET BPORT_LEC MODE command to cause an idle LAN Emulation Client (LEC) to join the emulated LAN (ELAN) of which it is configured to be a member or to cause an active LEC to disconnect from its emulated LAN.

This command controls the ability of the LEC to operate on an emulated LAN.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
enable	Causes an idle LEC to attempt to join the emulated LAN of which it is configured to be a member.
disable	Causes an active LEC to disconnect from its emulated LAN.

Example

The following command enables an active LEC in PHY in slot 4, port 1 to disconnect from its emulated LAN:

```
CB5000> set bport_lec 4.1 mode enable
Bridge Port 04.01 parameter set.
```

Related Commands

SHOW BPORT_LEC CONFIGURATION
SET BRIDGE_PORT VBRIDGE

SET BPORT_LEC MAX_RETRY_COUNT

Use the SET BPORT_LEC MAX_RETRY_COUNT command to specify the maximum number of retries for a LAN Emulation Address Resolution Protocol (LE-ARP) request following the first failed attempt.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec — *slot.lec* —— **max_retry_count** —— *option*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
option	Specify 0 if you do not want the system to retry following the first failed LE-ARP request attempt. Specify 1 to set the system to retry one time following the first failed LE-ARP request attempt. Specify 2 to set the system to retry two times following the first failed LE-ARP request attempt.

Example

The following command sets the maximum number of LE-ARP request retry attempts for a LAN Emulation Client (LEC) in slot 4, port 1 to 2:

```
CB5000> set bport_lec 4.1 max_retry_count 2
Bridge Port 04.01 parameter set.
```

Related Command

SHOW BPORT_LEC CONFIGURATION

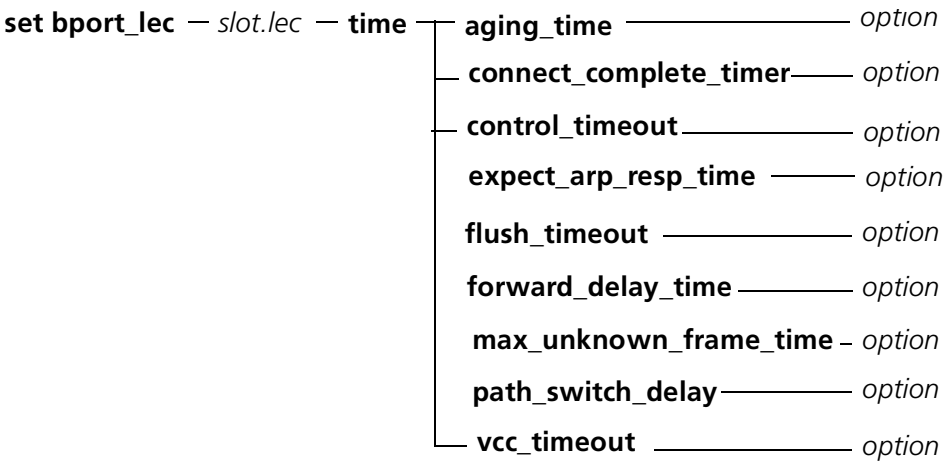
SET BPORT_LEC TIME

Use the SET BPORT_LEC TIME command to specify timeout options for LAN Emulation Client (LEC) ports.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
aging_time	Specifies the aging time (in seconds) for entries in the LAN Emulation Address Resolution Protocol (LE-ARP) cache.
option	Choose from a range of 10 through 300.
connect_complete_ timer	Specifies the time (in seconds) within which data or a READY_IND message is expected from the calling party.
option	Choose from a range of 1 through 10.
control_timeout	Specifies the time (in seconds) used for most LAN Emulation request/response control interactions.
option	Choose from a range of 10 through 300.
expect_arp_resp_ time	Specifies the maximum time (in seconds) that a LEC expects a LE-ARP response cycle to last.
option	Choose from a range of 1 through 30.
flush_timeout	Species the timeout (in seconds) for a flush response after a flush request has been sent.
option	Choose from a range of 1 through 4.
forward_delay_time	Specifies the aging time (in seconds) for entries in the LE-ARP cache when a LAN Emulation topology change is indicated.
option	Choose from a range of 4 through 30.

max_unknown_frame_time	Specifies the time (in seconds) in which a LEC will send no more than the maximum unknown frame count frames to the Broadcast and Unknown Server (BUS) for a given unicast LAN destination.
option	Choose from a range of 1 through 10.
path_switch_delay	Time (in seconds) since sending a frame to the BUS after which the LEC may assume the frame has been delivered or discarded. You can use this attribute to bypass the flush protocol.
option	Choose from a range of 1 through 8.
vcc_timeout	Timeout (in seconds) after which a Data Direct VCC should be released if it has not been used to transmit or receive data frames.
option	Choose from a range of 0 through 2147483647.

Example The following command sets the flush response timeout period for the LEC in slot 4, port 1 to 3 seconds:

```
CB5000> set bport_lec 4.1 time flush_timeout 3
Bridge Port 04.01 parameter set.
```

Related Command SHOW BPORT_LEC CONFIGURATION

SET BPORT_LEC NUM_ELAN_VCCS

Use the SET BPORT_LEC NUM_ELAN_VCCS command to specify the maximum number of virtual circuits available to the LAN Emulation Client (LEC).

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

set bport_lec — *slot.lec* — **num_elan_vccs** — *option*

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
option	Specifies the maximum number of virtual circuits available to the LEC. You can choose from 128 to Max VCCs. Where Max VCCs is equal to whatever is defined using the SET ATM NUM_VCCS command.

Example

The following command sets the maximum number of virtual circuits available to the LEC in slot 4, port 1 to 128:

```
CB5000> set bport_lec 4.1 num_elan_vccs 128
Bridge Port 04.01 parameter set.
```

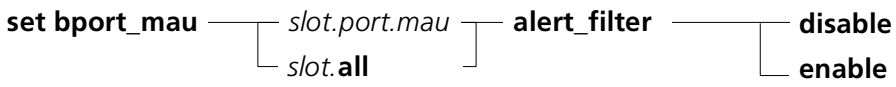
Related Commands

SHOW BPORT_LEC CONFIGURATION
SHOW ATM INTERFACE
SET ATM NUM_VCCS

SET BPORT_MAU ALERT_FILTER

Use the SET BPORT_MAU ALERT_FILTER command to configure bridge ports to generate or filter port up/down traps.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. The *mau* variable may be 1 (if no additional MAUs are configured) or 2 (for redundant ports). For example, to identify MAUs on port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all port MAUs in the *slot* are affected by this operation.
disable	Disables alert filtering and allows traps to be generated from the port MAU.
enable	Enables alert filtering that filters out traps from the port MAU.

Example

The following command enables filtering on port 3 mau 1 of the SwitchModule in slot 10:

```
CB5000> set bport_mau 3.10.1 alert_filter enable
Mau 03.10.1 Alert Filter set to ENABLED.
```

Related Command

SHOW BPORT_MAU

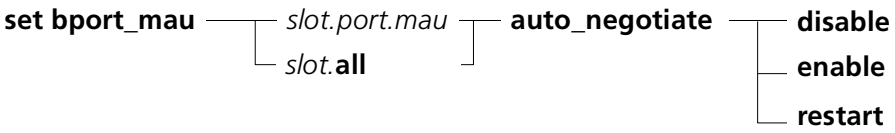
SET BPORT_MAU AUTO_NEGOTIATE

Use the SET BPORT_MAU AUTO_NEGOTIATE command to enable or disable autonegotiation on CoreBuilder 5000 100BASE-TX SwitchModules. By default, autonegotiation is enabled on 100BASE-TX SwitchModules.

The SwitchModule executes the autonegotiation process when you:

- Restart the hub or SwitchModule
- Plug a new connector into a SwitchModule port
- Restart autonegotiation using the SET BPORT_MAU AUTO_NEGOTIATE RESTART command

Format



slot.port.mau	Identifies the *port.mau* for this operation. *slot* is the slot number (1 through 17) and *port* (1 through 4) is the port number. The *mau* variable may be 1 (if no additional MAUs are configured) or 2 (for redundant ports). For example, to identify port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all *port.maus* in the *slot* are affected by this operation.
disable	Disables autonegotiation.
enable	Enables autonegotiation. Autonegotiation enables the port to: ■ Detect whether the device to which it is connected is in half-duplex or full-duplex mode. The SwitchModule port adjusts its duplex mode to match the other device. ■ Report an error through the SwitchModule LEDs if the SwitchModule port cannot connect to the other device.
restart	Executes the autonegotiation process on the SwitchModule.

Example

The following command enables autonegotiation on port mau 4 of the SwitchModule in slot 6, then executes the autonegotiation process:

```
CB5000> set bport_mau 6.4.1 auto_negotiate enable
CB5000> set bport_mau 6.4.1 auto_negotiate restart
```

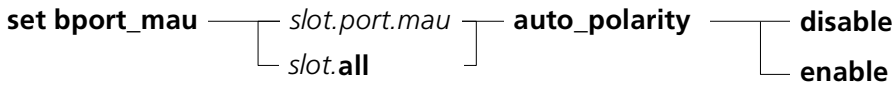
Related Command

SHOW BPORT_MAU

SET BPORT_MAU AUTO_POLARITY

Use the SET BPORT_MAU AUTO_POLARITY command to instruct CoreBuilder 5000 10BASE-T SwitchModules to automatically switch the polarity of twisted-pair cabling. By default, autopolarity is enabled on 10BASE-T SwitchModules.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. Use 1 for the *mau* variable. For example, to identify a MAU on port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all MAUs in the slot are affected by this operation.
disable	Disables autopolarity.
enable	Enables autopolarity. Autopolarity enables the MAU to automatically switch the polarity of twisted-pair cabling. If, for instance, you erroneously reverse the polarity of some twisted-pair cabling while assembling it, autopolarity enables you to automatically detect this problem and reverse the polarity.

Example

The following command disables autopolarity on mau 1 of port 1 on a CoreBuilder 5000 10BASE-T SwitchModule in slot 1:

```
CB5000> set bport_mau 1.1.1 auto_polarity disable
Port 01.01 Auto Polarity set to DISABLE.
```

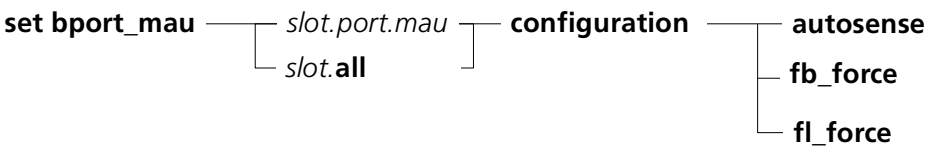
Related Command

SHOW BPORT_MAU

SET BPORT_MAU CONFIGURATION

Use the SET BPORT_MAU CONFIGURATION command to configure the protocol you want a 10BASE-FB/FL SwitchModule MAU to use. By default, 10BASE-FB/FL SwitchModule MAUs are set to autosense, which detects and adjusts to the protocol (either 10BASE-FB or 10BASE-FL) being used on the network.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 20) is the port number. Use 1 for the *mau* variable. For example, to identify port 4 on the module in slot 6, enter **6.4.1**
slot.**all**.*mau*	Specifies that all MAUs in the slot are affected by this operation.
fb_force	Forces the port to always use the 10BASE-FB protocol.
fl_force	Forces the port to always use the 10BASE-FL protocol.
autosense	Causes the port to detect the protocol in use on the link and adjust to match the protocol.

Example

The following command forces mau 1 of port 2 on a 10BASE-FB/FL SwitchModule in slot 6 to use the 10BASE-FB protocol:

```
CB5000> set bport_mau 6.2.1 configuration fb_force
```

Related Command

SHOW BPORT_MAU VERBOSE

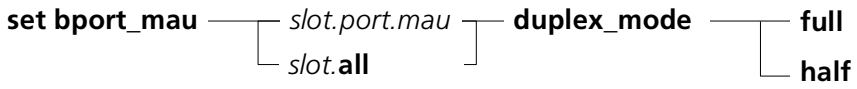
SET BPORT_MAU DUPLEX_MODE

Use the SET BPORT_MAU DUPLEX_MODE command to enable simultaneous two-way data flow on a 100BASE-FX SwitchModule MAU. By default, Fast Ethernet SwitchModule ports run in half-duplex mode.

Full-duplex mode disables Carrier Sense Multiple Access/Collision Detection (CSMA/CD), so enable full-duplex mode only when the SwitchModule MAU is connected to a single device (no collision domain exists).

When autonegotiation is enabled on a 100BASE-TX SwitchModule, 100BASE-TX SwitchModule MAUs are capable of changing to full-duplex mode automatically. If autonegotiation is disabled on a 100BASE-TX SwitchModule, you can use the SET BPORT_MAU DUPLEX_MODE command to manually set the 100BASE-TX MAU to full-duplex mode.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 4) is the port number. The *mau* variable may be 1 or 2 (for redundant ports). For example, to identify MAU 1 on port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all MAUs in the slot are affected by this operation.
full	Enables full-duplex mode on the MAU.
half	Enables half-duplex mode on the MAU.

Example

The following command enables full-duplex mode on mau 1 of port 4 on a 100BASE-FX SwitchModule in slot 2:

```
CB5000> set bport_mau 2.4.1 duplex_mode full
```

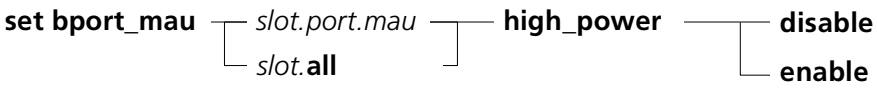
Related Command

SHOW BPORT_MAU

SET BPORT_MAU HIGH_POWER

Use the SET BPORT_MAU HIGH_POWER command to configure high or normal power transmission levels on a 10BASE-FB/FL SwitchModule MAU. By default, 10BASE-FB/FL SwitchModule MAUs transmit at the normal power setting.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* is the slot number and *port* (1 through 20) is the port number. Use 1 as the *mau* variable. For example, to identify MAU 1 on port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all MAUs in the slot are affected by this operation.
disable	Disables high power and enables normal power.
enable	Enables high power and disables normal power.

Example

The following command enables high power transmission on mau 1 of port 3 on a 10BASE-FB/FL SwitchModule in slot 5:

```
CB5000> set bport_mau 5.3.1 high_power enable
```

Related Command

SHOW BPORT_MAU

SET BPORT_MAU LINK_INTEGRITY

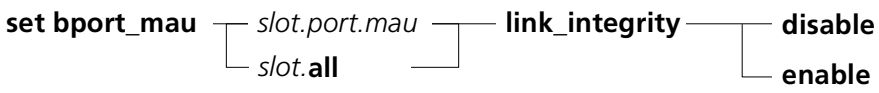
Use the SET BPORT_MAU LINK_INTEGRITY command to enable or disable link integrity for MAUs on 10BASE-T SwitchModules. By default, link integrity is enabled on 10BASE-T SwitchModule MAUs.

In general, enable link integrity for all MAUs on your 10BASE-T SwitchModule as stated in the 10BASE-T standard. You must disable link integrity to connect to older non-10BASE-T equipment.

Not all pre-10BASE-T equipment works with link integrity enabled.

You must enable or disable link integrity at both ends of the connection. If the settings at each end of the connection differ, the MAU with link integrity enabled reports a link integrity error.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. Use 1 as the *mau* variable. For example, to identify MAU 1 on port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all MAUs in the slot are affected by this operation.
disable	Disables link integrity.
enable	Enables link integrity.

Example

The following command disables link integrity on mau 1 on port 1 on the 10BASE-T module in slot 5:

```
CB5000> set bport_mau 5.1.1 link_integrity disable
Link integrity set to DISABLED.
```

Related Command

SHOW BPORT_MAU

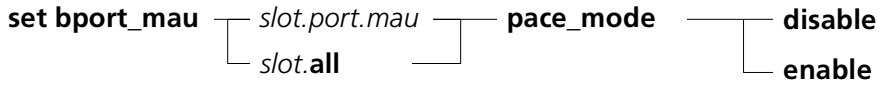
SET BPORT_MAU PACE_MODE

Use the SET BPORT_MAU PACE_MODE command to increase Ethernet transmission predictability. PACE® allows multimedia applications using voice and video traffic to transmit over standard Ethernet LANs with minimum jitter.

Enable PACE only on a connection between a SwitchModule MAU and a single end-station, switch, bridge, or router. Enable PACE when a SwitchModule MAU is connected to a repeater.

PACE_MODE is available only to the 10BASE-T SwitchModule and to ports 1 to 16 on the Ethernet Backplane SwitchModule.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. Use 1 as the *mau* variable. For example, to identify port 4 on the module in slot 6, enter **6.4.1**
*slot.***all**	Specifies that all MAUs in the slot are affected by this operation.
disable	Disables PACE. By default, PACE® is disabled.
enable	Enables PACE.

Example

The following command enables PACE on mau 1 of port 1 of the 10BASE-T module in slot 2:

```
CB5000> set bport_mau 2.1.1 pace_mode enable
MAU 02.01 PACE Mode set to ENABLED.
```

Related Command

SHOW BPORT_MAU

SET BPORT_MAU MODE

Use the SET BPORT_MAU MODE command to:

- Enable or disable a port MAU at the physical layer
- Create primary and secondary Fast Ethernet ports

This command is most useful on a SwitchModule port that is physically or logically configured to have more than one MAU. For example, use this command to disable one of the two FDDI port MAUs on a SwitchModule FDDI port.

When used on a port with only one MAU (such as a SwitchModule 10BASE-T port), the SET BPORT_MAU MODE command has the same functionality as the SET BRIDGE_PORT INTERFACE and SET BRIDGE_PORT STP BRIDGE_MODE commands (disables the port).

After a reset, backplane ports are disabled by default. The only exception to this default is if you save the enabled setting to NVRAM on the DMM by entering the SAVE command. In this case, after a module reset the backplane port is enabled.

To enable an Ethernet backplane port, enter the command SET BPORT_MAU <slot.bport.mau> MODE ENABLE or SET PORT <slot.port> MODE ENABLE. After the port is enabled, you can access the corresponding Ethernet backplane.

When used to create redundant links by configuring Fast Ethernet ports as primary and secondary; if the primary port goes down, the secondary port takes over and the link remains active.

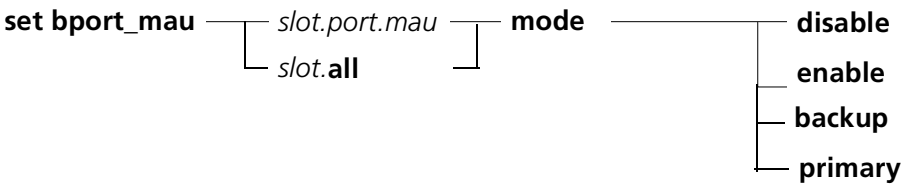
You configure redundant pairs as follows:

- Ports 1 and 2 are a redundant pair
- Ports 3 and 4 are a redundant pair

When you configure a redundant pair of ports, management programs view the two ports as one port with 2 MAUs. To configure redundant ports, use the SET BPORT_MAU MODE command. When you define one port as the primary port, the second port automatically becomes the backup port.

Variables PRIMARY and SECONDARY are available only to Fast Ethernet SwitchModules.

Format



slot.port.mau	Identifies the MAU for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. The *mau* variable may be 1 or 2 (for redundant ports). For example, to identify mau 1 of port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all MAUs in the slot are affected by this operation.
disable	Disables the port MAU.
enable	Enables the port MAU. This is the default setting when you install the module.

Example This command disables mau2 on port 4.1:

```
CB5000> set bport_mau 4.1.2 mode disable
Mau 04.01.02 Admin State set to DISABLED.
```

For the changes to take effect, you must save the configuration and reset the SwitchModule. When you reset the SwitchModule, it reconfigures as one logical bridge port (port 4.1) on which two MAUs exist.

To determine which portmau is primary or secondary, enter the SHOW BPORT_MAU VERBOSE command and examine the General Information field.

Related Command SHOW BPORT_MAU VERBOSE

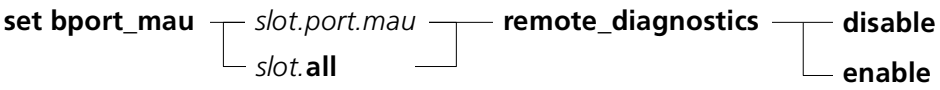
SET BPORT_MAU REMOTE_DIAGNOSTICS

Use the SET BPORT_MAU REMOTE_DIAGNOSTICS command to enable or disable remote diagnostics sensing on a 10BASE-FB/FL SwitchModule port MAUs operating in 10BASE-FL mode. Enable remote diagnostics when a 10BASE-FL SwitchModule port MAU is connected to a pair of 10BASE-FL ports configured for redundancy.

Remote diagnostics forces a SwitchModule 10BASE-FL port to stop transmitting if it stops receiving signalling from a remote primary port. When transmission ceases, the remote primary port detects that the link is down and switches to its redundant (backup) port, reenabling the fiber link.

By default, remote diagnostics is disabled.

Format



slot.port.mau	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 20) is the port number. Use 1 as the *mau* variable. For example, to identify port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
disable	Disables remote diagnostics.
enable	Enables remote diagnostics.

Example

The following command enables remote diagnostics on 10BASE-FL SwitchModule port 4 in slot 5:

```
CB5000> set bport_mau 5.4.1 remote_diagnostics enable
```

Related Command

SHOW BPORT_MAU VERBOSE

SET BPORT_MAU RESET_MODE

Use the SET BPORT_MAU RESET_MODE command to:

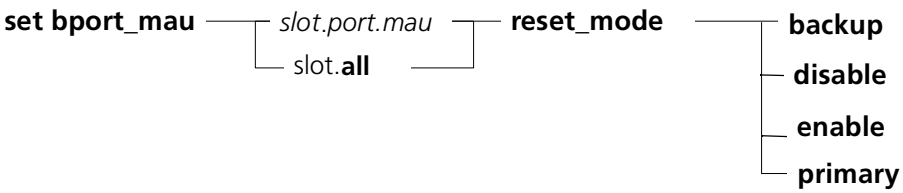
- Create redundant links by configuring SwitchModule ports as primary and backup.
- Disable redundancy mode on a port pair and return the ports to non-redundant mode or enable redundancy mode.

To determine whether a port is configured as part of a redundant pair, enter the SHOW BPORT_MAU command.

Options DISABLE and ENABLE are available only when a port is operating in redundant mode.

When you configure a redundant pair of ports, management applications view the two ports as one port with two MAUs.

Format



slot.port.mau	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. The *mau* variable may be 1 or 2 (for redundant ports). For example, to identify port 4 on the module in slot 6, enter **6.4.1**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
backup	If the primary port goes down; the backup port takes over and the link remains active.
disable	Disables redundancy mode on a port pair and returns the ports to non-redundant mode.
enable	Enables port redundancy mode.
primary	The active port of the pair of redundant ports.

Example

This command defines port 4.1 as the primary port. Port 4.2 automatically becomes the backup port.

```
CB5000> set bport_mau 4.1.1 reset_mode primary
Mau 04.01.01 set to PRIMARY.
```

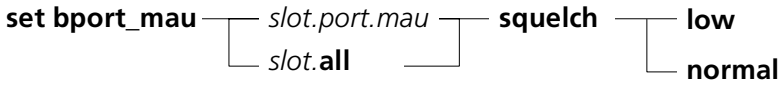
SET BPORT_MAU SQUELCH

Use the SET BPORT_MAU SQUELCH command to establish Squelch Mode as either normal or low for ports on 10BASE-T SwitchModules. By default, the squelch level is set to normal to conform to the 10BASE-T standard.

In general, 3Com recommends using normal squelch. Ensure the squelch level at both ends of the link matches. If you change the squelch level at the SwitchModule, you must change the squelch setting at the transceiver also.

If your network experiences too many illegally short packets (runts) in low squelch mode, change the setting back to normal.

Format



slot.port.mau	Selects a port for squelch mode setting. *slot* (1 through 17) is the slot ID and *port* (1 through 24) is the port number. Use 1 as the *mau* variable. For example, to specify port 4 on the slot with slot ID 6, enter **6.4**
slot.**all**	Selects a slot for squelch mode setting. For example, to specify all ports on the slot with slot ID 6, enter **6.all**
low	Sets squelch mode to low (sensitive). Ports are able to receive weaker signals, allowing longer link distances. Increases the achievable link distance, but with the added risk of losing packets to impulse noise.
normal	Sets squelch mode to normal. Ports receive signals compliant with the 10BASE-T standard.

Example

The following command sets port 1 in slot 5 to a low squelch level:

```
CB5000> set bport_mau 5.1.1 squelch low
Squelch set to LOW.
```

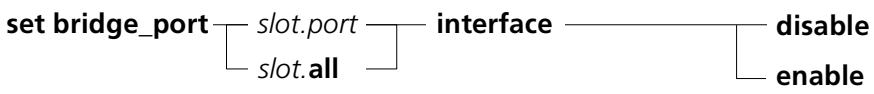
Related Command

SHOW BPORT_MAU VERBOSE

SET BRIDGE_PORT INTERFACE

Use the SET BRIDGE_PORT INTERFACE command to enable or disable interface functions on SwitchModule bridge ports.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
disable	Disables interface functions but leaves the physical interface enabled.
enable	Enables interface functions.

Example

The following command disables port 6 on the SwitchModule in slot 4:

```
CB5000> set bridge_port 4.6 interface disable
```

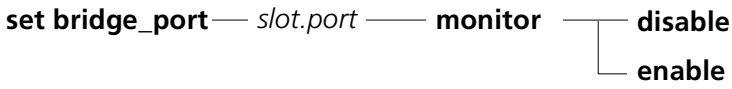
Related Commands

SET BPORT_MAU MODE
SET BRIDGE_PORT STP BRIDGE_MODE
SHOW BRIDGE_PORT

SET BRIDGE_PORT MONITOR

Use the SET BRIDGE_PORT MONITOR command to configure a SwitchModule port as a source port in a roving port analysis configuration. When you enter the SET BRIDGE_PORT MONITOR command, the port you specify begins to mirror traffic to the monitor sink port or backplane you have previously specified.

Format



slot.port	Iden*tifies the port for this operation.* *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4** You can enable traffic monitoring on the following types of ports: ■ 10 Mbps Ethernet SwitchModule ports. ■ 100 Mbps Ethernet SwitchModule ports when traffic is mirrored to a local 100 Mbps Ethernet monitor or system sink.
disable	Disables the port from mirroring traffic to the monitor or system sink.
enable	Enables the port to begin mirroring traffic to the monitor or system sink.

Example

The following command enables port 3 on the SwitchModule in slot 2 to mirror traffic to a monitor or system sink:

```
CB5000> set bridge_port 2.3 monitor enable
```

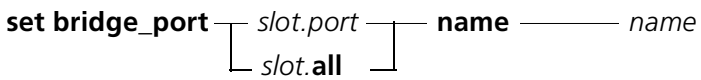
Related Commands

SET MODULE MONITOR_SINK
SET MODULE SYSTEM_SINK
SHOW MODULE

SET BRIDGE_PORT NAME

Use the SET BRIDGE_PORT NAME command to assign a name to a SwitchModule bridge port.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Specifies that all ports in the slot are affected by this operation.
name	The name (up to 32 characters) you want to identify this port.

Example

The following command assigns the name finance_1 to port 3 on the SwitchModule in slot 5:

```
CB5000> set bridge_port 5.3 name finance_1
```

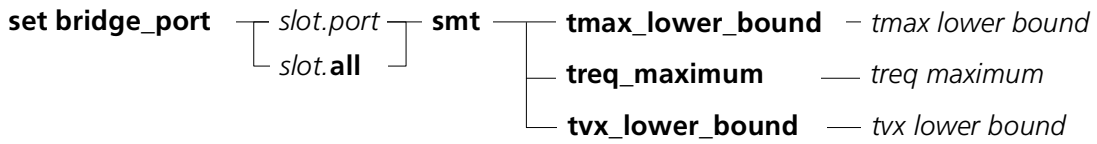
Related Command

SHOW BRIDGE_PORT

SET BRIDGE_PORT SMT

Use the SET BRIDGE_PORT SMT command to configure FDDI SwitchModule port values. These values affect the FDDI ring Target Token Rotation Time (TTRT). Refer to the *CoreBuilder 5000 SwitchModule User Guide* for more information about SwitchModule FDDI port values.

Format



slot.port	Identifies the port for this operation. The maximum port numbers are: ■ 4 for FDDI SwitchModule (3C96604M-F) ■ 14 for 10BASE-T and FDDI SwitchModule (3C96614M-FTP) ■ 12 for 10BASE-FB/FL and FDDI SwitchModule (3C96612M-FF) *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
tmax lower bound	Value from 10.4860 through 1342.1777. The default value is 167.77216. This value that determines the boundaries for the Treq.
treq maximum	Value from 0 through 1342.1777. The default value is 165.00736. This is the value that each FDDI station issues for the TTRT election process.
tvx lower bound	Value from 0.02048 through 5.24288. The default value is 2.519040. This value that resets to 0 when the beginning of a frame is detected.

Example

The following command sets the treq_maximum value to 1000 for SwitchModule FDDI port 1 in slot 6:

```
CB5000> set bridge_port 6.1 smt treq_maximum 1000
```

Related Command

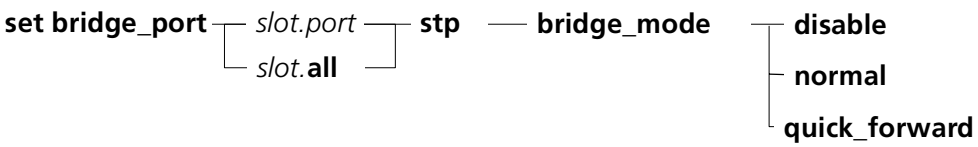
SHOW BRIDGE_PORT

SET BRIDGE_PORT STP BRIDGE_MODE

Use the SET BRIDGE_PORT STP BRIDGE_MODE command to disable the Spanning Tree Protocol on a SwitchModule port. Disable Spanning Tree only when no physical loops exist, such as when a port is directly connected to an end station.

To determine the current status of Spanning Tree on a port, enter the SHOW BRIDGE_PORT VERBOSE command and examine the Bridge Port Mode field.

Format



slot.port	Identifies the port for this operation. slot (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Specifies that all ports in the slot are affected by this operation.
disable	Disables the Spanning Tree Protocol on a SwitchModule port.
normal	Enables the Spanning Tree Protocol on a SwitchModule port. By default, Spanning Tree is enabled on SwitchModule ports.
quick_forward	Quick forwarding causes a port to skip the Listening and Learning states and go directly to the Forwarding state. A port in quick forward mode still receives and transmits BPDUs and can, if necessary, enter the blocking state to prevent loops.

Example 1

The following command disables Spanning Tree on port 4 of the SwitchModule in slot 14:

```
CB5000> set bridge_port 14.4 stp bridge_mode disable
```

Example 2

The following command configures quick forward mode on a port.

```
CB5000> set bridge_port 6.5 stp bridge_mode quick_forward
Bridge Port 06.05 Bridge Mode set to QUICK_FORWARD. Setting saved.
```

This command causes port 6.5 to go directly to the forwarding stage.

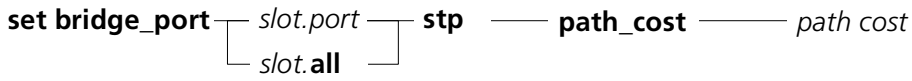
Related Commands

SET VBRIDGE STP MODE
SHOW BRIDGE_PORT

SET BRIDGE_PORT STP PATH_COST

Use the SET BRIDGE_PORT STP PATH_COST command to configure a Spanning Tree Protocol path cost parameter for a SwitchModule bridge port. For more information about Spanning Tree, refer to the *CoreBuilder 5000 SwitchModule User Guide*.

Format



slot.port	Identifies the port for this operation. slot (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
path cost	Value from 1 through 65535. The default value is 1000 divided by the speed of the link. For example, 1000 divided by FDDI link speed (100 Mbps) equals a path cost value of 10.

Example

The following command assigns a path cost value of 65000 to port 12 on the SwitchModule in slot 3:

```
CB5000> set bridge_port 3.12 stp path_cost 65000
```

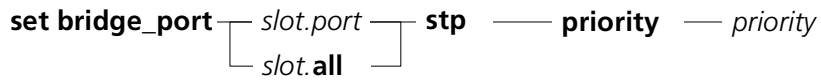
Related Commands

SET BRIDGE_PORT STP PRIORITY
SHOW BRIDGE_PORT

SET BRIDGE_PORT STP PRIORITY

Use the SET BRIDGE_PORT STP PRIORITY command to assign a Spanning Tree Protocol priority value to a SwitchModule bridge port. For more information about Spanning Tree, refer to the *CoreBuilder 5000 SwitchModule User Guide*.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port (*1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
priority	Value is an even number from 0 through 254. The default value is 128.

Example

The following command assigns a priority value of 200 to port 10 on the SwitchModule in slot 3:

```
CB5000> set bridge_port 3.10 stp priority 200
```

Related Commands

SET BRIDGE_PORT STP PATH_COST
SHOW BRIDGE_PORT

SET BRIDGE_PORT VBRIDGE

Use the SET BRIDGE_PORT VBRIDGE command to assign a SwitchModule bridge port to a virtual bridge or create a new virtual bridge.

Format

slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports in the slot are affected by this operation.
vbridge	Value from 1 through 240. If you assign a vbridge number that is not yet used as a virtual bridge number, you create a new virtual bridge that is automatically enabled to switch traffic.

Example

The following command assigns all ports on the SwitchModule in slot 3 to virtual bridge 2:

```
CB5000> set bridge_port 3.all vbridge 2
```

Related Commands

SHOW VBRIDGE CONFIGURATION
SHOW BRIDGE_PORT

SET CLOCK

Use the SET CLOCK command to set the time, date, and day of the DMM's internal clock. Set the internal clock during installation, and then for time changes due to daylight savings time (U.S.A.) and leap years. The clock has its own battery and keeps time even if power fails.

The DMM saves the clock information automatically when you set it. You do not need to use the SAVE command.

Format

set clock ——— *hh:mm yy/mm/dd day*

hh:mm	Hours and minutes. *hh* = 0 through 23; *mm* = 0 through 59.
yy/mm/dd	Year, month, and day. *yy* = 00 through 99, *mm* = 1 through 12, *dd* = 1 through 31.
day	Day of the week (for example, `monday`).

Example

The following command sets the internal clock to 05:53 am, for Friday, October 8, 1999:

```
CB5000> set clock 05:53 99/08/10 friday
Clock set to 05:53 Fri 08 October 99
```

Related Command

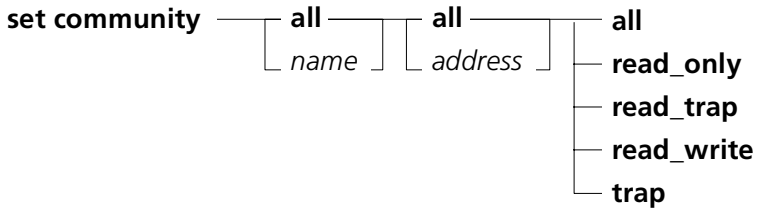
SHOW CLOCK

SET COMMUNITY

Use the SET COMMUNITY command to create entries in the SNMP community table. The SNMP community table defines access privileges for SNMP managers.

The community table contains a maximum of 10 entries. A community entry name cannot exceed 15 characters. Community names are case-sensitive. For example, Silver and silver are different community names.

Format



all	Specifies that this operation is to apply to all communities in the community table.
name	Specifies the name of the community to which this operation applies.
all	A wildcard IP address to be added to the community table.
address	A specific IP address to be added to the specified community. Enter an IP address as a series of four decimal bytes separated by periods. For example, 192.122.19.4.
all	The community can display and modify DMM monitoring and configuration data. Receives alerts from the DMM agent.
read_only	The community can display but not modify DMM monitoring and configuration data.
read_trap	The community can display but not modify DMM monitoring and configuration data and receive traps from the DMM agent.
read_write	The community can display and modify DMM monitoring and configuration data.
trap	The community can receive alerts from the DMM agent.

Example

The following command creates a community named public, and specifies that all workstations in this community have read_only access to the DMM:

```
CB5000> set community public all read_only
Community set.
```

Related Commands

CLEAR COMMUNITY
SHOW COMMUNITY

SET DEVICE CONTACT

Use the SET DEVICE CONTACT command to enter one line of up to 78 alphanumeric characters. You can use this command to store a service person's name, location, company, and telephone number.

Format

set device contact

Example

The following command informs the DMM that you want to enter contact information:

```
CB5000> set device contact
Enter one line of text:
>
```

Enter the desired information such as name, company, and telephone number:

```
>Susan Wu, 696-522-1219
Contact changed.
```

Related Commands

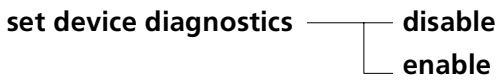
SAVE DEVICE
SHOW DEVICE

SET DEVICE DIAGNOSTICS

Use the SET DEVICE DIAGNOSTICS command to enable or disable diagnostics during startup (or reboot) of the DMM. Disabling diagnostics saves time during reboot of the DMM, but does not confirm correct operation.

The factory setting is diagnostics enabled.

Format



disable	Disables diagnostics upon reboot.
enable	Enables diagnostics upon reboot.

Example

The following command causes diagnostics to run during reset of the DMM:

```
CB5000> set device diagnostics enable
DIAGNOSTICS option ENABLED.
```

SET DEVICE DIP_CONFIGURATION

Use the SET DEVICE DIP_CONFIGURATION command to select if you want media modules in the hub to boot up either:

- Under the software settings stored on the DMM that you configured using the SET command
- Under the hardware DIP switch settings on the module, or, if supported, under the software settings stored on the module

The factory setting is DISABLE. This causes modules to boot using the configuration stored on the DMM. This is also the optimal setting for using the DMM's staging feature. Refer to your *CoreBuilder 5000 Media Module User Guide* for more information.

When the DEVICE DIP_CONFIGURATION command is set to ENABLE, configure the media module to boot using DIP switch or NVRAM configuration, whichever is supported and preferred. Refer to your *CoreBuilder 5000 Media Module User Guide* for more information.

When DIP configuration is enabled on CoreBuilder 5000 Token Ring modules, and there is a conflict between the ring speed DIP settings on different modules set to the same network, there is no way to determine which ring speed will be selected. This is because the DMM controls network speed resolution.

Format

Indicates in which state you want media modules to boot up:

- Disable (factory setting)
- Enable

Example

The following command causes media modules to operate from the DMM configuration settings rather than the module DIP switch or NVRAM settings:

```
CB5000> set device dip_configuration disable
DIP CONFIGURATION option disabled.
```

SET DEVICE LOCATION

Use the SET DEVICE LOCATION command to enter one line of up to 78 alphanumeric characters describing the location of the DMM.

Format

set device location

Example

The following command informs the DMM that you want to enter the hub location:

```
CB5000> set device location
Enter one line of text:
>
```

Enter the desired text:

```
>Lisbon, Building 1, Floor 3
Location changed.
```

Related Commands

SAVE DEVICE
SHOW DEVICE

SET DEVICE MAC_ADDR_ORDER

Use the SET DEVICE MAC_ADDR_ORDER command to specify the bit order in which the command interface displays MAC addresses. Token Ring networks generally use noncanonical address formats.

Here is an example of a MAC address in noncanonical format:
10-00-01-02-03-04

In canonical format, the same address is:
08-00-80-40-c0-20

08 is 10 in reverse bit order
00 is 00 in reverse bit order
80 is 01 in reverse bit order
40 is 02 in reverse bit order
c0 is 03 in reverse bit order
20 is 04 in reverse bit order

Format

canonical	Sets the command interface to display MAC addresses in canonical format.
noncanonical	Sets the command interface to display MAC addresses in noncanonical format.

Example

The following command sets the command interface to display MAC addresses in canonical format:

```
CB5000> set device mac_addr_order canonical
MAC Address Order option set to CANONICAL.
```

Related Commands

SAVE DEVICE
SHOW DEVICE

SET DEVICE NAME

Use the SET DEVICE NAME command to assign the DMM a unique name of up to 31 alphanumeric characters. (To make identification of the DMM easier, assign the same name to the terminal prompt.)

Format

set device name —— *name*

name	The name (up to 31 characters) you want to identify this device.

Example

The following command sets the DMM's name to Bart:

```
CB5000> set device name Bart
Device name changed.
```

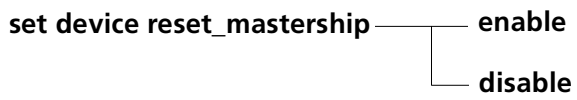
Related Commands

SAVE DEVICE
SET TERMINAL PROMPT
SHOW DEVICE

SET DEVICE RESET_MASTERSHIP

Use the SET DEVICE RESET_MASTERSHIP command to determine if the DMM causes a mastership election when inserted into a hub. Because the setting is stored in non-volatile RAM, you can set this option in one hub, and set it to take effect when you insert the module in a second hub.

Format



enable	DMM forces a mastership election when introduced into a hub. This may be useful if you want the module you are inserting to become the hub master.
disable	DMM does not force a mastership election. This setting ensures that the DMM is a slave when inserted into a hub. This is the default.

Example

The following command causes the DMM to force a mastership election if the DMM is removed and inserted into any hub:

```
CB5000> set device reset_mastership enable
RESET MASTERSHIP option enabled.
```

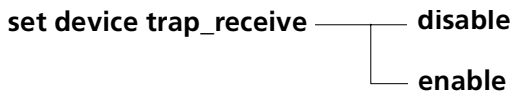
Related Commands

SAVE DEVICE
SHOW DEVICE

SET DEVICE TRAP_RECEIVE

Use the SET DEVICE TRAP_RECEIVE command to configure the DMM to receive alerts (traps) from other SNMP devices on the network. You must also add the DMM's IP address to the community tables of all other SNMP devices.

Format



disable	Disables the trap receive function.
enable	Enables the trap receive function. The factory setting is enable.

Example

The following command enables the DMM to receive traps from other SNMP devices on the network:

```
CB5000> set device trap_receive enable
TRAP option ENABLED.
```

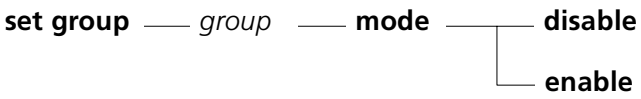
Related Commands

SAVE DEVICE
SHOW DEVICE

SET GROUP MODE

Use the SET GROUP MODE command to enable or disable all the ports in a port group.

Format



group	Specifes a group (group1 to group8). For example, the command SET GROUP GROUP6 MODE DISABLE disables all ports in group6.
disable	Disables all ports in the group.
enable	Enables all ports in the group.

Example

The following command disables the ports in group4:

```
CB5000> set group group4 mode disable
Port 04.09 set to DISABLED.
Port 04.10 set to DISABLED.
Port 04.12 set to DISABLED.
```

Related Commands

SET GROUP NAME
SET GROUP PORT

SET GROUP NAME

Use the SET GROUP NAME command to assign a name (up to 16 alphanumeric characters) to a port group. After you assign a group name, you must identify a group using this name, not by the group number. For example, if you rename Group1 to Eng1, you must refer to the group as Eng1 in future management commands.

Format

set group — *group* — **name** — *name*

group	Specifies a group. For example, the command SET GROUP GROUP6 NAME FINANCE renames group6 as Finance.
name	New name for the group, up to 16 characters in length.

Example

The following command renames group1 to Eng1:

```
CB5000> set group group1 name Eng1
Group1 named to Eng1.
```

Related Commands

SET GROUP MODE
SET GROUP PORT
SHOW GROUP

SET GROUP NETWORK

Use the SET GROUP NETWORK command to assign a port group to a network.

Format

set group —— *group* —— **network** —— *network*

group	Specifies a group.
network	The network to which you are assigning the port groups.

Example

The following command assigns group1 to ethernet 1:

```
CB5000> set group group1 network ethernet 1
Group1 set to Ethernet _1.
```

Related Commands

SET GROUP MODE
SET GROUP PORT
SHOW GROUP

SET GROUP PORT

Use the SET GROUP PORT command to assign ports to a port group. After the port groups are established, you can use the SET GROUP MODE command to enable or disable all of the ports in a port group.

Format

set group — *group* — **port** — *slot.port*

group	Specifies a group name.
slot.port	Identifies the port to be assigned to the group. *slot.port* identifies the port. *slot* (1 through 17) is the slot ID and *port* is the port number. For example, to identify port 4 on the 6, enter **6.4**

Example

The following command assigns port 1 on slot 5 to group1:

```
CB5000> set group group1 port 5.1
Port 5.1 set to group1
```

Related Commands

SET GROUP NAME
SET GROUP MODE
SHOW GROUP

SET HOST

Use the SET HOST command to assign host names to IP addresses. Doing this allows you to use the name *or* the IP address to identify a device. The host table can contain up to 20 entries. You can then use the name in place of the address for PING and TELNET commands.

Format

set host —— *name* —— *ip address*

name	The name to associate with the IP address. The name must begin with a letter. The remainder of the address can be either letters or numbers.
ip address	The IP address. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4.

Example

The following command assigns the name Calvin to IP address 153.17.9.2:

```
CB5000> set host Calvin 153.17.9.2
Host name ip address set.
```

Related Commands

CLEAR HOST
SHOW HOST

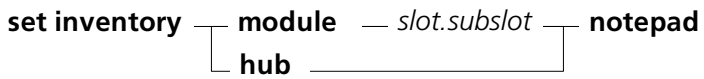
SET INVENTORY NOTEPAD

Use the SET INVENTORY NOTEPAD command to enter up to 55 characters of text in the notepad area that is displayed by the SHOW HUB VERBOSE command.

The SET INVENTORY command is rejected if:

- The specified module is an ONline System Concentrator module
- The slot/subslot is empty
- The CoreBuilder 5000 hub or module's inventory EEPROM is invalid

Format



slot.subslot	Identifies the module for this operation.

Example 1 The following commands enter the installation date for the module in slot 8:

```
CB5000> maintain

>> set inventory module 8.1 notepad
Enter note-pad:  Module installed in hub 10/08/99.

Do you want to enter this into module 8.1's EEPROM? (y/n)  y

Completed.

>> boot
```

Example 2 The following commands enter a repair date for the hub:

```
CB5000> maintain

>> set inventory hub notepad

Enter note-pad:  Fixed 10/08/99

Do you want to enter this into the HUB's EEPROM? (y/n)  y

Completed.

>> boot
```

Related Command SHOW INVENTORY

SET IP ACTIVE_ DEFAULT_GATEWAY

Use the SET IP ACTIVE_DEFAULT_GATEWAY command to set which default gateway is active currently when there are multiple default gateways configured for this DMM.

The active default gateway is the IP address of the gateway (for example, a router) that receives and forwards packets whose addresses are unknown to the local network. Use the default gateway to communicate with the DMM from different IP networks. Use this command to establish the desired active default gateway.

Only one gateway at a time is active. By default, the gateway selected is the Default Gateway assigned to the first interface that you assign to a network. This Default Gateway assignment changes only when you actively set a default gateway or when the interface that determined the Default Gateway loses network connectivity. If the DMM loses its connection to the active default gateway, it automatically searches all networks until it finds a new valid gateway.

Format

set ip active_default_gateway ——— *ip address*

ip address	Internet Protocol (IP) address in the following format: nnn.nnn.nnn.nnn

Example

The following command sets the gateway with the IP address 131.05.08.58 to be the active default gateway for the DMM:

```
CB5000> set ip active_default_gateway 131.05.08.58
Active Default Gateway changed.
```

Related Commands

SET IP DEFAULT_GATEWAY
SHOW IP

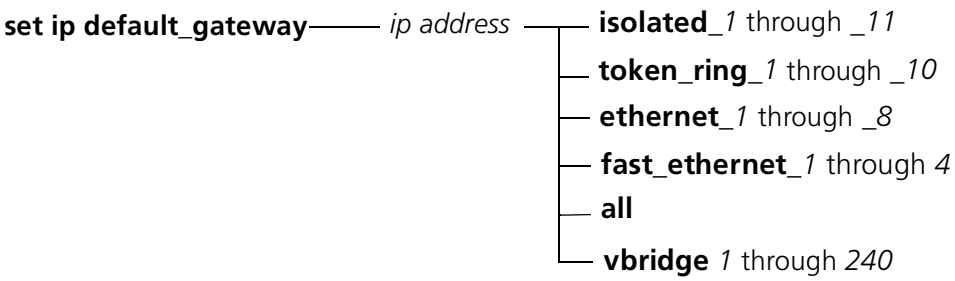
SET IP DEFAULT_GATEWAY

Use the SET IP DEFAULT_GATEWAY command to specify the IP address of a device (usually a router) that forwards packets to destinations other than the local IP network.

Use the SET IP DEFAULT_GATEWAY command to specify a default gateway if the DMM will be sending alert packets (SNMP traps) to management workstations on other IP networks.

You must reset the DMM for the new default gateway addresses to take effect.

Format



ip address	IP address of the default gateway. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4.
isolated_*1* through_*11*	Default gateway address applies to an isolated network.
token_ring_*1* through_*10*	Default gateway address applies to the specified Token Ring network.
ethernet_*1* through_*8*	Default gateway address applies to the specified Ethernet network.
fast_ethernet_*1* through_*4*	Default gateway address applies to the specified Fast Ethernet network.
all	Default gateway address applies to all hub networks.
vbridge *1* through *240*	Default gateway address applies to a virtual bridge network.

Example The following command configures a default gateway for virtual bridge 3:

```
CB5000> set ip default_gateway 123.123.4.6 vbridge 3
Default Gateway associated with VBRIDGE 3 set to 123.123.4.6.
```

Related Commands

SHOW IP
SET IP ACTIVE_DEFAULT_GATEWAY

SET IP IP_ADDRESS

Use the SET IP IP_ADDRESS command to set the IP (Internet Protocol) address for the DMM. The DMM must have an IP address if you plan in-band or SLIP-based management of the hub.

The IP address is four decimal numbers separated by periods. Each number can range from 0 to 255. However, the following addresses are illegal:

- 0.0.0.0
- 255.255.255.255

If you do not plan to connect your network to the Internet, you can use any address that meets the above requirements.

If you do plan to connect to the Internet, you must obtain a range of IP addresses for use by your organization. To obtain a range of addresses, apply to the Network Information Center (NIC):

- U.S.A. mail:

SAIC
7990 Boeing Court
Vienna, VA 22183
ATT: Network Information Center
U.S.A.

- E-mail:

registrar@nic.mil
hostmaster@nic.mil

- Web Site:

www.nic.mil

- Telephone:

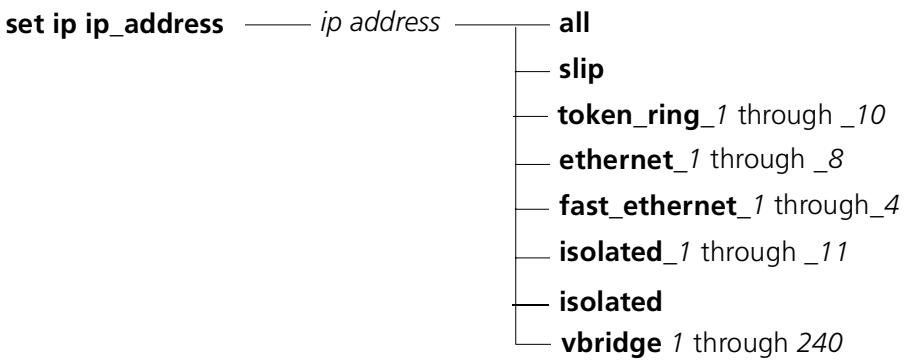
(703) 821-6266 (Outside U.S.A.)
(800) 365-3642 (U.S.A.)

3Com factory-sets the DMM with the IP address 127.0.0.1.

Set only one IP address per DMM. This approach makes IP connections more reliable.

Before you set an IP address for a network, you must set up a subnet mask using the SET IP SUBNET_MASK command.

Format



ip address	IP address of the DMM. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4.
all	Specifies that the DMM use this IP address on all hub networks.
slip	Specifies that the DMM use this IP address on SLIP connections.
token_ring_*1* through *10*	Specifies that the DMM use this IP address on the token ring network.
ethernet_*1* through *8*	Specifies that the DMM use this IP address on the Ethernet network.
fast_ethernet_*1* through *4*	Specifies that the DMM use this IP address on the Fast Ethernet network.
isolated_*1* through *11*	Specifies that the DMM use this IP address on the specified isolated network.
isolated	Specifies that the DMM use this IP address on the isolated network.
vbridge *1* through *240*	Specifies that the DMM uses this IP address on a virtual bridge.

Example The following command assigns an IP address to the DMM for the token_ring_1 network:

```
CB5000> set ip ip_address 151.5.31.60 token_ring_1
IP Address associated with token_ring_1 set to 151.5.31.60.
```

Related Commands

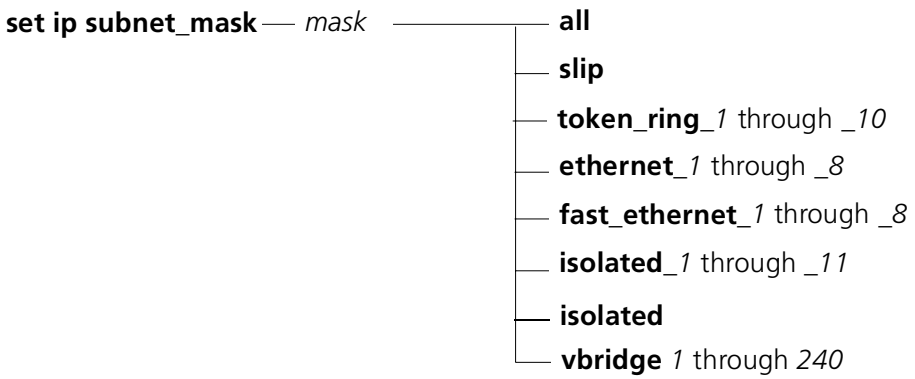
SAVE IP
SHOW IP

SET IP SUBNET_MASK

Use the SET IP SUBNET_MASK command to specify the subnet mask used for your class of Internet device.

In general, the subnet mask defines the network portion (which is masked) from the host portion of the decimal dot notation IP address. The host address is the group of unique characters on the right (Host ID).

Format



mask	Mask in hexadecimal bytes (xx.xx.xx.xx).
all	Specifies that the DMM use this subnet mask on all networks.
slip	Specifies that the DMM use this subnet mask on SLIP connections.
token_ring_*1* through_*10*	Specifies that the DMM use this subnet mask on the token ring network.
ethernet_*1* through_*8*	Specifies that the DMM use this subnet mask on the Ethernet network.
fast_ethernet_*1* through_*8*	Specifies that the DMM use this subnet mask on the Fast Ethernet network.
isolated_*1* through_*11*	Specifies that the DMM use this subnet mask on the specifed isolated network.
isolated	Specifies that the DMM use this subnet mask on the isolated network.
vbridge *1* through *240*	Specifies that the DMM use this subnet mask on virtual bridge networks.

Example

The following command sets the subnet mask for a class C device for all networks:

```
CB5000> set ip subnet_mask FF.FF.FF.0 all
Device subnet mask changed.
```

Related Commands

SET IP DEFAULT_GATEWAY
SET IP IP_ADDRESS
SHOW IP

SET LOGIN

Use the SET LOGIN command to add users to and change passwords for the CoreBuilder 5000 command interface. Any user can use this command to modify his or her own password. You must be logged in as super user to use this feature to create new logins.

The DMM allows up to 10 login names, so that you can authorize several users with differing privileges. Passwords are case sensitive (that is, myname and MYNAME are two different passwords).

You can assign user names at three access levels.

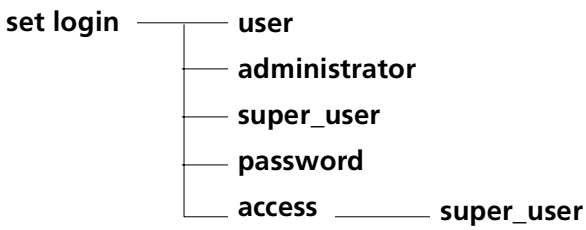
Newly set passwords are effective immediately. You are not prompted for a password until you log out and then try to log back in. You must enter the SAVE LOGIN command for the new user login names to be permanently saved.

If you lose or forget a user password, the super user can use the CLEAR LOGIN and SET LOGIN commands to remove, then re-create the user name.

The factory setting is a single super-user account with the user name *system* and no password.

A newly created login account is not available for use until you save it.

Format



user	Creates a user login. The user can use the following commands: ■ All SHOW commands (except SHOW COMMUNITY) ■ CLEAR RMON ■ CLEAR COUNTERS ■ SET RMON ■ MONITOR

administrator	Creates an administrator login. The administrator can use all user login commands plus the following commands: ■ All SET commands (except SET COMMUNITY, SET LOGIN, and SET IP) ■ All CLEAR commands (except CLEAR LOGIN and CLEAR COMMUNITY) ■ TELNET ■ MAINTAIN ■ DOWNLOAD ■ RESET ■ All REVERT and SAVE commands (except COMMUNITY, LOGIN, and IP)
super_user	Creates a super-user login. The super user can use all commands.
password	Changes the password of the current user.
access super_user	Because the DMM allows only one super-user login at a time, the software includes a special SET LOGIN ACCESS SUPER_USER command. If a super user logs in and is granted only user privileges, that user can issue the SET LOGIN ACCESS SUPER_USER command with the following implications: ■ The current super user is logged out of the DMM. ■ The super user who enters the command immediately assumes super-user privileges. ■ The new super user assumes responsibility for all unsaved changes from the logged out super-user session. This command can also be used to override sessions where communications have failed, but the super user remains logged in.

Example 1 The following command allows a super user to establish a new administrator name and password:

```
CB5000> set login administrator
```

You are prompted as follows:

```
Enter current session password for user "admin":{enter password}

Enter Login Name: {enter name you select}
Enter Login Password: {enter new password}
Verify - re-enter password:{re-enter password}
Login successfully entered.
Login account will not be activated until it is saved.
```

Example 2 The following command changes the password of the user logged in currently:

```
CB5000> set login password
```

You are prompted as follows:

```
Enter current password for user "system": {enter password}
```

Enter your password:

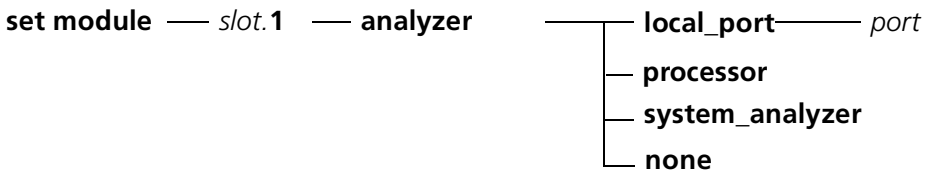
```
New password: {enter new user password}
Verify: {re-enter new user password}
User password changed.
```

Related Commands CLEAR LOGIN
SAVE LOGIN

SET MODULE ANALYZER

Use the SET MODULE ANALYZER command when setting up a roving port analysis configuration on a CoreBuilder 5000 SwitchModule. The SET MODULE ANALYZER command specifies the port or processor you want to use as the analyzer (destination) for mirrored traffic.

Format



slot.**1**	1 through 17. Indicates the slot number of the module you are configuring.
local_port	Specifies that the module mirrors packets to a port on the same module.
port	1 through 24. Specifies the port you want to define as the local_port.
analyzer	Specifies that the module mirrors traffic across the PacketChannel backplane to the port you enable as the system analyzer.
processor	Specifies that the module mirrors traffic to across the PacketChannel backplane to the SwitchModule processor you enable as the system analyzer.
none	Specifies no traffic.

Example

The following command configures port 2 on the SwitchModule in slot 6 as the analyzer:

```
CB5000> set module 6.1 analyzer local_port 2
Module 06 Analyzer set to BRIDGE PORT 2
```

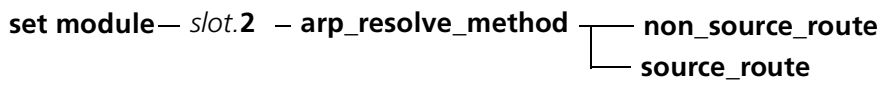
Related Commands

SET BRIDGE_PORT MONITOR
SET MODULE SYSTEM_ANALYZER
SHOW MODULE

SET MODULE ARP_RESOLVE_ METHOD

Use the SET MODULE ARP_RESOLVE_METHOD command to specify whether routing information is included in Address Resolution Protocol (ARP) requests sent by the Token Ring Network Monitor Card (TR-NMC).

Format



slot.**2**	Selects the TR-NMC for which you want to enable or disable routing information in ARP requests. Valid values are hub slot 1 through 17, subslot 2.
non_source_route	TR-NMC does not include the routing information (RI) field in ARP requests.
source_route	TR-NMC includes the routing information (RI) field in ARP requests. This is the factory-default setting.

Example

The following command includes routing information in ARP requests sent from the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 arp_resolve_method source_route
ARP resolve method set to source_route.
```

Related Command

SHOW MODULE

SET MODULE AUTOPARTITION_ THRESHOLD

Use the SET MODULE AUTOPARTITION_THRESHOLD command to assign the number of collisions the DMM allows before automatically partitioning a port. This command is available for the 3Com ONline™ 24-port 10BASE-T Module and the 12-port 10BASE-T Module.

The factory default is 63, which is the proper setting for most environments. The 10BASE-T specification lists a minimum of 31 collisions prior to partitioning, but 31 collisions can cause ports to partition more frequently than necessary. The additional options (127 and 255) are for debugging purposes, and therefore not recommended for use in live networks.

This command is not available for use with the CoreBuilder 5000 24-Port, 20-Port, 40-Port, 36-Port 10BASE-T Modules or the EtherFlex Module.

Format

set module —— *slot.***1** — **autopartition_threshold** —— *threshold*

*slot.***1**	Selects a module for setting the autopartition threshold. Valid values are slot 1 through 17, subslot 1.
threshold	Sets the autopartition threshold: ■ 31_collision ■ 63_collisions ■ 127_collisions ■ 255_collisions

Example

The following command sets the collision threshold of the ONline 24-port Module in slot 7 to a maximum of 63 collisions. If this threshold is exceeded for a port, that port is partitioned.

```
CB5000> set module 7.1 autopartition_threshold 63_collisions
Auto-partition threshold set to 63 COLLISIONS.
```

Related Commands

SHOW PORT
SHOW MODULE

SET MODULE BCN_THRESHOLD

Use the SET MODULE BCN_THRESHOLD to set the number of times that a CoreBuilder 5000 Token Ring port, which was removed from the ring by beacon recovery software, is allowed to reenter the ring.

The CoreBuilder 5000 hub implements beacon recovery by wrapping ports as needed. The port is unwrapped when a transition of phantom is detected.

The beacon threshold is the number of times that a phantom transition is allowed to cause a port to unwrap. When the threshold is exceeded, the port remains wrapped, with a status of BCN THRES ERROR, until you disable and then reenable the port.

The threshold is reset whenever a port successfully inserts into the ring, or when the module is reset.

This command is not available if beacon recovery is disabled (SET NETWORK TOKEN_RING BCN_RECOVERY).

Format

set module —— *slot.***1** — **bcn_threshold** —— *threshold*

*slot.***1**	Identifies the module for this operation.
threshold	Number of phantom transitions caused by beaconing to allow before the DMM shuts down the port. *threshold* = 0 through 255. The factory setting is 7.

Example

The following command sets the beacon threshold to 2:

```
CB5000> set module 4.1 bcn_threshold 2
Threshold set to 2.
```

Related Commands

SET NETWORK TOKEN_RING BCN_RECOVERY
SHOW MODULE

SET MODULE CABLE_IMPEDANCE

Use the SET MODULE CABLE_IMPEDANCE command to set the impedance level for Token Ring module lobe ports. This command is available for the 3Com ONline 20-Port Token Ring Module.

The impedance level for unshielded cable is usually 100 ohms. The impedance level for shielded cable is usually 150 ohms.

Format

set module —— *slot.***1** —— **cable_impedance** —— *impedance*

*slot.***1**	Selects a module to set impedance levels.
impedance	Sets the impedance level. Valid values are: ■ 100ohm ■ 150ohm

Example

The following command sets the cable impedance of the module in slot 1 to 100 ohms:

```
CB5000> set module 1.1 cable_impedance 100ohm
Cable impedance set to 100 OHM.
```

Related Command

SHOW MODULE

SET MODULE CONNECTOR_ NETWORK

Use the SET MODULE CONNECTOR_NETWORK command to assign a connector to a network. This command is available for the ONline 24-Port 10BASE-T Module and CoreBuilder 5000 connector-switched modules.

The connector-switched modules provide bank-level configuration flexibility using the TriChannel™ architecture. You can assign either of the two 50-pin connectors (36-Port Module has three 50-pin connectors), or the entire module, to any of the Ethernet networks available for modules (or isolated) on the CoreBuilder 5000 backplane.

For example, with the ONline 24-Port 10BASE-T Module, assigning one connector to ISOLATED_1 and the other connector to ISOLATED_2 creates two isolated 12-port subnetworks. Assigning both connectors to the same isolated network creates a single 24-port isolated network.

Format

set module — *slot.**1*** — **connector_** — *connector* — **_network** — *network*

slot.**1**	Selects a module to assign. Valid values are hub slot 1 through 17, subslot 1.
connector	Selects the connector to which this command applies. Valid values are 1, 2 or 3.
network	Selects a network to assign the connector to. Valid values are: ■ ethernet_1 through ethernet_8 ■ isolated_1 though isolated_8

Example

The following command sets all ports associated with connector 1 on the 24-Port 10BASE-T Module in slot 7 to Ethernet network 3:

```
CB5000> set module 7.1 connector_1_network ethernet_3
Module 7.01 connector 1 network ID set to ETHERNET 3.
```

Related Commands

SET MODULE
SHOW MODULE

SET MODULE CROSSOVER

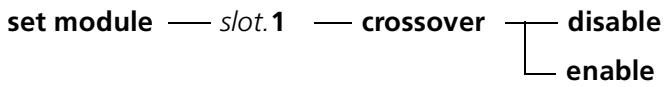
Use the SET MODULE CROSSOVER command to enable or disable crossover mode for port 8 of ONline Ethernet 10BASE-T Modules (Model Numbers 5108M-TP and 5108M-UTP).

Enabling crossover mode allows you to connect port 8 of the ONline 10BASE-T module directly to a 10BASE-T transceiver. This is the default setting for all 10BASE-T ports.

To connect port 8 of the ONline 10BASE-T module directly to any port on another 10BASE-T module or 10BASE-T hub, disable crossover mode.

When connecting two 10BASE-T modules, one port must be crossed over and the other port must be uncrossed. You can achieve this by using port 8 on one of the modules and disabling crossover, or by leaving crossover enabled and using an external crossover adapter.

Format



slot.**1**	Selects the module for which you want to enable or disable crossover mode. Valid values are hub slot 1 through 17, subslot 1.
Enables or disables crossover mode for the chosen port. Valid values are: ■ disable ■ enable	

Example

The following command sets the crossover mode of the module in slot 1 to enable:

```
CB5000> set module 1.1 crossover enable
Crossover set to ENABLED.
```

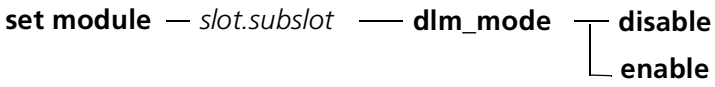
Related Command

SHOW MODULE

SET MODULE DLM_MODE

Use the SET MODULE DLM_MODE command to enable or disable DLM (Dynamically Loadable Module) mode on an A-ENMC. You must enable DLM mode before the A-ENMC can run DLMs. The factory default is DLM mode disabled.

Format



slot.subslot	Identifies the slot and subslot for this operation. *slot* (1 through 17) is the slot number in the hub and *subslot* (2 through 7) is the subslot number on the module in the specified slot. For example, to identify subslot 4 of slot 15, enter **15.4**
disable	Disables DLM mode.
enable	Enables DLM mode.

Example

The following command enables DLM mode on the A-ENMC in subslot 4 of the module in slot 15:

```
CB5000> set module 15.4 dlm_mode enable
```

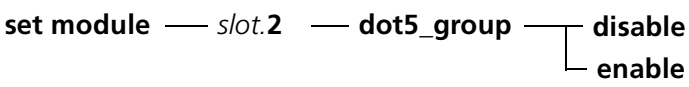
Related Command

SHOW DLM

SET MODULE DOT5_GROUP

Use the SET MODULE DOT5_GROUP command to enable or disable Token Ring (dot5) statistics collection as defined in the IEEE 802.5 Token Ring Management Information Base (MIB). This command applies to the Token Ring Network Monitor Card (TR-NMC).

Format



*slot.***2**	Selects the TR-NMC on which you want to enable or disable Token Ring (dot5) statistics collection. Valid values are hub slot 1 through 17, subslot 2.
Enables or disables Token Ring (dot5) statistics collection for the chosen TR-NMC. Valid values are: ■ disable ■ enable	

Example

The following command enables IEEE 802.5 MIB statistics collection on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 dot5_group enable

Module Group set to ENABLED.
```

Related Commands

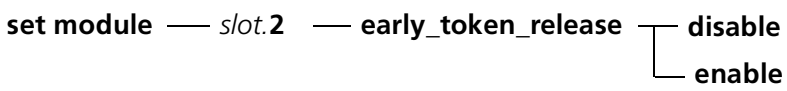
SHOW COUNTER
SHOW MODULE

SET MODULE EARLY_TOKEN_ RELEASE

Use the SET MODULE EARLY_TOKEN_RELEASE command to enable or disable early token release (ETR) mode on the Token Ring Network Monitor Card (TR-NMC).

Early token release allows a transmitting adapter to release a new token as soon as it has completed frame transmission, whether or not the frame header has returned to that adapter. This option is valid for 16 Mbps Token Ring networks only.

Format



slot.**2**	Selects the TR-NMC on which you want to enable or disable early token release mode. Valid values are hub slot 1 through 17, subslot 2.
Enables or disables early token release mode for the chosen TR-NMC. Valid values are: ■ disable ■ enable	

Example

The following command enables early token release mode on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 early_token_release enable
Early token release set to ENABLED.
```

Related Command

SHOW MODULE

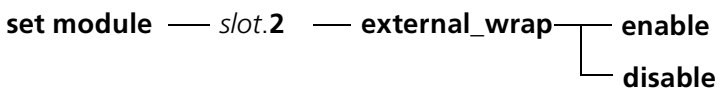
SET MODULE EXTERNAL_WRAP

Use the SET MODULE EXTERNAL_WRAP command to enable or disable external wrap mode on the Token Ring Network Monitor Card (TR-NMC).

An External Wrap Test performs a lobe wrap out to the cable, but the system does not insert the adapter (phantom not raised). This feature is provided for diagnostic use.

Disable the TR-NMC interface before changing this setting.

Format



*slot.***2**	Selects the TR-NMC on which you want to enable or disable external wrap mode. Valid values are hub slot 1 through 17, subslot 2.
Enables or disables external wrap mode for the chosen port. Valid values are: ■ disable ■ enable	

Example

The following command enables external wrap mode on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 external_wrap enable
External wrap set to ENABLED.
```

Related Commands

SET MODULE INTERFACE
SHOW MODULE

SET MODULE FIFO_FILL_LEVEL

Use the SET MODULE FIFO_FILL_LEVEL command to change the FIFO fill level. This command applies only to certain older ONline Ethernet Twisted Pair Modules (Model Number 5108M-UTP).

The FIFO fill level controls the number of received bits loaded into the internal FIFO buffer before the bits are unloaded. The factory-set FIFO fill level is 8 bits.

To increase the achievable link distance by approximately 20 meters, set the FIFO fill level to 7 bits (a savings of one bit or 100 ns). This savings allows connection to a device that might be too far away otherwise. However, if jitter is a problem, set the FIFO fill level to 8 bits.

Format

set module — *slot.***1** — **fifo_fill_level** — *number of bits*

*slot.***1**	Selects the module for which you want to set the fill level. Valid values are hub slot 1 through 17, subslot 1.
number of bits	Sets the number of bits. Valid values are 7 and 8.

Example

The following command sets the FIFO fill level for the module in slot 1 to 7:

```
CB5000> set module 1.1 fifo_fill_level 7
Fifo fill level set to 7.
```

Related Command

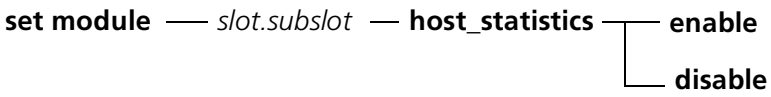
SHOW MODULE

SET MODULE HOST_STATISTICS

Use the SET MODULE HOST_STATISTICS command to enable RMON host statistics collection on an Ethernet Network Monitor Card (ENMC).

The SET MODULE HOST_STATISTICS command enables or disables RMON host statistics collection on an Ethernet Network Monitor Card. Disabling RMON host statistics collection frees ENMC resources for other tasks. The default setting is disabled.

Format



slot.subslot	Selects the ENMC on which you want to enable or disable RMON host statistics collection. Valid values are hub slot 1 through 17, subslot 2 through 7.
Enables or disables RMON host statistics collection. Valid values are: ■ disable ■ enable	

Example

The following command enables RMON statistics collection on the ENMC in subslot 4 of the DMM-EC in slot 15:

```
CB5000> set module 15.4 host_statistics enable
Rmon hosts table for module 15.04 set to ENABLE.
```

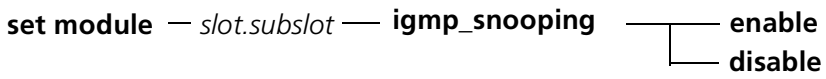
Related Commands

SET MODULE PROBE_MODE
SHOW RMON

SET MODULE IGMP_SNOOPING

Use the SET MODULE IGMP_SNOOPING command to enable or disable IGMP Snooping on a module. After you enter this command, it does not take affect until the module is rebooted. The sole purpose of this command is to allow the FTE based modules to share FTE Forwarding memory based on snooping versus non-snooping bridges.

Format



*slot.***1**	Selects the module on which you want to enable or disable IGMP snooping. Valid values are hub slot 1 through 17, subslot 1.
enable	Enables IGMP snooping on the specifed module.
disable	Disables IGMP snooping on the specifed module.

Example

The following command enables IGMP Snooping on the module in slot 15:

```
CB5000> set module 15.1 igmp_snooping enable
IGMP Snooping set to ENABLED.
```

SET MODULE INTERFACE

Use the SET MODULE INTERFACE command to enable or disable the network interface on Network Monitor Cards.

The A-ENMC has two network interfaces.

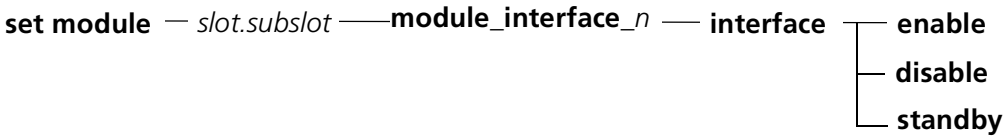
Before you enable an interface:

- Assign the Network Monitor Card (or A-ENMC interface) to a network
- Set IP parameters for the network it is assigned to (using SET IP commands)

This command allows you to set certain NMCs to be active, while others are set explicitly to standby mode.

This option is not available when the TR-NMC is installed on a module-switched Token Ring module. If you want an NMC to act as a standby for a module installed on a module-switched module, you must set the standby module (residing on another host card) to the same network.

Format



slot.subslot	Selects the NMC you want to enable, disable, or set to standby. Valid values are hub slot 1 through 17, subslot 2 through 7.
module_interface_*n*	Selects one of the two interfaces on the A-ENMC. This command option is available only if the subslot you entered contains an A-ENMC. *n* = 1 or 2
enable	Enables interface on the network it is assigned to.
disable	Disconnects the interface from a network.
standby	Interface assumes role of any failed (hardware failure, host module removed) or too heavily burdened active Network Monitor Card of the same protocol. When activated, the standby card assumes all IP parameters, and begins to monitor statistics on the network to which the now inactive card had been assigned. A TR-NMC in this state is not inserted in the ring or included in ring maps.

Example 1 The following command enables the ENMC in subslot 4 of the DMM-EC in slot 15:

```
CB5000> set module 15.4 interface enable
Interface Mode set to ENABLED.
```

Example 2 The following command enables slot 5, subslot 1, A-ENMC interface 2:

```
CB5000> set module 5.1 module_interface_2 interface enable
```

Related Commands
SET MODULE NETWORK
SET IP
SHOW INTERFACE

SET MODULE INTERNAL_WRAP

Use the SET MODULE INTERNAL_WRAP command to enable or disable internal wrap mode on the Token Ring Network Monitor Card (TR-NMC).

Use this command to indicate whether or not this module's Token Ring adapter performs an Internal Wrap Test, which wraps data internal to the Token Ring adapter (MAC Wrap). This feature is provided for diagnostic use.

Format

set module — *slot.***2** — **internal_wrap** — *setting*

*slot.***2**	Selects the TR-NMC on which you want to enable or disable internal wrap mode. Valid values are hub slot 1 through 17, subslot 2.
setting	Enables or disables internal wrap mode for the chosen port. Valid values are: ■ disable ■ enable

Example

The following command enables internal wrap mode on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 internal_wrap enable
Internal wrap set to ENABLED.
```

Related Command

SHOW MODULE VERBOSE

SET MODULE LOCALLY_ ADMINISTERED_ ADDRESS

Use the SET MODULE LOCALLY_ADMINISTERED_ADDRESS command to specify a locally administered MAC address for a TR-NMC. The TR-NMC rejects the command if you specify an illegal address (for example, if the MAC address you enter is a broadcast address or if the locally-administered bit is not 1).

Format

set module — *slot.***2** — **locally_administered_address** — *mac address*

*slot.***2**	Identifies the TR-NMC for this operation.
mac address	New locally administered MAC address for the identified hub. Enter the address as a series of six hexadecimal bytes separated by hyphens (for example, 10-00-f1-0f-0c-63). This address must be unique on your network.

Example

The following command sets the MAC address of the module in slot 2.2 to a new value:

```
CB5000> set module 2.2 locally_administered_address
48-03-e3-8f-02-00
Locally administered address set.
```

Related Commands

SET MODULE MAC_ADDRESS_TYPE
SHOW MODULE VERBOSE

SET MODULE LOW_LIGHT_WARNING

Use the SET MODULE LOW_LIGHT_WARNING command to enable a warning when the light level received is weak. This command pertains to the ONline Ethernet Fiber Modules (Model Number 5104M-FIB) only.

A low light condition does not affect network operation. Enable low light detection during system setup to see if any fiber connections are close to reaching their distance limits. If they are, the status LED on the Ethernet Fiber module blinks 6 times to indicate the condition, and the status is reported to the DMM. After the network is running successfully, there is less need for this type of detection.

You can disable the low light detection if you are aware that the light level is low, but prefer not to have a blinking status indicator signaling the condition.

Format

set module — *slot.***1** — **low_light_warning** — *setting*

*slot.***1**	The slot and subslot containing the module you are sending this command to.
setting	The possible settings are: ■ enable ■ disable

Example

The following command enables the low light warning on the module in slot 1:

```
CB5000> set module 1.1 low_light_warning enable
Low-light warning set to ENABLED.
```

Related Command

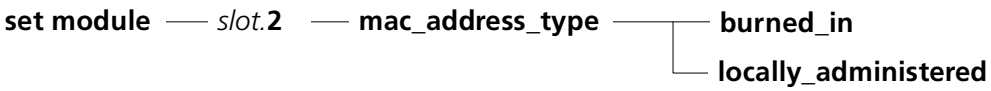
SHOW MODULE

SET MODULE MAC_ADDRESS_TYPE

Use the SET MODULE MAC_ADDRESS_TYPE command to specify whether a TR-NMC is to use its factory-set MAC address (burned_in) or a user-defined MAC address (locally_administered).

The DMM rejects this command if the MAC address to be used is an illegal value.

Format



*slot.***2**	Identifies the TR-NMC for this operation.
burned_in	Selects the factory-set MAC address. The factory setting is for the TR-NMC to use its factory-set MAC address rather than a locally administered MAC address.
locally_administered	Selects the locally administered MAC address.

Example

The following command specifies that the TR-NMC in slot 7.2 use the factory-set MAC address:

```
CB5000> set module 7.2 mac_address_type burned_in
Mac address set to burned_in.
```

Related Commands

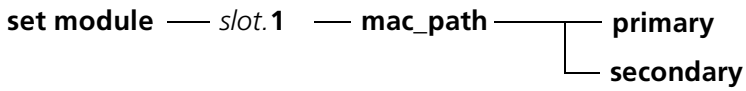
SET MODULE LOCALLY_ADMINISTERED_ ADDRESS
SHOW MODULE VERBOSE

SET MODULE MAC_PATH

Use the SET MODULE MAC_PATH command to change the transmission path through the ONline FDDI Management Modules.

This command allows you to switch from the Primary FDDI ring to the Secondary FDDI ring. This has the same effect as physically switching the A and B port connections.

Format



slot.**1**	Hub slot containing the FDDI module you are configuring.
primary	Switches port from the secondary ring to the primary ring.
secondary	Switches port from the primary ring to the secondary ring.

Example

The following command establishes a secondary backplane path for an FDDI module in slot 10:

```
CB5000> set module 10.1 mac_path secondary
Mac path set to secondary.
```

Related Command

SHOW MODULE

SET MODULE MASTERSHIP_PRIORITY

Use the SET MODULE MASTERSHIP_PRIORITY command to establish the order in which installed management modules assume command of the hub when the current hub master fails or resigns.

A master management module has configuration control, management responsibilities, and fault detection capabilities for the entire hub. This command allows you to assign a priority level to your management modules.

The management module with the highest priority is elected as a master for that hub. Set the master DMM to the highest priority level, which is 10. This causes other management modules in the hub to become stand-bys (CoreBuilder 5000) or slaves (ONline). If you assign the same mastership priority to two DMMs in the same hub, the election for a master is arbitrary. CoreBuilder 5000 DMMs always assume mastership over ONline management modules.

Mastership election completion time is dependent on a management module's mastership priority setting. Set a master DMM to 10 and standby DMMs to mastership priority values of 7, 8, or 9 to facilitate the election process.

SET MODULE MASTERSHIP_PRIORITY sets the mastership priority. You must enter the RESET MASTERSHIP command if you want to force election of a new hub master.

Format

set module — *slot.subslot* — **mastership_priority** — *priority*

slot.subslot	The slot of the DMM you are changing the mastership priority for: ■ DMM - *slot*.**1** ■ DMM-EC - *slot*.**8** ■ ADMM - *slot*.**2**
priority	The election priority that the module has during a mastership election. Valid values are 1 through 10, with 10 being the highest priority. The default is 10.

Example

The following command sets the mastership priority level for the module in slot 6 to level 1:

```
CB5000> set module 6.1 mastership_priority 1
Mastership priority set to 1.
```

Related Command

RESET MASTERSHIP

SET MODULE MAXIMUM_VBRIDGE

Use the SET MODULE MAXIMUM_VBRIDGE command to adjust the maximum number of virtual bridges you can use on a CoreBuilder 5000 SwitchModule.

The max vbridge values you can assign depend in part on the memory model setting you configure for the Switchmodule. If you set memory model to Small, you cannot set max vbridge to 256. All other max vbridge assignments are valid for any memory model setting.

To assign a max vbridge value of 256, the SwitchModule must have an installed 8 MB or 16 MB memory upgrade SIMM.

You must save the setting and reboot the SwitchModule for the change to take effect.

For more information about configuring the maximum vbridge value, refer to the *CoreBuilder 5000 SwitchModule User Guide.*

Format

set module — *slot*.**1** — **maximum_vbridge** — *max vbridge*

slot.**1**	Slot containing the SwitchModule you are configuring.
max vbridge	Value that is a power of 2. The following values are valid: 1, 2, 4, 8, 16, 32, 64, 128, and 256. The default setting is 32.

Example

The following command configures module 6 to the specified vbridge setting. You must reset the SwitchModule using the RESET MODULE command for the maximum vbridge change to take effect. The system displays the warning message in the example to remind you to reset the module.

```
CB5000> set module 6.1 maximum_vbridge 256
Administrative Maximum Vbridge set to 256
Warning: change does not take effect until module is reset.
CB5000> save all
```

Related Commands

SHOW MODULE
SET MODULE MEMORY_MODEL

SET MODULE MEMORY_MODEL

Use the SET MODULE MEMORY_MODEL command to adjust the amount of DRAM (dynamic random access memory) that a CoreBuilder 5000 SwitchModule allocates to address learning and to RMON. Increasing the setting increases the table capacity for RMON processing on the SwitchModule.

You must save the setting and reboot the SwitchModule for the change to take effect.

For more information about altering the memory module setting, refer to the *CoreBuilder 5000 SwitchModule User Guide.*

Format

slot.**1**	Slot containing the SwitchModule you are configuring.
small	DRAM allocation for address learning and RMON = 3.5 MB. This is the default setting. No memory upgrade SIMM necessary to use this setting. If you set memory model to Small, you cannot set the maximum virtual bridge to a value to greater than 128 for this SwitchModule.
medium	DRAM allocation for address learning and RMON = 3.0 MB. No memory upgrade SIMM necessary to use this setting.
large	DRAM allocation for address learning and RMON = 2.0 MB. You can set the memory model to Large only if you have installed an 8 MB or 16 MB memory upgrade SIMM on the SwitchModule.

Example

The following command changes the memory model setting to medium for the SwitchModule in slot 5:

```
CB5000> set module 5.1 memory_model medium
CB5000> save all
```

Related Commands

SHOW MODULE
SET MODULE MAXIMUM_VBRIDGE

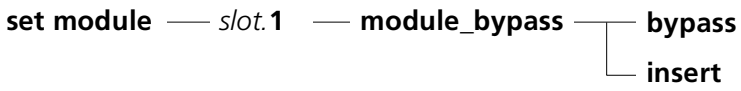
SET MODULE MODULE_BYPASS

Use the SET MODULE MODULE_BYPASS command to insert or bypass ONline Token Ring MAU Modules in a ring.

You must use this command to insert the module into the ring initially. When you insert a Token Ring module in a hub with an active network management module, the module is automatically placed into bypass mode so that unauthorized users cannot insert into the network.

Refer to the specific Token Ring Installation Guide for more information on insert and bypass mode.

Format



slot.**1**	Slot containing the Token Ring module you are configuring.
bypass	Traffic still goes through the Ring-In and Ring-Out ports on the module, but does not travel to the eight media ports.
insert	Insert Token Ring modules into the ring to which the Ring-In and Ring-Out cables are connected.

Example

The following command inserts the Token Ring MAU Module in slot 5 into the ring it is connected to:

```
CB5000> set module 5.1 module_bypass insert
Module 5.01 INSERTED.
```

Related Command

SHOW MODULE

SET MODULE MONITOR_ CONTENTION

Use the SET MODULE MONITOR_CONTENTION command to determine if a TR-NMC participates in active monitor contention if the opportunity arises. If the need to determine a new active monitor arises, the TR-NMC still detects and initiates the process regardless of this setting.

Format

slot.**2**	Indicates the slot number of the module you are configuring.
enable	TR-NMC participates fully in the active monitor election process, and accepts the role of active monitor if elected.
disable	TR-NMC detects and initiates the active monitor contention process, but cannot be elected active monitor.

Example

The following command enables active monitor contention on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 monitor_contention enable
Contention set to ENABLED.
```

Related Command

SHOW MODULE

SET MODULE NETWORK

Use the SET MODULE NETWORK command to assign each module or submodule to one of the selected networks that are available for the module type (Token Ring, Ethernet, Fast Ethernet, or FDDI), or isolate the module.

Modules assigned to the same network form a segment. Modules assigned to different networks are on different segments and cannot communicate unless the networks are connected using a bridge or router. Each isolated module forms its own segment that isolates the traffic on that module from all other modules in the hub.

If you switch ONline Token Ring modules from one ring to another ring, the rings are momentarily joined. To avoid this situation, switch modules to an isolated network before switching modules to another ring.

When modules are network-selectable per port, refer to the SET PORT NETWORK command.

Changing the Network Monitor Card network assignment clears all network statistics to zero.

If you change a module network assignment and the new network is on a different IP network (the old and new networks are separated by a router), then any IP stations attached to the module must be configured with new IP addresses.

Format

set module — *slot.subslot* — **module_interface**_*n* ——— **network** ——— *network*

slot.subslot	Identifies the slot and subslot for this operation. *slot* (1 through 17) is the slot number in the hub and *subslot* is the subslot number on the module in the specified slot. For example, to identify subslot 4 of slot 6, enter **6.4**
module_interface_*n*	Selects one of the two interfaces on the A-ENMC. This command option is only available if the subslot you entered contains an A-ENMC. n =1 or 2
network	The backplane (hub-wide) or isolated (local to module) network that you want to assign the module to.

Example 1 The following command assigns the media module in slot 1 to Ethernet network 3:

```
CB5000> set module 1.1 network ethernet_3
Module 1.1 network id set to ETHERNET_3.
```

Example 2 The following command assigns the Ethernet Network Monitor Card attached to subslot 5 in a Distributed Management Module for Ethernet in hub slot 4 to Ethernet network 1:

```
CB5000> set module 4.5 network ethernet_1
Module 04.05 network id set to ETHERNET_1.
```

Limitations on NMC Network Assignments

Network Monitor Card network assignments have the following limitations:

- You cannot assign two NMCs to the same network (for example, Ethernet_1) if both interfaces are enabled.
- You cannot assign two NMCs with the same IP address, regardless of network assignment.

The following scenarios describe these limitations in greater detail:

1 If you have an active NMC on Ethernet_1 and you try to set another NMC to Ethernet_1, or try to enable a disabled NMC on that network, the following message is displayed:

```
Interface module x.y already enabled for this network
Multiple Enabled Interface cards cannot be on the same network
Command aborted.
```

2 If you have an NMC on a network with an active (non-loopback) IP address, and you try to set another NMC to a different network with the *same IP address* (or try to enable a disabled one on that network), the following message is displayed:

```
Interface module x.y already enabled for ip address 151.xxx.x.xxx
Multiple Enabled Interface cards cannot share one ip address
Command aborted.
```

3 If you try to set an IP address for a network that has an enabled NMC on it, and there is already an enabled NMC with that IP address, the following message is displayed:

```
Interface module x.y already enabled for ip address 151.xxx.x.xxx
Multiple Enabled Interface cards cannot share one ip address
Command aborted.
```

You cannot assign a TR-NMC attached to a CoreBuilder 5000 module-switched Token Ring module to a network. A TR-NMC on this module is automatically assigned to the same network as the host module.

Related Command SHOW MODULE

SET MODULE PER_ PORT_COUNTERS_ CONNECTOR

Use the SET MODULE PER_PORT_COUNTERS_CONNECTOR command to select which connector to monitor ports statistics on for the 3Com ONline 24-Port 10BASE-T Module.

Format

set module — *slot.subslot* — **per_port_counters_connector** — *connector*

slot.subslot	The slot of the module that you are configuring. *slot* (1 through 17) is the slot number for the module in the hub and *subslot* is the subslot number on the module in the specified slot.
connector	The number of the connector (1 or 2) whose per-port statistics you want to monitor.

Example

The following command sets the per-port counters connector to 2 on the ONline 24-Port 10BASE-T Module in slot 3.1:

```
CB5000> set module 3.1 per_port_counters_connector 2
Module 3 port counters set to Connector 2.
```

Related Commands

SET MODULE CONNECTOR NETWORK
SHOW MODULE

SET MODULE PHY_AUTOMATIC_ FAILOVER

Use the SET MODULE PHY_AUTOMATIC_FAILOVER command in a dual port configuration to enable or disable the switching over of one physical port to another physical port in the event that the physical port currently in use experiences Loss of Frame or Loss of Signal errors.

A PHY is a physical port. Dual ports provide physical redundancy in the event a physical link or ATM switch fails.

Format

*slot.***1**	1 through 17. Indicates the slot number of the module you are configuring.
enable	Enables the switching over of the PHY when Loss of Frame or Loss of Signal errors occur.
disable	Disables the switching over of the PHY when Loss of Frame or Loss of Signal errors occur.

Example

The following command enables the switching over of one PHY to another when a Loss of Frame or Loss of Signal error occurs:

```
CB5000> set module 4.1 phy_automatic_failover enable
Phy Automatic Failover set to ENABLED.
```

Related Commands

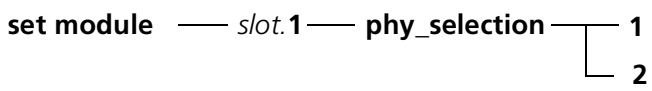
SET MODULE PHY_SELECTION
SHOW MODULE

SET MODULE PHY_SELECTION

Use the SET MODULE PHY_SELECTION command to specify the preferred PHY when two PHYs are installed and are operational.

A PHY is a physical port. Dual ports provide physical redundancy in the event a physical link or ATM switch fails.

Format



*slot.***1**	1 through 17. Indicates the slot number of the module you are configuring.
1	Selects PHY 1.
2	Selects PHY 2.

Example

The following command selects PHY 2 as the preferred PHY:

```
CB5000> set module 4.1 phy_selection 2
Phy Configuration Select set to 2.
Warning: change does not take effect until module is reset.
```

Related Commands

SET MODULE PHY_AUTOMATIC_FAILOVER
SHOW MODULE

SET MODULE PROBE_MODE

Use the SET MODULE PROBE_MODE command to add and delete control table entries for the following RMON groups:

- Statistics
- Host
- Matrix
- History
- Host Top N
- Events
- Alarms

Enabling or disabling probe mode causes the Ethernet Network Monitor Card (ENMC) to reset.

Setting an ENMC to probe mode prevents the ENMC from collecting per-port statistics.

Format

slot.subslot	The slot and subslot of the ENMC that you are configuring.
enable	Enables the ENMC's ability to act as an RMON probe. Enabling probe mode disables the ENMC's ability to collect per-port statistics.
disable	Disables the ENMC's ability to act as an RMON probe. Disabling probe mode enables the ENMC's ability to collect per-port statistics.

Example

The following command enables probe mode on the ENMC module in slot 1.2:

```
CB5000> set module 1.2 probe_mode enable

Changing the probe mode causes this card to reset.
Also, any unsaved module changes will be saved.
Do you wish to continue ? (y/n) : y
```

Related Commands

SET RMON
SHOW RMON
SHOW COUNTER RMON

SET MODULE RING_SPEED

Use the SET MODULE RING_SPEED command to set the module to run at a ring speed of 4 Mbps or 16 Mbps.

You can change the speed of a module only under the following conditions:

- The module is isolated from other hubs (SET NETWORK).
- No stations are connected to the module or all ports are disabled (SET PORT MODE).

This command does not set the ring speed for module-switched CoreBuilder 5000 Token Ring modules.

Format

slot.sublsot	Identifies the module for this operation.
4mbps **16mbps**	Selects a ring speed of 4 Mbps or 16 Mbps. The factory setting is 16mbps.

Example

The following command sets the module in slot 5 to a ring speed of 16 Mbps:

```
CB5000> set module 5.1 ring_speed 16mbps
Ring Speed set to 16 MBPS.
```

Related Commands

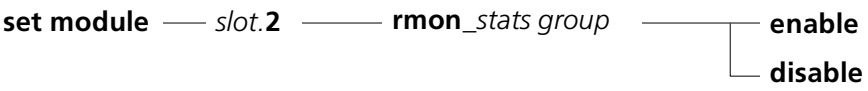
SAVE MODULE
SHOW MODULE
SET NETWORK TOKEN_RING RING_SPEED

SET MODULE RMON_*statistics group*

Use the SET MODULE RMON_*statistics group* command to enable or disable Token Ring RMON statistics collection groups on the Token Ring Network Monitor Card (TR-NMC). You must set the SET MODULE RMON_GROUP command to ENABLE for an individual group setting to take effect.

Enabling RMON groups consumes system resources. Enable only those groups that provide useful information about your network.

Format



slot.**2**	The slot and subslot of the TR-NMC you are configuring.
stats group	The statistics group you are enabling or disabling with the command. The options are: ■ host_stats ■ mac_layer_stats ■ promiscuous_stats ■ ring_station_stats ■ src_routing_stats
enable	Enables the TR-NMC's ability to collect the selected RMON statistics group.
disable	Disables the TR-NMC's ability to collect the selected RMON statistics group. Disable is the default selection.

Example

The following command enables RMON host statistics collection on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 rmon_host_stats enable
RMON Host Statistics set to ENABLED.
```

Related Commands

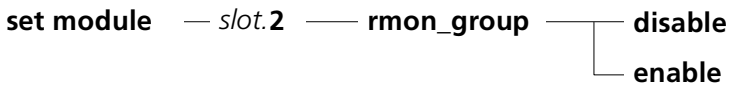
SHOW COUNTER RMON
SET MODULE INTERFACE

SET MODULE RMON_GROUP

Use the SET MODULE RMON_GROUP command to enable or disable Token Ring RMON statistics collection on the Token Ring Network Monitor Card (TR-NMC). This command enables RMON groups. Separate individual commands enable or disable collection of individual RMON groups.

Enabling RMON groups consumes system resources. Enable only those groups that provide useful information about your network.

Format



slot.**2**	Indicates the module that you are initiating RMON statistics on.
disable	Disables RMON statistics collection.
enable	Enables RMON statistics collection.

Example

The following command enables RMON MIB statistics collection on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 rmon_group enable
RMON group set to ENABLED.
```

Related Commands

SET MODULE RMON_*statistics group*
SET MODULE SURROGATE_GROUP
SHOW COUNTER RMON

SET MODULE SPEED_THRESHOLD

Use the SET MODULE SPEED_THRESHOLD command to set the number of consecutive times that a station is allowed to retry inserting into the ring at an incorrect ring speed before the DMM removes the port from the ring.

Speed detection prevents stations from inserting into a ring at the incorrect speed. When an incorrect speed station is detected:

1. The module wraps the port and sets the port status to SPEED MISMATCH.
2. The module retries speed detection the next time the station tries to insert into the ring.

The module counts the number of times that a station attempts to insert into the ring at an incorrect ring speed. When the threshold is exceeded, the port remains wrapped with a status of SPD THRES ERROR until you disable and then reenable the port. The next time the station attempts to insert into the ring, the module unwraps the port and clears the SPD THRES ERROR status.

When a port successfully inserts into the ring, the module resets the speed detection counter for that port.

Use the SET PORT SPEED_DETECT command to enable or disable this feature.

Format

set module — *slot.***1** — **speed_threshold** — *threshold*

*slot.***1**	Identifies the module for this operation.
threshold	The speed threshold for the ports on the identified module. Valid values are 0 through 255. A value of 0 allows an infinite number of retries. The factory setting is 7.

Example

The following command sets the speed threshold to 3 for the module in slot 3.1:

```
CB5000> set module 3.1 speed_threshold 3
Threshold set to 3.
```

Related Commands

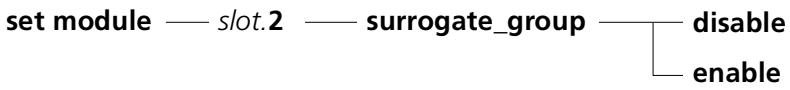
SAVE MODULE_PORT
SET PORT SPEED_DETECT
SHOW PORT

SET MODULE SURROGATE_GROUP

Use the SET MODULE SURROGATE_GROUP command to enable or disable the Token Ring Surrogate function on the Token Ring Network Monitor Card (TR-NMC). In addition to this command, you must use the SET TR_SURROGATE commands to enable or disable individual groups.

Enabling Token Ring Surrogate groups consumes system resources. Enable only those groups that provide useful information about your network.

Format



slot.**2**	Identifies the TR-NMC for this operation.
disable	Disables the Token Ring Surrogate function.
enable	Enables the Token Ring Surrogate function.

Example

The following command enables Token Ring Surrogate groups on the TR-NMC in slot 3.2:

```
CB5000> set module 3.2 surrogate_group enable
Surrogate Group set to ENABLED.
```

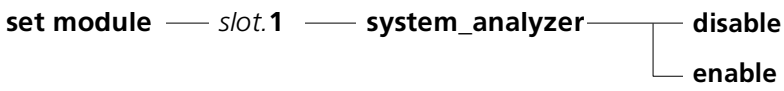
Related Commands

SET TR_SURROGATE SURR_STATUS
SHOW MODULE

SET MODULE SYSTEM_ANALYZER

Use the SET MODULE SYSTEM_ANALYZER command to enable or disable mirroring or monitoring.

Format



*slot.***1**	Identifies the module for this operation.
disable	Disables the System Analyzer function.
enable	Enables the System Analyzer function.

Example

The following command enables monitoring mode on module 7.1:

```
CB5000> set module 7.1 system_analyzer enable
WARNING: Only one Module may have System ANALYZER set to ENABLE.
If any other Module had System analyzer set to ENABLE, previously,
that Module will now have System ANALYZER set to DISABLE.
Module 07 System Analyzer set to ENABLED.
```

In this command, **module 7.1** specifies module 7, subslot 1. This command enables SwitchModule 7 as the system analyzer.

Related Command

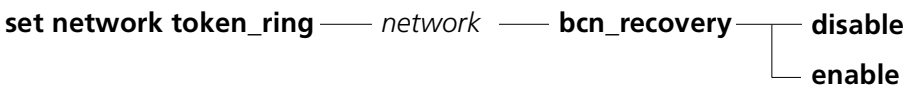
SET MODULE ANALYZER

SET NETWORK TOKEN_RING BCN_RECOVERY

Use the SET NETWORK TOKEN_RING BCN_RECOVERY command to enable or disable beacon recovery. Disable beacon recovery only as a troubleshooting tool to prevent rings from self-healing before you can isolate the problem or faulty device.

If beacon recovery is disabled, the Beacon LED does not light when the ring is beaconing.

Format



network	Identifies the network for this operation: ■ token_ring_1 through token_ring_10 ■ isolated slot ■ isolated_1 slot through isolated _11 slot
disable	Disables beacon recovery.
enable	Enables beacon recovery. The factory setting is enable.

Example

The following command disables beacon recovery on backplane network token_ring_1:

```
CB5000> set network token_ring token_ring_1 bcn_recovery disable
Beacon Recovery set to DISABLED.
```

Related Command

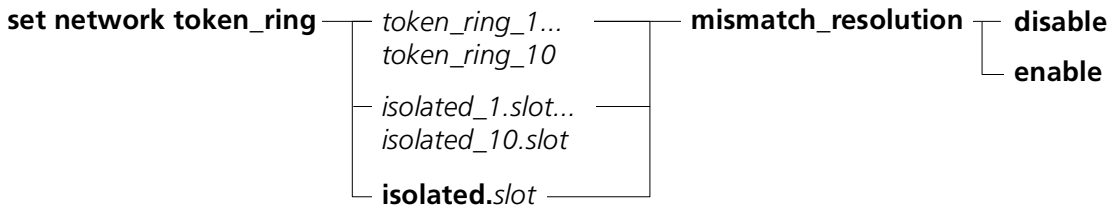
SHOW MODULE

SET NETWORK TOKEN_RING MISMATCH_ RESOLUTION

Use the SET NETWORK TOKEN_RING MISMATCH_RESOLUTION command to allow CoreBuilder 5000 Token Ring Passive Media Modules to perform address-to-port mapping when splitters and fan-out devices are used.

Mismatch resolution performs address-to-port mapping when you use a splitter or fan-out device on a CoreBuilder 5000 Token Ring port. The SET NETWORK TOKEN_RING MISMATCH_RESOLUTION command enables or disables the mismatch resolution algorithm on the media cards for the specified network. This setting is saved automatically, and is not affected by the SAVE or REVERT commands.

Format



slot	Identifies the module for this operation for isolated networks.
disable	Disables mismatch resolution. Media cards do not attempt to resolve the mapping to the port level
enable	Enables mismatch resolution. Media cards attempt address-to-port mapping

Example

The following command enables the mismatch resolution mechanism on backplane network token_ring_3:

```
CB5000> set network token_ring token_ring_3 mismatch_resolution
enable
Value set to ENABLED.
```

Related Command

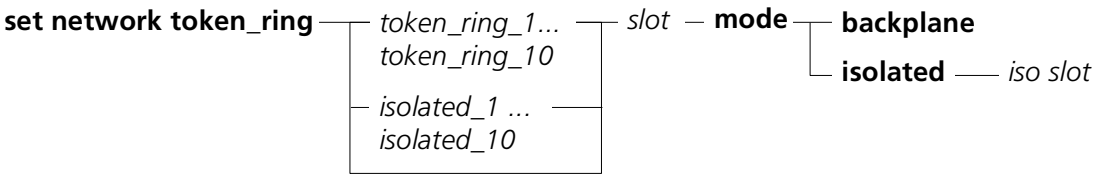
SHOW RING_MAP

SET NETWORK TOKEN_RING MODE

Use the SET NETWORK TOKEN_RING MODE command to toggle entire rings between isolated (module-level) and backplane (hub-wide) Token Ring networks. This command is valid for port-switched modules only. This setting is saved automatically, and is not affected by the SAVE or REVERT commands. The command affects only the specified slot and cannot be used to isolate every module in the hub.

You can implement each of the 10 available token rings on 3Com CoreBuilder 5000 port-switching media modules either on a backplane (hub-wide) or an isolated (module-level) network. Use this command to toggle sets of ports between backplane and isolated. You may toggle only rings 1 through 10.

Format



slot	Identifies the module for this operation.
iso slot	Identifies the isolated network the command affects.

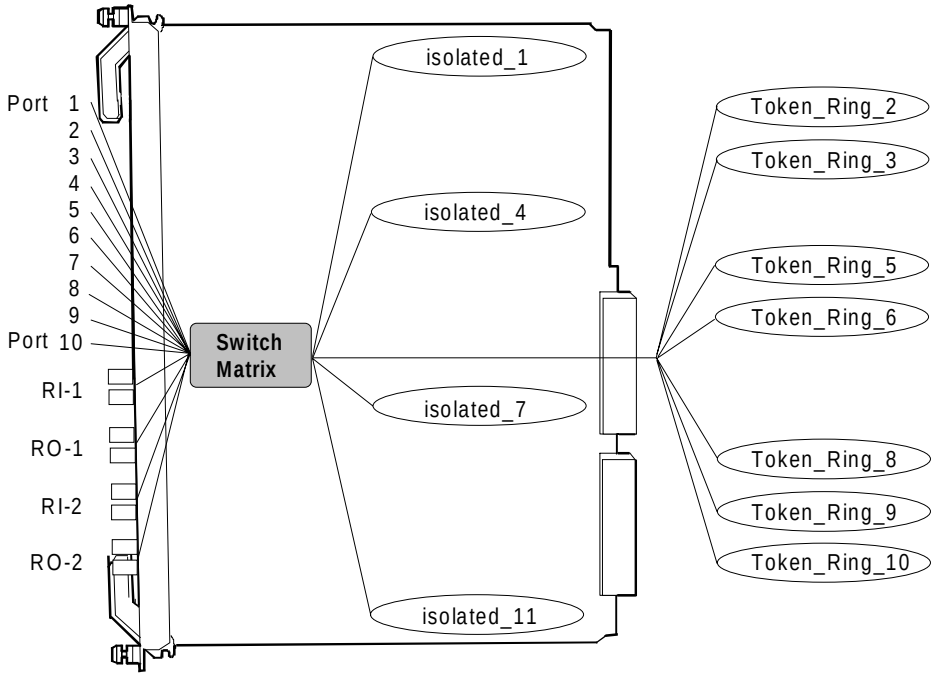
Example 1 The following command assigns all ports assigned to isolated_3 (module-level ring) in module 7 to token_ring_3 (backplane ring):

```
CB5000> set network token_ring isolated_3 7 mode backplane
Network mode set to BACKPLANE.
```

Example 2 The following command assigns all ports from slot 7 that are assigned to token_ring_3 (backplane ring) to isolated_3 (module-level ring) in module 7:

```
CB5000> set network token_ring token_ring_3 mode isolated 7
Network mode set to ISOLATED.
```

If you entered the command shown in the examples, all ports assigned to network isolated_3 join backplane network token_ring_3, as shown in the figure that follows.



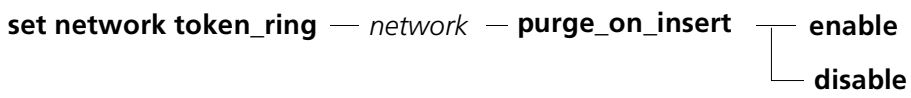
Related Commands SET MODULE NETWORK
SET PORT NETWORK
SHOW BACKPLANE_PATHS

SET NETWORK TOKEN_ RING PURGE_ON_INSERT

Use the SET NETWORK TOKEN_RING PURGE_ON_INSERT command to enable or disable the purge_on insert feature for Token Ring modules *only*.

Whenever a station is inserted into the ring (by plugging it into one of the ports on a TR module), a Ring Purge frame is sent out onto the ring for notification. A ring purge frame will always be generated when a station is inserted into a ring.

Format



network	Identifies the network for this operation: ■ token_ring_1 through token_ring_10 ■ isolated slot ■ isolated_1 slot through isolated _11 slot
enable	Enables the purge_on insert feature. Enable is the default value.
disable	Disables the purge_on insert feature.

Example

The following command disables the purge_on_insert feature on backplane network token_ring_1:

```
CB5000> set network token_ring token_ring_1 purge_on_insert disable
Purge on insert set to enable.
```

Related Command

SHOW NETWORK

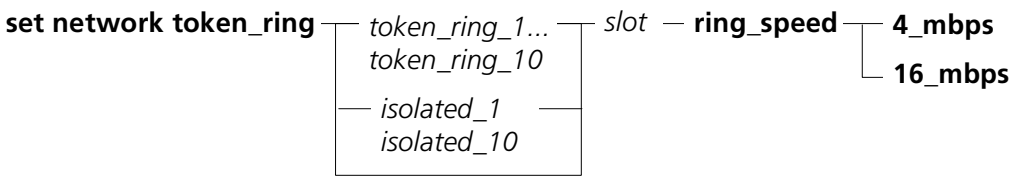
SET NETWORK TOKEN_RING RING_SPEED

Use the SET NETWORK TOKEN_RING RING_SPEED command to set the ring speed for any CoreBuilder 5000 Token Ring backplane (hub-wide) or isolated (module-level) network. Any module, port, trunk, or daughtercard assigned to the network is set automatically to the speed of the network.

This setting is saved automatically, and is not affected by the SAVE or REVERT commands.

When DIP configuration is enabled, and there is a conflict between the ring speed DIP settings on different modules set to the same network, there is no way to determine which speed will be selected. This is because the DMM controls network speed resolution.

Format



slot	Identifies the module for this operation.
4_mbps	Sets the ring speed to 4 Mbps.
16_mbps	Sets the ring speed to 16 Mbps.

Example

The following command sets the ring speed for backplane network token_ring_4 to 16 Mbps:

```
CB5000> set network token_ring token_ring_4 ring_speed 16_mbps
Value set to 16 MBPS.
```

Related Commands

SET MODULE RING_SPEED
SHOW MODULE

SET PORT ACTIVE_CONNECTOR

Use the SET PORT ACTIVE_CONNECTOR command to activate the correct connector on the front panel of the ONline Token Ring Bridge Module. Choose the connector according to the media (UTP or STP) you are using.

The setting for this command is saved automatically after you enter the command.

It is not necessary to issue the SAVE command. Consequently, the REVERT command cannot be used. You must reenter the SET command to change the setting.

Format

slot.**2**	The slot (1 through 17) and port (the port is always 2) to which you are issuing this command.
db9	Selects the DB-9 connector. This is the default setting. Shielded twisted pair (STP) cable attaches using a DB-9 connector.
rj45	Selects the RJ-45 connector. Unshielded twisted pair (UTP) cable attaches using an RJ-45 connector.

Example

The following command assumes the Token Ring Bridge Module in slot 11 is using unshielded twisted pair cable. In this case, set the port 2 connector to RJ-45.

```
CB5000> set port 11.2 active_connector rj45
Port 11.02 active connector set to RJ45.
```

Related Command

SHOW MODULE

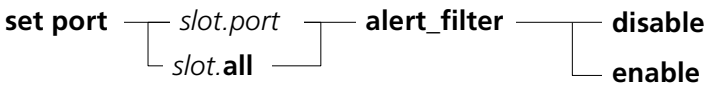
SET PORT ALERT_FILTER

Use the SET PORT ALERT_FILTER command to enable or disable filtering of port up/down trap generation for a specific port. This command works in conjunction with the SET ALERT PORT_UP_DOWN FILTER command. The order in which you enter these two commands does not matter.

After the PORT ALERT_FILTER has been set for a port, you must enter the SET ALERT PORT_UP_DOWN FILTER command to filter or not filter port up and port down traps on a per port basis, to be transmitted from the DMM to the designated trap receiver.

If the filter is enabled, no traps are generated. If the filter is disabled, traps are generated.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number on the specified module. For example, to identify port 4 on the 6, enter **6.4**
slot.**all**	Specifies that all ports in the module are affected by this operation.
disable	Disables filtering of port_up_down traps for the identified port. The factory setting is disabled.
enable	Enables filtering of port_up_down traps for the identified port.

Example

The following command enables port_up_down traps for port 2 on the module in slot 6:

```
CB5000> set port 6.2 alert_filter enable
Port 06.02 Alert Filter set to ENABLED.
```

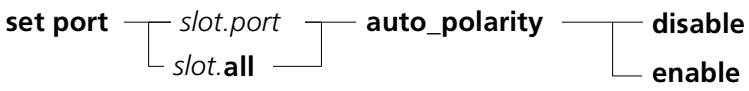
Related Commands

SET ALERT
SHOW ALERT

SET PORT AUTO_POLARITY

Use the SET PORT AUTO_POLARITY command to instruct the 3Com CoreBuilder 5000 24-Port 10BASE-T Module and CoreBuilder 5000 Ethernet modules to automatically switch the polarity of twisted-pair cabling.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables auto polarity.
enable	Enables auto polarity. Auto polarity enables the module to automatically switch the polarity of twisted-pair cabling. If, for instance, you erroneously reverse the polarity of some twisted-pair cabling while assembling it, auto polarity enables you to automatically detect this problem and reverse the polarity.

Example

The following command enables auto polarity on port 1 of the CoreBuilder 5000 24-Port 10BASE-T Module in slot 1:

```
CB5000> set port 1.1 auto_polarity enable
Port 01.01 Auto Polarity set to ENABLE.
```

Related Command

SHOW PORT

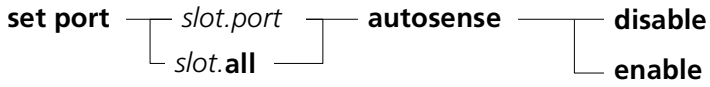
SET PORT AUTOSENSE

Use the SET PORT AUTOSENSE command to enable or disable the automatic sensing feature. This command applies to the CoreBuilder 5000 EtherFlex Module (Model Number 6104M-MOD) with a 10BASE-FB/FL I/O Card.

The autosense feature automatically determines the protocol (FB or FL) being used on the network.

If autosensing is enabled, the protocol running on the port is shown by the media sense field of the SHOW MODULE command, and not the media configuration field.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Specifies that all ports on the module are affected by this operation.
disable	Disables the automatic sensing feature. When it is disabled, the media configuration field shows whether the port is using FB or FL protocol.
enable	Enables the automatic sensing feature. When it is enabled, the media sense field shows whether the port is using the FB or FL protocol. The FB/FL chip on the Fiber I/O card uses the media module sense to determine the protocol on the line (either FB or FL).

Example

The following command enables the autosensing feature on all ports on the Etherflex module located in slot 1:

```
CB5000> set port 1.all autosense enable
AUTOSENSE mode set to ENABLE.
```

Related Command

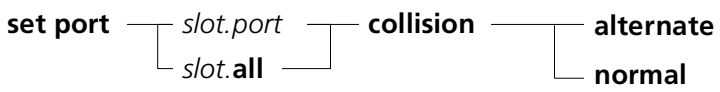
SHOW PORT

SET PORT COLLISION

Use the SET PORT COLLISION command to establish if normal or alternate collision mode is used for that port on the ONline Ethernet Transceiver Module.

Refer to the *ONline Ethernet Transceiver Module Installation Guide* for more information on collision mode and the Ethernet Transceiver module.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 3) is the port number on the specified module. For example, to identify port 3 on the module in slot 6, enter **6.3**
slot.**all**	Specifies that all ports on the module are affected by this operation.
alternate	Specifies alternate mode. Used primarily with non-IEEE 802.3 devices.
normal	Specifies normal mode. Default setting, used primarily with IEEE 802.3 devices and repeaters.

Example

The following command sets port 3 in slot 6 to normal collision mode:

```
CB5000> set port 6.3 collision normal
Collision set to NORMAL.
```

Related Command

SHOW PORT

SET PORT FAN_OUT_MODE

Use the SET PORT FAN_OUT_MODE command to make a CoreBuilder 5000 Token Ring port compatible with fan-out devices such as the IBM 8228. The fan-out function allows multiple stations to attach to a single port.

This feature requires that you have loaded Token Ring Media Module code Version v1.2 or later.

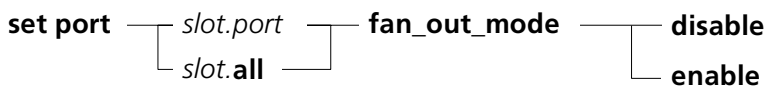
This feature is required because not all fan-out devices assert phantom (phantom indicates the presence of a station). When fan-out mode is disabled (the default), CoreBuilder 5000 Token Ring ports automatically wrap and unwrap based on the detection of phantom. In this mode, a fan-out device requires an adapter to assert phantom before it is allowed to insert into the ring. When fan-out mode is enabled, the port unwraps regardless of the presence of phantom.

CAUTION: *Enabling fan-out mode with no station or fan-out device attached breaks the ring and causes beaconing. This problem must be avoided because beacon recovery briefly disrupts all users on the ring.*

Because phantom is ignored when fan-out mode is enabled, the only way to clear a BEACON_WRAP or WRONG_SPEED condition when a port is in fan-out mode is to disable, then reenable the port. Ring speed detection does not operate when a port is in fan-out mode. Beacon recovery wraps fan-out devices that contain wrong speed stations.

When you disable a port, fan-out mode is automatically disabled. This forces you to explicitly enable fan-out mode when you reenable the port. This extra step helps prevent you from enabling fan-out mode with no device attached.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 24) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables fan-out mode for the identified port. The factory setting is all ports disabled.
enable	Enables fan-out mode for the identified port.

Example

The following command disables fan-out mode on port 6.2:

```
CB5000> set port 6.2 fan_out_mode disable
Port 06.02 fan_out_mode set to DISABLED.
```

Related Commands

SET PORT NETWORK
SHOW PORT

SET PORT FORCE_ CONFIGURATION

Use the SET PORT FORCE_CONFIGURATION command to force a network to use fiber backbone (FB) or fiber link (FL) signaling. This command applies to the CoreBuilder 5000 EtherFlex Module (Model Number 6104M-MOD) with a 10BASE-FB/FL I/O Card.

Because the Ethernet fiber ports in your configuration can be FB or FL, this command allows your network to be compatible with your existing equipment.

Format

slot.port	Identifies the port for this operation. slot (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
fb_mode	Enables fiber backbone mode.
fl_mode	Enables fiber link mode.

Example

The following command forces the network to use fiber backbone signaling for port 1 in slot 3.1:

```
CB5000> set port 3.1 force_configuration fb_mode
```

Related Command

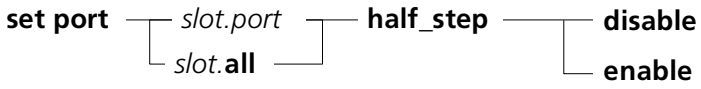
SHOW PORT

SET PORT HALF_STEP

Use the SET PORT HALF_STEP command to establish if half-step or full-step mode is used for that port on the ONline Ethernet Transceiver Module.

Refer to the *ONline Ethernet Transceiver Module Installation Guide* for more information on half-step mode and the Ethernet Transceiver Module.

Format



slot.port	Identifies the port for this operation. slot (1 through 17) is the slot number location of a module in the hub and *port* (1 through 3) is the port number on the specified module. For example, to identify port 3 on the module in slot 6, enter **6.3**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables half-step signaling. Full-step signaling is used instead. Full-step signaling is used primarily with non-IEEE 802.3 and earlier Ethernet devices.
enable	Enables half-step signaling. Half-step signaling is used primarily with IEEE 802.3 and Ethernet Version 2.0 devices and repeaters. This is the default setting.

Example

The following command sets port 2 in slot 7 to full-step mode:

```
CB5000> set port 7.2 half_step disable
Half_step set to DISABLED.
```

Related Command

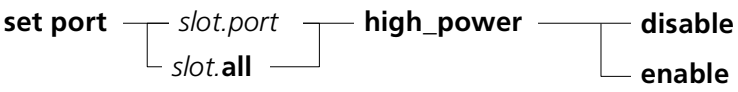
SHOW PORT

SET PORT HIGH_POWER

Use the SET PORT HIGH_POWER command to enable or disable a port from receiving or transmitting at high power. This command pertains to ONline Ethernet Port-Switching Fiber Modules (Model Numbers 5102M-FP and 5104M-FP) only.

This command allows you to increase the distance between connections by setting both ends of the link to high power. You must set this port to normal power (high_power disabled) to connect to certain ORnet fiber products (Model Numbers 9301T, 9308, 9314, and 9301A).

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 3) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables receiving or transmitting at high power.
enable	Enables receiving or transmitting at high power.

Example

The following command enables high power on port 1 on the module in slot 5:

```
CB5000> set port 5.1 high_power enable
High power optics ENABLED.
```

Related Command

SHOW PORT

SET PORT LINK_INTEGRITY

Use the SET PORT LINK_INTEGRITY command to enable or disable link integrity for ports on Ethernet 10BASE-T Modules.

In general, enable link integrity for all ports on your 10BASE-T module as stated in the 10BASE-T standard. You must disable link integrity to connect to older non-10BASE-T equipment.

Not all pre-10BASE-T equipment works with link integrity enabled.

You must enable or disable link integrity at both ends of the connection. If the settings at each end of the connection differ, the port with link integrity enabled reports a link integrity error.

Format

slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 4) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter 6.4.
slot.**all**	Specifies that all ports in the slot are affected by this operation.
disable	Disables link integrity.
enable	Enables link integrity.

Example

The following command enables link integrity on port 1 of the 10BASE-T module in slot 5:

```
CB5000> set port 5.1 link_integrity enable
Link integrity set to ENABLED.
```

Related Command

SHOW PORT

SET PORT LOW_LIGHT_WARNING

Use the SET PORT LOW_LIGHT_WARNING command to enable a warning that is displayed when the light level received is weak. This command pertains to ONline Ethernet Port-Switching Fiber Modules (Model Numbers 5102M-FP and 5104M-FP) only.

A low light condition does not affect network operation. Enable low light detection during system setup to see if any fiber connections are close to reaching their distance limits. If they are, the status LED on the Ethernet Fiber Module blinks six times to indicate the condition, and the status is reported to the DMM.

You can disable the low light detection if you are aware that the light level is low, but prefer not to have a blinking status indicator signaling the condition.

If you have enabled redundant ports on the ONline Ethernet Fiber Modules (Model Number 5104M-FIB), disabling low light warning allows the module to switch over to the backup port more quickly when the primary port fails.

Format

slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 4) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables low light warning.
enable	Enables low light warning.

Example

The following command enables the low light warning on port 1 of the module in slot 12:

```
CB5000> set port 12.1 low_light_warning enable
Low light warning set to ENABLED.
```

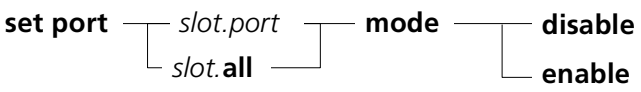
Related Commands

SHOW PORT
SET PORT HIGH_POWER

SET PORT MODE

Use the SET PORT MODE command to turn ports on or off.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies that all ports on the module are affected by this operation.
disable	Disables the identified port.
enable	Enables the identified port. The factory setting is all ports enabled.

Example

The following command disables (turns off) port 2 on the module in slot 6:

```
CB5000> set port 6.2 mode disable
Port 06.02 set to DISABLED.
```

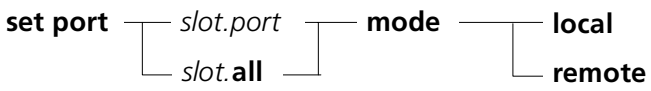
Related Commands

SET PORT NETWORK
SHOW PORT

SET PORT MODE LOCAL/REMOTE

Use the SET PORT MODE LOCAL or REMOTE command to set an ONline Terminal Server port to local or remote access.

Format



slot.port	Selects a port for local or remote access. *slot* (1 through 17) is the number location of a module in the hub and *port* (1 through 32) is the port number on the specified module. For example, to specify port 4 on the module with ID 6, enter **6.4**
slot.**all**	Selects a module for local or remote access. For example, to specify all ports on the module with slot ID 6, enter **6.all**
local	Selects local access. Connections can be made to the server through this port (for example, terminals). This is the default setting.
remote	Selects remote access. Connections can be made from the server to an external device (for example, dial-out modems).

Example

The following command sets port 2 in slot 6 to local access. Connections can be made to the server through this port.

```
CB5000> set port 6.2 mode local
Port 6.02 set to LOCAL.
```

Related Command

SHOW PORT

SET PORT MODE REDUNDANT/ NON_REDUNDANT

Use the SET PORT MODE REDUNDANT or NON_REDUNDANT command to establish redundancy between two ports on 10BASE-T modules or 100BASE-TX Workgroup FastModules.

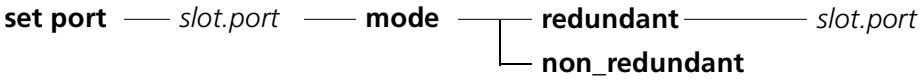
Initiating redundancy on ONline modules can cause a network loop in the unlikely event that:

- *Both the management module and the power fail concurrently*
- *Ports of both the primary and redundant links are enabled using DIP switches*

To prevent a potential network loop, disable either the primary or backup port through the DIP switch settings, then use the SET PORT MODE command to enable that port. This looping problem does not occur with CoreBuilder 5000 media modules.

When setting redundancy, you can configure a 100BASE-TX to be compatible with a 10BASE-T.

Format



slot.port	Selects a port for redundant or non-redundant mode. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to specify port 4 in slot 6, enter **6.4**
non_redundant	Selects non_redundant mode. When you remove port redundancy, you do not need to indicate the second *slot.port*. Using this command on any port in redundant mode removes that port from the redundancy relationship.
redundant	Selects redundant mode. When you enter the SET PORT MODE REDUNDANT command for two ports, the first port in the command line becomes the primary link, and the second port becomes the backup or redundant link. If the primary link fails, the redundant link is activated automatically, thereby preventing a network failure.

Example

The following command establishes port 1 in slot 6 as the primary port and port 3 in slot 6 as the backup port:

```
CB5000> set port 6.1 mode redundant 6.3
Port 06.01 set to REDUNDANT PRIMARY.Port 06.03 set to REDUNDANT
BACKUP.
```

Related Command

SHOW PORT

SET PORT MODE DIAGNOSTICS

Use the SET PORT MODE REMOTE_DIAGNOSTICS/NON_REMOTE_DIAGNOSTICS command to establish remote diagnostics on a port. Remote diagnostics allow the port to detect failures on both its transmits and receive wire pairs. Use this command when you are connecting two ports on 10BASE-T and 100BASE-T modules to a Fault-Tolerant 10BASE-T Transceiver Module (Model Number 5102T-TPFT) or establishing remote diagnostics on CoreBuilder 5000 24-Port, 20-Port, 40-Port, and 36-Port Modules and the EtherFlex Module.

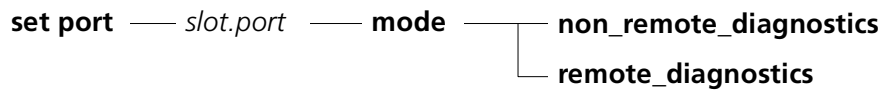
This command is most useful when you also have redundant ports set up to the transceiver. When you establish remote diagnostics and redundancy between two ports:

1. The first port becomes the primary link while the second port becomes the backup or redundant link.
2. If the primary link fails, the redundant link is activated automatically, thereby preventing a network failure.

The cross-module redundancy feature enables you to set ports in different modules as redundant pairs. For example, you can use a port in one 10BASE-T module as a primary link and a 10BASE-T port in another module as the backup link.

You must have link integrity enabled on both ports on the transceiver and on both ports on the module for this command to work correctly.

Format



slot.port	*slot* (1 through 17) is the and *port* (1 through 40) is the port number on the specified module. For example, to specify port 4 on the slot with slot ID 6, enter **6.4**
non_remote_diagnostics	Remote diagnostics disabled. Use this mode when there is not a remote diagnostics-capable device at the far end of the connection
remote_diagnostics	Remote diagnostics enabled. Use this option when there is a remote diagnostics-capable device at the other end of the connection.

Example

The following command establishes remote diagnostics on port 5 in slot 16:

```
CB5000> set port 16.5 mode remote_diagnostics
Port 16.05 REMOTE DIAGNOSTICS ENABLED.
```

Related Command

SHOW PORT

SET PORT MODE REMOTE_FAILURE_ SIGNALING

Use the SET PORT MODE REMOTE_FAILURE_SIGNALING command to establish Remote Failure Signaling on redundant fiber links.

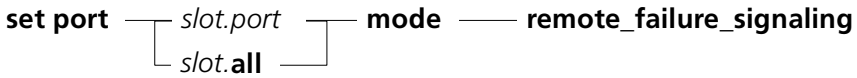
You can enable Remote Failure Signaling (RFS) for any of the four ports on the ONline FOIRL and 10BASE-FL modules. When you connect two FOIRL Modules and enable redundancy between two ports on one of the modules, you must enable RFS on the corresponding ports of the other module.

For example, if you:

- Enable redundancy between ports 1 and 2 on FOIRL Module #1 and these ports are connected to ports 1 and 2 on Module #2, you must enable RFS on ports 1 and 2 on Module #2.
- Disable redundancy on the corresponding port or disable the port itself, RFS disables automatically.

Refer to the ONline Ethernet FOIRL Module Installation Guide *for more information on RFS mode and the ONline Ethernet FOIRL and 10BASE-FL modules.*

Format



slot.port	Selects a port for remote failure signaling mode. *slot* (1 through 17) is the number location of a module in the hub and *port* (1 through 4) is the port number on the specified module. For example, to specify port 4 on the with ID 6, enter **6.4**
slot.**all**	Selects a slot for remote failure signaling mode. For example, to specify all ports on the slot with slot ID 6, enter **6.all**

Example

The following command establishes Remote Failure Signaling for port 3 in slot 9:

```
CB5000> set port 9.3 mode remote_failure_signaling
Port 09.03 set to REMOTE FAILURE SIGNALING.
```

Related Command

SHOW PORT

SET PORT MODE SHUTDOWN

Use the SET PORT MODE SHUTDOWN command to test fault detection at the remote end of a link.

This command applies to the following modules:

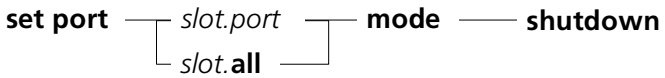
- CoreBuilder 5000 100BASE-TX Workgroup FastModule (Model Number 6512M-TX)
- CoreBuilder 5000 Ethernet 10BASE-FB Module (Model Number 6110M-FBP)
- CoreBuilder 5000 EtherFlex Module (Model Number 6104M-MOD)
- CoreBuilder 5000 10BASE-T 20-Port and 40-Port Modules (Model Numbers 6120M-TPP and 6140M-TPP)
- CoreBuilder 5000 10BASE-T 36-Port Module (Model Number 6136M-TP)

The SET PORT MODE SHUTDOWN command causes the port at the remote end of its link to lose its diagnostic signaling and therefore detect a fault.

When you place a port in shutdown mode, the port is disabled and the following occurs:

- For twisted-pair ports, link integrity is disabled
- For fiber ports, diagnostic light signaling over the link is disabled

Format



slot.port	Selects a port for shutdown mode. *slot* (1 through 17) is the slot number location of a module in the hub and *port* is the port number on the specified module. For example, to specify port 4 on the with ID 6, enter **`6.4`**
slot.**all**	Selects a module for shutdown mode. For example, to specify all ports on the module with slot ID 6, enter **`6.all`**

Example

The following command shuts down port 3 in slot 2:

```
CB5000> set port 3.2 mode shutdown
```

Related Commands

SHOW PORT
SET PORT NETWORK

SET PORT NETWORK

Use the SET PORT NETWORK command to assign a port to a specific network. This command applies to 3Com modules that support port-switching.

You may either:

- Assign each port to one of the selected networks that are available for the module type (Token Ring, Ethernet, or FDDI)
- Isolate the port

Ports assigned to:

- The same network form a segment (that is, they are on the same network).
- Different networks are on different segments and cannot communicate unless you bridge the networks. Each isolated port joins traffic from all other ports on the same isolated (module-level) network.

All Ethernet modules are factory-set through the DIP switches or non-volatile RAM so that the ports are assigned to channel 1 (Ethernet network 1). Change the DIP switch setting only if your hub is without a management module.

This command applies only to 3Com modules that have individual ports that are network-selectable. For modules that are network-selectable per module, refer to the SET MODULE NETWORK command.

Format

slot.port	Selects the port to assign to a network. *slot* (1 through 17) is the number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to specify port 4 on the with ID 6, enter **6.4**
slot.**all**	Selects a module to assign to a network. For example, to specify all ports on the module with slot ID 6, enter **6.all**
network	Specifies the network to which you are assigning the port. For example, ethernet_2.

Example 1 The following command sets port 2 on the module in slot 5 to network Ethernet 1:

```
CB5000> set port 5.2 network ethernet_1
Port 05.02 network id set to ETHERNET_1
```

Example 2 The following command sets port 1 on the ONline Ethernet Bridge Module in slot 7 to the AUI port on the front panel:

```
ONline> set port 7.1 network front_panel
Port 07.01 network id set to FRONT_PANEL
```

Example 3 The following command sets both ports on the ONline Ethernet Repeater Module in slot 4 to network Ethernet 2:

```
CB5000> set port 4.all network ethernet_2
Port 04.01 network id set to ETHERNET_2
Port 04.02 network id set to ETHERNET_2
```

Related Commands SHOW PORT
SHOW BACKPLANE_PATHS

SET PORT PERSONALITY

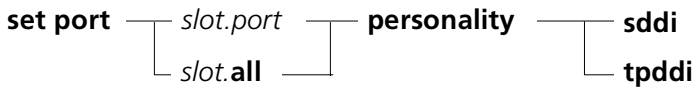
Use the SET PORT PERSONALITY command to designate the transmission mode for a port on the ONline FDDI Shielded Twisted Pair Module.

The FDDI STP Module:

- Supports both the SDDI and TPDDI standards for running FDDI on shielded twisted pair cable
- Allows you to designate whether the port transmits data using either SDDI or TPDDI signaling mode
- Allows you to connect the module to any vendor's device that supports either of the two standards

All ports default to SDDI mode when you first install the FDDI STP Module. You must use SDDI ports 1 and 2 on the FDDI Shielded Twisted Pair Module to configure SDDI ports as S-type ports.

Format



slot.port	Selects a port for personality setting. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 8) is the port number on the specified module. For example, to specify port 4 on the module with slot ID 6, enter **6.4**
slot.**all**	Selects a slot for personality setting. For example, to specify all ports on the module with slot ID 6, enter **6.all**
sddi	Specifies SDDI signaling mode. This is the default.
tpddi	Specifies TPDDI signaling mode.

Example

The following command sets SDDI as the transmission mode for port 2 of the FDDI Shielded Twisted Pair Module in slot 8:

```
CB5000> set port 8.2 personality sddi
Port Personality set to sddi.
```

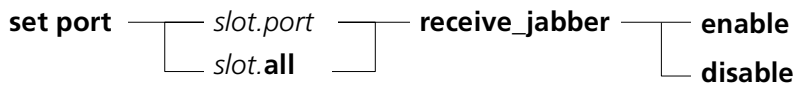
Related Command

SHOW PORT

SET PORT RECEIVE_JABBER

Use the SET PORT RECEIVE_JABBER command to enable or disable Receive Jabber for a port on the 3Com ONline Ethernet 50-Pin Module.

Format



slot.port	Selects a port for receiving jabber. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 12) is the port number on the specified module. For example, to specify port 4 on the module with slot ID 6, enter **6.4**
slot.**all**	Selects a module for receiving jabber. For example, to specify all ports on the module with slot ID 6, enter **6.all**
enable	Enables receiving jabber. When enabled, if a jabber condition occurs and the transceiver or repeater device fails to halt it, Receive Jabber protects the network by disconnecting the link after 10 msecs. Refer to the *Ethernet 50-Pin Module Installation Guide* for more information on Receive Jabber mode and the Ethernet 50-Pin Module.
disable	Disables receiving jabber. This is the default. Receive Jabber is set to a default of disabled to conform to the 10BASE-T standard.

Example

The following command enables Receive Jabber for port 2 in slot 12:

```
CB5000> set port 12.2 receive_jabber enable
Receive Jabber on Port 12.02 set to ENABLED.
```

Related Command

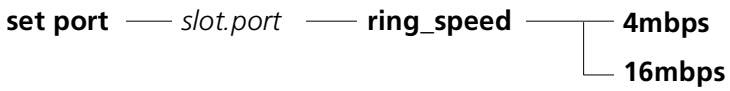
SHOW PORT

SET PORT RING_SPEED

Use the SET PORT RING_SPEED command to set either port on the ONline Token Ring Bridge Module to operate at a transmission rate of 4 Mbps or 16 Mbps, depending on the network ring speed.

This command enables you to set port 1 (backplane) or port 2 (front panel) on the Token Ring Bridge Module to a transmission rate of 4 Mbps or 16 Mbps. The DMM saves the setting for this command automatically. It is not necessary to enter the SAVE command. Consequently, the REVERT command does not affect the command setting. To change the setting, you must reenter the SET command.

Format



slot.port	Selects a port for ring speed setting. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 or 2) is the port number on the specified module. For example, to specify port 2 on the module with slot ID 6, enter **6.2**
4mbps	Sets the ring speed on the port to 4 Mbps.
16mbps	Sets the ring speed on the port to 16 Mbps.

Example

The following command sets port 1 of the Token Ring Bridge Module in slot 5 to 16 Mbps ring speed:

```
CB5000> set port 5.1 ring_speed 16mbps
Port 05.01 ring speed set to 16mbps.
```

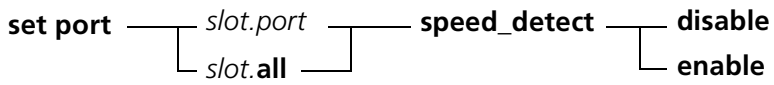
Related Command

SET NETWORK TOKEN_RING RING_SPEED

SET PORT SPEED_DETECT

Use the SET PORT SPEED_DETECT command to enable speed detection for a CoreBuilder 5000 Token Ring port. This command prevents stations from inserting on the ring at an incorrect ring speed.

Format



slot.port	Selects a port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number on the specified module. For example, to specify port 4 on the module with slot ID 6, enter **6.4**
slot.**all**	Selects a slot for enabling speed detection. For example, to specify all ports on the module with slot ID 6, enter **6.all**
disable	Disables speed detection for the identified port. The factory setting is speed detection disabled.
enable	Enables speed detection for the identified port.

Example

The following command disables speed detection for port 2 on hub 1:

```
CB5000> set port 1.2 speed_detect disable
Port 01.02 Speed Detection set to DISABLED.
```

Related Commands

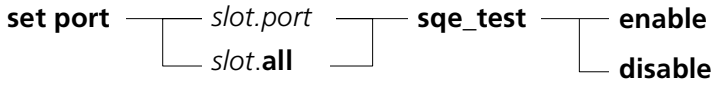
SAVE PORT
SHOW PORT

SET PORT SQE_TEST

Use the SET PORT SQE_TEST command to establish if SQE Test is enabled or disabled for ports on the ONline Ethernet Transceiver Module.

Refer to the ONline Ethernet Transceiver Module Installation Guide *for more information on SQE Test mode and the Ethernet Transceiver Module.*

Format



slot.port	Selects a port for SQE test mode setting. *slot* (1 through 17) is the slot nubmer location of the module in the hub and *port* (1 through 3) is the port number on the specified module. For example, to specify port 3 on the module with slot ID 6, enter **`6.3`**
slot.**all**	Selects a slot for SQE test mode setting. For example, to specify all ports on the module with slot ID 6, enter **`6.all`**
enable	Enables SQE test mode. You can connect this port to most devices, except repeaters. This is the default.
disable	Disables SQE test mode. You can connect this port to baseband Repeaters and Multiport Transceivers.

Example

The following command enables SQE Test for port 1 in slot 8:

```
CB5000> set port 8.1 sqe_test enable
SQE_test on Port 08.01 set to ENABLED.
```

Related Commands

SAVE MODULE_PORT
SHOW PORT

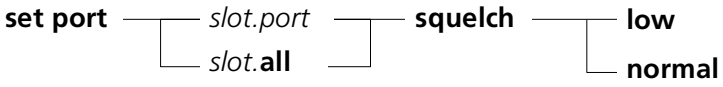
SET PORT SQUELCH

Use the SET PORT SQUELCH command to establish Squelch Mode as either normal or low for ports on Ethernet 10BASE-T Modules. The squelch level is factory set to NORMAL to conform to the 10BASE-T standard.

In general, 3Com recommends using normal squelch. Ensure the squelch level at both ends of the link matches. If you change the squelch level at the module, you must change the squelch setting at the transceiver also.

If your network experiences too many illegally short packets (runts) in low squelch mode, change the setting back to NORMAL.

Format



slot.port	Selects a port for squelch mode setting. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to specify port 4 on themodule with slot ID 6, enter **6.4**
slot.**all**	Selects a slot for squelch mode setting. For example, to specify all ports on the module with slot ID 6, enter **6.all**
low	Sets squelch mode to low (sensitive). Ports are able to receive weaker signals, allowing longer link distances. Increases the achievable link distance, but with the added risk of losing packets to impulse noise.
normal	Sets squelch mode to normal. Ports receive signals compliant with the 10 BASE-T standard.

Example

The following command sets port 1 in slot 5 to a low squelch level:

```
CB5000> set port 5.1 squelch low
Squelch set to LOW.
```

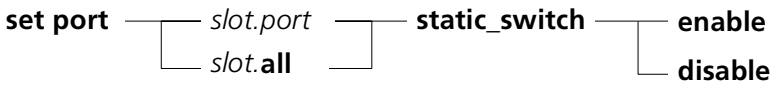
Related Commands

SAVE MODULE_PORT
SHOW PORT

SET PORT STATIC_SWITCH

Use the SET PORT STATIC_SWITCH to force CoreBuilder 5000 Token Ring users to power off a station before switching rings. Use this command to prevent ports from being switched from one ring to another when there is a phantom present. This command works only for port-switched CoreBuilder 5000 Token Ring modules.

Format



slot.port	Selects a port for static switch. *slot* (1 through 17) is the slot number location on a module in the hub and *port* (1 through 24) is the port number on the specified module. For example, to specify port 4 on the module with slot ID 6, enter **`6.4`**
slot.**all**	Selects a slot for static switch. For example, to specify all ports on the module with slot ID 6, enter **`6.all`**
enable	Forces users to power stations down before switching networks. This forces the station to perform a duplicate address test before entering a new ring.
disable	Does not force users to power stations off before switching networks.

Example

The following command disables static switch on port 2 on the module in slot 6:

```
CB5000> set port 6.2 static_switch disable
Port 6.02 static switch set to DISABLED.
```

Related Commands

SAVE MODULE_PORT
SET TRUNK STATIC_SWITCH
SHOW PORT

SET PORT STATION_TYPE

Use the SET PORT STATION_TYPE command to designate a station that does not have a MAC address (for example, a network analyzer). This command applies to ONline System Concentrator Token Ring modules only.

Stations that assert a phantom signal but do not have a MAC address cause problems in the DMM mapping algorithm. To prevent this problem, set the station_type parameter to MAC_NOT_PRESENT. This eliminates the stations from the mapping algorithms running on a DMM. Failure to designate a MAC-less station can cause incorrect mapping.

Security settings configured for a port are bypassed when you set the port to a station type of MAC_NOT_PRESENT.

Format

slot.port	Selects a port for setting station type. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number For example, to specify port 4 on the module with slot ID 6, enter **6.4**
slot.**all**	Selects a slot for setting station type. For example, to specify all ports on the module with slot ID 6, enter **6.all**
mac_not_present	Specifies that the station the port is attached to does not have a MAC address.
mac_present	Specifies that the station the port is attached to has a MAC address. This is the default.

Example

The following command informs port 6 on the module in slot 3 that the station the port is attached to does not have a MAC address:

```
CB5000> set port 3.6 station_type mac_not_present
Station type set to MAC_NOT_PRESENT
```

Related Command

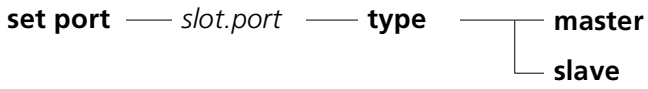
SHOW PORT

SET PORT TYPE

Use the SET PORT TYPE command to define ports on any ONline FDDI Media Module as master or slave ports. All FDDI Media Module ports default to a Type M (master). Ports 1 and 2 can, however, be designated as Type S (slave) ports. Designate your S ports before enabling the ports on the module.

Ports 3 through 8 operate only as Type M ports. Therefore, the SET PORT TYPE command is not available for ports 3 through 8. Refer to the appropriate FDDI module documentation for information on Type M and Type S ports.

Format



slot.port	Selects a port to define as master or slave. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 8) is the port number on the specified module. For example, to specify port 2 on the module with slot ID 6, enter **6.2**
master	Specifies the port as the primary communication port. This is the default.
slave	Specifies that the port runs as a backup to the master port in redundant configurations. Used when a cable failure could take down an entire network.

Example

The following command sets port 1 in slot 7 to be a slave port:

```
CB5000> set port 7.1 type slave
Type set to SLAVE.
```

Related Commands

SHOW PORT
SET PORT PERSONALITY

SET POWER MODE

Use the SET POWER MODE command to choose between normal and fault-tolerant power supply operation using the CoreBuilder 5000 hub intelligent power management system.

For example:

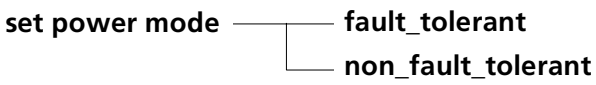
- Each power supply provides approximately 200 watts at +5 Volts
- You have three power supplies available (approximately 600 watts)

In this scenario, non-fault tolerant mode allows you to use approximately 600 watts. Fault-tolerant mode allows you to use approximately 400 watts, reserving approximately 200 watts to use in the event of a failure.

Regardless of the power mode setting, the power load being used is shared across all installed power supplies.

Refer to documentation for your power supply to determine the power supply's maximum power output.

Format



fault_tolerant	Power Management calculations hold a power supply's worth of power in reserve, so that there is still enough power available if a power supply fails. To use fault-tolerant mode, you must have one more power supply than is required to power all modules in the hub.
non_fault_tolerant	Power Management calculations use the entire capacity of all installed power supplies when calculating available power. To use normal mode, you must have enough power supplies to power all modules in the hub.

Example

The following command attempts to set the CoreBuilder 5000 hub power mode to fault tolerant:

```
CB5000> set power mode fault_tolerant
Power will switch to FAULT-TOLERANT mode when sufficient power is
available.
```

The command fails because the installed power is insufficient to support fault-tolerant mode. Fault-tolerant mode automatically enables when sufficient power becomes available (when you add another power supply).

Related Command

SHOW POWER

SET POWER MODULE POWER_ REQUIREMENTS

Use the SET POWER MODULE POWER_REQUIREMENTS (maintenance mode only) command to change the power requirement values of modules to reflect the module's true power use.

Most modules and submodules automatically display valid power management information. Some module/submodule combinations (for example, the Network Interconnect Module) do not provide complete power information. Because of this, you must set power management information manually for these modules.

To set power manually:

1. Determine the hardware configuration that the module/submodule can carry, and use information in the module user guide to determine the total power requirements of the configured card.
2. To determine if there is enough power available in the hub to support the module you are installing, use the SHOW POWER BUDGET command.
3. At the DMM command prompt, enter **maintain**
4. Use the SET POWER MODULE POWER_REQUIREMENTS command to enter the valid power information into the module EEPROM.
5. Remove the module and install additional hardware required, then reinsert the module.
6. At the maintenance (>>) prompt, enter **boot** to reboot the DMM with the newly entered power information.

Format

set power module — *slot.subslot* — **power_requirements**

slot.subslot	Selects a module in a slot (1 through 17) for changing power requirements.

Example

The following command sets the power requirements for the module in slot 9:

```
CB5000> maintain
>> set power module 9.1 power_requirements
Enter +5V power requirements in units of 1 Watt: 10
Enter -5V power requirements in units of .25 Watt: 1
Enter +12V power requirements in units of .5 Watt: 4
Enter -12V power requirements in units of .25 Watt: 2
Enter +2V power requirements in units of .1 Watt: 1
Do you want to enter this into module 9.1's EEPROM? (y/n)  y
Completed.
>> boot
```

Related Command

SHOW POWER

SET POWER OVERHEAT_AUTO_ POWER_DOWN MODE

Use the SET POWER OVERHEAT_AUTO_POWER_DOWN MODE command to have the controller decide whether or not to power down slots that contain CoreBuilder 5000 modules when it senses an overheating condition.

Format

set power overheat_auto_power_down mode ┬ **enable**
└ **disable**

enable	Causes slots containing CoreBuilder® 5000 modules to power down automatically when the hub overheats.
disable	Causes the controller to send notification to network management, but the hub keeps operating.

Example

The following command disables the hub's automatic CoreBuilder 5000 module shutdown when it detects an overheating condition:

```
CB5000> set power overheat_auto_power_down mode enable
Power overheat_auto_power_down_mode enable
```

Related Command

SHOW POWER

SET POWER SLOT CLASS

Use the SET POWER SLOT CLASS command to determine the order in which modules power down if there is inadequate power to run the system. Modules with the lowest priority power down first.

Modules set to power class 10 do not power down automatically under *any* circumstances.

ONline modules cannot use this power priority feature. ONline modules automatically draw the amount of power you specify regardless of the power priority setting of the modules installed in the hub. Refer to the CoreBuilder 5000 Distributed Management Module User Guide *for information on power management information.*

Format

set power slot — *slot* — **class** — *class*

slot	Selects the slot (1 through 17) for which you are setting power class.
class	Selects the class number you are assigning to the selected slot (1 through 10, 10 is highest priority).

Example

The following command sets the power class for slot 6 to 1:

```
CB5000> set power slot 6 class 1
Slot  6 power class is set to  1.
```

Related Commands

SHOW POWER
SET POWER MODE

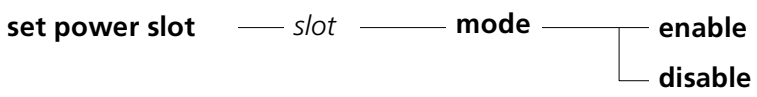
SET POWER SLOT MODE

Use the SET POWER SLOT MODE command to manually select which modules in the hub receive power.

Use this command to selectively disable power to modules installed in your hub. This allows you to manually select which modules in the hub receive power and to power down modules without removing them from the hub.

This command does not work with ONline modules.

Format



slot	Selects a slot (1 through 17) for power mode.
enable	Enables power mode.
disable	Disables power mode.

Example

The following command disables power to slot 14:

```
CB5000> set power slot 14 mode disable
Slot 14 power set to DISABLE.
```

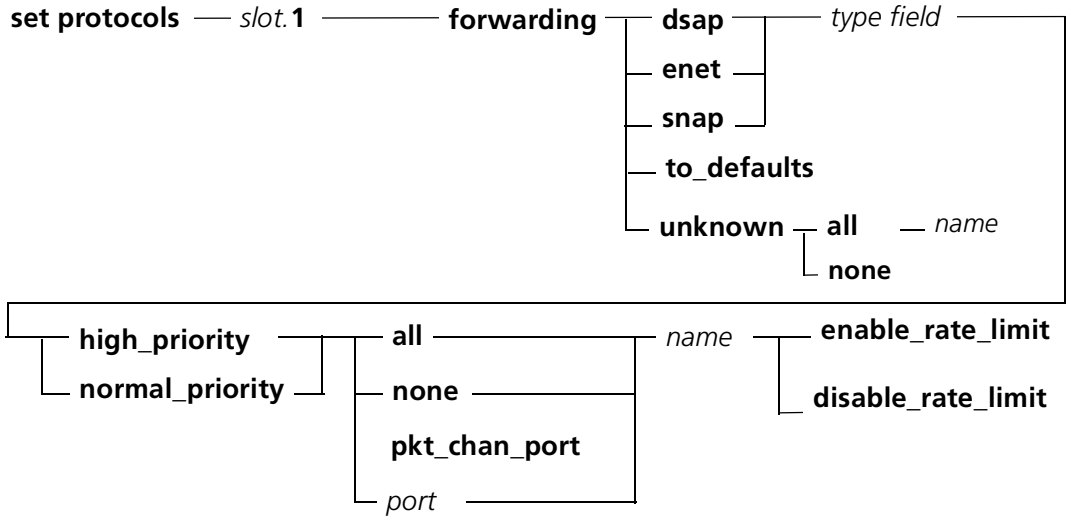
Related Command

SHOW POWER

SET PROTOCOLS FORWARDING

Use the SET PROTOCOLS FORWARDING command to create filters that filter according to a specific type of protocol and define thresholds at which broadcast packets of a certain protocol type are rate limited (discarded). For example, use this feature to prevent broadcast storms by limiting ARP broadcasts on a SwitchModule.

Format



*slot.***1**	Selects a slot (1 through 17) for setting protocol forwarding. Subslot is always **1**.
dsap	Specifies that the filter you create affects DSAP protocol packets.
enet	Specifies that the filter you create affects Ethernet protocol packets.
snap	Specifies that the filter you create affects SNAP (SubNetwork Access Protocol) packets.
to_defaults	Deletes all user-created entries from the protocol forwarding table. The default protocol filters remain in the table.
unknown	Specifies a protocol that is not a default protocol in the protocol forwarding table.
type field	Filters are based on the location of the protocol ID field (type field) in a packet.
high_priority	The protocol you are creating a filter for transmits at higher priority (experiences lower latency levels) than other protocols.
normal_priority	The protocol you are creating a filter for transmits at the normal priority level.
all	Specifies that all ports on the SwitchModule are affected.
none	Specifies that no ports on the SwitchModule are affected.
pkt_chan_port	Specifies the PacketChannel backplane port.
port	The port (1 through 24) you want to be affected by the filter you create.
name	The name (up to 16 characters) you want to identify this filter.
enable_rate_limit	Limits the broadcast packets for this protocol.
disable_rate_limit	Does not limit the broadcast packets for this protocol. This is the factory setting.

SET PROTOCOLS FORWARDING commands follow the DMM SET MODULE command syntax (slot.subslot). SwitchModules use the value 1 for subslot.

When you enter the SET PROTOCOLS FORWARDING command, the DMM interface prompts you for the necessary information.

Example 1

```
CB5000> set protocols 4.1 forwarding enet

Enter filter in hex: 60-03
   Enter value in Hex (with dash dividing bytes).

Enter queue priority: normal_priority
   high_priority
   normal_priority

Enter forward to ports: all
   all
   none
   pkt_chan_port
OR
   (port)

Enter filter name: decnet
Filter set
```

This command configures an ENET filter for the SwitchModule in slot 4, sets it to filter on all ports at normal priority, and names the filter decnet.

Example 2 The SwitchModule defines an unknown protocol as any protocol that is not a default protocol in the protocol forwarding table. Use the SHOW PROTOCOLS FORWARDING command to display the protocol forwarding table.

By default, SwitchModule ports forward all unknown protocols.

To filter (drop) unknown protocols, use the SET PROTOCOLS FORWARDING command as follows:

```
CB5000> set protocols 7.1 forwarding unknown none
Enter filter name: Filter1
Filter set
```

This command filters unknown protocols at all ports on the SwitchModule in slot 7.

This command deletes all user-created entries from the protocol forwarding table for slot 4. The default protocol filters remain in the table.

For example:

```
> set protocols 4.1 forwarding to_defaults
Filters reset to defaults.
```

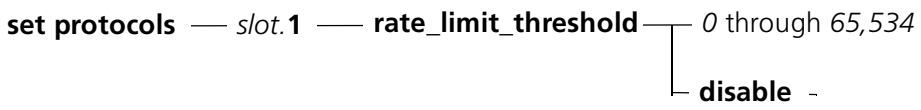
Related Command SHOW PROTOCOLS FORWARDING

SET PROTOCOLS RATE_LIMIT_ THRESHOLD

Use the SET PROTOCOLS RATE_LIMIT_THRESHOLD command on SwitchModules to define the threshold at which you want the SwitchModule to begin discarding packets.

You can configure rate limiting on a per SwitchModule basis, not per port or virtual bridge. This means that to configure the same rate limit settings on a virtual bridge that spans multiple SwitchModules, you must configure each SwitchModule that participates in the virtual bridge.

Format



slot.**1**	Selects a slot (1 through 17) for setting protocol rate limiting. Subslot is always **1**.
0 through *65,534* **disable**	Value (frames per second) at which you can set the threshold or disable the feature.

Example

To configure rate limiting, define the protocol type of the broadcast packets you want to limit. Use the SET PROTOCOLS FORWARDING command with the ENABLE_RATE_LIMIT option.

```
CB5000> set protocols 7.1 forwarding enet 08-06 normal_priority
all ip_arp enable_rate_limit

Filter set
```

Define the threshold at which you want the SwitchModule to begin discarding packets. Use the SET PROTOCOLS RATE_LIMIT_THRESHOLD command.

```
CB5000> set protocols 7.1 rate_limit_threshold 300
```

The previous commands enable rate limiting on the SwitchModule in slot 7. When the SwitchModule receives more than 300 frames per second of Ethernet type 08-06 packets, these packets are discarded.

If you set the rate limit threshold to 0 frames per second, the SwitchModule filters all broadcast packets.

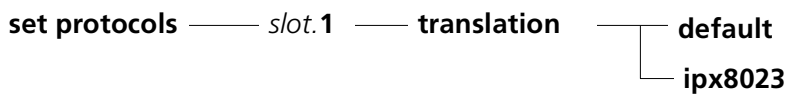
Related Commands

SET PROTOCOLS FORWARDING
SHOW PROTOCOLS RATE_LIMIT_THRESHOLD

SET PROTOCOLS TRANSLATION

Use the SET PROTOCOLS TRANSLATION command to select the setting for translation between the Ethernet and FDDI protocols on CoreBuilder 5000 SwitchModules.

Format



*slot.***1**	Selects a slot (1 through 17) for setting protocol forwarding. Subslot is always **1**.
ipx8023	Enables translation using the ipx8023 setting. Select this setting if your network is running Novell configured as raw 802.3 IPX between Ethernet and FDDI.
default	Enables translation at the default setting. Select this setting if your network is running Novell configured as Ethernet II or Ethernet 802.3/802.2 between Ethernet and FDDI.

Example

The following command enables ipx802.3 translation on the SwitchModule in slot 17:

```
CB5000> set protocols 17.1 translation ipx8023
Filter set.
```

Related Command

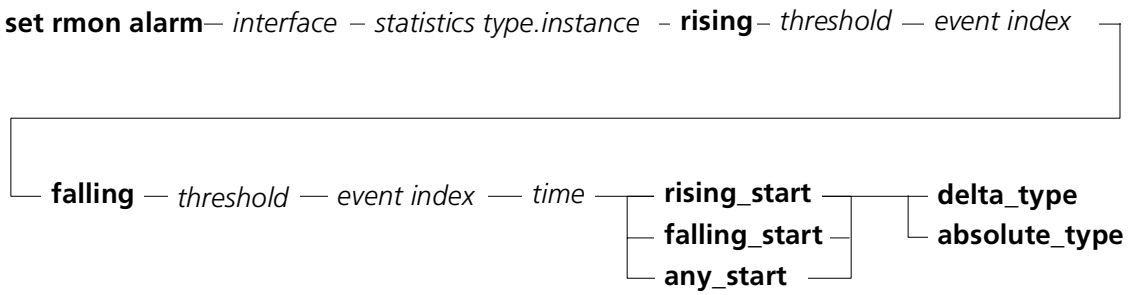
SHOW PROTOCOLS TRANSLATION

SET RMON ALARM

Use the SET RMON ALARM command to set up an alarm that triggers an event based on the parameters you specify.

Each sample is compared against two thresholds, a rising threshold and a falling threshold. Each sample can be either an absolute value or a delta value (the difference between the current value and the value of the previous sample). If the value crosses the threshold, an event associated with that threshold may be generated. The threshold is not rearmed until the opposite threshold is crossed (rising or falling). This prevents the generation of multiple events as a sample crosses just above and below a specific threshold.

Format



interface	The interface whose statistics you are collecting. Use the SHOW INTERFACE command for a list of interface numbers.
statistics type	The type of statistics you want to collect. The list of statistics are: ■ BroadcastPackets ■ Collisions ■ CRCAlignErrors ■ Fragments ■ Jabbers ■ MulticastPackets ■ Octets ■ OversizePackets ■ Packets ■ UndersizePackets
instance	The specific instance for the selected *statistics type*.
rising	Introduces the parameters for the rising threshold.
falling	Introduces the parameters for the falling threshold.
threshold	The statistic value falling below the *threshold* triggers the *event*.
event index	Index number of the RMON event triggered by the rising or falling threshold. Use the SET RMON EVENT command to create events, and the SHOW RMON EVENTS command to view event index numbers.
time	Time between samples in hh:mm format.
rising_start	Specifies that the first event must be triggered by the rising threshold.
falling_start	Specifies that the first event must be triggered by the falling threshold.
any_start	Specifies that the first event can be triggered by the rising threshold or falling threshold.
delta_type	Specifies that the threshold value is compared to the change in the statistic value since the last sample.
absolute_type	Specifies that the threshold value is compared to the absolute statistic value.

Example The following command sets thresholds that trigger an alarm when there are more than five in an hour:

```
CB5000> set rmon alarm ethernet crcalignerror.3 rising 5 2 falling
1 3 01:00 rising_start delta_type
Entry 2 created.
```

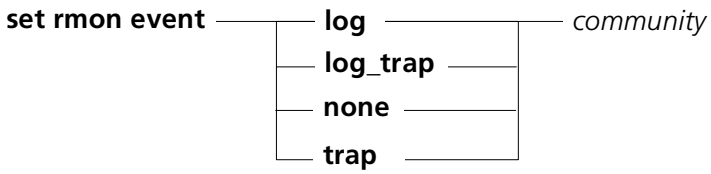
Related Commands

SET RMON EVENT
SHOW RMON
SHOW INTERFACE

SET RMON EVENT

Use the SET RMON EVENT command to create events that are triggered by alarms created using the SET RMON ALARM command.

Format



log	Writes an entry in the event log.
log_trap	Writes an entry in the event log and sends a trap to the specified community.
none	Takes no action.
trap	Sends a trap to the specified community.
community	The SNMP community name for trap receivers. The default is public.

Example

The following command sets up a trap message sent when the CRC Alignment Error alarm is triggered:

```
CB5000> set rmon event trap
Enter one line for event description:

> CRC Alignment Error Threshold Exceeded!!

Entry 2 created.
```

Related Commands

SHOW RMON
SET RMON ALARM

SET RMON HISTORY

Use the SET RMON HISTORY command to add entries to the RMON History Table for various MACs in the hub. This command works for Ethernet modules only.

The history group generates reports. A history is a sample of statistical information, taken periodically. The MAC stores each sample in the history report.

The history report is similar to the DMM's MONITOR command. It logs the difference between counters at regular intervals. The history control table specifies the:

- Data source of the history report
- Collection interval
- Number of entries to store

If the probe has more entries to store than it is configured to hold, the oldest history entry is deleted (the lowest-numbered sample) and a new entry is appended (as the highest numbered sample).

The Ethernet History incorporates Ethernet statistic counters. For each sample entry, the report provides utilization of the network during that interval. Each entry is stamped with the date and time that the entry was started.

Format

set rmon history — **interface** — *interface* — *interval*

interface	Specifies the number of the interface for which you are creating a matrix table. Use the SHOW INTERFACE command for a list of interface numbers.
interface	Interface number.
interval	Specifies the number of minutes and seconds between history table entries. The format is mm:ss.

Example

The following command causes the ENMC assigned to interface 3 to record an RMON History Table entry every 30 seconds:

```
CB5000> set rmon history interface 3 00:30
Entry 1 created.
```

Related Command

SHOW RMON

SET RMON HOST INTERFACE

Use the SET RMON HOST INTERFACE command to enable host table collection.

The RMON agent in the DMM detects hosts on the network by observing source and destination addresses in network packets. It creates an entry in the RMON host table for each detected host. The RMON agent also collects traffic statistics for each host based on observed network packets.

Format

set rmon host interface —— *index*

index	The index number of the DMM's RMON interface.

Example

The following command enables host table monitoring by the RMON agent:

```
CB5000> set rmon host interface 1
Entry 1 created.
```

Related Commands

CLEAR RMON HOST
SHOW RMON HOST

SET RMON MATRIX

Use the SET RMON MATRIX command to set up a particular interface to track conversations between hosts. This command works with Ethernet modules only.

The matrix table is similar to the host table, but tracks network conversations between hosts, instead of host traffic. For every frame, the MAC extracts the source and destination address and associates the frame with a conversation.

Network conversations are important for performance modeling. Using Matrix Table information, you can model the network across bridging devices and along shared segments. You can optimize network performance by ensuring that heavy conversations are isolated to shared LANs and do not occur across heavily-burdened bridging devices.

The ENMC stores up to 2,000 conversations, then discards any new conversations that arrive.

Format

set rmon matrix — **interface** —— *interface*

interface	Specifies the number of the interface for which you are creating a matrix table. Use the SHOW INTERFACE command for a list of interface numbers.
interface	The number of the interface.

Example

The following command creates a matrix of conversations monitored by interface 3:

```
CB5000> set rmon matrix interface 3
Entry 1 created.
```

Related Command

SHOW RMON

SET RMON STATISTICS

Use the SET RMON STATISTICS command to enable monitoring by the RMON agent in the DMM for one of the RMON statistics groups.

Format

set rmon statistics — *statistics group* — **interface** — *interface index*

statistics group	The specific statistics group for which you want statistics. The groups can be Ethernet, Token Ring, or Isolated.
interface	Specifies the interface for which you are creating a matrix table. Use the SHOW INTERFACE command for a list of interfaces supported in the switch.
interface index	Specifies the specific interface index number for which you want RMON Statistics.

Example

The following command enables RMON Ethernet statistics collection on interface 1:

```
CB5000> set rmon statistics ethernet interface 1
Entry 1 created.
```

Related Commands

CLEAR RMON STATISTICS
SHOW RMON STATISTICS

SET RMON TOPN_HOSTS

Use the SET RMON TOPN_HOSTS command to create a table of the Top Hosts accruing the statistics entry you select. This command works only with Ethernet modules.

This report sorts hosts based on that statistic, over a period of time you select. For example, the topN group can generate a report indicating the top 10 hosts that generated errors over the last half hour. The control table specifies:

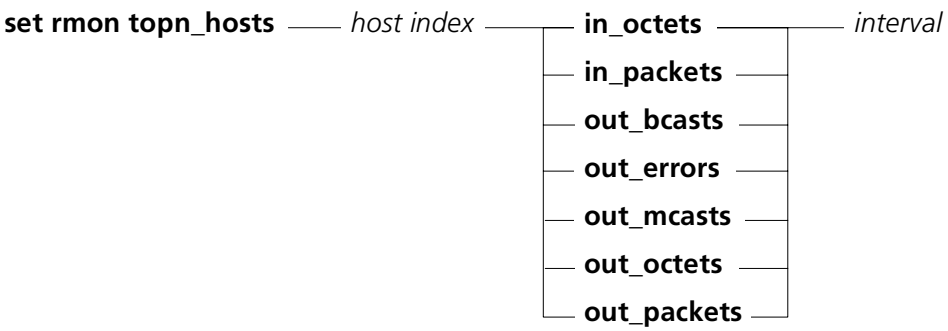
- Statistic to use for the sort (Rate Base)
- Duration of the monitoring period
- Number of hosts to report (you cannot configure this from the command line)

You can sort the data using any of the host table statistics. The generated report indicates in decreasing order:

- Hosts
- Actual rate for the sorted statistic for that host

A topN report is generated directly from the host table. Therefore, the topN report points to a host control entry.

Format



host index	Specifies the host index number from the host control table (use the SHOW RMON HOST CONTROL ALL command for a list).
in_octets	Specifies that the in_octets statistic is used to compile the Top Hosts list. The in_octets statistic specifies the number of octets coming into the network.
in_packets	Specifies that the in_packets statistic is used to compile the Top Hosts list. The in_packets statistic specifies the number of packets coming into the network.
out_bcasts	Specifies that the out_bcasts statistic is used to compile the Top Hosts list. The out_bcasts statistic specifies the number of broadcast packets being sent out onto the network.
out_errors	Specifies that the out_errors statistic is used to compile the Top Hosts list. The out_errors statistic specifies the number of errors being sent out onto the network.
out_mcasts	Specifies that the out_mcasts statistic is used to compile the Top Hosts list. The out_mcasts statistic specifies the number of multicast packets being sent out onto the network.

out_octets	Specifies that the out_octets statistic is used to compile the Top Hosts list. The out_octets statistic specifies the number of octets being sent out onto the network.
out_packets	Specifies that the out_packets statistic is used to compile the Top Hosts list. The out_packets statistic specifies the number of packets being sent out onto the network.
interval	Specifies the period of time (hh:mm) between samples.

Example The following command creates a table every 30 seconds of the top stations sending out packets onto the network:

```
CB5000> set rmon topn_hosts 1 out_packets 00:30
Entry 1 created.
```

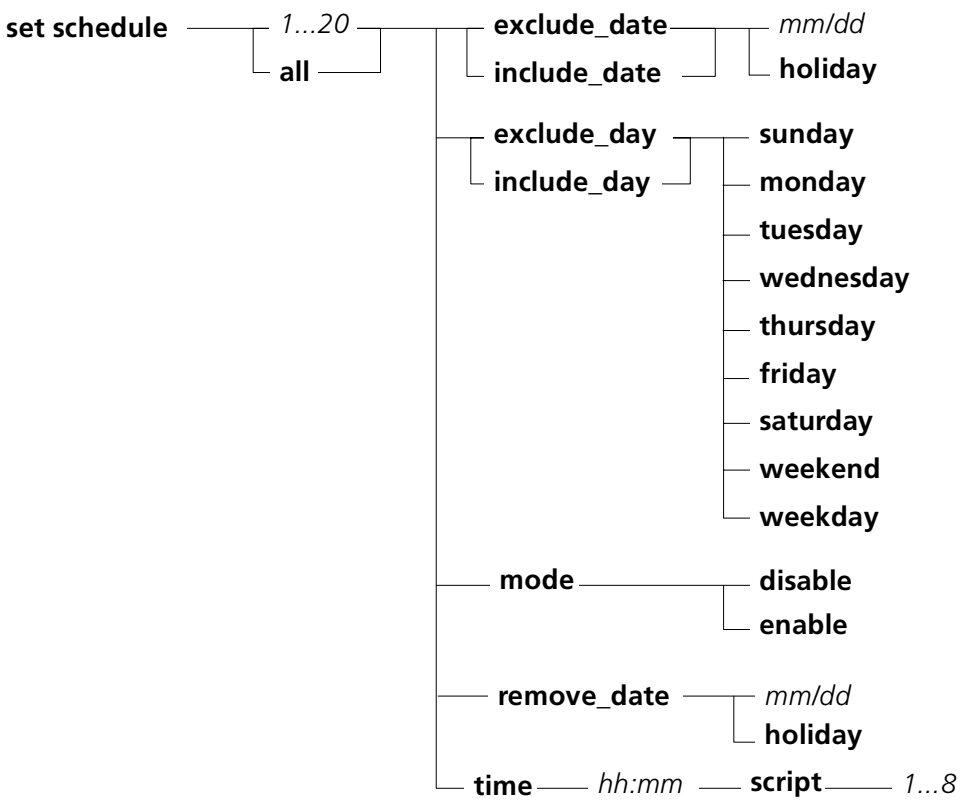
Related Command SHOW RMON

SET SCHEDULE

Use the SET SCHEDULE command to define the time a specified schedule runs a specified script.

Prior to configuring schedules, use the SHOW CLOCK command to verify that the DMM's time and date are correct.

Format



1...20	Identifies the schedule to be modified.
all	Modifies all schedules.
exclude_date	Specifies a date to be excluded from the schedule. The script for this schedule does not run on the specified date. *mm* = 1 through 12, *dd* = 1 through 31
exclude_date holiday	Excludes holidays from the schedule. The script for this schedule does not run on holidays. Use the SET SCHEDULE HOLIDAY command to define which dates are holidays.
include_date	Specifies a date to be included in the schedule. The script for this schedule runs on the specified date. *mm* = 1 through 12, *dd* = 1 through 31
include_date holiday	Includes holidays in the schedule. The script for this schedule runs on holidays. Use the SET SCHEDULE HOLIDAY command to define which dates are holidays.

exclude_day sunday...saturday	Specifies a day to exclude from the schedule. The script for this schedule does not run on the specified day.
exclude_day weekend	Excludes weekends from the schedule. The script for this schedule does not run on weekends. Use the SET SCHEDULE WEEKEND command to define which days are weekend days.
exclude_day weekday	Excludes weekdays from the schedule. The script for this schedule does not run on weekdays. Use the SET SCHEDULE WEEKDAY command to define which days are weekdays.
include_day sunday...saturday	Specifies a day to include in the schedule. The script for this schedule does not run on the specified day.
include_day weekend	Includes weekends in the schedule. The script for this schedule does run on weekends. Use the SET SCHEDULE WEEKEND command to define which days are defined as weekends.
include_day weekday	Includes weekdays in the schedule. The script for this schedule does run on weekdays. Use the SET SCHEDULE WEEKDAY command to define which days are defined as weekdays.
enable	Enables the schedule (specified at the beginning of the command).
disable	Disables the schedule (specified at the beginning of the command).
remove_date *mm/dd* **remove_date holiday**	Removes the given date or holiday from the list of dates for the schedule.
time *hh:mm*	Time the script (specified at the end of the command) runs on days included in the schedule (specified at the beginning of the command). *hh* = 0 through 23, *mm* = 0 through 59
script *1...8*	Specifies the script to run for this schedule (specified at the beginning of the command).

Example The following command specifies that schedule 1 run script 3 at 7:00 am:

```
CB5000> set schedule 1 time 7:00 script 3
Schedule 1 set to run script 3 at time 07:00.
```

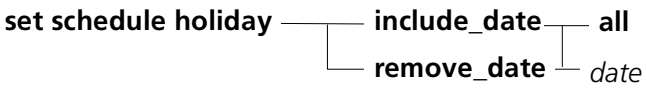
Related Commands

SET SCHEDULE HOLIDAY
SET SCHEDULE STARTUP_REPLAY_TIME
SET SCHEDULE WEEKDAY
SET SCHEDULE WEEKEND
SHOW SCHEDULE

SET SCHEDULE HOLIDAY

Use the SET SCHEDULE HOLIDAY command to define a holiday list of up to 10 dates. After it is defined, you can use the Holiday option in the SET SCHEDULE command to run or not to run scripts on the dates specified in the holiday list.

Format



include_date	Specifies a date to include in a holiday list. *mm* = 1 through 12, *dd* = 1 through 31
remove_date	Removes a date from the holiday list. *mm* = 1 through 12, *dd* = 1 through 31
all	Removes all dates from the holiday list.

Example

The following command defines January 1 as a holiday:

```
CB5000> set schedule holiday include_date 1/1
Date 1/1 included in HOLIDAY list.
```

Related Commands

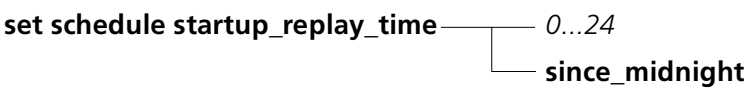
SET SCHEDULE
SET SCHEDULE STARTUP_REPLAY_TIME
SET SCHEDULE WEEKDAY
SET SCHEDULE WEEKEND
SHOW SCHEDULE

SET SCHEDULE STARTUP_REPLAY_ TIME

Use the SET SCHEDULE STARTUP_REPLAY_TIME to configure the DMM to run previously scheduled scripts whenever the DMM is reset. The command lets you define how far back (up to 24 hours) the DMM should search for scripts to run.

For example, after a DMM is reset, if the Startup Replay Time is defined as 6 (hours) and the current time is 8:00 am, the DMM executes all scripts that should have occurred since 2:00 am.

Format



0...24	When the DMM is reset, it runs scripts that were scheduled to run prior to the reset. The number you enter is the number of hours the DMM searches backwards for scripts to run. A value of 0 disables the function.
since_midnight	When the DMM is reset, it runs all scripts that were scheduled to run since the preceding midnight.

Example

The following command causes the DMM to execute all scripts defined in schedules that were scheduled to run 6 hours or less previous to the time it is reset:

```
CB5000> set schedule startup_replay_time 6
The startup_replay_time is set to 6 hour(s).
```

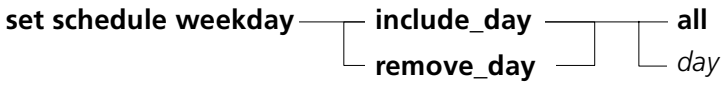
Related Commands

SET SCHEDULE
SET SCHEDULE HOLIDAY
SET SCHEDULE WEEKDAY
SET SCHEDULE WEEKEND
SHOW SCHEDULE

SET SCHEDULE WEEKDAY

Use the SET SCHEDULE WEEKDAY command to define a list of weekdays containing up to seven days. After it is defined, you can use the Weekday option in the SET SCHEDULE command to run or not run scripts on the days in the list of weekdays.

Format



include_day	Adds a specified day to the list of weekdays.
remove_day	Removes the specified day from the list of weekdays.
all	Specifies all days to include or remove.
day	List of days. Monday, Tuesday, Wednesday, Thursday, Friday

Example

The following command includes Monday in the list of weekdays:

```
CB5000> set schedule weekday include_day monday
MONDAY included in WEEKDAY variable.
```

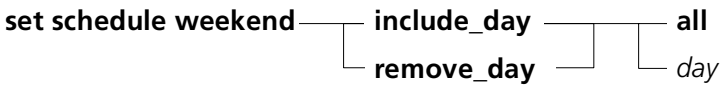
Related Commands

SET SCHEDULE
SET SCHEDULE HOLIDAY
SET SCHEDULE STARTUP_REPLAY_TIME
SET SCHEDULE WEEKEND
SHOW SCHEDULE

SET SCHEDULE WEEKEND

Use the SET SCHEDULE WEEKEND command to define a list of weekend days containing up to seven days. After it is defined, you can use the Weekend option in the SET SCHEDULE command to run or not run scripts on the days in the list of weekend days.

Format



include_day	Specifies a day to add to the list of weekend days.
remove_day	Removes the specified day from the list of weekend days.
all	Adds or removes all days from the list of weekend days.

Example

The following command removes Sunday from the lists of days defined as weekend days:

```
CB5000> set schedule weekend remove_day sunday
SUNDAY removed from WEEKEND variable.
```

Related Commands

SET SCHEDULE
SET SCHEDULE HOLIDAY
SET SCHEDULE STARTUP_REPLAY_TIME
SET SCHEDULE WEEKDAY
SHOW SCHEDULE

SET SCRIPT DELETE

Use the SET SCRIPT DELETE command to delete a line from a script.

Format

set script —— *1...8* —— **delete** —— *1...15*

1...8	Identifies the script to be modified. Use the SHOW SCRIPT command with the ALL option for a numbered list of scripts.
1...15	Identifies the line to be deleted. Use the SHOW SCRIPT command with the VERBOSE option to view the lines in a script.

Example

The following command removes line 6 from script 1:

```
CB5000> set script 1 delete 6
Line 6 deleted from SCRIPT 1.
```

Related Commands

SET SCRIPT INSERT
SET SCRIPT NAME
SET SCRIPT OVERWRITE
SHOW SCRIPT

SET SCRIPT INSERT

Use the SET SCRIPT INSERT command to insert new commands into a script.

Format

set script —— *1...8* —— **insert** —— *1...15*

1...8	Identifies the script to be modified. Use the SHOW SCRIPT command with the ALL option for a numbered list of scripts.
1...15	Identifies the line to be inserted. Use the SHOW SCRIPT command with the VERBOSE option to view the script with line numbers.

Example

The following command opens script 1 for editing at line 11:

```
CB5000> set script 1 insert 11
Enter line(s) to insert. Enter a blank line to quit this mode.
```

Related Commands

SET SCRIPT DELETE
SET SCRIPT NAME
SET SCRIPT OVERWRITE
SHOW SCRIPT

SET SCRIPT NAME

Use the SET SCRIPT NAME command to assign a name to a script.

Format

set script —— *1...8* —— **name** —— *scriptname*

1...8	Identifies the script to be named. Use the SHOW SCRIPT command with the ALL option for a numbered list of scripts and their current names.
scriptname	Name for the script, up to 16 characters.

Example

The following command assigns the name Engineering1 to script 3:

```
CB5000> set script 3 name Engineering1
Name set for script 3.
```

Related Commands

SET SCRIPT DELETE
SET SCRIPT INSERT
SET SCRIPT OVERWRITE
SET SCRIPT RUN_ON_EVENT
SHOW SCRIPT

SET SCRIPT OVERWRITE

Use the SET SCRIPT OVERWRITE command to add new commands to a script starting at a specified line number, replacing current lines.

Format

set script —— *1...8* —— **overwrite** —— *1...15*

1...8	Identifies the script to be modified. Use the SHOW SCRIPT command with the ALL option for a numbered list of scripts.
1...15	Number of the line to be overwritten. Use the SHOW SCRIPT command with the VERBOSE option to view the script with line numbers.

Example

The following command opens script 3 at line 1 for editing. New lines overwrite current lines.

```
CB5000> set script 3 overwrite 1
Enter line(s) to overwrite. Enter a blank line to quit this mode.
```

Related Commands

SET SCRIPT DELETE
SET SCRIPT INSERT
SET SCRIPT NAME
SET SCRIPT RUN_ON_EVENT
SHOW SCRIPT

SET SCRIPT RUN_ON_EVENT

Use the SET SCRIPT RUN_ON_EVENT command to associate a script with an RMON event. When the RMON event occurs, the associated script runs automatically.

Format

set script —— *1...8* —— **run_on_event** ———— *event*

1...8	Identifies the script name to be modified. Use the SHOW SCRIPT command with the ALL option for a numbered list of scripts.
event	Use the SHOW RMON EVENT CONTROL ALL command to view index names.

Example

The following command associates RMON event 3 with script 5:

```
CB5000> set script 5 run_on_event 3
```

Related Commands

SET SCRIPT DELETE
SET SCRIPT INSERT
SET SCRIPT NAME
SHOW SCRIPT

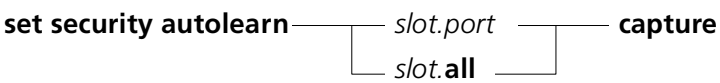
SET SECURITY AUTOLEARN CAPTURE

Use the SET SECURITY AUTOLEARN CAPTURE command to initiate the Autolearn feature for a specified port.

This command applies to the CoreBuilder 5000 Token Ring modules only.

Autolearning allows the DMM to continuously monitor network activity and automatically learn the valid MAC addresses associated with a port on the module.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Specifies all ports in a slot. *slot* is the slot number.
capture	Instructs the DMM to learn all valid addresses for a port.

Example

The following command allows the MAC addresses associated with all ports on the module in slot 3 to be learned by the DMM during Autolearning:

```
CB5000> set security autolearn 3.all capture
Autolearn capture done; learned 3 addresses total.
```

Related Commands

CLEAR SECURITY AUTOLEARN
SHOW SECURITY AUTOLEARN

SET SECURITY AUTOLEARN DOWNLOAD

Use the SET SECURITY AUTOLEARN DOWNLOAD command to download the contents of the Autolearning database to the specified ports for the MAC addresses to be associated with a port. This command is available for Token Ring modules only.

Downloading the Autolearning database allows the learned MAC addresses for a port to be associated with the ports specified in the AUTOLEARN DOWNLOAD command line.

The DMM allows a maximum of 360 MAC addresses in the Autolearning database per hub.

Because no more than seven MAC addresses can be associated with one port, only seven MAC addresses are downloaded per port. The seven MAC addresses with the lowest alphanumeric values are downloaded from the Autolearning database to a module port.

The following message is displayed upon completion of the AUTOLEARN DOWNLOAD command (where *y* indicates the total number of addresses copied to a port's MAC address table):

```
Autolearn download done; downloaded y addresses total.
```

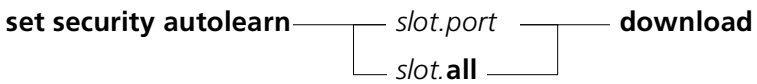
If a port has more than seven MAC addresses in the Autolearning database at the time of the download, the following message is displayed upon completion of the AUTOLEARN DOWNLOAD command:

```
Note:  at least one autolearned address was skipped because the
port with which it is associated has more than 7 autolearned
addresses.
```

If any MAC address was skipped because the hub limit of 360 addresses was reached, the following message is displayed upon completion of the AUTOLEARN DOWNLOAD command:

```
Note: the number of autolearned addresses exceeds the hub limit.
Only the first 360 addresses (as ordered by slot, port, and addr)
were downloaded.
```

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.

Example The following command initiates a download of the Autolearning database to all ports on the module in slot 3:

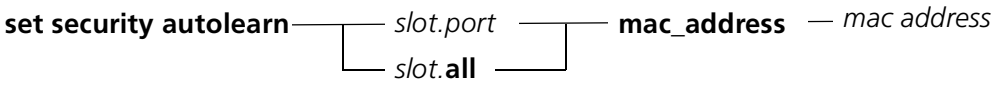
```
CB5000> set security autolearn 3.all download
Autolearn download done; downloaded 3 addresses total.
```

Related Command SHOW SECURITY

SET SECURITY AUTOLEARN MAC_ADDRESS

Use the SET SECURITY AUTOLEARN MAC_ADDRESS command to manually add a MAC address to the Autolearning database. This command applies to Token Ring modules only.

Format



slot.port	Identifies the port for this operation. *slot (*1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Specifies all ports in a slot. *slot* is the slot number.
mac address	MAC address you are configuring using this command. The format for MAC addresses is nn-nn-nn-nn-nn-nn The address 00-00-00-00-00-00 is invalid for this command.

Example

The following command adds the MAC address 07-34-24-02-0F-00 to the Autolearning database and associates it with port 1 in slot 3:

```
CB5000> set security autolearn 3.1 mac_address 07-34-24-02-0F-00
Address 07-34-24-02-0F-00 associated with port 03.01 in
Autolearning area.
```

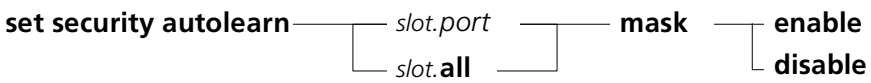
Related Commands

CLEAR SECURITY AUTOLEARN
SHOW SECURITY AUTOLEARN

SET SECURITY AUTOLEARN MASK

Use the SET SECURITY AUTOLEARN MASK command to allow or prevent a port's MAC addresses from being learned by the DMM during Autolearning. This setting also determines whether the DMM is allowed or prevented from downloading learned MAC addresses to the port. This command applies to Token Ring modules only.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 20) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.
enable	Masks learning by preventing the DMM security feature from automatically learning MAC addresses associated with this port.
disable	Does not mask learning. Allows the DMM to automatically learn MAC addresses associated with this port.

Example

The following command allows the MAC addresses associated with all ports on the module in slot 3 to be learned by the DMM during Autolearning:

```
CB5000> set security autolearn 3.all mask disable
Port 03.all autolearn mask set to DISABLED.
```

Related Commands

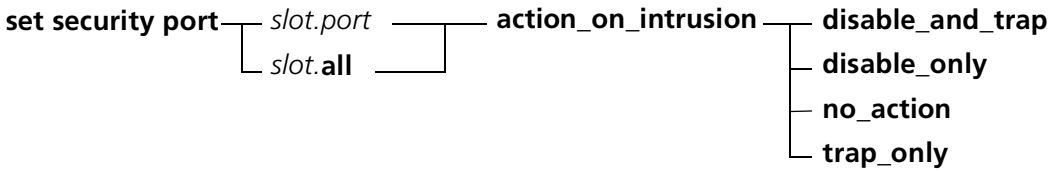
CLEAR SECURITY AUTOLEARN
SHOW SECURITY AUTOLEARN

SET SECURITY PORT ACTION_ON_ INTRUSION

Use the SET SECURITY PORT ACTION_ON_INTRUSION command to define the action the DMM takes when a port-to-MAC address security intrusion occurs.

The DMM always logs the intrusion in the Intruder List.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the location of a module in the hub and *port* is the port number on the specified module. For example, to identify port 4 on the 6, enter **6.4**
slot.**all**	Specifies all ports on the module in a slot.
disable_and_trap	When an intrusion occurs, the DMM disables the port and sends traps as defined in the community table. This is the factory setting.
disable_only	When an intrusion occurs, the DMM disables the port, but sends no traps.
no_action	When an intrusion occurs, the DMM takes no action.
trap_only	When an intrusion occurs, the DMM send traps as defined in the community table, but does not disable the port.

Example

The following command specifies that the DMM take no action when an intrusion occurs on port 1 in slot 3:

```
CB5000> set security port 3.1 action_on_intrusion no_action
Port 03.01 action_on_intrusion set to NO_ACTION.
```

Related Command

SHOW SECURITY INTRUDER_LIST

SET SECURITY PORT MAC_ADDRESS

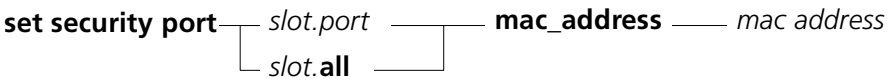
Use the SET SECURITY PORT MAC_ADDRESS command to enter a MAC address into the secure MAC address table. The secure MAC address table contains a maximum of eight MAC addresses for each port in the hub.

When you enable security using the SET SECURITY PORT MODE command, the DMM monitors each port for packets containing a source address not found in the secure MAC address table for that port. If the DMM detects such a packet, it takes action based on the settings of the SET SECURITY ACTION_ON_INTRUSION command.

The following addresses are invalid for this command:

- 00-00-00-00-00-00
- ff-ff-ff-ff-ff-ff

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports on a module in a specified slot.
mac address	MAC address to be entered into the secure MAC address table. Enter the address as a series of six hexadecimal bytes separated by hyphens. For example, 10-00-f1-0f-0c-63.

Example

The following command enters MAC address 07-34-24-02-0F-00 into the secure MAC address table for port 2 on slot 3:

```
CB5000> set security port 3.2 mac_address 07-34-24-02-0F-00
Security MAC address (noncanonical) 07-34-24-02-0F-00 on port
03.02.
```

Related Command

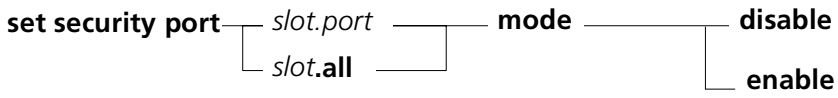
SET SECURITY PORT MODE

SET SECURITY PORT MODE

Use the SET SECURITY PORT MODE command to enable or disable address security for a specified port.

If you enable security mode for a port that does not have MAC addresses associated with it, the DMM treats each packet as an intrusion.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the location of a module in the hub and *port* is the port number on the specified module. For example, to identify port 4 on the module in slot 6 enter **6.4**
slot.**all**	Specifies all ports on a module in a slot.
disable	Disables security mode for the specified port.
enable	Enables security mode for the specified port.

Example

The following command enables security on port 2 in slot 3:

```
CB5000> set security port 3.2 mode enable
Port 03.02 security mode set to ENABLED.
```

Related Command

SET SECURITY PORT MAC_ADDRESS

SET SECURITY_ADVANCED ADDRESS_TABLE ADDRESS

Use the SET SECURITY_ADVANCED ADDRESS_TABLE ADDRESS command to manually configure your security address table for the Ethernet Private Line Card.

In some instances, it is preferable to manually configure your security address table. For example, if you work in an environment that demands a high level of security, you may not want to enable autolearning on a secure network.

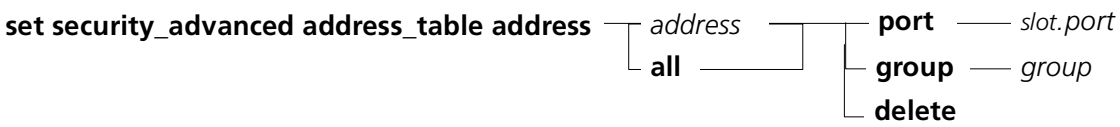
In this type of environment, manually add users to the security address table.

To add address information to your table manually, you can enter either:

- A MAC address and associated port
- A MAC address and associated group code

The host module cannot autolearn group codes. You must set them manually.

Format



address	Address you want to add to the security address table.
all	Adds all addresses to this port or group.
delete	Deletes the indicated MAC address, or all MAC addresses, from the address table.
slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
group	Specifies a port group which to apply this command.

Example The following command adds a MAC address and port 5.1 to your security address table:

```
CB5000> set security_advanced address_table address
40-40-34-e5-00-23 port 5.1
Security Address Table update in progress...
```

Related Command SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED INTRUDER_TABLE DELETE

Use the SET SECURITY_ADVANCED INTRUDER_TABLE DELETE command to delete an intruder table for the Ethernet Private Line Card.

In some instances you may consider deleting your intruder table. For example, in the event that you receive a large amount of network intrusions due to the failsafe parameter, you may opt to delete the intruder table after you correct the source of the problem.

Format

set security_advanced intruder_table delete

Example The following command deletes the current intruder table:

```
CB5000> set security_advanced intruder_table delete
No such intruder
```

Related Command SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK AUTOLEARNING

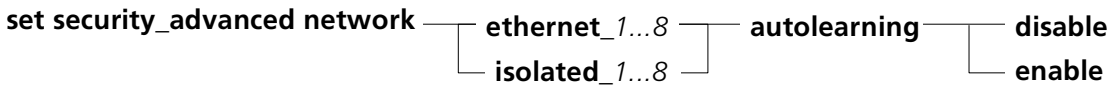
Use the SET SECURITY_ADVANCED NETWORK AUTOLEARNING command to enable port autolearning on a secure network.

After it is enabled, you can use this command, with other port and network parameters, to secure ports connected to the secure network.

If network autolearning is enabled, you must also enable per-port autolearning.

Any time you manually add an address to the Security Address Table, the system removes previous port assignments for that address. However, if you enable autolearning, the system does not modify the Security Address Table entries if they are assigned to a group code.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply the command.
isolated_*1...8*	Specifies which isolated network to apply the command.
disable	Disables autolearning.
enable	Enables autolearning.

Example

The following command enables autolearning on ethernet_1:

```
CB5000> set security_advanced network ethernet_1 autolearning
enable
ETHERNET_1 Autolearning: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK EAVESDROP_ PROTECTION

Use the SET SECURITY_ADVANCED NETWORK EAVESDROP_PROTECTION command to enable eavesdropping protection on an Ethernet network that has an Ethernet Private Line Card assigned to it.

Enabling eavesdrop protection on a secure network allows you to prevent all ports with per-port jamming enabled from eavesdropping on a secure network. This prevents intruders and other valid users from examining the contents of a packet destined for another port.

When you enable network eavesdropping and autolearning, the network passes packets with unknown destinations to all ports.

Format

set security_advanced network { **ethernet**_*1...8* | **isolated**_*1...8* } **eavesdrop_protection** { **disable** | **enable** }

ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
disable	Disables eavesdrop protection.
enable	Enables eavesdrop protection.

Example

The following command assigns eavesdrop protection to ethernet_1:

```
CB5000> set security_advanced network ethernet_1
eavesdrop_protection enable
ETHERNET_1 Eavesdrop Protection: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

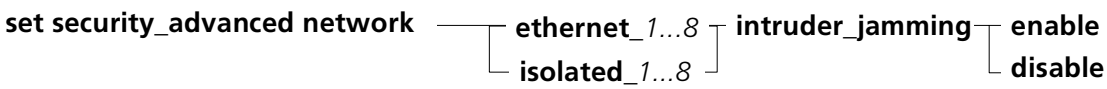
SET SECURITY_ADVANCED NETWORK INTRUDER_JAMMING

Use the SET SECURITY_ADVANCED NETWORK INTRUDER_JAMMING command to enable intruder jamming protection on an Ethernet network that has a Ethernet Private Line Card assigned to it.

When an intruder packet is detected on a secure network, the intruder jamming network parameter enables the host module to transmit a jam message to all ports on the network. This prevents all end nodes from receiving or examining the contents of the intruder packets.

If you enable intruder jamming on your network, you must also enable either the source port checking or the source address checking network parameter. If you do not enable either of these parameters, the host module does not detect intruder packets.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
enable	Enables intruder jamming.
disable	Disables intruder jamming.

Example

The following command assigns intruder jamming to ethernet_1:

```
CB5000>  set security_advanced network ethernet_1 intruder_jamming
enable
ETHERNET_1 Intruder Jamming: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK INTRUDER_PORT_ DISABLING

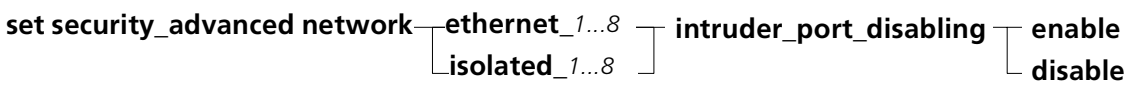
Use the SET SECURITY_ADVANCED NETWORK INTRUDER_PORT_DISABLING command to automatically disable ports that receive intruder packets on an Ethernet network that has an Ethernet Private Line Card assigned to it.

When you enable intruder port disabling, ports that transmit intruder packets are disabled automatically.

If you enable intruder port disabling on your network, you must also enable either the source port checking or the source address checking network parameter. If you do not enable either of these parameters, the host module does not detect intruder packets.

If you enable intruder port disabling, intruder reporting is automatically enabled as well.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
enable	Enables intruder port disabling.
disable	Disables intruder port disabling.

Example

The following command disables intruder ports on ethernet_1:

```
CB5000>  set security_advanced network ethernet_1
intruder_port_disabling enable
ETHERNET_1 Intruder Port Disabling: set to ENABLED.
ETHERNET_1 Intruder Reporting: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK INTRUDER_REPORTING

Use the SET SECURITY_ADVANCED NETWORK INTRUDER_REPORTING command to track intrusion attempts on an Ethernet network that has an Ethernet Private Line Card assigned to it.

To track intrusion attempts on a secure network, you must enable the intruder reporting network parameter. This parameter enables the Ethernet Private Line Card to instruct a media module to report intrusion attempts on a secure network. The DMM stores all reported intrusion attempts in the Intruder Table.

The Security Intruder Table has a limit of 100 intrusion entries. After the table reaches the maximum limit, older entries expire automatically.

To report intruders on a secure network, you must enable the source address checking or the source port checking network parameter. If you do not enable either of these parameters, the system does not detect intruders.

Format

ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
enable	Enables intruder reporting.
disable	Disables intruder reporting.

Example

The following command enables intruder reporting on ethernet_1:

```
CB5000>  set security_advanced network ethernet_1
intruder_reporting enable
ETHERNET_1 Intruder Reporting: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

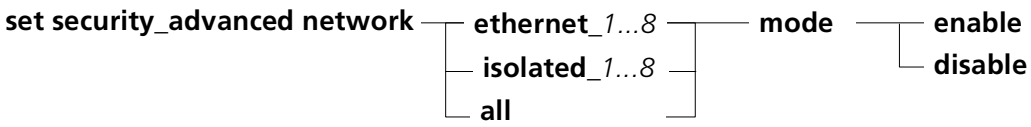
SET SECURITY_ADVANCED NETWORK MODE

Use the SET SECURITY_ADVANCED NETWORK MODE command to enable or disable security functions on an Ethernet network that has an Ethernet Private Line Card assigned to it.

The security mode network parameter allows you to disable or enable all network security functions. When this function is disabled, the Ethernet Private Line Card does not send security messages to any media module connected to a secure network. Consequently, if this parameter is disabled, none of the network parameters function.

Do not enable this network parameter until you have completed configuring the remaining network parameters. This ensures that your network security configuration is completed when you enable security on the network.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
all	Specifies that this command applies to all Ethernet networks.
enable	Enables security mode.
disable	Disables security mode.

Example

The following command enables security functions on ethernet_1:

```
CB5000> set security_advanced network ethernet_1 mode enable
ETHERNET_1 Administrative Mode set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK SOURCE_ADDRESS_ CHECKING

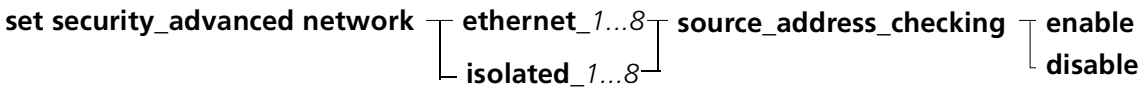
Use the SET SECURITY_ADVANCED NETWORK SOURCE_ADDRESS_CHECKING command to enable source address checking on an Ethernet network that has a Ethernet Private Line Card assigned to it.

When you enable source address checking, the source address of each packet transmitted on a secure network is checked against an established list of valid MAC addresses in the security address table. If the source address of the port does not match an address in the security table, the packet is treated as an intruder.

If you enable source address checking on your network, only ports with intruder checking enabled are looked up in the security address table.

When you enable source port checking, the Ethernet Private Line Card enables source address checking automatically.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
enable	Enables source address checking.
disable	Disables source address checking.

Example

The following command enables source address checking on ethernet_1:

```
CB5000> set security_advanced network ethernet_1
source_address_checking enable
ETHERNET_1 Source Address Checking: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED NETWORK SOURCE_PORT_ CHECKING

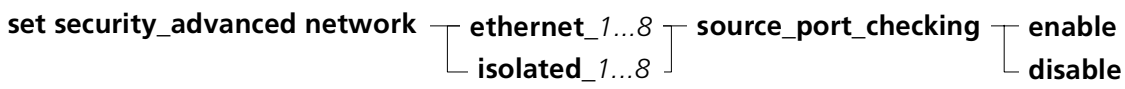
Use the SET SECURITY_ADVANCED NETWORK SOURCE_PORT_CHECKING command to enable source port checking on an Ethernet network that has a Ethernet Private Line Card assigned to it.

When you enable source port checking, the source port number and MAC address of each packet transmitted on a secure network is checked against an established list of valid port numbers and MAC addresses in the security address table. If the source port number and MAC address of the packet does not match the port number and MAC address in the security table, the packet is treated as an intruder.

If you enable source port checking on your network, only ports with intruder checking enabled are looked up in the security address table.

When you enable source port checking, the Ethernet Private Line Card enables source address checking automatically.

Format



ethernet_*1...8*	Specifies which Ethernet network to apply this command.
isolated_*1...8*	Specifies which isolated network to apply this command.
enable	Enables source port checking.
disable	Disables source port checking.

Example

The following command enables source port checking on ethernet_1:

```
CB5000> set security_advanced network ethernet_1
source_port_checking enable
ETHERNET_1 Source Port Checking: set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

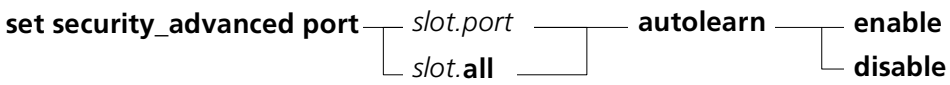
SET SECURITY_ADVANCED PORT AUTOLEARN

Use the SET SECURITY_ADVANCED PORT AUTOLEARN command to automatically discover MAC addresses associated with ports on an Ethernet network that has an Ethernet Private Line Card assigned to it.

Autolearning enables the CoreBuilder 5000 Ethernet Private Line Card to scan a secure network and store the MAC address and associated port of each node on the network in the security address table. After it is enabled, you can use this parameter, with other port and network parameters, to secure the port.

If autolearning is enabled on a per-port level, you must also enable network autolearning and connect each port to a secure network.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.
enable	Enables the autolearn feature.
disable	Disables the autolearn feature.

Example

The following command enables autolearning on port 5.1:

```
CB5000> set security_advanced port 5.1 autolearn enable
Port 05.01 autolearn set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED PORT FAILSAFE

Use the SET SECURITY_ADVANCED PORT FAILSAFE command to require security message transmissions on an Ethernet network that has an Ethernet Private Line Card assigned to it.

This port parameter instructs any media module connected to a secure network to expect a security message transmission from the Ethernet Private Line Card for each transmitted packet. This message provides information on whether or not the module should jam a transmitted packet.

If, however, a security message for a packet is not transmitted to the media module, and per-port jamming as well as failsafe are enabled, the media module automatically jams all outgoing packets.

You must enable both failsafe and per-port jamming for the failsafe feature to function. Do not enable failsafe on a port until that port is operational and the appropriate security port and network parameters are set.

After security is configured, do not disable security on a network that has per-port failsafe enabled, or switch a secure port to an unsecured network. Disabling security or switching the port to an unsecured network causes the failsafe port parameter to jam all transmitted packets destined for the port.

Format

slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.
enable	Enables port failsafe.
disable	Disables port failsafe.

Example

The following command enables failsafe on port 5.1:

```
CB5000> set security_advanced port 5.1 failsafe enable
Port 05.01 failsafe set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED PORT GROUP_CODE_(A,B)

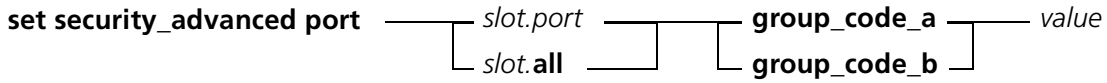
Use the SET SECURITY_ADVANCED PORT GROUP_CODE_(A,B) command to assign the same MAC address to two ports on an Ethernet network that has a CoreBuilder 5000 Ethernet Private Line Card assigned to it. Group codes enable you to assign a single MAC address to multiple ports on a secure network. This is an important feature when you use two ports to form a redundant link to a node. You can also assign each port to a maximum of two group codes. Refer to the module user guide for a sample configuration that uses group codes.

If you assign multiple ports to a single group code, data sourced from addresses also associated with the group code are transmitted to the network.

Group code 256 is a *global group code.* The global group code lets certain ports route packets with unknown destinations. If, for example, one of the ports on a media module connects to another hub or to an external bridge, you must configure that port using the global group code. This prevents traffic destined for another hub from being jammed.

If you configure a port with jamming and assign the global group code to that port, any packets that the system transmits on the originating hub that are not destined for a node on a remote hub are still jammed at that port. Only packets with an unknown destination are sent to the remote hub.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number in the hub.
group_code_(a,b)	The group code you are assigning the MAC address to.
value	User-defined group code number: 0 (no group) 1 through 254

Example

The following command assigns a group code a value of 23 on port 5.1:

```
CB5000>  set security_advanced port 5.1 group_code_a 23
Port 05.01 group_code_A set to 23.
```

Related Command

SHOW SECURITY_ADVANCED

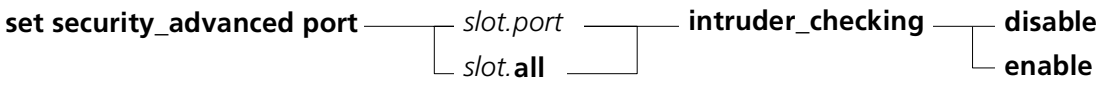
SET SECURITY_ADVANCED PORT INTRUDER_CHECKING

Use the SET SECURITY_ADVANCED PORT INTRUDER_CHECKING command to enable intruder checking on ports in an Ethernet network that has an Ethernet Private Line Card assigned to it.

When you enable per-port intruder checking, the Ethernet Private Line Card compares each packet's source MAC address against an established list of valid MAC addresses in the security address table. If the source address of the port does not match an address in the security table, the packet is treated as an intruder.

You must have the source address checking network parameter enabled to look up the source address of a transmitted packet. To look up the source port number, you must have the source port checking network parameter enabled. If both of these network parameters are enabled, both the source address and related source port number must match a port number *and* MAC address in the security address table, or the packet is treated as an intruder.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports on a module. *slot* is the slot number of the module.
disable	Disables intruder checking.
enable	Enables intruder checking.

Example

The following command enables intruder checking on port 5.1:

```
CB5000> set security_advanced port 5.1 intruder_checking enable
Port 05.01 intruder_checking set to ENABLED.
```

Related Command

SHOW SECURITY_ADVANCED

SET SECURITY_ADVANCED PORT JAMMING

Use the SET SECURITY_ADVANCED PORT JAMMING command to prevent eavesdropping and intruder packets on an Ethernet network that has an Ethernet Private Line Card assigned to it.

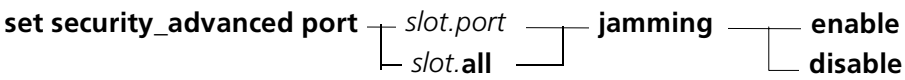
Port jamming enables you to prevent eavesdropping, jam frames sourced from an intruder on a secure network, and optionally jam all packets for which there is no associated security message.

When you enable port jamming and the system transmits a packet on the network, the Ethernet Private Line Card sends a security message to all media modules on the secure network. This message instructs the media module to jam all ports on the secure network except the port that is the intended recipient of the transmitted packet.

If jamming is enabled on a per-port level, you must also enable network eavesdrop protection and connect each port to a secure network. If you also want to prevent each port from seeing intruder transmissions, you must enable the intruder jamming network parameter.

The port jamming parameter is enabled by default. This prevents new users from both eavesdropping and seeing packets sourced from an intruder on another port.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number location of a module in the hub and *port* (1 through 40) is the port number on the specified module. For example, to identify port 4 on the module in slot 6, enter **6.4**
slot.**all**	Specifies all ports in a slot. *slot* is the slot number.
enable	Enables jamming.
disable	Disables jamming.

Example

The following command enables port jamming on port 5.1:

```
CB5000> set security_advanced port 5.1 jamming enable
Port 05.01 jamming set to ENABLED.
```

Related Command

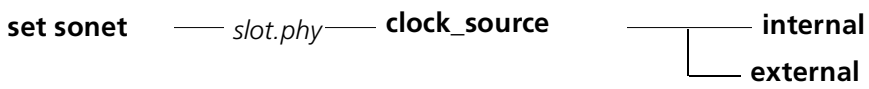
SHOW SECURITY_ADVANCED

SET SONET CLOCK_SOURCE

Use the SET SONET CLOCK_SOURCE command to determine whether the module generates SONET timing locally (internal) or derives timing from the received signal on the SONET interface (external). This parameter is configurable per physical port (PHY).

Setting this parameter takes effect immediately and does not require a module reset.

Format



slot.phy	Identifies the slot and port for this operation. *slot* (1 through 17) is the slot number and *phy* (1 or 2) is the PHY port number. For example, to identify PHY port 1 on the module in slot 4, enter **4.1**
internal	Generates SONET timing locally.
external	Derives timing from the received signal on the SONET interface. The default value is external.

Example

The following command sets the clock source to internal:

```
CB5000> set sonet 4.1 clock_source internal
Slot 04.01 parameter set.
```

Related Command

SHOW SONET STATUS

SET TERMINAL BAUD

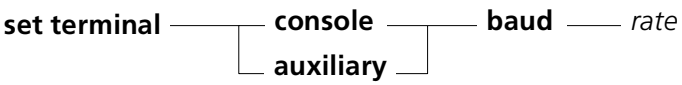
Use the SET TERMINAL BAUD command to set the baud rate for a serial (Console or Auxiliary) port. The baud rates of the serial port and the connected device must match.

When using higher baud rates (19200 and 38400), enable Xon/Xoff flow control on the connected device.

To connect a device that is set to a different baud rate than the serial port, change the serial port baud rate to the baud rate used by the device as follows:

1. Set a terminal to 9600 baud and press Enter to access the DMM.
2. Enter the SET TERMINAL BAUD command to set the baud rate to your specifications. After you set the new rate, you lose your connection to the DMM.
3. Remove the terminal connection and connect the device that has the different baud rate to resume your connection to the DMM or change the connected device to the new baud rate.
4. Enter the SAVE TERMINAL command to save the new terminal setting.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
rate	Selects the baud rate for the Console or Auxiliary port. *rate* = 300, 1200, 2400, 4800, 9600, 19200, 38400 The factory default setting is 9600.

Example

The following command sets the Auxiliary port baud rate to 2400:

```
CB5000> set terminal auxiliary baud 2400
Terminal parameter changed.
```

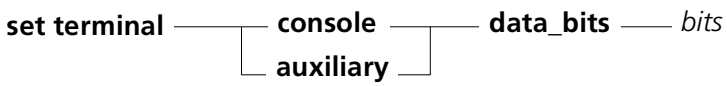
Related Command

SHOW TERMINAL

SET TERMINAL DATA_BITS

Use the SET TERMINAL DATA_BITS command to set the number of data bits used for a serial (Console or Auxiliary) port.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
bits	Selects the number of data bits for the serial port. *bits* = 7 or 8 The factory default setting is 8.

Example

The following command sets the Auxiliary port data bits to 7:

```
CB5000> set terminal auxiliary data_bits 7
Terminal parameter changed.
```

Related Command

SHOW TERMINAL

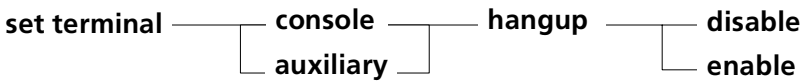
SET TERMINAL HANGUP

Use the SET TERMINAL HANGUP command to set the hangup parameter for the DMM. The hangup parameter value applies to both the Console and Auxiliary ports. When hangup is enabled, the DMM automatically disconnects the modem when you log out.

The default factory setting is disable. If hangup is disabled, the modem is disconnected either by the terminal timing out or by your manually hanging up the modem.

If you fail to hang up the modem connection, an unauthorized user may pick up the last login session.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
disable	Disables hangup for the Console and Auxiliary ports. The factory setting is disable.
enable	Enables hangup for the Console and Auxiliary ports.

Example

The following command disables hangup on the Console port:

```
CB5000> set terminal console hangup disable
Terminal parameter changed.
```

Related Command

SHOW TERMINAL

SET TERMINAL MODE

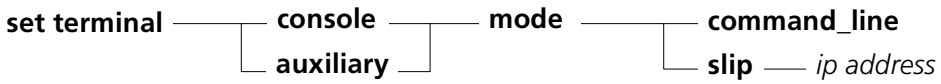
Use the SET TERMINAL MODE command to set a serial (Console or Auxiliary) port to command_line or SLIP (Serial Line Interface Protocol) mode. SLIP allows TCP/IP connections over a serial line. Its primary application in the hub is to allow you to connect a workstation running network management software to a DMM serial port.

To open a SLIP session, enter the following commands from either serial port or by using TELNET:

- SET IP SUBNET_MASK *mask* SLIP (where the mask is the workstation's IP subnet)
- SET IP IP_ADDRESS *address* SLIP (where the address is the DMM IP address for the SLIP network)
- SET TERMINAL *port* (*baud*, *data_bits*, *parity*, *stop_bits*) (set as appropriate for the serial connection running SLIP)
- SET TERMINAL *port* MODE SLIP (which sets the port to SLIP)

Use a standard break character to end the SLIP session and return the SLIP port to command line mode.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
command_line	Sets the selected port to command_line mode. The default factory setting is command_line.
slip	Sets the selected port to SLIP mode.
ip address	The destination IP address for the SLIP connection.

Example

The following command sets the console port to SLIP mode:

```
CB5000> set terminal console mode slip 155.104.12.16
Terminal parameter changed.
```

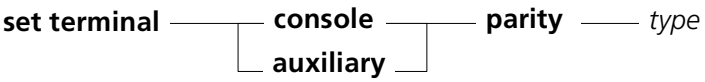
Related Command

SHOW TERMINAL

SET TERMINAL PARITY

Use the SET TERMINAL PARITY command to set the parity for the serial (Console or Auxiliary) port.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
type	Selects the parity type for the serial port. *type* = even, odd, none The default factory setting is none.

Example

The following command sets the Console port parity to even:

```
CB5000> set terminal console parity even
Terminal parameter changed.
```

Related Command

SHOW TERMINAL

SET TERMINAL PROMPT

Use the SET TERMINAL PROMPT command to customize the management prompt that is displayed on your terminal during a terminal session. The prompt is used for both the Console and Auxiliary ports.

If you log in to a number of different DMMs remotely, make the terminal prompt and the device name the same for each individual DMM. Using the same name makes it easy to identify the hub you are currently logged in to. The factory default setting is `CB5000>`.

Format

set terminal —— **prompt** —— *prompt text*

prompt text	The prompt that appears during a terminal session. Use up to 15 characters.

Example

The following command sets the prompt to my_hub>:

```
CB5000> set terminal prompt my_hub>
Terminal parameter changed.

my_hub>
```

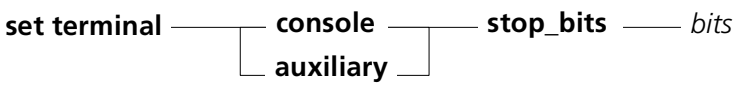
Related Command

SHOW TERMINAL

SET TERMINAL STOP_BITS

Use the SET TERMINAL STOP_BITS command to set the number of stop bits used for a serial (Console or Auxiliary) port.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
bits	Selects the number of stop bits for the serial port. *bits* = 1 or 2 The default factory setting is 2.

Example

The following command sets the Auxiliary port stop bits to 1:

```
CB5000> set terminal auxiliary stop_bits 1
Terminal parameter changed.
```

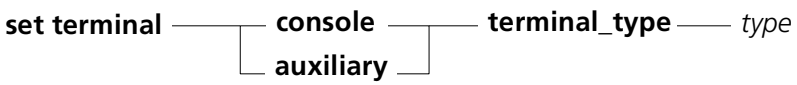
Related Command

SHOW TERMINAL

SET TERMINAL TERMINAL_TYPE

Use the SET TERMINAL TERMINAL_TYPE command to define the type of terminal connected to a serial (Console or Auxiliary) port. The DMM uses the terminal type when establishing a TELNET session. The terminal type informs the remote device which control sequences to transmit to the DMM.

Format



console	Selects the Console port as the serial port for this operation.
auxiliary	Selects the Auxiliary port as the serial port for this operation.
type	Identifies the type of terminal connected to the serial port. Use up to 40 characters. The default factory setting is VT100.

Example

The following command sets the Console terminal type to VT200:

```
CB5000> set terminal console terminal_type
Enter terminal type: vt200
Terminal parameter changed.
```

Related Command

SHOW TERMINAL

SET TERMINAL TIMEOUT

Use the SET TERMINAL TIMEOUT command to configure the DMM to automatically log you out of the system if you have not typed anything for a specified number of minutes.

You only lose the changes if the DMM is reset before you log back in and save them.

Format

set terminal timeout — *timeout period*

timeout period	Selects the length of the timeout interval in minutes. A value of 0 disables the timeout function, allowing inactive terminal sessions to last indefinitely. The default factory setting is 0.

Example 1 The following command logs you out of the DMM after 10 minutes of inactivity:

```
CB5000> set terminal timeout 10
```

Example 2 The following message is displayed if changes are not saved before the timeout occurs:

```
Warning: Unsaved changes.
Bye
```

Related Command SHOW TERMINAL

SET TFTP FILE_NAME

Use the SET TFTP FILE_NAME command to specify the name of the file to be downloaded over the network (in-band) to the DMM. Enter up to 128 alphanumeric characters. The DMM assumes a default pathname of `/tftpboot`. When you enter the command, the DMM prompts you for the filename of the download file in the /tftpboot directory.

You must enter the TFTP filename within 10 seconds or the command times out.

Format

set tftp file_name ___ *filename*

filename	Filename of the download file in the /tftpboot directory, which you select when prompted.

Example 1

The following command specifies that the DMM request the file `newfile.bin` in the `/tftpboot` directory when you enter the DOWNLOAD IN_BAND command:

```
CB5000> set tftp file_name
Enter tftp file name:
> newfile.bin
TFTP file name changed.
```

Example 2

The following command specifies that the DMM request the file `newfile.bin` in the directory `/my_directory` when you enter the DOWNLOAD IN_BAND command:

```
CB5000> set tftp file_name
Enter tftp file name:
> /my_directory/newfile.bin
TFTP file name changed.
```

Some TFTP servers need to be reconfigured to allow the use of directories other than `/tftpboot`.

Related Commands

DOWNLOAD IN_BAND
SAVE TFTP
SET TFTP SERVER_IP_ADDRESS
SHOW TFTP

SET TFTP SERVER_IP_ADDRESS

Use the SET TFTP SERVER_IP_ADDRESS command to set the IP address of the TFTP server to be used for in-band downloads.

Format

set tftp server_ip_address ——— *ip address*

ip address	The IP address of the TFTP server. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4.

Example

The following command sets the IP address of the TFTP server:

```
CB5000> set tftp server_ip_address 156.12.2.3
TFTP server ip-address set.
```

Related Commands

DOWNLOAD IN_BAND
SAVE TFTP
SET TFTP FILE_NAME
SHOW TFTP

SET TR_SURROGATE CRS_STATION

Use the SET TR_SURROGATE CRS_STATION command to enable the TR-NMC's Configuration Report Server Station features.

Format

set tr_surrogate — *slot.***2** — **crs_station** — *setting* — *mac address* — *setting*

slot	Specifies the hub slot number where *slot* = 1 through 17
setting	The following settings are available: ■ allow_acc_pri Lets you specify the maximum token access priority that the station with the indicated MAC address is allowed to transmit. ■ enb_fun_class Lets you enter the function classes that the station with the indicated MAC address is allowed to transmit. ■ phy_loc Lets you set the physical location subvector that is transmitted as part of Report Ring Station Addresses MAC Frames sent by the station with the indicated MAC address. ■ remove_sta Lets you send a request to remove the station with the indicated MAC address from the ring.
mac address	The MAC address for which you are setting this parameter.
setting	Enable or disable.

Example

The following command enables maximum token access priority on the TR-NMC in slot 11.2:

```
CB5000> set tr_surrogate 11.2 crs_station allow_acc_pri
00:04:e4:40:00:c0 enable
```

Related Commands

SET TR_SURROGATE SURR_STATUS CRS_ADMIN
SHOW TR_SURROGATE

SET TR_SURROGATE CRS_STATUS

Use the SET TR_SURROGATE CRS_STATUS command to enable the generate traps option on the TR-NMC's Configuration Report Server. When enabled, this option instructs the CRS function to report configuration change traps.

Format

set tr_surrogate ——— *slot.***2** ——— **crs_status crs_traps** ——— *setting*

slot	Specifies the hub slot number, where *slot* = 1 through 17
setting	CRS server generates configuration change traps. Values are: ■ Enable ■ Disable

Example

The following command allows the TR-NMC in slot 11.2 to generate traps:

```
CB5000> set tr_surrogate 11.2 crs_status crs_traps enable
```

Related Command

SHOW TR_SURROGATE

SET TR_SURROGATE REM_STATUS

Use the SET TR_SURROGATE REM_STATUS command to enable the TR-NMC's Ring Error Monitor (REM) features.

Format

set tr_surrogate ——— *slot.***2** ——— **rem_status** —— *option* —— *setting*

slot	Specifies the hub slot number. where *slot* = 1 through 17
option	See table that follows for REM option descriptions.
setting	Enables or disables REM and CRS features.

Option	Description
all_flags	Activates all items listed in this table.
rem_traps	Determines if REM sends traps to a Network Manager monitoring the segment.
weight_excded_traps	Determines if REM generates weight-exceeded traps. These traps indicate that a soft-error threshold has been exceeded for a particular fault domain.
preweight_excded_traps	Determines if REM generates pre-weight-exceeded traps. These traps indicate that an impending soft-error threshold has been exceeded by a station.
rcvr_congestion_traps	Determines if REM generates receiver congestion traps. These traps indicate that a station's receive buffer has been overloaded by incoming traffic.
noniso_threshold_excd_traps	Determines if REM generates Non-Isolating Threshold Exceeded traps. These traps indicate that one of the non-isolating error counters being monitored has exceeded its threshold.
forward_frames_traps	Determines if REM forwards information in the Report Neighbor Notification MAC frames and the Report Monitor Error MAC frames to a LAN manager on the segment.
ring_line_error_data	Determines if REM includes line error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_internal_error_data	Determines if REM includes internal error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_burst_error_data	Determines if REM includes burst error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_ac_error_data	Determines if REM includes A/C error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_abortxmt_error_data	Determines if REM includes abort transmit error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_lostframes_error_data	Determines if REM includes lost frames error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_rcvrcngst_error_data	Determines if REM includes receiver congestion error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_framecopy_error_data	Determines if REM includes frame copied error data in the ring-intensive REM Forward Soft Error MAC Frame trap.

Option	Description
ring_frequency_error_data	Determines if REM includes frequency error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
ring_token_error_data	Determines if REM includes token error data in the ring-intensive REM Forward Soft Error MAC Frame trap.
auto_line_error_data	Determines if REM includes line error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_internal_error_data	Determines if REM includes internal error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_burst_error_data	Determines if REM includes burst error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_ac_error_data	Determines if REM includes A/C error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_abortxmt_error_data	Determines if REM includes abort transmit error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_lostframes_error_data	Determines if REM includes lost frames error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_rcvrcngst_error_data	Determines if REM includes receiver congestion error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_framecopy_error_data	Determines if REM includes frame copied error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_frequency_error_data	Determines if REM includes frequency error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
auto_token_error_data	Determines if REM includes token error data in the auto-intensive REM Forward Soft Error MAC Frame trap.
crs_traps	Determines if the CRS function is configured to report Ring Topology Change traps.
reset	Resets all REM options.

Example The following command includes token error data in the auto-intensive REM forward soft error MAC frame trap from the TR-NMC in slot 11.2:

```
CB5000> set tr_surrogate 11.2 rem_status auto_token_error_data
enable
REM status - REM admin set to ENABLED.
```

Related Command SHOW TR_SURROGATE

SET TR_SURROGATE SURR_STATUS

Use the SET TR_SURROGATE SURR_STATUS command to enable the TR-NMC's Ring Error Monitor (REM) and Configuration Report Server (CRS) features.

Format

set tr_surrogate ——— *slot*.**2** —— **surr_status** —— *option* —— *setting*

slot.**2**	Specifies the hub slot number, where *slot* = 1 through 17
option	See table that follows for Surrogate option descriptions.
setting	Enables or disables REM and CRS features.

Option	Description
surr_admin	Enables or disables the Token Ring surrogate functions (REM and CRS) for the indicated slot or subslot. If you do not use the surrogate information that the TR-NMC provides, you should set surr_admin status to disable to conserve system resources.
ring_segment	Enables or disables the surrogate ring segment feature.
rem_admin	Enables or disables the Ring Error Monitor (REM) feature. To activate REM, surr_admin must also be enabled.
crs_admin	Enables or disables the Configuration Report Server (CRS) feature. To activate CRS, surr_admin must also be enabled.

Example

The following command enables Ring Error Monitor on the TR-NMC in slot 11.2:

```
CB5000> set tr_surrogate 11.2 surr_status rem_admin enable
Surrogate status - REM admin set to ENABLED.
```

Related Command

SHOW TR_SURROGATE

SET TRUNK CABLE_MONITOR

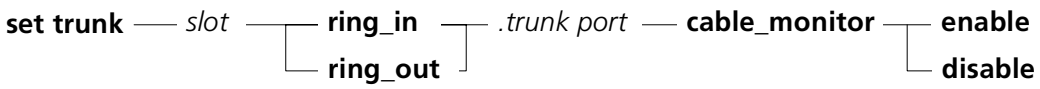
Use the SET TRUNK CABLE_MONITOR command to enable or disable cable monitor mode on the copper Ring-In and Ring-Out ports on ONline Token Ring modules.

Cable monitor mode sets the ports so they wrap the ring to keep the ring running if the module senses a cable fault. For this mode to work, you must use the 3Com TRCABLE-10 or TRCABLE-30 cable to connect the hub ports.

You can enable cable monitor mode to connect a Token Ring module in a different hub (up to 30 inches apart) if you also set the port to network map external. This scenario is discussed in the description of the SET TRUNK NETWORK_MAP EXTERNAL command.

Refer to the appropriate Token Ring Module Installation Guide for more information on cable monitor mode.

Format



slot	Hub slot 1 through 17.
ring_in	Specifies if the port is a Ring-In port.
ring_out	Specifies if the port is a Ring-Out port.
.trunk port	1 or 2 (required only on Model Number 3CB6210-OFR).
enable	Use when connecting Ring-In and Ring-Out ports of Token Ring modules in the same hub.
disable	Use when connecting to equipment not made by 3Com.

Example

The following command enables cable monitor mode for the Ring-In port of the ONline Token Ring Fiber Repeater Module in slot 5 of the hub:

```
CB5000> set trunk 5 ring_in.1 cable_monitor enable
Cable Monitor set to ENABLED.
```

Related Commands

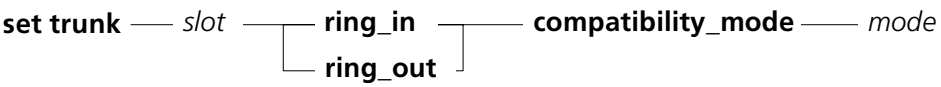
SHOW TRUNK
SET TRUNK NETWORK

SET TRUNK COMPATIBILITY_MODE

Use the SET TRUNK COMPATIBILITY_MODE command to set the trunk operating mode to a mode compatible with the remote Ring-In/Ring-Out product.

Be sure to configure the trunks of the remote products according to the user documentation for those products.

Format



slot	Identifies the slot for this operation.
ring_in	Selects the Ring-In trunk for this operation.
ring_out	Selects the Ring-Out trunk for this operation.
mode	■ onsemble — Configures the selected trunk to interoperate with a remote ONsemble® Token Ring Hub. The factory setting is onsemble. ■ CoreBuilder 5000 — Configures the selected trunk to interoperate with a remote CoreBuilder® 5000 hub. (You need to use CoreBuilder 5000 mode when connecting to older ONcore Integrated System hubs) ■ online — Configures the selected trunk to interoperate with a remote ONline™ System Concentrator. ■ 8230 — Configures the selected trunk to interoperate with a remote IBM 8230 CAU. ■ 8238 — IBM Token Ring stackable hub. ■ 8250 — Configures the selected trunk to interoperate with a remote IBM 8250 Multiprotocol Intelligent Hub. ■ 8260 — Configures the selected trunk to interoperate with a remote IBM 8260 Multiprotocol Intelligent Switching Hub.

Example

The following commands set the Ring-In/Ring-Out trunks to interoperate with a remote CoreBuilder 5000 hub:

```
CB5000> set trunk 1 ring_in compatibility_mode CoreBuilder 5000
Compatibility mode set to CoreBuilder 5000.

CB5000> set trunk 1 ring_out compatibility_mode CoreBuilder 5000
Compatibility mode set to CoreBuilder 5000.
```

Related Commands

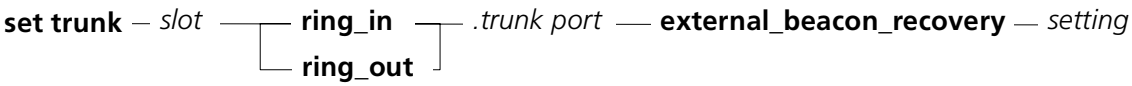
SAVE MODULE_PORT
SHOW MODULE

SET TRUNK EXTERNAL_BEACON_ RECOVERY

Use the SET TRUNK EXTERNAL_BEACON_RECOVERY command when using 8250 Token Ring modules with devices that do not support beacon recovery (for example IBM 8228). Modules that do not support beacon recovery may cause a multi-hub ring to segment at all trunk ports. To prevent this problem, set the external beacon recovery parameter to non_exists for trunks connected to devices that do not support beacon recovery.

This parameter informs the DMM that the connected device does not support beacon recovery and enables the DMM to isolate the beaconing device. Failure to designate a device that does not support beacon recovery can cause the entire ring to segment if beaconing occurs on the remote device.

Format



slot	Hub slot 1 through 17.
ring_in	Specifies if the port is a Ring-In port.
ring_out	Specifies if the port is a Ring-Out port.
.trunk port	1 or 2 (required only on Model Number 3CB6210M-OFR).
setting	■ exists — Connected device supports beacon recovery. ■ non_exists (default) — Connected device does not support beacon recovery.

Example

The following command assumes a 3822TR in slot 3 in one hub, configured in a multi-hub ring, is connected to an 8228 (which does not have beacon recovery capabilities). To prevent the ring from segmenting in the event the 8228 beacons, enter the following command:

```
CB5000> set trunk 3 ring_in.1 external_beacon_recovery non_exists
External beacon recovery set to non_exists.
```

Related Command

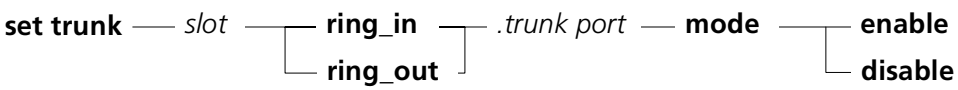
SHOW TRUNK

SET TRUNK MODE

Use the SET TRUNK MODE command to enable or disable the Ring-In and Ring-Out ports on Token Ring modules.

Refer to the appropriate Token Ring Installation Guide for more information on Ring-In and Ring-Out ports.

Format



slot	Hub slot 1 through 17.
ring_in	Selects the Ring-In trunk for this operation.
ring_out	Selects the Ring-Out trunk for this operation.
.trunk port	1 or 2 (required only on Model Number 3CB6210M-OFR).
enable	Allows you to add a module to the ring.
disable	Deactivates the selected port.

Example

The following commands enable the Ring-In and Ring-Out ports of the Token Ring module in slot 5 of the hub:

```
CB5000> set trunk 5 ring_in mode enable
Trunk 05.01 ring_in set to ENABLED.

CB5000> set trunk 5 ring_out mode enable
Trunk 05.01 ring_out set to ENABLED.
```

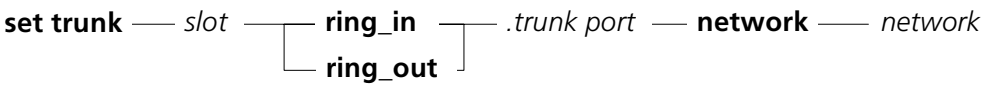
Related Commands

SHOW TRUNK
SET TRUNK COMPATIBILITY_MODE

SET TRUNK NETWORK

Use the SET TRUNK NETWORK command to assign a Ring-In or Ring-Out port to a specific network.

Format



slot	Specifies the hub slot number, where *slot* = 1 through 17
ring_in	Specifies if the port is a Ring-In port.
ring_out	Specifies if the port is a Ring-Out port.
.trunk port	Specifies the trunk port. *.trunk port* = 1 or 2 (required only on Model Number 6210M-DFR)
network	Specifies the network to which you are assigning the Ring-In or Ring-Out port. *network* = *token_ring_1* through *token_ring_10* (ring_in), *isolated_1* through *isolated_10* (ring_out), isolated

Example

The following command sets the Ring-In port on the Token Ring Dual Fiber Repeater Module in slot 3 to token_ring_1:

```
CB5000> set trunk 3 ring_in.1 network token_ring_1
Trunk 03 ring_in.1 network id set to TOKEN_RING_1.
```

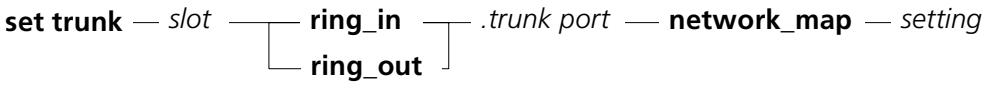
Related Commands

SHOW TRUNK
SET PORT

SET TRUNK NETWORK_MAP

Use the SET TRUNK NETWORK_MAP command to determine if the Network Map feature should be extended from one hub to the next hub between Token Ring copper trunk ports. This command is valid for ONLine Token Ring modules only.

Format



slot	Hub slot 1 through 17.
ring_in	Specifies if the port is a Ring-In port.
ring_out	Specifies if the port is a Ring-Out port.
.trunk port	1 or 2 (required only on Model Number 5202M-FR).
setting	External — Ensures a correct port-to-address mapping when you connect copper trunk ports on modules in different hubs.
	Internal — Ensures a correct port-to-address mapping when you connect copper trunk ports on modules in the same hubs.

Example

The following command sets the Ring-In port of the Token Ring module in slot 5 to an internal network map, meaning that this port is connected to another trunk port in the same hub:

```
CB5000> set trunk 5.1 ring_in network_map internal
Network map state set to INTERNAL.
```

Related Commands

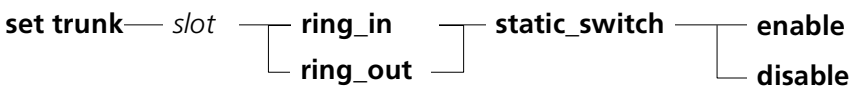
SHOW TRUNK
SHOW RING_MAP

SET TRUNK STATIC_SWITCH

Use the SET TRUNK STATIC_SWITCH command to prevent the network configuration of a trunk from being changed when either trunk in a pair (either the Ring-In or the Ring-Out) is enabled. This prevents inadvertent changes to live rings.

Because setting the network of a trunk simultaneously affects both members of the trunk pair, this command works on a pair basis. Enabling or disabling the static switch on one trunk automatically changes it on the other.

Format



slot	*slot* (1 through 17) is the slot that contains the trunk ports you are configuring.
enable	Forces users to disable trunks before switching networks. This prevents inadvertent changes to live rings.
disable	Does not force users to disable trunks down before switching networks.

Example

The following command disables static switch on trunks on the module in slot 6:

```
CB5000> set trunk 6 ring_in static_switch disable
Trunk static switch set to DISABLED.
```

Related Commands

SAVE MODULE_PORT
SET PORT STATIC_SWITCH
SHOW PORT

SET VBRIDGE AFT AGING_TIME

Use the SET VBRIDGE AFT AGING_TIME command to adjust the address table aging time (the time it takes for an entry to "age out" of the address table) for a particular SwitchModule virtual bridge.

Format

set vbridge — *vbridge* — **aft** — **aging_time** — *aging time*

vbridge	The virtual bridge (1 through 240) whose aging time you want to adjust.
aging time	Either: ■ 0 to disable the aging process. ■ 10 through 1,000,000 (seconds). The default is 300 seconds.

Example

The following command sets the aging time for virtual bridge 24 to 500 seconds:

```
CB5000> set vbridge 24 aft aging_time 500
```

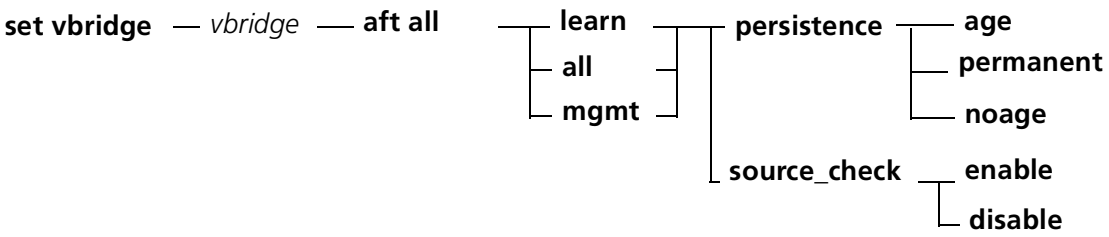
Related Command

SHOW VBRIDGE AFT

SET VBRIDGE AFT ALL

Use the SET VBRIDGE AFT ALL command to create filters and add entries to the address table of a particular SwitchModule virtual bridge.

Format



vbridge	The virtual bridge (1 through 240) you want this command to affect.
all	Specifies that the command affects all learned and user-created (mgmt) addresses in the virtual bridge's address table.
learn	Specifies that the command affects all addresses learned by the SwitchModule in the virtual bridge's address table.
mgmt	Specifies that the command affects all user-created addresses in the virtual bridge's address table.
persistence	Specifies the length of time you want an address entry or set of entries to remain in the virtual bridge's address table.
age	The address entry ages out of the address table during the next virtual bridge aging process. This is the default setting for learned address entries.
noage	The address entry remains in the address table until you reboot the SwitchModule. The aging process does not affect the entry.
permanent	The address entry remains in the address table permanently, even after you reboot the SwitchModule.
source_check	Specifies a filter that filters according to packet source MAC address. Use this option to "lock down" an address or set of addresses to a particular port.
disable	Disables source checking for the entry or set of entries you specify.
enable	Enables source checking for the entry or set of entries you specify.

Example

The following command locks the address table. After you enter this command, devices moved to a different location cannot transmit on virtual bridge 2:

```
CB5000> set vbridge 2 aft all all source_check enable
AFT Set Succeeded: Vbridge 2 Address 00-00-0c-01-a2-03
AFT Set Succeeded: Vbridge 2 Address 00-00-0c-04-25-26
AFT Set Succeeded: Vbridge 2 Address 00-00-b5-07-18-a9
AFT Set Succeeded: Vbridge 2 Address 00-00-b5-21-02-53
```

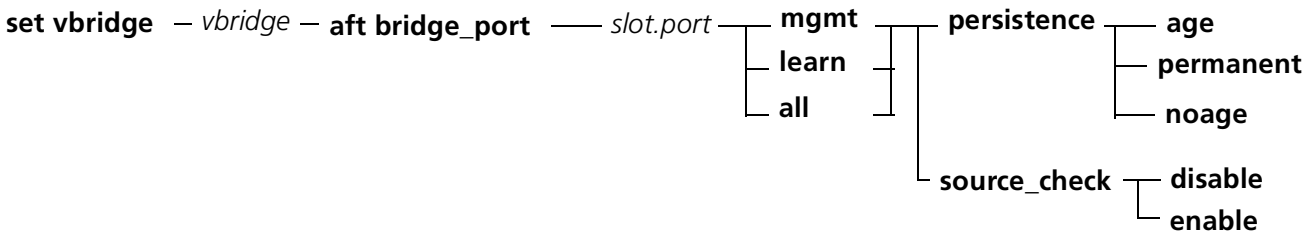
Related Commands

SET VBRIDGE AFT BRIDGE_PORT
SET VBRIDGE AFT MAC
SHOW VBRIDGE AFT

SET VBRIDGE AFT BRIDGE_PORT

Use the SET VBRIDGE AFT BRIDGE_PORT command to enable source checking for all MAC addresses of devices attached to a port. Before forwarding any packet that arrives on the specified port, the SwitchModule checks the address table to verify that the packet's source MAC address is valid for the specified port.

Format



vbridge	1 through 240. The assigned virtual bridge number.
slot.port	*slot* is 1 through 17. *port* is 1 through 24. The command affects all entries in the address table associated with this bridge port.
slot.**all**	*slot* is 1 through 17. The command affects all entries in the address table associated with all bridge ports on this SwitchModule.
all	Specifies that the command affects all learned and user-created (mgmt) addresses in the virtual bridge's address table.
learn	Specifies that the command affects all addresses learned by the SwitchModule in the virtual bridge's address table.
mgmt	Specifies that the command affects all user-created addresses in the virtual bridge's address table.
persistence	Specifies the length of time you want an address entry or set of entries to remain in the virtual bridge's address table.
age	The address entry ages out of the address table during the next virtual bridge aging process. This is the default setting for learned address entries.
noage	The address entry remains in the address table until you reboot the SwitchModule. The aging process does not affect the entry.
permanent	The address entry remains in the address table permanently, even after you reboot the SwitchModule.
source_check	Specifies a filter that filters according to packet source MAC address. Use this option to "lock down" an address or set of addresses to a particular port.
disable	Disables source checking for the entry or set of entries you specify.
enable	Enables source checking for the entry or set of entries you specify.

Example The following command enables source checking for all MAC addresses of devices attached to port 3.5. Before forwarding any packet that arrives on port 3.5, the SwitchModule searches the address table to verify that the packet's source MAC address is valid for port 3.5.

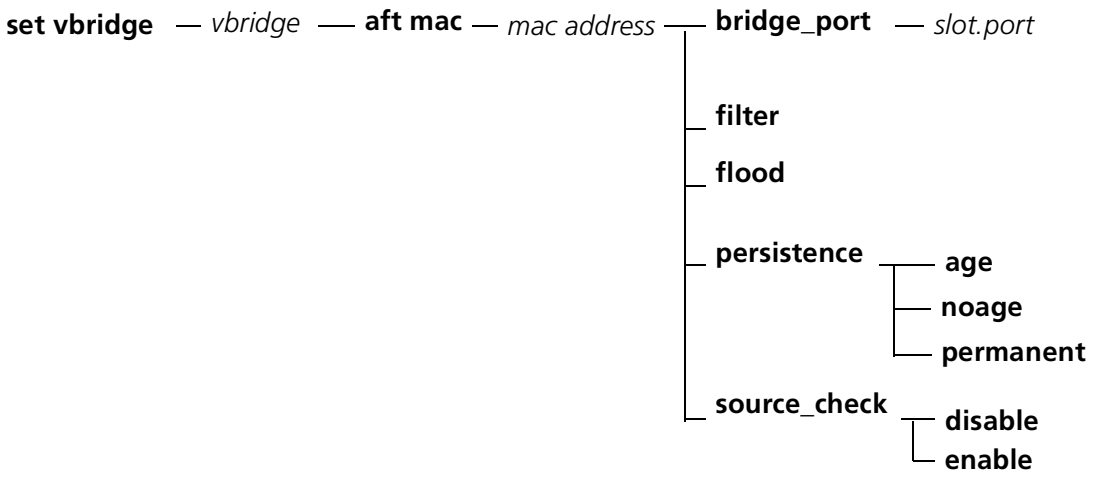
```
CB5000> set vbridge 2 aft bridge_port 3.5 all source_check enable
AFT Set Succeeded: Vbridge 2 Address 10-00-5a-f1-23-45
AFT Set Succeeded: Vbridge 2 Address 10-00-53-11-23-4a
```

Related Commands SET VBRIDGE AFT ALL
SET VBRIDGE AFT MAC
SHOW VBRIDGE AFT

SET VBRIDGE AFT MAC

Use the SET VBRIDGE AFT MAC command to create filters and add entries to an SwitchModule address table (address forwarding table or AFT). You also use this command to adjust the address table aging time (the time it takes for an entry to "age out" of the address table).

Format



vbridge	The assigned virtual bridge number. Values are 1 through 240.
mac address	Specifies the MAC address that the command affects.
bridge_port	Assigns a MAC address to a particular bridge port. Packets that contain the destination MAC address go to the bridge port only.
slot.port	*slot* (1 through 17) and *port* (1 through 24) for which you are creating a MAC address filter.
filter	Specifies that the filter you create filters, or drops, the type of packet you specify.
flood	Specifies that the filter you create floods the type of packet you specify to all ports in the virtual bridge.
persistence	Specifies the length of time you want an address entry or set of entries to remain in the virtual bridge's address table.
age	The address entry ages out of the address table during the next virtual bridge aging process. This is the default setting for learned address entries.
noage	The address entry remains in the address table until you reboot the SwitchModule. The aging process does not affect the entry.
permanent	The address entry remains in the address table permanently, even after you reboot the SwitchModule.
source_check	Specifies a filter that filters according to packet source MAC address. Use this option to "lock down" an address or set of addresses to a particular port.
disable	Disables source checking for the entry or set of entries you specify.
enable	Enables source checking for the entry or set of entries you specify.

Example The following command creates a filter for virtual bridge 2, then assigns the filter a persistence of noage. The filter causes any packet whose destination MAC address is 12-34-56-78-9f-10 to flood to all ports assigned to virtual bridge 2.

```
CB5000> set vbridge 2 aft mac 12-34-56-78-9f-10 flood
CB5000> set vbridge 2 aft mac 12-34-56-78-9f-10 persistence noage
```

Related Commands SET VBRIDGE AFT ALL
SET VBRIDGE AFT BRIDGE_PORT
SHOW VBRIDGE AFT

SET VBRIDGE IGMP_SNOOPING MODE

Use the SET VBRIDGE IGMP_SNOOPING MODE command to enable or disable IGMP Snooping on a defined Vbridge.

Format

vbridge	The assigned virtual bridge number. Values are 1 through 240.
enable	Enables IGMP Snooping on the Vbridge.
disable	Disables IGMP Snooping on the Vbridge. This is the default.

Example

The following command enables IGMP Snooping on virtual bridge 12:

```
CB5000> set vbridge 12 igmp_snooping mode disable
```

Related Commands

SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME

Use the SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME command to set the IGMP Snooping group IP address aging time in seconds on a defined Vbridge.

Format

set vbridge — *vbridge* — **igmp_snooping** — **group** — **age_time** – *time*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
time	Group aging time in seconds. The default is 300.

Example

The following command sets the IGMP Snooping group aging time on virtual bridge 12 to 400 seconds:

```
CB5000> set vbridge 12 igmp_snooping group age_time 400
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME

Use the SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME command to set the IGMP Snooping router and querier port aging time in seconds on a defined Vbridge.

Format

set vbridge — *vbridge* — **igmp_snooping** — **port** — **age_time** – *time*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
time	Group aging time in seconds. The default is 300.

Example

The following command sets the IGMP Snooping router and querier port aging time on virtual bridge 12 to 400 seconds:

```
CB5000> set vbridge 12 igmp_snooping port age_time 400
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL

Use the SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL command to set the IGMP Snooping querying interval in seconds for a Vbridge that is acting as a IGMP Snooping device.

Format

set vbridge — *vbridge* — **igmp_snooping** — **query_interval**— *time*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
time	Group aging time in seconds. The default is 300.

Example

The following command sets the IGMP Snooping router and querier port aging time on virtual bridge 12 to 350 seconds:

```
CB5000> set vbridge 12 igmp_snooping query_interval 350
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME

Use the SET VBRIDGE IGMP SNOOPING QUERY LISTEN_TIME command to set the time in seconds for a Vbridge to listen for a router acting as a IGMP Snooping device.

Format

set vbridge – *vbridge* – **igmp_snooping** – **query** — **listen_time** — *time*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
time	Group aging time in seconds. The default is 300.

Example

The following command sets the time in seconds for a Vbridge to listen for a router acting as a IGMP Snooping device on virtual bridge 12 to 500 seconds:

```
CB5000> set vbridge 12 igmp_snooping query listen_time 500
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING QUERY MODE

Use the SET VBRIDGE IGMP_SNOOPING QUERY MODE command to set the Vbridge to an IGMP Snooping querying bridge.

Format

vbridge	The assigned virtual bridge number. Values are 1 through 240.
enable	Enables IGMP Snooping Query mode on the Vbridge.
disable	Disables IGMP Snooping Query mode on the Vbridge. This is the default.

Example

The following command sets the IGMP Snooping Query mode on virtual bridge 12:

```
CB5000> set vbridge 12 igmp_snooping query mode enable
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING QUERY RESET_TO_DEFAULT

Use the SET VBRIDGE IGMP_SNOOPING QUERY RESET_TO_DEFAULT command to reset the IGMP snooping query parameters to their factory defaults.

Format

set vbridge – *vbridge* – **igmp_snooping** – **query** – **reset_to_default** – *slot.port*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
slot.port	Specifies the slot and port for this operation. *port* (1 through 24) is a multicast port.

Example

The following command sets slot 8, port 1 on virtual bridge 12 as a router port:

```
CB5000> set vbridge 12 igmp_snooping query reset_to_default 8.1
```

Related Commands

SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

SET VBRIDGE IGMP_SNOOPING ROUTER_PORT

Use the SET VBRIDGE IGMP_SNOOPING ROUTER_PORT command to declare that the specified bridge port is a multicast port.

Format

set vbridge – *vbridge* – **igmp_snooping** — **router_port** — *slot.port*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
slot.port	Specifies the slot and port for this operation. *slot* (1 through 17) is the location of the module in the chassis and port (1 through 24) is a multicast port.

Example

The following command sets slot 8, port 1 on virtual bridge 12 as a router port:

```
CB5000> set vbridge 12 igmp_snooping router_port 8.1
```

Related Commands

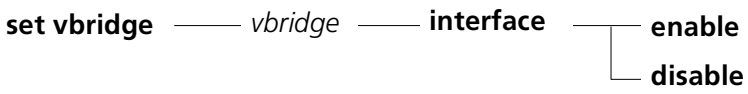
SET VBRIDGE IGMP_SNOOPING MODE
SET VBRIDGE IGMP_SNOOPING GROUP AGE_TIME
SET VBRIDGE IGMP_SNOOPING PORT AGE_TIME
SET VBRIDGE IGMP_SNOOPING QUERY_INTERVAL
SET VBRIDGE IGMP_SNOOPING QUERY LISTEN_TIME
SET VBRIDGE IGMP_SNOOPING QUERY MODE
SET VBRIDGE IGMP_SNOOPING RESET_TO_DEFAULT

SET VBRIDGE INTERFACE

Use the SET VBRIDGE INTERFACE command to enable or disable connectivity between a virtual bridge and the DMM. Virtual bridges continue to switch traffic even when the virtual bridge interface is disabled.

A virtual bridge interface is automatically enabled after you assign an IP address to the virtual bridge.

Format



vbridge	The assigned virtual bridge number. Values are 1 through 240.
enable	Enables connectivity to the DMM.
disable	Disabled connectivity to the DMM.

Example

The following command disables connectivity between the DMM and virtual bridge 12:

```
CB5000> set vbridge 12 interface disable
```

Related Commands

SHOW VBRIDGE
SHOW INTERFACE

SET VBRIDGE NAME

Use the SET VBRIDGE NAME command to assign a name to a SwitchModule virtual bridge. If you do not assign a name, the name defaults to vbridge_x where x is the virtual bridge number.

Format

set vbridge — *vbridge* — **name** — *name*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
name	Up to 32 characters.

Example

The following command assigns the name engineering to virtual bridge 10:

```
CB5000> set vbridge 10 name engineering
```

Related Command

SHOW VBRIDGE

SET VBRIDGE STP BRIDGE_FORWARD_ DELAY

Use the SET VBRIDGE STP BRIDGE_FORWARD_DELAY command to change the Spanning Tree Protocol forward delay value on a SwitchModule virtual bridge. The default forward delay value is 15 seconds.

Refer to the *CoreBuilder 5000 SwitchModule User Guide* for more information about Spanning Tree parameters.

Format

vbridge	The assigned virtual bridge number. Values are 1 through 240.
forward delay	Forward delay time in seconds for the specified virtual bridge. Values are 11 through 30.

Example

The following command configures the virtual bridge 9 forward delay value to 25:

```
CB5000> set vbridge 9 stp bridge_forward_delay 25
Bridge Forward Delay for vbridge 9 set to 25 seconds. Setting
saved.
```

Related Command

SHOW VBRIDGE CONFIGURATION VERBOSE

SET VBRIDGE STP BRIDGE_HELLO_TIME

Use the SET VBRIDGE STP BRIDGE_HELLO_TIME command to change the Spanning Tree Protocol hello time value on a SwitchModule virtual bridge. The default hello time value is 2 seconds.

Refer to the *CoreBuilder 5000 SwitchModule User Guide* for more information about Spanning Tree parameters.

Format

set vbridge — *vbridge* — **stp** — **bridge_hello_time** — *hello time*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
hello time	Assigns a Spanning Tree hello time to the virtual bridge. Values are 1 through 9.

Example

The following command configures the virtual bridge 9 hello time to 5 seconds:

```
CB5000> set vbridge 9 stp bridge_hello_time 5
Bridge Hello Time for vbridge 9 set to 5 seconds. Setting saved.
```

Related Command

SHOW VBRIDGE CONFIGURATION VERBOSE

SET VBRIDGE STP BRIDGE_MAX_AGE

Use the SET VBRIDGE STP BRIDGE_MAX_AGE command to change the Spanning Tree Protocol maximum age value on a SwitchModule virtual bridge. The default max age value is 20 seconds.

Refer to the *CoreBuilder 5000 SwitchModule User Guide* for more information about Spanning Tree parameters.

Format

set vbridge — *vbridge* — **stp** — **bridge_max_age** — *max age*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
max age	Values are 6 through 28.

Example

The following command configures the virtual bridge 9 maximum age value to 10 seconds:

```
CB5000> set vbridge 9 stp bridge_max_age 10
Bridge Max Age for vbridge 9 set to 10 seconds. Setting saved.
```

Related Command

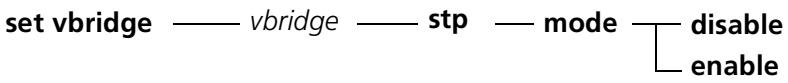
SHOW VBRIDGE CONFIGURATION VERBOSE

SET VBRIDGE STP MODE

Use the SET VBRIDGE STP MODE command to enable or disable the Spanning Tree Protocol on a SwitchModule virtual bridge. By default, Spanning Tree is enabled.

Disabling Spanning Tree can cause network loops and broadcast storms, resulting in network failure. Refer to the CoreBuilder 5000 SwitchModule User Guide *for more information about Spanning Tree parameters.*

Format



vbridge	The assigned virtual bridge number. Values are 1 through 240.
disable	Disable Spanning Tree on the virtual bridge you specify.
enable	Enable Spanning Tree on the virtual bridge you specify.

Example

The following command disables Spanning Tree on virtual bridge 9:

```
CB5000> set vbridge 9 stp mode disable
Spanning Tree Mode for vbridge 9 set to DISABLED. Setting saved.
```

Related Commands

SET VBRIDGE STP BRIDGE_FORWARD_DELAY
SET VBRIDGE STP BRIDGE_HELLO_TIME
SET VBRIDGE STP BRIDGE_MAX_AGE
SET VBRIDGE STP PRIORITY
SHOW VBRIDGE CONFIGURATION

SET VBRIDGE STP PRIORITY

Use the SET VBRIDGE STP PRIORITY command to change the Spanning Tree Protocol bridge priority value on a SwitchModule virtual bridge. The default priority value is 32,768.

Refer to the *CoreBuilder 5000 SwitchModule User Guide* for more information about Spanning Tree parameters.

Format

set vbridge —— *vbridge* —— **stp** —— **priority** —— *priority*

vbridge	The assigned virtual bridge number. Values are 1 through 240.
priority	Assigns the virtual bridge a Spanning Tree priority value for becoming the root bridge. Values are 0 through 65535. Default is 32768.

Example

The following command configures the virtual bridge 9 bridge priority value to 65,000:

```
CB5000> set vbridge 9 stp priority 65000
Priority for vbridge 9 set to 65000. Setting saved
```

Related Command

SHOW VBRIDGE CONFIGURATION VERBOSE

SET VBRIDGE STP RESET_TO_DEFAULT

Use the SET VBRIDGE STP RESET_TO_DEFAULT command to reset a SwitchModule in the hub back to its default values.

All SwitchModule ports are automatically connected to the PacketChannel backplane. You do not need to enter a command to assign ports to the backplane, as other types of CoreBuilder 5000 media modules may require.

All SwitchModule ports are enabled and assigned to virtual bridge 1.

If you create additional virtual bridges, the assigned ports are automatically enabled to switch traffic. For further information on default values, refer to the *CoreBuilder 5000 SwitchModule User Guide.*

Format

set vbridge —— *vbridge* —— **stp** —— **reset_to_default**

vbridge	The assigned virtual bridge number. Values are 1 through 256.
reset_to_default	Sets the Spanning Tree to enable (default).

Example

The following command resets the virtual bridge 9 to default values:

```
CB5000> set vbridge 9 stp reset_to_default
Settings saved.
```

Related Command

SHOW VBRIDGE CONFIGURATION VERBOSE

SHOW ALERT

Use the SHOW ALERT command to list the current alert settings.

Format

show alert

Example The following command displays current alert settings:

```
CB5000> show alert
Alert AUTHENTICATION    set to  ENABLE
Alert CHANGE            set to  ENABLE
Alert CONSOLE_DISPLAY   set to  ENABLE
Alert HELLO             set to  ENABLE
Alert NEW_ENVIRONMENT   set to  DISABLE
Alert PORT_UP_DOWN      set to  DISABLE
Alert SCRIPT            set to  DISABLE
```

The settings shown are the default settings.

Related Command SET ALERT

SHOW ALERT BRIDGE_PORT

Use the SHOW ALERT BRIDGE_PORT command to display the settings of the bridge_port up/down and STP state alert filters. If the filter is set to enabled, a trap is not generated. The factory setting is ENABLED, filter out traps.

Format

slot.port	Identifies the bridge port for which you want to show settings. *slot* (1 through 17) is the slot number for the module. *port* (1 through 24) is the bridge port number on the module.
*slot.***all**	Displays information about all bridge ports on the module in the slot (1 through 17).
all	Displays information about all bridge ports in the hub.

Example

The following command displays information about the bridge port alert filter settings for bridge port 3.1:

```
CB5000> show alert bridge_port 3.1

BPort      Port Up Down Trap    Stp State Trap
-----      ------------------   ----------------
03.01      ENABLED              ENABLED
```

Related Command

SET ALERT

SHOW ATM INTERFACE

Use the SHOW ATM INTERFACE command to display the configurable interface parameters for the ATM.

Format

show atm —— *slot* —— **interface**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays configurable interface information for the ATM:

```
CB5000> show atm 4 interface

Slot  Module      Version     Network      General Info
----  ------------------     ------------------------------
 04   6602M-MOD   v1.00       N/A

 Current                                   Next Reset
 ----------                                -------------
Max VCCs: 512                              128
Active VPI/VCI Bits: 0/9                   0/9
Number of LECs: 8                          20
UNI Version: 3.1                           3.1
LEARP Quiet Time (secs)                    20
Neighbor IP Address: 2.4.                  80.20
Neighbor Interface Name:                   Test
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SET ATM

SHOW ATM ILMI_CONFIGURATION

Use the SHOW ATM ILMI_CONFIGURATION command to display the configurable Interim Local Management Interface (ILMI) parameters for the ATM.

Format

show atm — *slot* — **ilmi_configuration**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays configurable ILMI information for the ATM:

```
CB5000> show atm 4 ilmi_configuration

Slot      Module      Version Network      General Info
----      ------------------- -------------------------------
 04       6602M-MOD   v1.00   N/A

   Current                                 Next Reset
   ----------                              -------------
ILMI PVC: 0/16                             0/8
ILMI Peak Cell Rate (% line rate):         13
ILMI Sust Cell Rate (% line rate):         1
ILMI Max Burst Size (cells):               20
ILMI Request Timeout (secs): 5             5
ILMI Request Retries: 2                    2
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SET ATM ILMI

SHOW ATM Q93B

Use the SHOW ATM Q93B command to display the configurable Q93b parameters for the ATM.

CAUTION: *Do not change the default settings for this command. Any changes you make to the settings may cause interoperability problems with other ATM equipment.*

Format

show atm — *slot* — **q93b**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays configurable Q93b information for the ATM:

```
CB5000> show atm 4 q93b

Slot      Module      Version  Network      General Info
----      ------------------- ------------------------------
 04       6602M-MOD   v1.00    N/A

   Current                                  Next Reset
   ----------                               -------------
T303 (secs): 4                              4
T308 (secs): 30                             30
T309 (secs): 10                             10
T310 (secs): 10                             2
T313 (secs): 4                              4
T316 (secs): 120                            120
T317 (secs): 60                             60
T322 (secs): 4                              4
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SET ATM Q93B

SHOW ATM QSAAL

Use the SHOW ATM QSAAL command to display the configurable Qsaal parameters for the ATM.

CAUTION: *Do not change the default settings for this command. Any changes you make to the settings may cause interoperability problems with other ATM equipment.*

Format

show atm — *slot* — **qsaal**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays configurable Qsaal information for the ATM:

```
CB5000> show atm 4 qsaal

Slot      Module      Version Network      General Info
----      ------------------- ------------------------------
 04       6602M-MOD   v1.00   N/A

   Current                                 Next Reset
   ----------                              -------------
Poll Timer (msecs): 750                    750
Keepalive Timer (secs): 2                  2
No Response Timer (secs): 7                7
Idle Timer (secs): 15                      20
CC Timer (secs): 1                         1
Max CC Retries: 4                          4
Max PD Retries: 25                         25
Stat Max Ranges: 67                        67
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information*.

Related Command

SET ATM QSAAL

SHOW ATM SIGNAL_ CONFIGURATION

Use the SHOW ATM SIGNAL_CONFIGURATION command to display the configurable signal parameters for the ATM.

Format

show atm — *slot* — **signal_configuration**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays configurable signal information for the ATM:

```
CB5000> show atm 4 signal_configuration

Slot      Module      Version Network      General Info
----      ------------------- -------------------------------
 04       6602M-MOD   v1.00   N/A

  Current                                  Next Reset
  ----------                               -------------
Sig PVC: 0/5
Sig Peak Cell Rate (% line rate):          5
Sig Sust Cell Rate (% line rate):          1
Sig Max Burst Size (cells):                9
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SET ATM SIGNAL

SHOW ATM STATISTICS

Use the SHOW ATM STATISTICS command to display the ATM and ATM Adaptation Layer 5 (AAL5) error statistics for the entire set of AAL5 circuits.

Format

show atm — *slot* — **statistics**

slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.

Example

The following command displays the ATM and AAL5 error statistics for the entire set of AAL5 circuits for the module in slot 4:

```
CB5000> show atm 4 statistics

Slot      Module      Version Network      General Info
----      ------------------ -----------  ------------------
 04       6602M-MOD   v1.00   N/A

                      ATM                  AAL5
                      --------             ----------
In Octets:            0                    0
In Frames             0                    0
In Discards:          0                    0
In Unknown Protocols: 0                    0
Out Octets:           0                    0
Out Frames:           0                    0
Out Errors:           0                    0
Out Discard:          0                    0
```

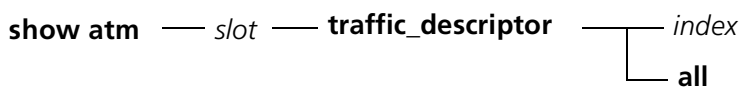
Related Command

SET ATM

SHOW ATM TRAFFIC_DESCRIPTOR

Use the SHOW ATM TRAFFIC_DESCRIPTOR command to display the traffic descriptor for a specific index or to display the entire traffic descriptor table.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
index	Specify an index number to display the traffic descriptor for that index.
all	Specify **all** to display the entire traffic descriptor table.

Example

The following command displays the entire traffic descriptor table:

```
CB5000> show atm 4 traffic_descriptor all

Index   Descr    Type       PeakCellRate SustCellRate MaxBurstSize
-----   -----    ----       ------------ ------------ ------------
1       ILMI     NoClpScr   17661        3533         11
2       SIG      NoClpScr   17661        3533         12
3       155M     NoClpNoScr 353208       N/A          N/A
4       100M     NoClpNoScr 235849       N/A          N/A
5       50M      NoClpNoScr 117925       N/A          N/A
6       25M      NoClpNoScr 58962        N/A          N/A
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

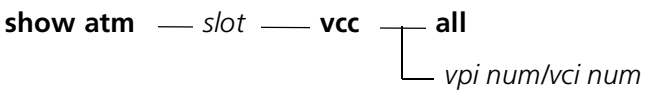
Related Command

SET ATM

SHOW ATM VCC

Use the SHOW ATM VCC (Virtual Channel Connection) command to display the virtual circuit table.

Format



slot	Identifies the slot for this operation. *slot* (1 through 17) is the slot number.
all	Displays the entire virtual circuit table.
vpi num	Displays the Virtual Path Identifier
vci num	Displays the Virtual Channel Identifier

Example

The following command displays the entire virtual circuit table:

```
CB5000> show atm 4 vcc all

VCC      Status   TxDescr  RxDescr  Type   TxSDU   RxSDU   Encap
---------------  -------  -------  -----  -----   ------  ---------
0/5      up       SIG      N/A      AAL5   300     300     other
0/16     up       ILMI     N/A      AAL5   484     484     other 0/32
up       155M     N/A      AAL5     1518   1518            LANE 802.3
```

Related Command

SET ATM NUM VCCS

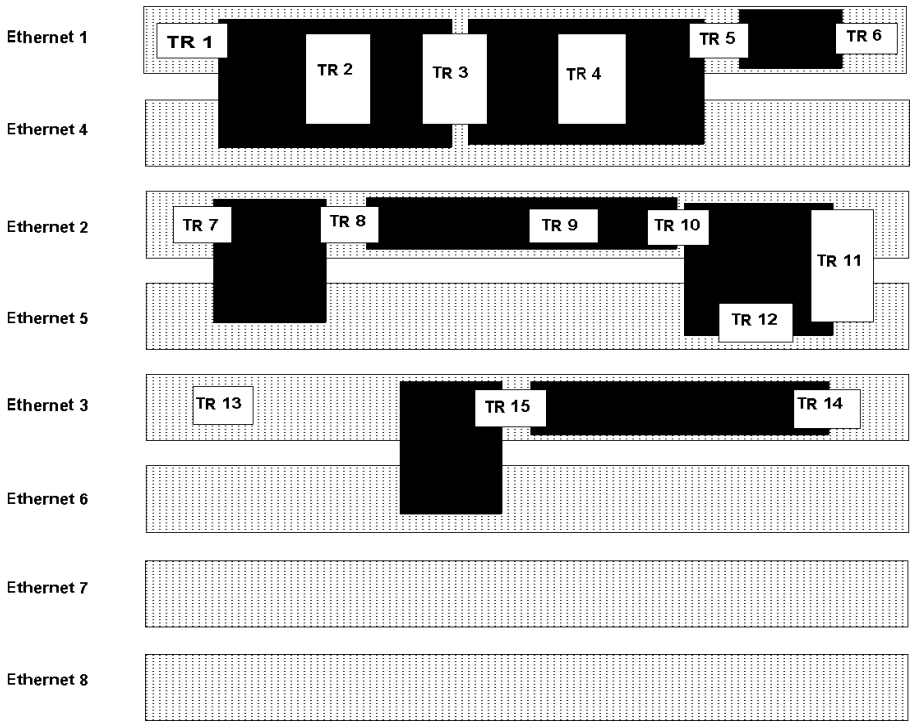
SHOW BACKPLANE_PATHS

Use the SHOW BACKPLANE_PATHS command to display a list of the logical network assignments and their corresponding physical backplane path connections.

The command shows you which backplane resources are available and which are used in the hub. It displays a list of which logical network assignments are using which physical channel (backplane path) connections.

Because the various protocols in the hub (Ethernet, ONline Token Ring, ONline FDDI) share backplane resources, the SHOW BACKPLANE_PATHS command can help you to determine which networks are still available. For example, you can use the command to determine which Token Ring and FDDI networks are no longer available when you implement a particular Ethernet network.

The following figure diagrams the interrelationship of the three hub protocols in terms of backplane resource use. The examples on the next page indicate you how you can use the diagram to help make decisions regarding backplane resource use.



If Ethernet 1 is in use, any networks that overlap Ethernet 1 (meaning that they share the same backplane resources) are unavailable. As the diagram shows, using Ethernet 1 makes TR 1 through 6 unavailable.

If Token Ring 15 is in use, any networks that overlap Token Ring 15 (meaning that they share the same backplane resources) are unavailable. As the diagram shows, using Token Ring 15 makes Ethernet 3 unavailable.

Format

show backplane_paths —— *protocol*

protocol	One of the following: ■ all ■ ethernet ■ fast_ethernet ■ fddi ■ token_ring

Example The example on the next page uses the terms in the following table to diagram the current usage for all shared backplane paths in the hub:

Term	Definition
Physical Path	A list of all possible backplane network paths on the hub.
Logical Network	A list of the status or availability of the backplane resources required to implement the corresponding physical path.
available	The resources needed to implement this physical path are available.
in use	The resources needed to implement this physical path are in use by another protocol.
network (for example, ETHERNET_1)	The logical network currently using the corresponding physical path. Non-Ethernet networks are not shown.

```
CB5000> show backplane_paths all

Physical Path              Logical Network
---------------            ---------------
ETHERNET_PATH_1            ETHERNET_1
ETHERNET_PATH_2            available
ETHERNET_PATH_3            available
ETHERNET_PATH_4            available
ETHERNET_PATH_5            available
ETHERNET_PATH_6            available
ETHERNET_PATH_7            available
ETHERNET_PATH_8            available

Physical Path              Logical Network
---------------            ---------------
FDDI_PATH_ONLINE_1         in use
FDDI_PATH_ONLINE_2         in use
FDDI_PATH_ONLINE_3         in use
FDDI_PATH_ONLINE_4         available
FDDI_PATH_ONLINE_5         available
FDDI_PATH_ONLINE_6         available
FDDI_PATH_ONLINE_7         available
FDDI_PATH_ONLINE_8         available

Physical Path              Logical Network
---------------            ---------------
TR_PATH_ONLINE_1           in use
TR_PATH_ONLINE_2           in use
TR_PATH_ONLINE_3           in use
TR_PATH_ONLINE_4           in use
TR_PATH_ONLINE_5           in use
TR_PATH_ONLINE_6           in use
TR_PATH_ONLINE_7           available
TR_PATH_ONLINE_8           available
TR_PATH_ONLINE_9           available
TR_PATH_ONLINE_10          available
TR_PATH_ONLINE_11          available
TR_PATH_ONLINE_12          available
TR_PATH_ONLINE_13          available
TR_PATH_ONLINE_14          available
TR_PATH_ONLINE_15          available
```

With ETHERNET_PATH_1 in use...

...FDDI paths 1 through 3 are unavailable...

...as are Token Ring paths 1 through 6.

Related Commands SET MODULE NETWORK
SET PORT NETWORK

SHOW BOOTP

Use the SHOW BOOTP command to display the current BootP settings.

Format

show bootp

Example

The following command displays current BootP settings:

```
CB5000> show bootp

——- BOOTP VARIABLES ——-
Bootp Server IP Address:  255.255.255.255
BootP Power Up Mode:      ENABLED
BootP Result:             NO RESPONSE
```

BootP Result	Definition
CLEAR	The last BootP result was cleared by the user (CLEAR BOOTP command).
REQUEST IN PROGRESS	The hub has sent a BootP request.
OKAY	BootP completed successfully.
NO RESPONSE	The hub did not receive a response to its BootP request.
FATAL ERROR	The BootP software reported a fatal error in operation.

Related Commands

BOOTP
CLEAR BOOTP
SET BOOTP POWER_UP_MODE
SET BOOTP SERVER_IP_ADDRESS

SHOW BPORT_LEC CONFIGURATION

Use the SHOW BPORT_LEC CONFIGURATION command to display configuration information for the specified LAN Emulation Client (LEC) including the BUS rate limit from the DMM.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

show bport_lec —— *slot.lec* ——— **configuration**

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**

Example

The following command displays configuration information for the LEC in slot 4, port 1:

```
CB5000> show bport_lec 4.1 configuration

Bridge Port LEC Display for Module 6602M-MOD:

BP LEC    Mode           I/F Status           General Info
------    ----           -------              --------------
04.01     ENABLED        DISABLED

Configuration Mode:             MANUAL
ELAN Name:                      NONE
ELAN Type:                      UNSPECIFIED
Maximum Data Frame Size:        1516
LES ATM Address:
        39.00.99.99.99.99.ac.00.99.99.99.99.99.99.99.99.99.99.99
LECS ATM Address:
        39.99.99.99.ac.00.00.00.00.99.99.01.02.03.04.05.06.07.08.00

Aging Time (secs):                          300
BUS Rate Limit (packets/secs):              5000
Connection Complete Timer (secs):           4
Control Timeout (secs):                     120
Expected ARP Response Time (secs):          1
Flush Timeout (secs):                       3
Forward Delay Time (secs):                  15
Maximum Retry Count:                        2
Maximum Unknown Frame Count:                1
Maximum Unknown Frame Time (secs):          1
Number of ELAN VCCs:                        512
Path Switching Delay (secs):                6
VCC Timeout Period(secs):                   1200
```

The values for the following parameters do not necessarily reflect the values in effect when the LEC is joined to an emulated LAN (ELAN):

- *Configuration Mode*
- *ELAN Name*
- *ELAN Type*
- *Maximum Data Frame Size*
- *LES ATM Address*
- *LECS ATM Address*

These values are examined the next time the LEC attempts to join an ELAN.

Related Commands SET BPORT_LEC MODE
SHOW BPORT_LEC STATUS

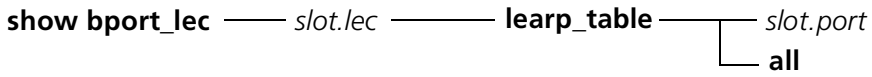
SHOW BPORT_LEC LEARP_TABLE

Use the SHOW BPORT_LEC LEARP_TABLE command to display the contents of the LE-ARP (MAC address to ATM address) mapping cache.

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format



slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**
address	MAC address you are configuring using this command. The format for MAC addresses is nn-nn-nn-nn-nn-nn The address 00-00-00-00-00-00 is invalid for this command.

Example

The following command displays the contents of the LE-ARP mapping cache in slot 4, port 2:

```
CB5000> show bport_lec 4.2 learp_table all

BP LEC  Mode    I/F Status         General Info
-----   ----    -----------        -------------
04.02   ENABLED ENABLED

MAC Address     ATM Address
--------        ------------
00-08-00-11-22-33   39.99.99.99.99.99.99.00.00.99.05.06.01.02.03.04.05.06.01
00-08-00-44-55-66   39.99.99.99.99.99.99.00.00.99.05.06.01.02.03.04.05.06.02
```

SHOW BPORT_LEC SERVER_CIRCUITS

Use the SHOW BPORT_LEC SERVER_CIRCUITS command to display the LAN emulation control and multicast circuits for the specified LAN Emulation Client (LEC).

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

show bport_lec —— *slot.lec* ——— **server_circuits**

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**

Example

The following command displays the multicast circuits for the LEC in slot 4, port 1:

```
CB5000> show bport_lec 4.1 server_circuits

Bridge Port LEC Display for Module 6602M-MOD:

BP LEC     Mode       Status       General Info
------     --------   --------------------------
04.01      ENABLED    OKAY

Configuration Direct VPI/VCI:     0/0
Control Direct VPI/VCI:           0/51
Control Distribute VPI/VCI:       0/52
Multicast Send VPI/VCI:           0/53
Multicast Forward VPI/VCI:        0/54
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SHOW BPORT_LEC STATUS

SHOW BPORT_LEC STATISTICS

Use the SHOW BPORT_LEC STATISTICS command to display statistics for the specified LAN Emulation Client (LEC).

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

show bport_lec —— *slot.lec* —— **statistics**

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**

Example

The following command displays the statistics for the specified LEC:

```
CB5000> show bport_lec 4.1 statistics

BP LEC     Mode       Status       General Info
------     --------   ------------ --------------
04.01      ENABLED    OKAY

LEARP Requests Out:               15
LEARP Requests In:                15
LEARP Replies Out:                34
LEARP Replies In:                 34
Control Frames Out:               100
Control Frames In:                100
SVC Failures:                     2
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SHOW BPORT_LEC STATUS

SHOW BPORT_LEC STATUS

Use the SHOW BPORT_LEC STATUS command to display the status for the specified LAN Emulation Client (LEC).

BPORT is an abbreviation for Bridge Port.

LEC ports are logical ports, all of which overlay one physical ATM/Synchronous Optical Network (SONET) port.

Format

show bport_lec —— *slot.lec* ——— **status**

slot.lec	Identifies the slot and LEC for this operation. *slot* (1 through 17) is the slot number and *lec* is one of up to 64 LAN Emulation Clients defined as logical ports for the ATM Backbone SwitchModule. For example, to identify LEC 32 on the ATM Backbone SwitchModule in slot 4, enter **4.32**

Example

The following command displays the status for the specified LEC:

```
CB5000> show bport_lec 4.1 status

BP LEC     Mode       Status       General Info
------     --------   ------------ -----------------
04.01      ENABLED    OKAY
Actual ELAN Name:                  LANE32
Actual ELAN Type:                  802.3
Actual Maximum Data Frame Size:    1516
LECS ATM Address:
   39.99.99.99.ac.00.00.00.00.99.99.01.02.03.04.05.06.07.08.00
LECS Address Source:               ILMI SERVICE REGISTRY MIB
Actual LES ATM Address:
   39.00.99.99.99.99.ac.00.99.99.99.99.99.99.99.99.99.99.99.99
LEC ID:                            17
Interface State:                   OPERATIONAL
Last Failure Response code:        NONE
Last Failure State:                INITIAL
LANE Protocol:                     1
LANE Version:                      1
Topology Change:                   OFF
Proxy Client:                      YES
LEC ATM Address:
   39.00.00.99.99.00.00.00.00.99.99.01.02.03.04.05.06.07.08.00
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Related Command

SHOW BPORT_LEC CONFIGURAtION

SHOW BPORT_MAU

Use the SHOW BPORT_MAU command to display information about SwitchModule bridge ports at the mau level. The information displayed depends in part upon the media type of the SwitchModule port (Ethernet, Fast Ethernet, or FDDI).

Format

slot.port.mau	Identifies the bridge port MAU you want to display information about. *slot* (1 through 17) is the slot number. *port* (1 through 24) is the port number. *mau* (1 or 2) is the MAU number.
slot.**all**	Displays information about all bridge port MAUs in the slot (1 through 17).
no_verbose	Displays bridge port mode and state. This is the default if you do not specify a verbose setting.
verbose	Displays the same information as the no_verbose option plus additional media-specific information.

Example

The following command displays information about SwitchModule FDDI port 13, MAU 2:

```
CB5000> show bport_mau 3.13.2 verbose

Bridge Port MAU Display for Module 3C96614M-FTP:

BP Mau     Mode       Status             General Info
--------   --------   ----------------------------------------
03.13.02   ENABLED    OKAY

Connector:                              MIC
Alert Filter:                           DISABLED
PMD Class:                              MULTIMODE
Port Type:                              B
PCM State:                              Active
Port Neighbor Type:                     A
Remote MAC Indicated:                   FALSE


CB5000>
```

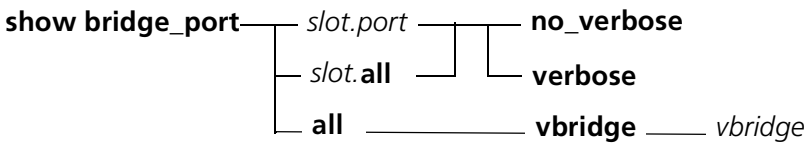
Related Command

SHOW BRIDGE_PORT

SHOW BRIDGE_PORT

Use the SHOW BRIDGE_PORT command to display information about SwitchModule bridge ports.

Format



slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot number and *port* (1 through 24) is the port number. For example, to identify port 4 on the module in slot 6, enter **6.4**
*slot.***all**	Displays information about all bridge ports in the slot (1 through 17).
all vbridge	Displays all bridge ports on a specified Vbridge.
no_verbose	If you do not enter a verbose setting, the command defaults to no_verbose. Displays the following information: ■ Bridge port mode and state ■ Virtual bridge the bridge port is assigned to ■ Logical port number ■ Master bridge port status
verbose	Displays the same information as the no_verbose option plus: ■ Spanning Tree values ■ RMON monitor status ■ General information (for example, port name)

Example

The following command displays information about all bridge ports on vbridge 1:

```
CB5000> show bridge_port all vbridge 1

Bridge Ports on Vbridge 1

BPort   I/F Status Stp State  Logical  General Info
-----   ---------- ----------  -------  ----------------------
04.02   ENABLED    FORWARDING  73
13.01   ENABLED    FORWARDING  289
13.04   DISABLED   DISABLED    292
13.05   DISABLED   DISABLED    293
13.06   DISABLED   DISABLED    294
13.07   DISABLED   DISABLED    295
13.08   DISABLED   DISABLED    296
13.09   DISABLED   DISABLED    297
13.10   DISABLED   DISABLED    298
13.11   DISABLED   DISABLED    299
13.12   DISABLED   DISABLED    300
13.13   DISABLED   DISABLED    301
15.02   DISABLED   DISABLED    338      Master bport
15.03   DISABLED   DISABLED    339
```

Related Command

SET BRIDGE_PORT

SHOW CLOCK

Use the SHOW CLOCK command to display the current setting of the management hub's internal clock.

Format

show clock

Example

The following command displays the current clock setting:

```
CB5000> show clock
Clock is set to 05:53 Sun 25 Jul 99
```

Related Command

SET CLOCK

SHOW COMMUNITY

Use the SHOW COMMUNITY command to list the current community settings.

Format

show community

Example

The following command displays the current community settings:

```
CB5000> show community

Index    Community Name    Protocol Address  Access
_____    ______________    ________________  _________
  1       user1            155.024.038.054   Read
  2       ncs              155.024.035.041   All
  3       super            155.024.043.083   Read
  4       admin            155.024.056.098   Read-Write
  5       [empty]
  6       [empty]
  7       [empty]
  8       [empty]
  9       [empty]
  10       [empty]
```

Related Command

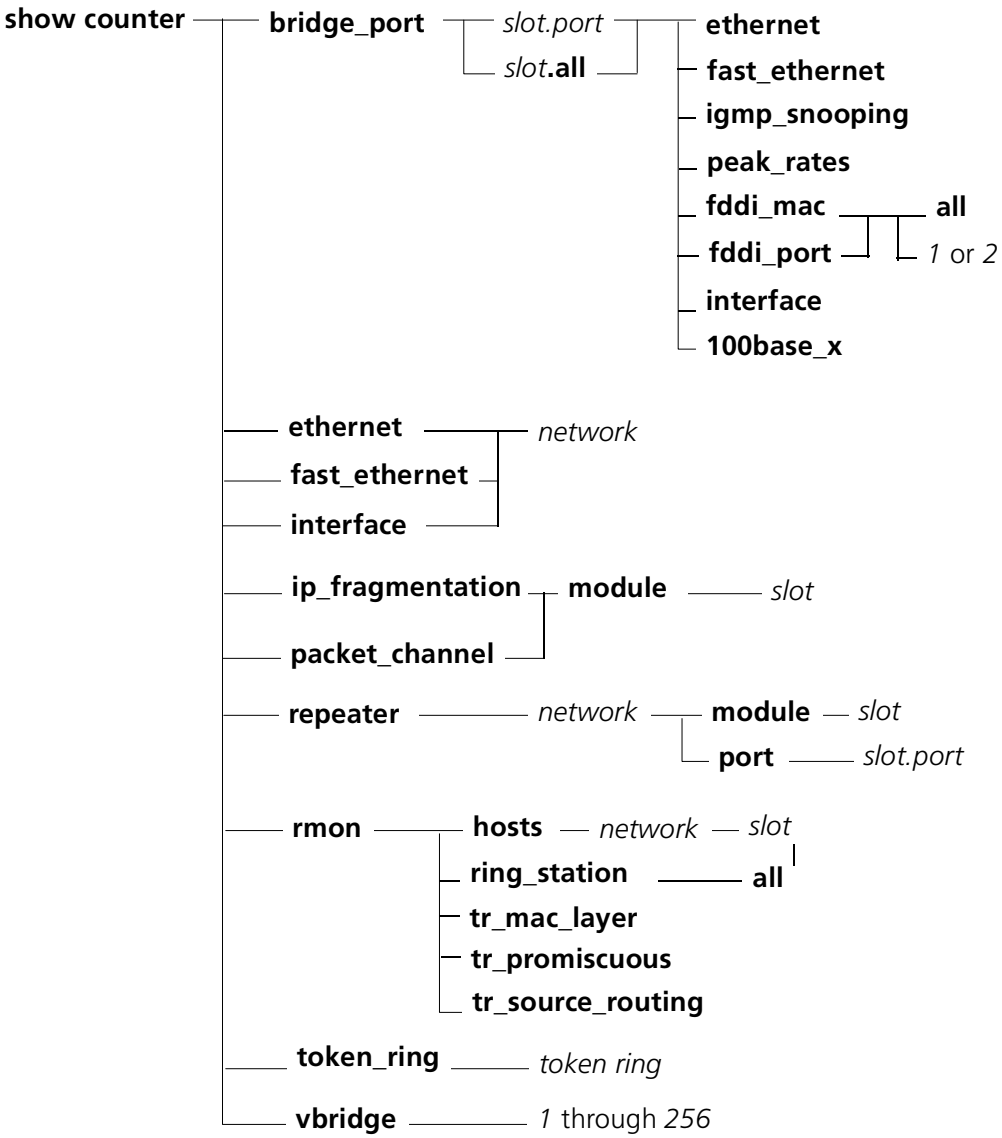
SET COMMUNITY

SHOW COUNTER

Use the SHOW COUNTER command to report statistics for a network to which an NMC is assigned. All counters are displayed since the last clear or reset.

A Network Monitor Card is not required to gather repeater statistics.

Format



bridge_port	Specifies that you want to display statistics for a SwitchModule bridge port.
slot.port	Identifies the port for this operation. *slot* (1 through 17) is the slot where the module is installed in the hub and *port* (1through 24) is the port number.
slot.**all**	Displays information about all of the bridge ports in a specified slot (1 through 17).
ethernet	Specifies that you want to display statistics for an Ethernet network.

fast_ethernet	Specifies that you want to display counter error statistics for a Fast Ethernet network.
igmp_snooping	Specifies that you want to display counter error statistics for igmp_snooping.
peak_rates	Specifies that you want to display counter error statistics for peak_rates.
fddi_mac	Specifies that you want to display all FDDI mac address counter error statistics.
fddi_port	Specifies that you want to display FDDI port counter error statistics from port 1 or port 2.
all	Specifies that you want to display counter error statistics for all FDDI MACs.
1 or *2*	Specifies that you want to display counter statistics for FDDI MAC addresses from port 1 or port 2.
interface	Specifies that you want to display counter statistics for the interface connected to a specified network.
100base_x	Specifies that you want to display 100base_x counter statistics for a specified module or all modules.
network	Specifies any network implemented in your CoreBuilder® 5000 hub (ethernet_1 or fast_ethernet_2, for example).
ip_fragmentation	Specifies that you want to display ip fragmentation counter statistics.
packet_channel	Specifies that you want to display information about traffic and activity on the PacketChannel backplane.
module	Indicates a specific module for which you want display counter statistics.
slot	Indicates the slot location for a specific module.
repeater	Displays counter statistics for a repeater.
port	Specifies the port for which you want to display counter statistics for a repeater.
rmon	Displays Token Ring Remote Monitoring (RMON) counter statistics from several Token Ring error counters. RMON works best with a workstation-based SNMP manager, but can also be used from the DMM command interface.
hosts	Specifies the RMON hosts that contain counter error statistics that summarize network activity. For each packet that travels the network, the TR-NMC extracts the source and destination address and adds the MAC addresses to the host table, and updates appropriate host-specific counters. The CoreBuilder® 5000 host table does not allow you to delete entries. If the table becomes full, new hosts are dropped
ring_station	Tracks the following status and statistics: ■ Control status and statistics for each active ring ■ Token Ring status information for each station that has been a ring member ■ Token Ring error and diagnostic statistics for each station that has been a ring member ■ Station order on monitored rings (Order group) ■ Download of configuration information, and removal of ring stations (Config group) This group collects information from the MAC layer, including ring use and error counters.
tr_mac_layer	Specifies counter error statistics from the RMON Token Ring MAC layer, including ring use and error counters.

tr_promiscuous	Specifies that you want to display counter error statistics from the Token Ring promiscuous error counter.
tr_source_routing	Specifies that you want to display counter error statistics from the Token Ring source routing error counter.
token_ring	Specifies that you want to display counter statistics for a Token Ring network.
token ring	Identifies the Token Ring network.
vbridge	Specifies that you want to display the number of Spanning Tree topology changes and learned entry discards for a SwitchModule virtual bridge.
1 through *256*	Identifies the vbridge for which you want to display counter statistics.

Example 1 The following command displays counter error statistics for Ethernet network 1.

Some modules report a Late Collision if the collision becomes active after 512 bits from the start of the transmission. Other modules log Late Collisions if the collision is active exactly 512 bit times, even if the collision was asserted before 512 bit times.

```
CB5000> show counter ethernet ethernet_1
Ethernet Statistics for ETHERNET_1
------------------------------------------------------------------
FCS Errors                      0
SQE Test Errors                 58
Alignment Errors                0
Carrier Sense Errors            1
Frame Too Longs                 0
Deferred Transmissions          5
Late Collisions                 0
Excessive Collisions            0
Single Collision Frames         3
Multiple Collision Frames       0
Internal MAC Receive Errors     6
Internal MAC Transmit Errors    0
```

Each error type is followed by the number of packets received that contains that error.

Field	Description
FCS Errors	Frame Check Sequence errors.
SQE Test Errors	Errors during Signal Quality Error test.
Alignment Errors	Number of CRC errors that do not end on a byte boundary.
Carrier Sense Errors	Loss of carrier sense detected.
Frame Too Longs	Too long errors received (packets greater than 1518 bytes).
Deferred Transmissions	Channel busy when sender ready to transmit. Sender retries.
Late Collisions	Collision occurs late in packet. No retry.
Excessive Collisions	More than 16 retries on the same packet.
Single Collision Frames	1 retry needed to send packet.
Multiple Collision Frames	2 to 15 retries needed to send packet.
Internal MAC Receive Errors	Lost packets during receive.
Internal MAC Transmit Errors	Lost packets during send.

Example 2 The following commands display module and port repeater statistics, respectively, for module 3. (This command displays the number of collisions that occurred when the module tried to access the backplane segment. Ethernet_2 displays the number of times the COLLISON EVENT Signal went active.)

```
CB5000> show counter repeater ethernet_2 module 3

Repeater Statistics for Module 3 on ETHERNET_2
-----------------------------------------------------------------
Readable Frames         142257566
Readable Octets         2554907443
Runts                   502857
FCS Errors              0
Late Events             0
Short Events            0
Frame Too Longs         0
Very Long Events        0
Alignment Errors        0
Collisions              0
Data Rate Mismatches    0
Auto Partition Count    0
```

Example 3 The following command displays the number of collisions that occurred when the port tried to access the backplane segment. Ethernet_2 displays the number of times the COLLISON EVENT Signal went active.

```
CB5000> show counter repeater ethernet_2 port 3.1

Repeater Statistics for Port 3.1 on ETHERNET_2
-----------------------------------------------------------------
Readable Frames         142251726
Readable Octets         2554052041
Runts                   502857
FCS Errors              0
Late Events             0
Short Events            0
Frame Too Longs         0
Very Long Events        0
Alignment Errors        0
Collisions              0
Data Rate Mismatches    0
Auto Partition Count    0
Last Source Address     00-00-0c-01-a2-25
```

Example 4 The following command sums up the number of collisions that occurred on all repeaters trying to transmit across the backplane segment fast_ethernet_1.

```
CB5000> show counter repeater fast_ethernet_1 module 3

Repeater Statistics for Module 3 on FAST_ETHER_1
-----------------------------------------------------------------
Readable Frames         0
Readable Octets         2554052041
Upper 32 Readable Octets0
Runts                   502857
FCS Errors              0
Late Events             0
Short Events            0
Frame Too Longs         0
Very Long Events        0
Alignment Errors        0
Collisions              0
Data Rate Mismatches    0
Auto Partition Count    0
Isolates                0
Symbol Errors           0
Last Source Address     00-00-0c-01-a2-25
```

Each error type is followed by the number of packets received containing that error.

Field	Description
Readable Frames	Readable (uncorrupted) frames received at repeater.
Readable Octets	Readable (uncorrupted) octets received at repeater (the lower 32 bits are contained in the rptrMonitorPortReadableOctets object).
Upper 32 Readable Octets	Upper readable (uncorrupted) octets (2**32) received at repeater. It contains the upper 32 bits of a 64-bit octets counter.
Runts	Packets less than 64 bytes.
FCS Errors	Frame Check Sequence errors.
Late Events	Collision detected after 512 bits were received from a port.
Short Events	Packets less than 80 bit times received.
Frame Too Longs	Frames in excess of 1518 bytes received.
Very Long Events	Port entered a jabber lockup state due to a timeout.
Alignment Errors	Number of CRC errors that do not end on a byte boundary.
Collisions	Total number of collisions detected.
Data Rate Mismatches	Number of FIFO overflow and underflow occurrences.
Autopartition Count	Number of times autopartition threshold has been passed.
Isolates	The number of automatic repeater port isolates as a consequence of false carrier events.
Symbol Errors	The number of packets containing symbol errors.
Last Source Address	The source address of the last packet received by this port.

Example 5 The following command displays interface statistics for Ethernet network 1. This command displays the number of errors that occurred when the DMM's EMAC tried to access backplane segment ethernet_1. This command does not separate errors from collisions.

```
CB5000> show counter interface ethernet_1

Interface Statistics for ETHERNET_1
-------------------------------------------------------------------
Received Octets                 2544983138
Received Unicast Packets        181659531
Received Non-Unicast Packets    1473448
Received Discards               0
Received Errors                 5991
Received Unknown Protocols      0
Transmitted Octets              4544
Transmitted Unicast Packets     71
Transmitted Non-Unicast Packets 0
Transmitted Discards            0
Transmitted Errors              0
```

Each error type is followed by the number of packets received containing that error.

Field	Description
Received Octets	Octets received at the network interface.
Received Unicast Packets	Single-address packets received at the network interface.
Received Non-Unicast Packets	Broadcast and multicast packets received at the network interface.
Received Discards	Discard packets received at the network interface. Received Discards is composed of Bridge Receive Discards in addition to Buffer Overflows (Also a counter on the FTE). If any Buffer Overflow display, buffer recovery will be triggered. Bridge Received Discards is composed of Management Filtered Packets, Dynamic Unicast Filtered Packets, and Management Unicast Filtered Packets. Bridge Receive Discards is accessed through the MIB variable (dot1dTpPortInDiscards).
Received Errors	Errors received at the network interface.
Received Unknown Protocols	Packets from unknown protocols received at the network interface.
Transmitted Octets	Octets transmitted at the network interface.
Transmitted Unicast Packets	Single-address packets transmitted at the network interface.
Transmitted Non-Unicast Packets	Broadcast and multicast packets transmitted at the network interface.
Transmitted Discards	Discard packets transmitted at the network interface.
Transmitted Errors	Errors transmitted at the network interface.

Example 6 The following command shows Token Ring (DOT5) Statistics for Token Ring network 1:

```
CB5000> show counter token_ring token_ring_1

Token Ring Statistics for TOKEN_RING_1
-----------------------------------------------------------------
Ring Status:    No Problems Detected Ring State:  Opened
Ring Open Status:Ring Open        Ring Speed:  16 MBPS
Upstream Station:08-01-20-0c-9e-d7 Functional Addr.: c0-00-00-00-00-00
Active Monitor Selection Participation: Disabled

Line Errors:                      0
Burst Errors:                     0
AC Errors:                        0
Abort Transmitted Errors:         0
Internal Errors:                  0
Lost Frame Errors:                0
Receiver Congestion Errors:       0
Frame Copied Errors:              0
Token Errors:                     0
Soft Errors:                      0
Hard Errors:                      0
Signal Losses:                    0
Transmit Beacons:                 0
Recoveries:                       0
Lobe Wires:                       0
Removes:                          0
Singles:                          0
```

Field	Description
Ring Status	Current operating status of the ring (refer to the table on the next page). The Ring Status value is a sum of values, derived from values for each condition that applies. When a single condition exists, text displays to describe the condition. When multiple conditions exist, the value displayed is a hexadecimal number that represents the sum of all conditions.
Ring State	Current interface state in terms of entering or leaving the ring.
Ring Open Status	Indicates the success, or the failure reason, for the station's most recent attempt to enter the ring.
Ring Speed	4 or 16 Mbps.
Upstream Station	MAC address of the Nearest Active Upstream Neighbor of this station.
Functional Addr.	A bit mask that describes the functional addresses for which this interface accepts frames.
Active Monitor Selection Participation	Indicates whether or not this station participates in the Active Monitor Contention process.

The following table describes Token Ring (DOT5) Interface Ring Status information:

Field Text	Hex Code	Description
No Problems Detected	00000000	No problems detected at this time.
Ring Recovery	00000020	TR-NMC is transmitting or receiving Monitor Contention frames.
Single Station	00000040	TR-NMC is opened onto the ring, but is the only station on the ring.
Remove Received	00000100	TR-NMC has received a Removed MAC frame.
Auto-Removal Error	00000400	Auto-removal error detected.
Lobe Wire Fault	00000800	TR-NMC has detected a wire fault.
Transmit Beacon	00001000	TR-NMC is transmitting beacon frames.
Soft Error	00002000	TR-NMC has transmitted a Soft Error Report MAC Frame. If any of the DOT5 statistics counters are increasing, it indicates that the TR-NMC has sent one or more Soft Error Report MAC Frames. Note: The TR-NMC clears this condition after a short period.
Hard Error	00004000	TR-NMC is either transmitting or receiving beacon frames.
Signal Loss	00008000	TR-NMC has detected the absence of a receive signal.
No Status	20000000	TR-NMC open process in progress, but not completed.

Each packet type is followed by the number of packets received.

Field	Description
Line Errors	Number of Line Errors detected at this station.
Burst Errors	Number of Burst Errors detected at this station.
AC Errors	Number of AC Errors detected at this station.
Abort Transmitted Errors	Number of Abort Transmitted Errors detected at this station.
Internal Errors	Number of Internal Errors detected at this station.
Lost Frame Errors	Number of Lost Frame Errors detected at this station.
Receiver Congestion Errors	Number of Receiver Congestion Errors detected at this station.
Frame Copied Errors	Number of Frame Copied Errors detected at this station.
Token Errors	Number of Token Errors detected at this station.
Soft Errors	Number of Soft Errors detected at this station.
Hard Errors	Number of Hard Errors detected at this station.
Signal Losses	Number of Signal Losses detected at this station.
Transmit Beacons	Number of times this station has transmitted a beacon frame.
Recoveries	Number of times this station has been purged from the ring, and then recovered.
Lobe Wires	Number of times this station has detected an open or short circuit in the lobe data path.
Removes	Number of times this station has been removed from the ring following a Remove Ring Station MAC Frame request.
Singles	Number of times this station has sensed that it is the only station on the ring. May indicate a hardware problem.

Example 7 The following command displays RMON host statistics for all hosts on Ethernet network 1 configured on the module in slot 1. This command displays the number of errors that occurred when the EMAC tried to access backplane segment ethernet_1. This command does not separate errors from collisions.

```
CB5000> show counter rmon hosts ethernet_1 1

RMON Hosts Table for Host Address 08-00-20-10-c9-79 on Port 1.1
-----------------------------------------------------------------
Received Packets               3092
Received Octets                1621681
Transmitted Packets            3976
Transmitted Octets             3032372
Transmitted Errors             0
Transmitted Broadcast Packets  1
Transmitted Multicast Packets  0

RMON Hosts Table for Host Address 00-00-00-28-00-00 on Port 0.0
-----------------------------------------------------------------
Received Packets                    13
Received Octets                     832
Transmitted Packets                 0
Transmitted Octets                  0
Transmitted Errors                  0
Transmitted Broadcast Packets       0
Transmitted Multicast Packets       0
```

Each packet type is followed by the number of packets received.

Field	Description
Received Packets	Packets received by the indicated host.
Received Octets	Octets received by the indicated host.
Transmitted Packets	Number of packets generated by this host.
Transmitted Octets	Number of octets generated by this host.
Transmitted Errors	Number of packets with errors sent by this host.
Transmitted Broadcast Packets	Number of broadcast packets sent by this host.
Transmitted Multicast Packets	Number of multicast packets sent by this host.

Example 8 The following command shows host table statistics for stations on token_ring_1 configured on the module in slot 7:

```
CB5000> show counter rmon hosts token_ring_1 7
RMON Hosts Table for Host Address 00-00-30-40-31-f6 on Port 7.1
-----------------------------------------------------------------
Received Packets                180600
Received Octets                 20404972
Transmitted Packets             188185
Transmitted Octets              108541926
Transmitted Errors              0
Transmitted Broadcast Packets   6968
Transmitted Multicast Packets   0
```

Related Commands

SET MODULE INTERFACE
SET MODULE RMON_GROUP ENABLE
SET RMON
SHOW RMON

SHOW DEVICE

Use the SHOW DEVICE command to display information about the DMM.

Format

show device

Example

The following command displays information about the DMM:

```
CB5000> show device

3Com CB5000 Distributed Management Module (6106M-MGT) 2.XX.X pSOS+
SNMP

Name: CB5000
Location:
  Unknown
For assistance contact:
  System Administrator

Operational EPROM Version: V2.XX     Boot EPROM Version: v1.01

Serial Number: 12345678               Service Date:  99/06/01
Restarts: 36

Dip Configuration: DISABLED          Diagnostics:  ENABLED
Reset Mastership:  DISABLED          Trap Receive: DISABLED
MAC Address Order: CANONICAL
```

Field	Description
Name	Assigned by the system administrator.
Location	Assigned by the system administrator.
For assistance contact	Assigned by the system administrator.
Operational Version	Software version number for the operational software.
Boot Version	Software version number for the boot software.
Serial Number	3Com serial number.
Service Date	Last date (yy/mm/dd) hardware or software was changed.
Restarts	Number of system restarts logged.
Dip Configuration	Indicates media module configuration status: if enabled, media modules configure themselves to DIP switches or NVRAM locally on the module; if disabled, the DMM configures the media module.
Diagnostics	Indicates if diagnostics are run when reset.
Reset Mastership	Indicates if this DMM is configured to cause a mastership election when it is inserted into a live hub.
Trap Receive	Setting for the trap receive function.
MAC Address Order	Canonical or noncanonical.

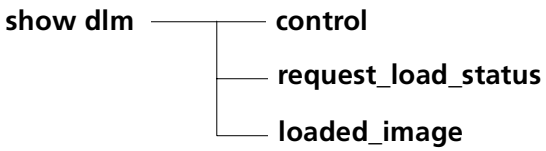
Related Commands

SET DEVICE
SHOW INVENTORY
SHOW MODULE

SHOW DLM

Use the SHOW DLM command to display information about DLMs (Dynamically Loadable Modules).

Format



control	Displays control table entries.
request_load_status	Displays status of requests made to the DMM to load DLMs.
loaded_image	Displays a table showing DLM images currently loaded on the DMM.

Example 1 The following command displays DLM-related control table entries stored in the DMM:

```
CB5000> show dlm control
DLM Control Table:
Index   Status    Owner
-----   ------    -----
1       VALID     Monitor
```

Example 2 The following command displays the status of requests made to the DMM to load DLMs:

```
CB5000> show dlm request_load_status
DLM Image Load Table:
Name        Status        Destination Module
----        ------        ------------------
ecam         executing          01.01
```

Example 3 The following command identifies any DLM images currently loaded on the DMM:

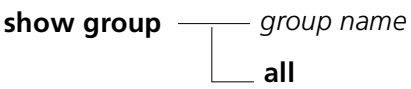
```
CB5000> show dlm loaded_image
Loaded DLM Table:
Name      Reason     Version   Load Source
----      ------     -------   -----------
ecam     application    01.00      PATH:TFTP:ecam:151.104.20.81
```

Related Command SET MODULE DLM_MODE

SHOW GROUP

Use the SHOW GROUP command to display the ports associated with a specific group.

Format



group name	Displays ports belonging to the specified group.
all	Displays ports belonging to all groups.

Example

The following command displays all of the ports associated with all groups:

```
CB5000> show group all

Group         Ports
-------       -----------------
group1        4.9    4.12 10.1
group2        4.12
group3        4.2    4.6
group4        3.6    4.9   4.12
group5        [empty]
group6        [empty]
group7        [empty]
group8        [empty]
```

Related Command

SET GROUP

SHOW HOST

Use the SHOW HOST command to display the DMM's host table.

Format

show host

Example

The following command displays the DMM's host table:

```
CB5000> show host

Index   Host Name                IP Address

 1      samuel                   155.104.56.20
 2      eng1                     155.3.6.58
 3      mkt                      155.2.2.27
 4      finance                  155.12.23.6
 5      education                155.102.17.4
 6      support                  155.102.16.5
 7      [empty]
 8      [empty]
 9      [empty]
 10     [empty]
 11     [empty]
 12     [empty]
 13     [empty]
 14     [empty]
 15     [empty]
 16     [empty]
 17     [empty]
 18     [empty]
 19     [empty]
 20     [empty]
```

Related Commands

CLEAR HOST
SET HOST

SHOW HUB

Use the SHOW HUB command to display information about the hub.

Format

show hub

Example

The following command displays information about the hub in which the DMM is installed:

```
CB5000> show hub

Hub Information:

Hub Type: 6017C-A

Backplane Information:

Backplane Type                          Revision
--------------------                    -----------
Load-Sharing Power Distribution Board     0
Enhanced TriChannel Backplane             0
RingChannel Backplane                     0

Power Supply Information:

      Power Supply    Status              Model Number
      ------------    ----------          ------------
       1              OKAY                6000PS
       2              OKAY                6000PS
       3              REMOVED
       4              REMOVED



Temperature Information:

      Probe            Location               Temperature
      -----            --------               -----------
       1                FAN_1                  31 Degrees Celsius
       2                FAN_2                  31 Degrees Celsius
       3                FAN_3                  29 Degrees Celsius

Fan Information:

      Fan              Status
      ---              ------
       1                OKAY
       2                OKAY
       3                OKAY
```

The following table explains the fields that are displayed:

Field	Description
Hub Type	Indicates that this is a Model 6017C hub.
Backplane Information	Indicates the type and revision level of all installed backplanes.
Power Supply Information	Indicates if a power supply is present in the slot, its normal or faulty status, and its model number.
Temperature Information	Indicates hub temperature at three locations.
Fan Information	Indicates status of each hub fan.

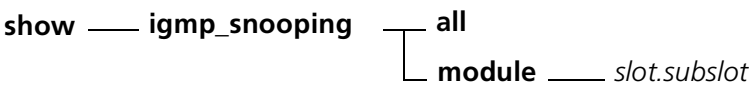
Related Commands

SHOW INVENTORY
SHOW MODULE ALL

SHOW IGMP_SNOOPING

Use the SHOW IGMP_SNOOPING command to display a detailed table of the IGMP Snooping groups associated with snooping vbridges or to display the current and future states of IGMP Snooping for a particular module.

Format



all	Displays information about all IGMP Snooping groups associated with all snooping vbridges.
module	Displays the current and future states of IGMP Snooping for the specified module.
slot.subslot	Specifies location of the module in the hub. *slot* (1 through 17) is the slot number and *subslot* is the module subslot number.

Example

The following table displays information about all IGMP Snooping groups:

```
CB5000> show igmp_snooping all

                                    MAC
Entry   Vbridge    IP_Address      Address            Port
----    ------     ---------       ------------------ ----
1       1          224.0.0.35      01-00-5e-00-00-23  2.1
2       1          224.0.0.139     01-00-5e-00-00-8b  2.1
3                                                     3.4
4                                                     5.6
5       2          224.0.0.12      01-00-5e-00-00-0c  2.3
6       3          224.0.0.35      01-00-5e-00-00-23  2.4
7       3          224.0.0.121     01-00-5e-00-00-79  6.1
8       4          224.0.0.39      01-00-5e-00-00-27  12.12
```

Field	Description
Entry	Interface entry number for this interface.
Vbridge	Vbridge number.
IP_Address	IP address for the corresponding Vbridge.
MAC Address	MAC address for the corresponding Vbridge.
Port	Slot and port number for the corresponding Vbridge.

SHOW INTERFACE

Use the SHOW INTERFACE command to display the location and status of DMM network interfaces (through NMCs). Only interfaces actually allocated (as compared to potential installed networks) are displayed. A hub can have up to 45 interfaces.

Format

show interface

Example

The following command displays the status and location of DMM network interfaces:

```
CB5000> show interface

                          Admin   Oper    MAC                          General
Idx     Network      Type Stat    Stat    Address            Slot      Information
----    -----------  ------ -----  -----   -------            ----      ----------
2       SLIP         SLIP   DOWN   DOWN    N/A                N/A
3       ETHERNET_1   ETH    UP     UP      67-4b-0e-63-7a-f9  02.01.01
4       VBRIDGE 1    VB     UP     UP      08-00-8f-20-e5-f8  17.01.01
```

Field	Description
Idx	Interface index. Several commands use this index to identify a particular interface.
Network	Network interface described on the current line.
Type	ETH (Ethernet), TR (Token Ring), or SLIP (Serial Line Interface Protocol), or VB (Vbridge).
Admin Stat	Setting applied to this network using the SET MODULE INTERFACE command.
Oper Stat	Operating status of the network interface.
MAC Address	MAC address of the interface used to attach to this network.
Slot	The slot and subslot location of the interface in the hub. For NMCs, this field also identifies the interface. For example, 03.02.01 identifies slot 3, subslot 2, interface 1. For Vbridges, it identifies the IP relay port. For example, 07.01.01 identifies slot 7, subslot 1, port 1.
General Information	If interface is in: ■ Standby (NMC only) — The NMC is an extra card placed in the hub for redundancy. ■ Module Down — The module for this interface is down. ■ Interface Disabled — The interface is disabled.

Related Command

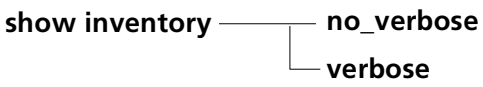
SET MODULE INTERFACE

SHOW INVENTORY

Use the SHOW INVENTORY command to display hub inventory information. This list includes the hub, all modules and submodules, and the controller module.

The SHOW INVENTORY command displays Jitter Attenuator cards, even though they are not manageable cards. Inventory information is provided for power budgeting.

Format



no_verbose	Displays summary information.
verbose	Displays extended information (all module and hub information, including software version).

Example The following command shows the inventory for a DMM:

```
CB5000> show inventory verbose

HUB/                    Hardware
Slot   Module           Version    Serial #   Vendor   Date
-----  -------------    ---------- ---------- -------- --------
HUB    6                017C       123456     3Com     930914

12.01  5103M-AUIM       N/A        N/A        N/A      N/A

       Note Pad: N/A
       Operational EPROM Version: 001        Boot EPROM Version: 1.00

14.01  6106M-MGTv1.00              23456      3Com     931027

       Note Pad: Carrier Card Installed 3/6/95
       Operational EPROM Version: 1.00          Boot EPROM Version: 1.00

DMM:  Operational EPROM Version: 1.00        Boot EPROM Version: 1.00

14.02  6100D-MAC        2.01       3456789    3Com     Jul 93

       Operational EPROM Version: 1.00          Boot EPROM Version: 1.00
       Note Pad:

16.01  6124M-TPL62      12345678              3Com     931116

       Operational EPROM Version: 1.00          Boot EPROM Version: 1.00
       Note Pad: Six ports assigned to engineering.

16.02  6100D-MGT        v1.00      125213     3Com     931101

       Operational EPROM Version: 1.00          Boot EPROM Version: 1.00
       Note Pad: 5

18.016000M-RCTL         v1.00      123123123  3Com     930601

       Operational EPROM Version: 1.00          Boot EPROM Version: 1.00
       Note Pad: Purchased backup 4/18/95
```

Field	Description
Slot	Slot and subslot of the module.
Module	Module part number.
Hardware Version	Version number for the module hardware.
Serial #	Serial number of the module.
Vendor	Vendor that manufactured the module.
Date	Date the module was manufactured.
Operational EPROM Version	Version number of the module's embedded operational code.
Boot EPROM Version	Version number of the module's startup code.
Note Pad	Optional information about CoreBuilder 5000 modules entered using the SET INVENTORY command (maintenance mode).

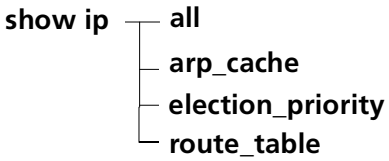
Related Commands

SET INVENTORY
SHOW HUB
SHOW MODULE

SHOW IP

Use the SHOW IP command to display Internet Protocol information for the networks configured in the hub.

Format



all	Show all IP parameters.
arp_cache	Show the DMM's current ARP cache.
election_priority	Show the DMM's current Vbridge IP relay election slot priority.
route_table	Show the DMM's routing table.

Example The following command displays IP information on DMM network interfaces:

```
CB5000> show ip all

 Active Default Gateway : 151.104.4.1

 Operational Active Default Gateway: 151.104.4.1

Index   Network       Slot  IP Address      Subnet Mask    Default Gateway
-----   ------------- ----  -----------     -----------    ----------------

 1      ETHERNET_1    N/A   151.104.4.255   ff.ff.ff.00    151.104.4.1
 2      TOKEN_RING_1  N/A   151.106.7.32    ff.ff.ff.00    151.106.7.254
 3      VBRIDGE 1     N/A   151.107.9.99    ff.ff.ff.00    151.107.9.2


IP ARP Cache:

Interface   Address          Physical Address
---------   ---------        ----------------

   5        151.104.99.1      00-00-30-20-9e-5a
   6        151.104.94.42     10-00-5a-f2-54-33
   6        151.104.94.46     10-00-5a-f2-80-67
```

```
IP Routing Table:

Destination      Next Hop          Interface
-----------      --------          ---------
127.0.0.1        127.0.0.1         46
127.0.0.3        127.0.0.3         2
0.0.0.0          151.104.99.1      5
151.104.4.0      151.104.94.250    3
151.104.6.0      151.104.69.254    4
151.104.40.0     151.104.90.254    6
151.104.41.0     151.104.49.254    7
151.104.9.0      151.104.90.252    5
151.104.252.0    151.104.99.7      1
127.0.0.0        127.0.0.9         8

IP Relay Election Slot Priority: low_to_high
```

Field	Description
Active Default Gateway	Default gateway you have configured to be active.
Operational Active Default Gateway	Default gateway that is active currently.
Index	Index assigned to this network.
Network	Identity of the network.
Slot	Slot that houses the module where this interface resides.
IP Address	IP address assigned to this network by the DMM. The IP stack resides on the DMM, not the interface (NMC)
Subnet Mask	Subnetwork mask for this interface.
Default Gateway	Default Gateway assigned to this interface.
IP ARP Cache	
Interface	Interface number described in this entry.
Address	IP address for the interface.
Physical Address	MAC address of the interface.
IP Routing Table	
Destination	Destination address for this routing table entry.
Next Hop	Next hop for packets associated with this interface.
Interface	Number of the interface entry.
IP Relay Election Slot Priority	Prioritizes Vbridge ports for IP Relay Master Election. Options are low_to_high and high_to_low.

Related Commands

SET IP
CLEAR IP
IP ELECTION_PRIORITY

SHOW LOG EVENT_LOG

Use the SHOW LOG EVENT_LOG command to display the values in the DMM event log.

Display the DMM event log after receiving a fatal error. Record the DMM event information in a file (or to a printer) and call 3Com Technical Support to determine why the DMM failed.

Format

show log event_log

Example

The following command displays the event log:

```
CB5000> show log event_log
Display of Last Error - Flash Version: vx.xx
Crash Date/Time: 05:58 Sat 4 Mar 95
Date/Time:         06:17 Sun 5 Mar 95
    -0-        -1-        -2-        -3-        -4-       -5-        -6-       -7-
A=12345678 2000044C    20000001 00000000    00000000 00000000 200D124C   200D1208

D=11111111 0000023D 00000000 00000000 00000000 00000000 00000000  00000000
Vector = 20020494    PC = 20000000    SR = 3009
Stack Dump:
200D1208   00 2C 20 02 5D B6 00 00 - 00 00 00 00 00 00 00 00 .......
200D1218   00 02 20 00 00 03 00 00 - 00 00 DE AD DE AD 00 00 .......
200D1228   00 00 00 00 00 00 00 00 - 00 04 00 00 00 00 00 00 .......
200D1238   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1248   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1258   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1268   00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 .......
200D1278    00 00 00 00 00 00 00 00 -  00 00 00 00 00 00 00 00 .......
```

Related Command CLEAR LOG EVENT_LOG

SHOW LOG MODULE EVENT_LOG

Use the SHOW LOG MODULE EVENT_LOG command to display the event log for the SwitchModule in the specified slot. If no information currently exists, the following message is displayed:

```
Module Event Log empty - no event to display.
```

If a module other than a SwitchModule is selected, the following message is displayed (for example, if you specified slot 8).

```
show module log 8
Module in slot 8 does not support this feature.
```

This command supports SwitchModules only, running Version v1.10 or higher.

Format

show log module —— *slot* —— **event_log**

Example If there was a crash on a particular SwitchModule, a screen dump is displayed. The following command displays the event log:

```
CB5000> show log module 2 event_log

            Module Sys Up Time at Crash: 1679
            Ack Date/Time: 17:36 Tue 01 Oct 96

- 0 -     - 1 -     - 2 -     - 3 -     - 4 -     - 5 -     - 6 -     - 7 -
A = 02010000 040CB740 040CB484 040CB5EC 00077E02 040386D8 040CB42C 040CB3DC
D = 00000087 00000002 00000087 02010000 00000000 00000000 00000005 00000000
        Vector = 7008    PC = 00077E4C         SR = 3010

Stack Dump:

40CB3DC   30 10 00 07 7E 4C 70 08 - 04 0C B4 28 00 C5 00 85   0....Lp.........
40CB3EC   00 45 00 C5 02 01 00 00 - 04 0C B4 1C 00 00 00 87   .E..............
40CB3FC   02 01 00 00 00 00 00 87 - 02 01 00 00 00 87 00 00   ................
40CB40C   04 03 2B 40 00 12 50 32 - 04 0C B4 38 00 11 C6 A0   ......P2...8....
40CB41C   00 00 00 01 00 00 00 0D - 04 0C B4 84 04 0C B4 5C   ................
40CB42C   00 07 EC 4E 04 0C B4 84 - 00 00 00 01 00 00 00 01   ...N............
40CB43C   00 00 00 00 00 00 00 00 - 00 00 00 00 04 0C B5 EC   ................
40CB44C   00 00 00 00 00 00 00 00 - 00 00 00 00 04 0C B5 D8   ................
```

Related Command CLEAR LOG EVENT_LOG

SHOW LOG TRAP_LOG

Use the SHOW LOG TRAP_LOG command to display the log entries for the most recently sent traps. The trap log is a circular buffer that can hold up to 15 traps. When the log exceeds the buffer, the software writes over the oldest trap with the newest trap information. The oldest trap is always displayed first.

The log is lost if the hub is reset or if power is lost to the hub.

Because the trap log captures only the trap information that is displayed on the console, you must set alerts to capture those traps you want to view.

Format

show log trap_log

Example

The following command displays a list of nonfatal system traps:

```
CB5000> show log trap_log

------------------TRAP 1 ---------------------------


Message received from this device on 15:43 Mon 24 Jul 95:

Enterprise:               3Com
Enterprise Specific trap:  Security Environment Change

Message Information:
     Security Trap Reason:  INTRUSION_ATTEMPT
     Slot Number:  3
     Port Number:  1
     Port Mode:  ENABLED
     Intruder MAC Address:  08 00 8f 30 09 0a
```

Related Command

CLEAR LOG TRAP_LOG

SHOW LOGIN

Use the SHOW LOGIN command to display the login table.

Format

show login

Example

The following command displays the login table:

```
CB5000> show login

Login Table:

        Index   Login Name      Access        Active Sessions
        -----   --------------- ----------------------------
             1  system          Super User         1
             2  clark           Super User         0
             3  lois            Administrator      0
             4  jimmy           User               0
             5  [not used]
             6  [not used]
             7  [not used]
             8  [not used]
             9  [not used]
             10 [not used]

Active Login Sessions:

     Login Name         Session Type            Session Time
     ----------         ------------            ------------
     system             Remote Super User       0 days 00:05:01
```

Related Command

SET LOGIN

SHOW MODULE

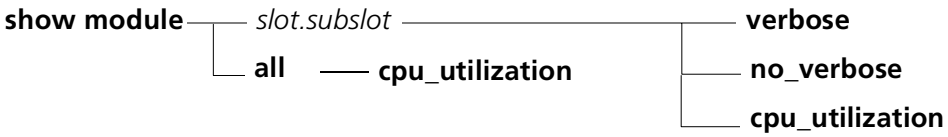
Use the SHOW MODULE command to display the status and configuration for modules currently installed in your hub.

The SHOW MODULE command displays information for all of the modules currently installed in your hub. Use the VERBOSE option only when you use the SHOW command with a single module in the hub. This option gives detailed information about the software and DIP switch settings for the module.

To display information about port-switched modules, use the SHOW PORT command.

This command has two additional values: RMON Analyzer and RMON System Analyzer.

Format



slot	Hub slot 1 through 19.
subslot	Module subslot.
all	Displays information for all modules.
cpu_utilization	Displays CPU statistics for the specified module(s).
verbose	Displays extended information.
no_verbose	Displays summary information.

Example 1

The following command uses the VERBOSE option to display the detailed settings of the CoreBuilder 5000 24-Port 10BASE-T Module in slot 1. The first line and the Module Information settings describe the software settings of the module. The DIP Switch Information settings describe the hardware settings of the module.

```
CB5000> show module 1.1 verbose

Slot    Module          Version      Network    General Information
-----   --------------- -------      ---------- -------------------
01.01   6124M-TPL6      a1.00.5      PER_PORT

6124M-TPL6: CoreBuilder 5000 Ethernet 24-PORT 10BASE-T Module

Non-Volatile DIP Setting:                    DISABLED
```

Example 2 The following command shows the type and location of all modules installed in the hub:

```
CB5000> show module all

Slot  Module       Version   Network     General Information
----- ------------ -------   ----------- -------------------
01.01 6124M-TPL6   V1.00     PER_PORT
01.02 6100D-MGT    V1.00     ETHERNET_1

02.01 6106M-CAR    V1.00     N/A
02.08 6000M-MGT    V1.00     N/A
                                         Master Management Module

09.01 5112M-TPPL      004    PER_PORT

10.01 5104M-FP        001    PER_PORT

15.01 5102M-AUIF      004    PER_PORT

18.01 6000M-RCTL      V1.01  N/A         Active Controller Module

19.01 6000M-RCTL      V1.01  N/A         Standby Controller Module
```

Example 3 The following command displays the A-ENMC's interface-specific attributes:

```
CB5000> show module 2.3 verbose
Slot    Module          Version    Network      General Information
-----   --------------- -------    ------------ -------------------
02.01   6100D-AMGT      V1.00
6100D-AMGT: CoreBuilder 5000 DualEthernet Network Monitor Card
Boot Version:           V1.00
DLM Mode:               DISABLED
CPU RAM Size (Mb):      8
       Module Interface_1       ETHERNET_1
IP Address:          127.0.0.1
Subnetwork Mask:     ff.ff.00.00
Default Gateway:     0.0.0.0
Station Address:     00-00-00-00-9a-0e
Interface Mode:      ENABLED
Interface Number:    3
       Module Interface_2       ETHERNET_2
IP Address:          151.104.15.1
Subnetwork Mask:     ff.ff.ff.00
Default Gateway:     0.0.0.0
Station Address:     aa-10-00-00-9a-0e
Interface Mode:      STANDBY
Interface Number:    4
```

Example 4 The following command shows CPU utilization statistics for the module in slot 12.1:

```
cb5000> show module 12.1 cpu_utilization
CPU Statistics for module 12.1

-------------------------------------------------------------------------------
                            Current      Peak      TimeStamp
-------------------------------------------------------------------------------
CPU Load Percentage:        14%          58%       15:49:11 23 Sep 99
Fragmented Packets:          0            0        13:50:14 06 Oct 99
IP Relay Packets:            0            0        13:50:14 06 Oct 99
ARP Packets:                 0            0        13:50:14 06 Oct 99
Learn Packets:               0            0        13:50:14 06 Oct 99
RMON Packets:                0            0        13:50:14 06 Oct 99
SNMP Packets:                0            0        13:50:14 06 Oct 99
STAP Packets:                0            0        13:50:14 06 Oct 99
SMT Packets:                 0            0        13:50:14 06 Oct 99
FDDI Events:                 0            0        13:50:14 06 Oct 99
MLAN Packets:                2          152        15:47:17 23 Sep 99
```

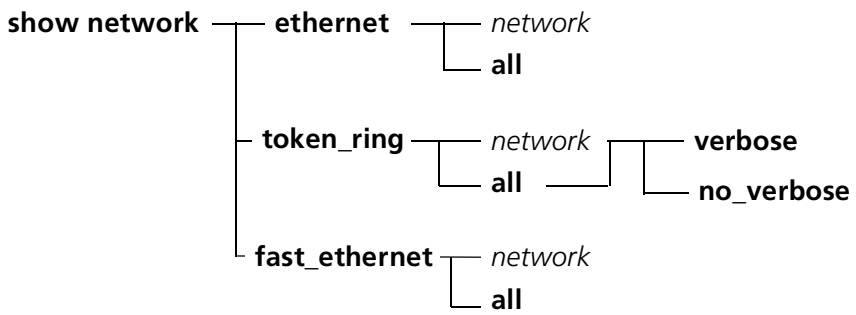
Related Commands SHOW DLM
SHOW INTERFACE
SHOW HUB

SHOW NETWORK

Use the SHOW NETWORK command to display status information about the networks in the hub.

The SHOW NETWORK command displays status information about the hub's networks. The VERBOSE option displays the state of beacon recovery and mismatch resolution. Both have values of enabled and disabled. Refer to the SET commands for descriptions of these objects.

Format



network	The values are: ■ ethernet_1...8 ■ token_ring_1...10 ■ fast_ethernet_1...4
all	Displays information about all the networks in the hub.
verbose	Displays detailed information about the network or networks you have selected.
no_verbose	Displays basic information only.

Example 1 The following command displays the status of the all hub's Ethernet networks:

```
CB5000> show network ethernet all

Network Display:

Network      Slot  Network State Status      MAC State Speed   General Info
----------   ----  ------------- ----------- ---------- ------- ------------
ETHERNET_1   N/A   ALLOCATED     OKAY        UNASSIGNED 10 MBPS
ETHERNET_2   N/A   ALLOCATED     OKAY        UNASSIGNED 10 MBPS
ETHERNET_3   N/A   ALLOCATED     OKAY        UNASSIGNED 10 MBPS
ETHERNET_4   N/A   UNUSED        OKAY        UNASSIGNED 10 MBPS
ETHERNET_5   N/A   UNUSED        OKAY        UNASSIGNED 10 MBPS
ETHERNET_6   N/A   UNUSED        OKAY        UNASSIGNED 10 MBPS
ETHERNET_7   N/A   UNUSED        OKAY        UNASSIGNED 10 MBPS
ETHERNET_8   N/A   UNUSED        OKAY        UNASSIGNED 10 MBPS
```

Example 2 The following command displays the status of the hub's Token Ring networks:

```
CB5000> show network token_ring all

Network Display:

Network      Slot  Network State Status      MAC State  Speed   General Info
----------   ----  ------------- ----------  ---------- ------- ------------
TOKEN_RING_1 N/A   ALLOCATED     OKAY        UNASSIGNED 16 MBPS
TOKEN_RING_2 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_3 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_4 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_5 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_6 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_7 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
TOKEN_RING_9 N/A   UNUSED        UNMONITORED UNASSIGNED 16 MBPS
```

Field	Description
Network	Network described on the current line.
Slot	Indicates the slot number containing the indicated isolated (module-level) Token Ring network.
Network State	States if the network is allocated or unused.
Status	Operating status of the network.
MAC State	Indicates whether or not a network monitor card (NMC) was assigned to the network.
Speed	Indicates if the ring is running at 4 Mbps or 16 Mbps (Token Ring), 10 Mbps (Ethernet), or 100 Mbps (Fast Ethernet).

Example 3 The following command displays the status of the hub's Fast Ethernet networks:

```
CB5000> show network fast_ethernet all
Network Display:

Network      Slot  Network State  Status       MAC State  Speed   General Info
----------   ----  -------------  -----------  ---------- ------- ------------
FAST_ETHER_1 N/A   UNUSED         UNMONITORED  UNASSIGNED 100 MBPS
FAST_ETHER_2 N/A   UNUSED         UNMONITORED  UNASSIGNED 100 MBPS
FAST_ETHER_3 N/A   UNUSED         UNMONITORED  UNASSIGNED 100 MBPS
FAST_ETHER_4 N/A   UNUSED         UNMONITORED  UNASSIGNED 100 MBPS
```

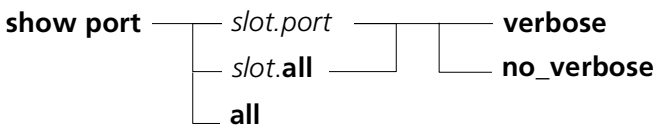
Related Commands

SET MODULE NETWORK
SHOW BACKPLANE PATHS
SHOW MODULE

SHOW PORT

Use the SHOW PORT command to display the mode and status of all ports or a specific port.

Format



slot.port	Selects a port for this operation. *slot* (1 through 17) is the module location in the chassis and *port* (1 through 20) is the port number. For example, to select port 4 on the module in slot 6, enter **6.4**
slot.**all**	Displays information for all ports on the module in the selected slot.
all	Displays information about all ports on all modules.
verbose	Displays extended information.
no_verbose	Displays summary information.

Example for Ethernet

The following command displays summary status for all ports on the module in slot 2:

```
CB5000>  show port 2.all no_verbose

Port Display for Module 6120M-TPP :

Port  Mode     Status              Network     General Information
----- -------- ------------------- --------------------------------
02.01 ENABLED  LINK FAILURE        ETHERNET_1
02.02 ENABLED  LINK FAILURE        ETHERNET_1
02.03 ENABLED  LINK FAILURE        ETHERNET_1
02.04 ENABLED  LINK FAILURE        ETHERNET_1
02.05 ENABLED  LINK FAILURE        ETHERNET_1
02.06 ENABLED  LINK FAILURE        ETHERNET_1
02.07 ENABLED  LINK FAILURE        ETHERNET_1
02.08 ENABLED  LINK FAILURE        ETHERNET_1
02.09 ENABLED  LINK FAILURE        ETHERNET_1
02.10 ENABLED  LINK FAILURE        ETHERNET_3
02.11 ENABLED  LINK FAILURE        ETHERNET_1
02.12 ENABLED  LINK FAILURE        ETHERNET_1
02.13 ENABLED  LINK FAILURE        ETHERNET_1
02.14 ENABLED  LINK FAILURE        ETHERNET_2
02.15 ENABLED  LINK FAILURE        ETHERNET_2
02.16 ENABLED  LINK FAILURE        ETHERNET_2
02.17 ENABLED  LINK FAILURE        ETHERNET_2
02.18 ENABLED  LINK FAILURE        ETHERNET_2
02.19 ENABLED  LINK FAILURE        ETHERNET_2
02.20 ENABLED  LINK FAILURE        ETHERNET_2
```

Example for Fast_Ethernet

The following command displays detailed status for a specific Fast_Ethernet port:

```
CB5000> show port 1.1 verbose

Port Display for Module 6512M-TX:

Port  Mode    Status       Network      General Information
----- ------------------   ------------ ------------
01.02 ENABLED  OK          FAST_ETHER_1

Port Alert Filter:                DISABLED
Port Connector:                   RJ45
```

Example for ONline Token Ring

The following command displays extended information for the module in slot 6:

```
CB5000> show port 6.all verbose
Port Display for Module 5202M-FR:

Port    Mode     Status       Network          General Information
-----   -------- ------------ ---------------- -------------------
06.01   DISABLED NO PHANTOM   TOKEN_RING_5

Port Connector:                   RJ45S
Mode Dip Setting:                 ENABLED
Cable Impedance Dip Setting:      150 OHM

06.02   ENABLED  OKAY         TOKEN_RING_5

Port Connector:                   RJ45S
Mode Dip Setting:                 ENABLED
Cable Impedance Dip Setting:      150 OHM
```

Status Display	Indicates
OKAY	Port is operating properly.
LINK FAILURE	Port is not receiving a good signal. Possible causes include a cable break or lost connection.
FATAL ERROR	An error has occurred that makes the module inoperable.
NO CABLE	A copper trunk port with Cable Monitor mode enabled cannot detect a cable.
NO SQUELCH	Data cannot be detected on an incoming path of a copper trunk port.
NO PHANTOM	Indicates that the phantom current is not detected at the Token Ring port because the station is powered down, no station is attached, a cable fault occurred, or because the adapter card removed itself from the ring.
BEACON WRAPPED	Port has been wrapped by the beacon recovery feature.
SPEED MISMATCH	Wrong speed station attached to port. Port wrapped by speed detect algorithm.
BCN THRESH ERROR	Number of beacon wraps recorded has exceeded a user-set threshold.
SPD THRESH ERROR	Number of speed detect wraps recorded has exceeded a user-set threshold.

Example for CoreBuilder 5000 Token Ring

The following command displays extended information for all ports on the module in slot 7:

```
CB5000> show port 7.all verbose
Port Display for Module 6218M-ATPP:

Port    Mode     Status       Network          General Information
-----   -------- ------------ ---------------- -------------------
07.01   ENABLED  NO PHANTOM   TOKEN_RING_1     Port is down

Port Alert Filter:                DISABLED
Port Connector:                   RJ45S
Dip Network Setting:              ISOLATED_11
Static Switch:                    DISABLED

07.02   ENABLED  NO PHANTOM   TOKEN_RING_1     Port is down

Port Alert Filter:                DISABLED
Port Connector:                   RJ45S
Dip Network Setting:              ISOLATED_11
Static Switch:                    DISABLED
```

Example 1 for ONline FDDI

The following command displays summary status for all ports on the module in slot 8:

```
CB5000> show port 8.all no_verbose
Port Display for Module 5308M-FIB-ST:

Port    Mode     Status       Network          General Information
-----   -------- ------------ ---------------- -------------------
08.01   ENABLED  OKAY         FDDI_1           Active Slave Port
08.02   DISABLED OFF          FDDI_1           Slave Port
08.03   ENABLED  OKAY         FDDI_1
08.04   ENABLED  OKAY         FDDI_1
08.05   DISABLED OFF          FDDI_1
08.06   ENABLED  LINK FAILURE FDDI_1           Withholding M-M
08.07   ENABLED  OKAY         FDDI_1
08.08   DISABLED OFF          FDDI_1
```

Example 2 for ONline FDDI

The following command displays detailed status for a specific FDDI port:

```
CB5000> show port 3.2 verbose
Port Display for Module 5308M-FIB-ST:

Port    Mode     Status       Network          General Information
-----   -------- ------------ ---------------- -------------------
03.2    ENABLED  OKAY         FDDI_1           Active Slave Port

Port_Connector:                   ST
Port Type:                        Slave
PCM State:                        Active
Port Neighbor_Type:               Master
Remote MAC Indicated:             FALSE
```

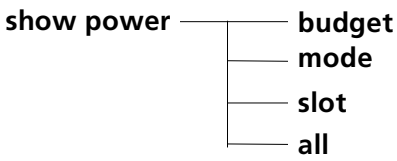
Field	Description
Port	Indicates the slot number and the port number, in the format slot/port, for the port of the designated module.
Mode	Identifies the mode (enabled or disabled) of the designated module.
Status	Indicates if the port is inserted onto the ring (OKAY), not inserted onto the ring (OFF), attempting insertion onto the ring (CONNECTING), configured as a backup slave port (BACKUP-LINK), or experiencing a problem (LINK FAILURE).
Network	Specifies the network to which the module is assigned.
General Information	Reports the following information: ■ Active Slave Port ■ Slave Port ■ Withholding M-M ■ PCM Break State ■ Break in Connection ■ Port Hardware Failure! (Note: If this message appears, try resetting the module. If this does not correct the problem, call 3Com Technical Support.) ■ Bad Bypass/Remote Port (This error occurs only when the FMM boots up.)

Related Command SET PORT

SHOW POWER

Use the SHOW POWER command to display the power budget, power modes, and power information on a per-slot basis. The SHOW POWER command displays the power settings for the hub, including the amount of power available, and the amount of power consumed, in the hub.

Format



budget	Show power budget table only.
mode	Show power fault tolerance and overheat mode settings.
slot	Show power information on slot (1 through 17), or all slots.
all	Show all power settings.

Example

The following command shows the output of the SHOW POWER ALL command:

```
CB5000> show power all

     Power Management Information
     ----------------------------
Hub Power Modes:

   Fault-Tolerant Mode:         NON_FAULT_TOLERANT
   Fault-Tolerant Status:       NON_FAULT_TOLERANT
   Overheat Power Down Mode:    ENABLE

Slot Power Information:

Slot     Class       Admin Status        Operating Status
----     -----       ------------        ----------------
1        N/A         ENABLE              ENABLED
2        N/A         ENABLE              ENABLED
4        N/A         ENABLE              ENABLED
5        N/A         ENABLE              ENABLED
8        N/A         ENABLE              ENABLED
9        N/A         ENABLE              ENABLED
10       N/A         ENABLE              ENABLED

Slot     Class       Admin Status        Operating Status
----     -----       ------------        ----------------
11       N/A         ENABLE              ENABLED
14       3           ENABLE              ENABLED
15       3           ENABLE              ENABLED
17       3           ENABLE              ENABLED
```

```
Hub Power Budget:

Voltage Type  Voltage Level Watts Capacity Watts Available  Watts Consumed
------------  ------------- -------------- --------------- --------------
   +5V          5.128        367.00        204.00           163.00

   -5V         -5.058         27.00         24.75             2.25

   +12V        11.803         81.50         42.00            39.50

   -12V       -11.993         30.50         29.50             1.00

   +2V          2.125         14.30         10.10             4.2
```

Field	Description
Hub Power Modes	Indicates if the hub is set to fault-tolerant or non-fault-tolerant mode, if it remains in fault-tolerant status currently (that is, there is still enough power to maintain fault tolerance), and if the hub is configured to power down when it overheats.
Slot	Slot the row describes.
Class	Power class setting, which determines which modules power down if there is a shortage of power in the hub. Lower numbers lose power first. ONline™ modules always have highest priority.
Admin Status	Current Admin Status of the slot.
Operating Status	Current Operating Status of the slot.
Voltage Type	Type of voltage being budgeted.
Voltage Level	Actual voltage level of each type.
Watts Capacity	Maximum potential watts produced by the power supplies available in the hub.
Watts Available	Number of watts not being used by currently installed modules and fans.
Watts Consumed	Number of watts consumed by currently installed modules and power supplies.

Related Commands

SET POWER
SET POWER MODULE POWER_REQUIREMENTS

SHOW PROTOCOLS

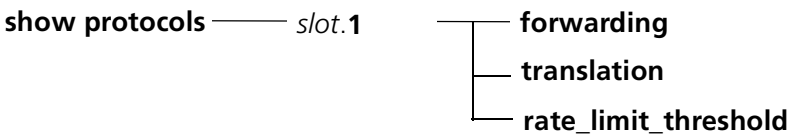
Use the SHOW PROTOCOLS command to display the following information about a CoreBuilder 5000 SwitchModule:

- The FDDI-to-Ethernet translation settings the SwitchModule is using
- The user-created and default protocol filters the SwitchModule is using
- Rate limiting status (You can display a counter of the number of packets discarded by entering the MONITOR BRIDGE_PORT or SHOW COUNTER BRIDGE_PORT command. The counter displays in the Received Discards field.)

The Bridge Receive Discards is composed of Management Filtered Packets, Filtered Packets, and Management Unicast Filtered Packets. These packets are all counters on the FTE.

You can use this command to display information about one SwitchModule at a time.

Format



slot.**1**	Selects a slot you want to display information about. Valid values are slot 1 through 17, subslot 1.
forwarding	Displays information about user-created and default protocol filters. By default, the SwitchModule uses the following filters: ■ Spanning Tree ■ IP ■ IP ARP ■ Appletalk ARP ■ Unknown Protocol
translation	Displays the FDDI-to-Ethernet translation settings the SwitchModule is using.
rate_limit_threshold	Displays the status of rate limiting for a: ■ SwitchModule ■ Particular protocol type Rate_Limit_Threshold values range from 0 through 65,534. (If you set the rate limit threshold to 0 frames per second, the SwitchModule filters all broadcast packets.)

Example 1 This command displays the protocol type field, protocol name, priority setting, and ports affected by the default filters in the protocol forwarding table for the SwitchModule in slot 6. The table displays the default filters used by the SwitchModule, as well as any additional filters you create.

The following command shows only the default filters:

```
CB5000> show protocols 6.1 forwarding

Protocol             Name             Priority   Forward On Ports
-------------------------------------------------------------------
dsap 42              spanning tree    normal     ALL
enet 08-00           ip               normal     ALL
enet 08-06           ip arp           normal     ALL
snap 00-00-00-80-f3  appletalk arp    normal     ALL
unkn 00              unknown protocol normal     ALL
```

Example 2 The following command displays the translation setting that the SwitchModule in slot 3 is using:

```
CB5000> show protocols 3.1 translation
IPX translation: ipx enet II - default
CB5000>
```

Example 3 To display the status of rate limiting:

- **For a SwitchModule** – Enter the SHOW PROTOCOLS RATE_LIMIT_THRESHOLD command. For example:

  ```
  > show protocols 7.1 rate_limit_threshold
  Rate limit threshold set to 300 (frames/second)
  ```

- **For a particular protocol type** – Enter the SHOW PROTOCOLS FORWARDING command and look at the Rate Limit field. For example:

```
CB5000> show protocols 7.1 forwarding
Protocol     Name             Priority  Rate Limit Forward On Ports
-----------------------------------------------------------------
dsap 42      spanning tree    normal    disable    ALL
enet 08-00   ip               normal    disable    ALL
enet 08-06   ip_arp           normal    enable     ALL
enet 80-f3   appletalk arp    normal    disable    ALL
unkn 00      unknown protocol normal    disable    ALL
```

In this example, rate limiting is enabled for the protocol type enet 08-06.

To disable rate limiting, enter the SET PROTOCOLS command with the DISABLE_RATE_LIMIT option. For example:

```
> set protocols 7.1 forwarding enet 08-06 normal_priority all ip_arp
disable_rate_limit
```

Related Commands CLEAR PROTOCOLS
SET PROTOCOLS FORWARDING
SET PROTOCOLS TRANSLATION

SHOW RING_MAP

Use the SHOW RING_MAP command to display a ring topology of the Token Ring and FDDI networks currently configured in the hub.

Format

show ring_map —— *protocol* —— *option*

protocol	■ fddi — Displays a ring map of FDDI stations in the hub. ■ token_ring – Displays a map of Token Ring stations, using the format you select (option).
option (Token Ring)	■ logical — Lists the MAC address and slot and port identification for each Token Ring port. If a MAC-less device is the only station on the ring, the map reports NO ENTRIES. ■ mac_address *mac address* — When you supply a MAC address, this option returns the slot and port associated with that address. ■ physical — This option applies to ONline™ System Concentrator modules in a CoreBuilder® 5000 hub. ■ port *slot.port* — When you supply a slot and port, this option returns the MAC address associated with that port.

Example 1 (FDDI)

The following command shows an FDDI ring map:

```
CB5000> show ring_map fddi
Slot    Status    Upstream_Slot  Downstream_Slot
_____________________________________________
12      OKAY      16             14
14      OKAY      12             16
```

FDDI Description

For FDDI modules, this command displays the physical ring topology of the FDDI networks in the hub. The map displays the modules that comprise each network, and their respective upstream and downstream slots. The map also displays module status.

Field	Description
Slot	Slot numbers of the modules that compose each FDDI network.
Status	OKAY — condition normal. PARTIAL FAIL — partial hardware failure.
Downstream_Slot	Hub slot number for the adjoining module on the ring. Identifies the module the specified FDDI module will pass the token to.
Upstream_Slot	Identifies the hub slot number for the adjoining module on the ring. This field identifies the module passing the token to the specified FDDI module.

Example 2 (ONline) The following command displays a Token Ring map. This map does not include CoreBuilder 5000 modules.

```
CB5000> show ring_map token_ring
Physical wiring map for backplane isolated or front ring:

      Upstream       Connection     Downstream
      Slot ID        Type           Slot ID
      ---------------------------------------
      External       Fiber          9
      9              Copper         External
      External       Copper         9
      9              Backplane      9
      9              Fiber          External
      11             Backplane      11
      13             Backplane      13
```

ONline Token Ring Description For ONline Token Ring modules, the SHOW RING_MAP TOKEN_RING PHYSICAL command shows the physical topology of ONline Token Ring modules in the hub. To end the display and return to the command line, press Ctrl+C.

Field	Description
Upstream Slot ID	Hub slot number for the adjoining module on the ring. Identifies the module passing the token to the specified Token Ring module.
Connection Type	Media connection between the two ports. The available types are: ■ Backplane — Backplane connection on the same Token Ring network. ■ Copper — Copper Ring-In/Ring-Out connection. ■ Fiber — Fiber Ring-In/Ring-Out connection.
Downstream Slot ID	Hub slot number for the adjoining module on the ring. Identifies the module to which the specified Token Ring module passes the token.

If the connection type is copper or fiber, the upstream and downstream slot ID is external. External means that the connection is from another hub, or that there is no connection on that end. A remote connection indicates a station that is not on the local ring.

Example 3 The following command displays a map of Token Ring stations attached to the ring associated with backplane network token_ring 1:

```
CB5000> show ring_map token_ring logical token ring
Token Ring Logical Map for Network TOKEN_RING_1

MAC Address         Slot      Port
-----------------   ----      ----
10-00-f1-0b-00-4f   04.02     N/A
00-00-c9-1a-2e-0c   04.01      8
00-00-c9-1a-2e-0b   04.01     12
00-00-c9-1a-1c-aa   04.01     13
00-00-c9-1a-29-ab   04.01     15
00-00-c9-1a-2e-a3   04.01     16
00-00-c9-1a-6e-78   07.01      1
00-00-c9-1a-af-3f   07.01      2
00-00-c9-1a-1b-43   07.01      4
00-00-c9-1c-0a-fb   07.01      6
00-00-c9-1a-2c-a0   07.01      7
00-00-c9-1a-28-b1   07.01     10
00-00-c9-1a-18-72   07.01     11
00-00-c9-1a-28-4    07.01     13
10-00-f1-0b-29-a6   External
00-00-03-0c-0b-1a   External
00-00-c9-1a-29-a9   External
08-00-5a-0b-5d-a6   External
00-00-c9-1a-29-8b   External
08-00-20-0c-9e-d7   External
```

CoreBuilder 5000 Token Ring Description

When a TR-NMC monitors a network, and the TR-NMC RMON ring station statistics are enabled, the TR-NMC can resolve port-to-address mapping for external stations. The map lists stations by MAC address, and correlates each address in a local hub to a slot and port. Stations on the ring that are external to the hub are described as external.

The TR-NMC itself is always located in slot.2 and has no port assignment.

Related Commands

SHOW NETWORK
SHOW PORT

SHOW RMON CONTROL

Use the SHOW RMON CONTROL command to show control table entries for individual RMON groups.

Each RMON group provides control tables and data tables:

- **Control tables** — Used by the Network Management Station to add monitoring (using more resources and degrading performance) or to remove monitoring (freeing memory and improving performance)
- **Data tables** — Store and provide the information collected, using the instructions in the control table

Control tables are structured to support multiple Network Management Stations per probe. If an NMS configures probe resources, it is the responsibility of that NMS to free those resources when no longer used.

If you use the DMM as the NMS, manually delete unused control table entries.

Each control table entry has:

- A table index
- An owner string identifying the NMS that created the control entry
- Status of the control entry
- Other objects that define the behavior of the group to be monitored

The history control table defines which interface (MAC) to monitor, the sampling interval, the number of history reports the MAC stores for a sampling interval, and so on.

If you enter a valid control entry, the DMM creates or appends the associated data table. When an NMS no longer requires the collected data, it may free up the resources used by invalidating the control entry. When this occurs, the probe removes the control entry and all of the data associated with it, thus freeing resources for other monitoring functions. Again, if you use the DMM as the NMS, you must delete unused control table entries manually.

When a MAC initializes, it creates some default control entries:

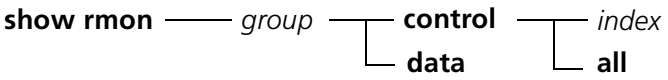
- Collecting statistics on the MAC interface
- Monitoring host and matrix information
- Generating two history reports, one every 30 seconds, and one every 30 minutes

The owner of these entries is the MAC itself. The owner string for these entries is "monitor." Typically, these entries exist for as long as the MAC is an active RMON probe.

When you move an NMC from one network to another, the DMM deletes all control and data tables and restores the basic default entries.

RMON configurations are not stored in NVRAM. The DMM reverts to default RMON settings after a power failure.

Format



group	Values are: ■ alarm ■ event ■ history ■ host ■ matrix ■ topN_hosts
index	Index number of the host table.

Example The following command displays control table entries for a hub's RMON History Table:

```
CB5000> show rmon history control all

RMON History Control Information:

Index  Data Source   Buckets      Interval   Owner
-----  ------------  ----------   ---------- -------------------
    3  Interface 3        120     00:30      monitor
    4  Interface 4        120     00:30      monitor
    6  Interface 3         96     30:00      monitor
    8  Interface 4         96     30:00      monitor
```

Related Commands SET RMON CONTROL
SHOW RMON DATA

SHOW RMON DISTRIBUTION ETHERNET DATA

Use the SHOW RMON DISTRIBUTION ETHERNET DATA command to show packet distribution (by size) on an Ethernet network.

The SHOW RMON DISTRIBUTION ETHERNET DATA command displays a graph that shows the percentage of network traffic that is made up of various packets sizes.

Format

index	Index from the RMON distribution control table.

Example

The following command displays RMON distribution statistics for all entries in the RMON distribution control table:

```
CB5000> show rmon distribution ethernet data all

RMON Ethernet Distribution:

Data Source Interface 3 (Ethernet Statistics Index 3):

               0%         25%        50%        75%        100%
Packet Size   |          |          |          |          |    Packets
-------------------------------------------------------------------------

64            |                                          | 0
65   to 127   |                                          | 0
128  to 255   |                                          | 41
256  to 511   |                                          | 30
512  to 1023  |                                          | 3
1024 to 1518  |                                          | 0
```

Related Commands

SET RMON
SET RMON INTERFACE
SHOW RMON CONTROL

SHOW RMON HISTORY DATA

Use the SHOW RMON HISTORY DATA command to display network statistics information sampled at an interval you configure. This command works with Ethernet modules only.

The history report is similar to the information displayed using the MONITOR command. It logs the difference between counters at regular intervals. The history control table specifies the:

- Data source of the history report
- Collection interval
- Number of entries to store

If the probe has more entries to store than it is configured to hold, the oldest history entry is deleted (the lowest-numbered sample) and a new entry is appended (as the highest-numbered sample).

The Ethernet history report incorporates Ethernet statistics counters. For each sample entry, the report provides utilization of the network during that interval. Each entry is stamped with the date and time that the entry was started.

Format

control index	Index from RMON History Control Table for the history you want to view.
data index	Index of the specific history collected that you want to view.

Example

The following command displays all history samples collected using RMON History Control Table entry 3. (The example shows a single bucket. Histories typically show many.)

```
CB5000> show rmon history data 3 all


RMON History display for Interface 3:
Sample Index:   2387
Interval Start: 06 Oct 94 06:53:46
Drop Events:    0
Octets:         374107
Packets:        1927
Broadcast Packets: 40
Multicast Packets: 22
CRC and Alignment Errors:0
Undersize Packets: 0
Oversize Packets: 0
Fragments:      0
Jabbers:        0
Collisions:     0
Utilization:    1
```

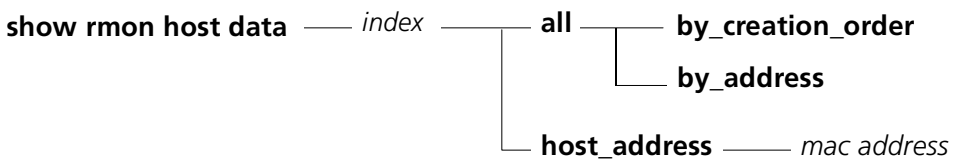
Related Commands SET RMON
SET MODULE INTERFACE
SHOW RMON HISTORY CONTROL

SHOW RMON HOST DATA

Use the SHOW RMON HOST DATA command to display data from the RMON host table. The host table collects statistics related to hosts on the network. As each packet is monitored, the MAC adds the source address of the frame to the host table, incrementing the appropriate "out" counters, and the probe adds the destination address of the frame to the host table, incrementing the appropriate "in" counters.

The host table also collects information for the Host TopN group that indicates which hosts are generating and receiving the most network traffic (typically the servers and routers), the most network errors, and so on.

Format



index	The index entry in the RMON host table.
all	Lists all hosts.
by_creation_order	Lists hosts by the order in which the RMON agent detected them.
by_address	Lists hosts by numerical MAC address order.
host_address	Displays host data for the specified address.
mac address	Specifies the MAC address for the host whose host data you want to display.

Example

The following command displays RMON host statistics for one MAC address:

```
CB5000> show rmon host data 1 host_address 0-0-1a-24-0-0

RMON Host display for Interface 1:

Creation Order: 13
Host Address:   00-00-1a-24-00-00
Input Packets:  1
Output Packets: 0
Input Octets:   8812
Output Octets:  0
Output Errors:  0
Output Packets (Broadcast): 0
Output Packets (Multicast): 0
```

Related Commands

SET RMON HOST
SET MODULE INTERFACE
SHOW MODULE

SHOW RMON MATRIX DATA

Use the SHOW RMON MATRIX DATA command to display information on conversations between hosts on a network.

The matrix table is similar to the host table, but tracks network conversations between hosts, instead of host traffic. For each frame, the MAC extracts the source and destination address and associates the frame with a conversation.

Network conversations are important for performance modeling. Using matrix table information, you can model the network across bridging devices and along shared segments. You can optimize network performance by ensuring that heavy conversations are isolated to shared LANs and do not occur across heavily burdened bridging devices.

Format

show rmon matrix data —— *selection*

selection	■ *index* (an entry from the RMON matrix control table) ■ involving *mac address* ■ by_insertion_order ■ all

Example

The following command displays the RMON Matrix Table for RMON Matrix Control Table entry 3:

```
CB5000> show rmon matrix data 3

RMON Matrix display for Interface 3 :
Source Address  : 00-00-0D-04-F9-5C
Destination Address: 00-00-F6-00-7F-E4
Index           : 3
Packets         : 130637
Octets          : 9714430
Errors          : 0
```

Related Commands

SET RMON MATRIX
SET MODULE INTERFACE
SHOW MODULE

SHOW RMON STATISTICS

Use the SHOW RMON STATISTICS command to display general statistic information on a specified group.

Format

Example

The following command displays all RMON Ethernet data statistics:

```
CB5000> show rmon statistics ethernet data all

RMON Ethernet Statistics:

Index                       : 3
Data Source                 : Interface 3
Drop Events                 : 0
Octets                      : 0
Packets                     : 0
Broadcast Packets           : 0
Multicast Packets           : 0
CRC and Alignment Errors    : 0
Undersize Packets           : 0
Oversize Packets            : 0
Fragments                   : 0
Jabbers                     : 0
Collisions                  : 0
```

Related Commands

SET RMON
SET MODULE INTERFACE

SHOW RMON TOPN_HOSTS DATA

Use the SHOW RMON TOPN_HOSTS DATA command to display data on the stations that generate the most data of the type you specify. This command applies to Ethernet modules only.

This report picks a statistic associated with hosts and sorts the hosts based on that statistic, over a period of time you select. For example, the TopN group can generate a report indicating the top 10 hosts that generated errors over the last half hour. The control table specifies:

- Statistic to use for the sort (Rate Base)
- Duration of the monitoring period
- Number of hosts to report (this cannot be set from the command line)

You can sort the data using any of the host table statistics. The generated report indicates in decreasing order:

- Hosts
- Actual rate for the sorted statistic for that host

A TopN report is generated directly from the host table. Therefore, the TopN report points to a host control entry.

Format

show rmon topn_hosts data — *control index* — *data index*
└ **all**

control index	Index from RMON Top N Hosts Control Table.
data index	Index of the specific Top N Hosts entry that you want to view.

Example

The following command displays all TopN entries for TopN Hosts Control entry 1:

```
CB5000> show rmon topn_hosts data 1 all

RMON Host Top N Display for Interface 3:

Index Address           Input Packets
----- ----------------  -------------
   1  00-00-0C-04-F9-5C            765
   2  08-00-8F-30-02-E3            651
   3  08-00-09-75-48-6C            107
   4  FF-FF-FF-FF-FF-FF             59
   5  02-60-8C-8C-26-7D             18
   6  01-80-C2-00-00-00             15
   7  02-60-8C-A4-9B-13              9
   8  00-00-F6-00-5F-E4              9
   9  02-60-8C-3F-6F-5C              9
  10  02-60-8C-6B-13-61              8
```

Related Commands

SET RMON TOPN_HOSTS
SET MODULE INTERFACE
SHOW MODULE

SHOW ROVING_ANALYSIS_ PORT

To display information about the roving analysis configuration, use the SHOW ROVING_ANALYSIS_PORT commands.

The system output that is displayed when you enter these commands contains the following columns:

- **System-Analyzer** — Shows whether a SwitchModule is configured to receive mirrored traffic.
- **Analyzer** — Shows where the mirrored traffic is being sent for analysis.
- **Monitor-Source** — Lists the bridge port whose traffic is being mirrored (source port).

Format

hub_info	Option to use when you want to show roving analysis information for all SwitchModules in the hub
system_analyzer_info	Option to use when you want to display information about the SwitchModule configured as the system analyzer

Example 1

The following example shows roving analysis information for all SwitchModules in the hub, use the SHOW ROVING_ANALYSIS_PORT command with the HUB_INFO option:

```
> show roving_analysis_port hub_info

Slot    Module      System-Analyzer  Analyzer       Monitor-Source
-----   --------------------------- ---------------  --------------
03.1    6604M-F     DISABLED         NONE           NONE
04.1    6612M-TP    DISABLED         NONE           NONE
07.1    6604M-TX    ENABLED          BRIDGE PORT 3  BRIDGE PORT 8.2
08.1    6604M-TX    DISABLED         SYSTEM ANALYZER
13.1    6612M-TP    DISABLED         NONE           NONE
14.1    6614M-FTP   ENABLED          PROCESSOR      BRIDGE PORT 14.01
16.1    6604M-F     DISABLED         NONE           NONE
17.1    6604M-F     DISABLED         NONE           NONE
```

In the previous example:

- The SwitchModule in slot 7 is enabled as the system analyzer. It is receiving mirrored traffic from bridge port 8.2, the monitor-source, and sending the mirrored traffic out bridge port 7.3 for analysis.
- Bridge port 14.1 is configured to mirror traffic locally to its own processor.

Example 2 To display information about the SwitchModule configured as the system analyzer, use the SHOW ROVING_ANALYSIS_PORT command with the SYSTEM_ANALYZER_INFO option:

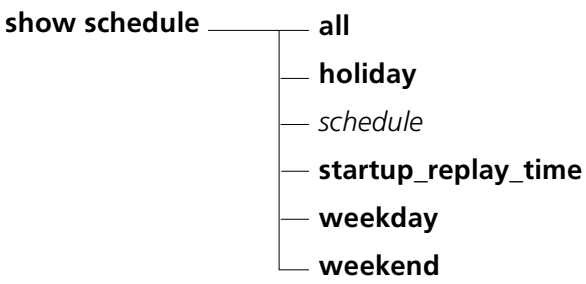
```
> show roving_analysis_port system_analyzer_info

Slot    Module      System-Analyzer Analyzer        Monitor-Source
------  --------------------------- ------------------------------
07.1    6604M-TX    ENABLED         BRIDGE PORT 3   8.2
```

This command display shows that slot 7 is configured as the system analyzer.

SHOW SCHEDULE

Use the SHOW SCHEDULE command to display schedule information for all schedules or a specific schedule.

Format



all	Displays information about all schedules.
holiday	Displays the holiday list.
schedule	Displays information about the specified schedule. Use the SHOW SCHEDULE ALL command to display a numbered list of schedules. The options are 1 through 20.
startup_replay_time	Refer to the SET SCHEDULE STARTUP_REPLAY_TIME command for a description of startup_replay_time.
weekday	Displays the list of days defined as weekdays.
weekend	Displays the list of days defined as weekend days.

Example

The following command displays all current schedule information:

```
CB5000> show schedule all

Schedule                Script                  Days      Dates
Index      Mode         Time        Number      MTWTFSS
-----      ----         ----        ------      -------   ------
1          enabled      08:00       1           +++++     -09/06
2          enabled      20:00       2           +++++     +08/28
3          enabled      00:00       2           ++        +09/06
4          enabled      17:00       2           +         -09/06
5          enabled      08:00       3           +         08/28
```

A plus (+) next to a date indicates the date is included in the schedule. A minus (-) indicates a date is excluded from the schedule.

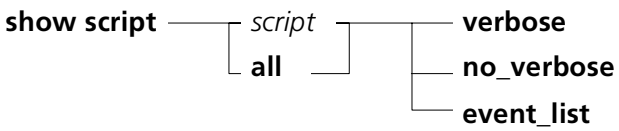
Related Commands

SET SCHEDULE
SET SCHEDULE HOLIDAY
SET SCHEDULE STARTUP_REPLAY_TIME
SET SCHEDULE WEEKDAY
SET SCHEDULE WEEKEND

SHOW SCRIPT

Use the SHOW SCRIPT command to display information about a specific script or all scripts.

Format



script	The number of the script for which you want to display information.
all	Displays information about all scripts.
verbose	Displays extended information, including a list of commands in the script.
no_verbose	Displays summary information.
event_list	Displays script-to-event associations. For more information, refer to the description of the SET SCRIPT RUN_ON_EVENT command.

Example

The following command displays script information for all eight scripts:

```
CB5000> show script all

Script Number           Script Name
    1                   downloader
    2                   status
    3                   (No Name Assigned)
    4                   (No Name Assigned)
    5                   (No Name Assigned)
    6                   (No Name Assigned)
    7                   (No Name Assigned)
    8                   (No Name Assigned)
```

Related Commands

SET SCRIPT DELETE
SET SCRIPT INSERT
SET SCRIPT NAME
SET SCRIPT OVERWRITE
SET SCRIPT RUN_ON_EVENT

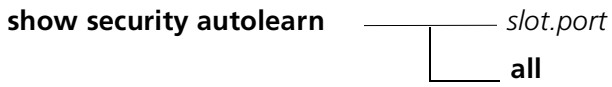
SHOW SECURITY AUTOLEARN

Use the SHOW SECURITY AUTOLEARN command to display the entries in the Autolearning database. Only the entries for the ports specified in the command line are displayed.

When using the SHOW SECURITY AUTOLEARN command, a single asterisk (*) marks entries for a port that exceeds the maximum of seven MAC addresses per port. A double asterisk (**) marks entries that have exceeded the hub capacity of 360 MAC addresses.

If your hub is near full capacity, or if you have ports connected to bridges, you may want to use the SET SECURITY AUTOLEARN CAPTURE command to perform two or more autolearn captures. This may prevent the ports from exceeding the DMM limit of 360 MAC addresses per hub.

Format



slot.port	Selects a port for displaying the entries in the Autolearning database. *slot* (1 through 17) is the slot location of the module in the hub and port (1 through 20) is the port.
all	Displays Autolearning database for all modules installed in the hub.

Example

The following command displays the Autolearning database entries for the ports on the ONline 10BASE-T Security Module in slot 3:

```
CB5000> show security autolearn 3.all
Autolearned Addresses for Module E12MSS5112M-TPLS in Slot 3:
Port       MAC Address(s)
-----      ---------------
3.01       01-01-01-01-01-01
3.06       08-00-8f-01-02-03
           08-00-8f-02-03-04
           08-00-8f-04-05-06
           08-00-8f-05-06-07
           08-00-8f-06-07-08 *
           08-01-01-01-01-01 *
3.09       09-00-8c-09-09-09
           09-00-8c-09-09-0a
3.12       12-00-01-12-12-12
Note: At least one port on this module has more than 7 security
addresses autolearned for it.  Only the first 7 addresses per port
(as ordered by MAC address) will be downloaded; extraneous addresses
are marked in the display above with an asterisk.
```

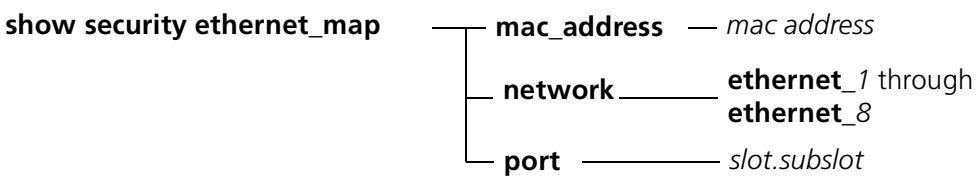
Related Command

CLEAR SECURITY AUTOLEARN MAC_ADDRESS

SHOW SECURITY ETHERNET_MAP

Use the SHOW SECURITY ETHERNET_MAP command to display all MAC addresses within the specified network.

Format



mac_address	Source addresses. The number of MAC addresses does not exceed the maximum_security_addresses_per_port, which is 8.
mac address	The MAC address entry for which you want to display information.
network	Selects the network to display the MAC addresses.
ethernet_*1* through **ethernet**_*8*	Specifies the specific Ethernet network for which you want to display the security ethernet map.
port	Identifies the port for this operation.
slot.subslot	Selects a module installed in the hub to display all of its port MAC addresses. *slot* (1 through 17) is the location of a module in the hub and subslot is the port number on the specified module.

Example

The following command displays the MAC addresses for the specified port 1 in slot 10:

```
CB5000> show security ethernet_map network ethernet_1
Network Map for Network Ethernet_1:
MAC Address(s)       SLOT   PORT
-----------------    ----   ----
01-01-01-01-01-01    10     1
08-00-8f-01-02-03    10     1
08-00-8f-02-03-04    10     1
```

Related Command

SET SECURITY PORT MODE

SHOW SECURITY INTRUDER_LIST

Use the SHOW SECURITY INTRUDER_LIST command to display information about the 10 most recent security intrusions.

The display lists:

- The port that experienced the intrusion and its MAC address (if available)
- The time (in days (d), hours (h), minutes (m), and seconds (s)) that has elapsed since the intrusion attempt occurred
- Whether the DMM automatically disabled the port

The intruder list contains a maximum of 10 entries. When the intruder list is full and a new entry is added, the oldest entry is cleared automatically.

Format

show security intruder_list

Example

The following command displays the intruder list:

```
CB5000> show security intruder_list

Port    MAC Address       Time Since     Auto-Disabled?
----    ----------------- -------------  --------------
12.01   08-00-8F-02-C6-BE 0d 0h 15m 27s  Yes
05.03   09-D3-74-00-2E-01 1d 5h 32m 53s  Yes
```

Related Command

CLEAR SECURITY INTRUDER_LIST

SHOW SECURITY PORT

Use the SHOW SECURITY PORT command to display the security mode and MAC address for a specific port, all ports on a specific module, or all ports on all modules in the hub.

Format

slot.subslot	Selects a port from a module installed in the hub for which to display security information. *slot* (1 through 17) is the slot number and *subslot* is the port number. For example, to specify port 4 on the module in slot 6, enter **6.4** To specify all the ports on the module in slot 6, enter **6.all**
all	Selects the ports from all the modules installed in the hub slot for which to display security information.

Example

The following command displays security information for all ports on hub 3:

```
CB5000> show security port 3.all

Security Display for Module 6218M-ATPP in slot 3:
Port    Mode        MAC Addresses    General Information
----    --------    ---------------  -------------------
3.01    DISABLED    NONE             TOKEN_RING_1
3.02    DISABLED    NONE             TOKEN_RING_1
3.03    DISABLED    NONE             TOKEN_RING_1
3.04    DISABLED    NONE             TOKEN_RING_1
```

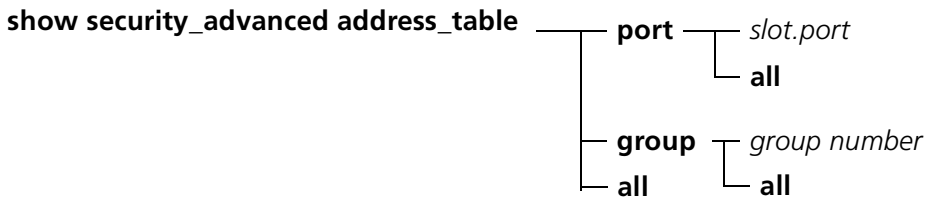
Related Command

SET SECURITY_ADVANCED_ADDRESS_TABLE ADDRESS

SHOW SECURITY_ADVANCED ADDRESS_TABLE

Use the SHOW SECURITY_ADVANCED ADDRESS_TABLE command to display a MAC address or group of addresses for Ethernet networks that have been assigned a CoreBuilder 5000 Ethernet Private Line Card. These addresses are stored in the Ethernet security table.

Format



slot.port	The slot and port number of the port for which you want to view an address table
group number	1 through 256.

Example

The following command displays the entire security address table:

```
CB5000> show security_advanced address_table all

Entry   Port     Group_Code  MAC_Address
-----   -----    ----------  -----------------
   1.            25          08-00-8f-00-17-d0
   2.            25          08-00-8f-00-17-d1
   3.   8.15                 08-00-8f-00-17-da
   4.   8.16                 08-00-8f-00-17-db
   5.   8.17                 08-00-8f-00-17-ce
   6.   8.18                 08-00-8f-00-17-cf
   7.   8.19                 08-00-8f-00-17-d3
   8.   8.20                 08-00-8f-00-17-d2
   9.   8.21                 08-00-8f-00-17-d9
  10.   8.22                 08-00-8f-00-17-d8
```

The first two MAC addresses in the table are assigned to Group_Code 25. The remaining addresses are paired with module port numbers.

Related Commands

SET SECURITY_ADVANCED
CLEAR SECURITY

SHOW SECURITY_ADVANCED INTRUDER_TABLE

Use the SHOW SECURITY_ADVANCED INTRUDER_TABLE command to display information on recent intrusion attempts for Ethernet networks with CoreBuilder 5000 Ethernet Private Line Cards.

The security intruder table contains a detailed log on the last 100 intrusion attempts on each secured network. To log intrusion attempts in the security intruder table, you must:

- Enable the intruder reporting network parameter
- Enable per-port intruder checking
- Enable either source address or source port checking

After intrusion detection is properly configured, the Ethernet Private Line Card reports intruders to the DMM, which then stores the information in the security intruder table.

Each table entry contains the MAC address and associated port or group code, the date and time of the attempted intrusion, the network on which the intrusion occurred, and the number of the intrusion attempts on the secured network.

The Ethernet Private Line Card does not save intruder table information in non-volatile RAM (NVRAM).

Format

show security_advanced intruder_table — **chronological** | **port**

chronological	Displays the list of intruder attempts from the Intruder table in chronological order.
port	Displays the list of intruder attempts from the Intruder table by port number.

Example

The following command displays the currently stored Ethernet security intruder table:

```
CB5000> show security_advanced intruder_table port

Port    MAC Address      Time Stamp   Network      Attempts  Description
-----   -------------------------   -------      --------  ----------------
02.03   08-00-2b-00-00-0108FEB95     ETHERNET_7   13        Intruder station
                         10:04:34                           08-00-2b-00-00-01 accesse
                                                            port 02.03 13 times...
Port    MAC Address      Time Stamp   Network      Attempts  Description
-----   -------------------------   -------      --------  -----------
02.04   08-00-2b-00-00-0108FEB95     ETHERNET_3   4         Intruder station
                         09:02:45                           08-00-2b-00-00-01 accesse
                                                            port 02.04 4 times...
```

Related Command

CLEAR SECURITY ADVANCED

SHOW SECURITY_ADVANCED NETWORK

Use the SHOW SECURITY_ADVANCED NETWORK command to view the configuration of each security attribute on your network for Ethernet networks that have been assigned a CoreBuilder 5000 Ethernet Private Line Card.

Refer to the descriptions of each feature in the *CoreBuilder 5000 Ethernet Private Line Card User Guide* for more information.

Format

show security_advanced network ____ *network*

network	Displays the security settings for the network you specify. For example, if you enter ethernet_1, the system displays the configuration for ethernet_1. The options are: ■ ethernet_1 through ethernet_8 ■ isolated_1 through isolated_8 ■ all (to display information for all secure networks)

Example The following command displays security settings for all hub networks:

```
CB5000> show security_advanced network all

ETHERNET_4 Network Security Configuration
------------------------------------------------------------------------
Securing Module:          Slot 01.02 Version a1.00.6
                          6100D-SEC: Ethernet Security Private LineCard

Operational Mode:         ENABLED
Administrative Mode:      ENABLED

Autolearning:             ENABLED
Eavesdrop Protection:     ENABLED

Intruder Detection:                 Intruder Actions:
   Source Address Checking:ENABLED    Intruder Reporting:    DISABLED
   Source Port Checking:   DISABLED   Intruder Jamming:      DISABLED
                                      Intruder Port DisablingDISABLED
```

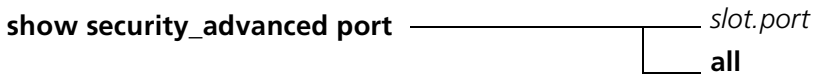
Related Command SET SECURITY_ADVANCED

SHOW SECURITY_ADVANCED PORT

Use the SHOW SECURITY_ADVANCED PORT command to view the security configuration of ports on Ethernet networks that have been assigned a CoreBuilder 5000 Ethernet Private Line Card.

Refer to the descriptions of each feature in the *CoreBuilder 5000 Ethernet Private Line Card User Guide* for more information.

Format



slot.port	The slot and port number of the port for which you want to view port configuration.

Example

The following command shows security configuration for all ports in a hub (only the output for ports 1, 2, 3, and 4 are shown):

```
CB5000> show security_advanced port all

Security Port Table Display for Module 1 6124M-TPL6:
-------------------------------------------------------------------------
---

Port    Autolearn   FailSafe  Group_A  Group_B  Intruder_Check  Jamming
-----   ---------   --------  -------  -------- --------------  --------
08.01   ENABLED     DISABLED       0        0   ENABLED         DISABLED
08.02   ENABLED     DISABLED       0        0   ENABLED         ENABLED
08.03   ENABLED     DISABLED       0        0   ENABLED         ENABLED
08.04   ENABLED     DISABLED       0        0   ENABLED         ENABLED
.
.
>
```

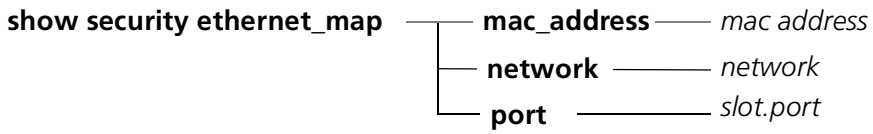
Related Command

SET SECURITY_ADVANCED

SHOW SECURITY ETHERNET_MAP

Use the SHOW SECURITY ETHERNET_MAP command to view all MAC addresses on every port within the specified network.

Format



mac address	The MAC address for the specified port.
network	Displays the security settings for the network you specify. For example, if you enter **ethernet_1**, the system displays the configuration for ethernet_1. The options are: ■ ethernet_1 through ethernet_8 ■ isolated_1 through isolated_8 ■ all (to display information for all secure networks)
slot.port	Displays the slot and port number of the port whose security map you want to view.

Example

The following command shows security ethernet map for port 1 on slot 10:

```
CB5000> show security ethernet_map port 10.1

Network map for Network Ethernet_1:
------------------------------------------------------------
MAC ADDRESS              SLOT      PORT
--------------           --------  -------

02-00-00-00-80-00        10        1
02-00-00-00-80-e0        10        1
02-00-00-00-80-60        10        1

>
```

Related Command

SET SECURITY_PORT MODE

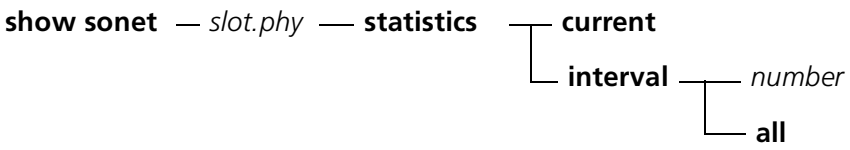
SHOW SONET STATISTICS

Use the SHOW SONET STATISTICS command to display Synchronous Optical Network (SONET) interval information for a PHY port.

A PHY is a physical port.

SONET error statistics are collected for 15-minute intervals over a period of 24 hours.

Format



slot.phy	Identifies the slot and port for this operation. *slot* (1 through 17) is the slot number and *phy* (1 or 2) is the PHY port number. For example, to identify PHY port 1 on the module in slot 4, enter **4.1**
current	Specifies the current interval.
interval	Specifies an interval other than the current interval.
number	Specifies the interval number.
all	Specifies all intervals.

Example 1

The following command displays the SONET information for the current interval in slot 4, PHY port 1:

```
CB5000> show sonet 4.1 statistics current

Slot  Module       Version  Network      General Info
----  -------------------  -------------  ------------------
04    6602M-MOD    v1.00    N/A

SONET Statistics for 04.1 in interval: Current
-----------------------------------------------
Sect Errored Seconds:                  0
Sect Severely Errored Seconds:         0
Sect Severely Errored Frame Seconds:   0
Sect Coding Violations:                0

Line Errored Seconds:                  0
Line Severely Errored Seconds:         0
Line Unavailable Seconds:              0
Line Coding Violations:                0

Path Errored Seconds:                  0
Path Severely Errored Seconds:         0
Path Unavailable Seconds:              0
Path Coding Violations:                0
```

Example 2 The following command displays the SONET information for interval 2 in slot 4, PHY port 1:

```
CB5000> show sonet 4.1 statistics interval 2

Slot  Module       Version  Network      General Info
----  ----------   -------  -----------  ------------------
04    6602M-MOD    v1.00    N/A

SONET Statistics for 04.1 in interval: 2
------------------------------------------------------------
Sect Errored Seconds:                   0
Sect Severely Errored Seconds:          0
Sect Severely Errored Frame Seconds:    0
Sect Coding Violations:                 0

Line Errored Seconds:                   0
Line Severely Errored Seconds:          0
Line Unavailable Seconds:               0
Line Coding Violations:                 0

Path Errored Seconds:                   0
Path Severely Errored Seconds:          0
Path Unavailable Seconds:               0
Path Coding Violations:                 0
```

Refer to the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

Example 3 The following command displays the SONET information for all intervals in slot 4, PHY port 1. This example shows a sample of five intervals. See the notes following the sample screen for more information.

```
CB5000> show sonet 4.1 statistics interval all

Slot  Module       Version  Network       General Info
----  -------------------  ------------ -----------------
04    6602M-MOD    v1.00    N/A

SONET Statistics for 04.1 in interval: All
-----------------------------------------------
                   SECTION            LINE             PATH
-------------------------------------------------------------------------
Int   hh:mm    ES  SES  SFS  CV  ES  SES  UAS  CV  ES  SES  UAS  CV
-------------------------------------------------------------------------
 1   -00:10    0    0    0    0   0   0    0    0   0   0    0    0
 2   -00:30    0    0    0    0   0   0    0    0   0   0    0    0
 3   -00:45    0    0    0    0   0   0    0    0   0   0    0    0
 4   -01:00    0    0    0    0   0   0    0    0   0   0    0    0
 5   -01:15    0    0    0    0   0   0    0    0   0   0    0    0
```

The interval table displays a history of SONET error statistics accumulated over a maximum of ninety-six 15-minute intervals (24 hours), with lower-numbered intervals showing the most recently accumulated statistics. The number of intervals actually displayed depends on the amount of time elapsed from the last module reset.

From module reset, time is measured as a succession of 15-minute intervals. When each 15-minute interval expires, the statistics for each existing interval are placed in the next higher-numbered interval. A new interval is added to receive the statistics from the then highest-numbered interval, and the statistics for the just-completed 15-minute interval are placed in Interval 1.

After 96 intervals have accumulated, the statistics in the 96th interval disappear from the display when the next 15-minute interval expires.

Field	Definition
Int	Interval number. Each interval represents a 15-minute time period.
hh:mm	Hours/minutes of elapsed time relative to current 15-minute interval. For example, the statistics in Interval 4 were accumulated during the 15-minute interval that elapsed one hour ago.
ES	Errored Seconds.
SES	Severely Errored Seconds.
SFS	Severely Errored Framing Seconds.
UAS	Unavailable Seconds.
CV	Coding Violations.

SHOW SONET STATUS

Use the SHOW SONET STATUS command to display Synchronous Optical Network (SONET) status information for a PHY port.

A PHY is a physical port.

Format

show sonet — *slot.phy* — **status**

slot.phy	Identifies the slot and port for this operation. *slot* (1 through 17) is the slot number and *phy* (1 or 2) is the PHY port number. For example, to identify PHY port 1 on the module in slot 4, enter **4.1**

Example The following command displays the SONET status information for slot 4:

```
CB5000> show sonet 4.1 status

Slot  Module       Version  Network       General Info
----  ----------   -------  ----------- 3 ------------------
04    6602M-MOD    v1.00    N/A

Medium Type                              SONET
Medium Time Elapsed (sec):               500
Medium Valid Intervals:                  50
Medium Line Coding:                      NRZ
Medium Line Type:                        SHORT
Medium Clock Source:                     EXTERNAL

Section Current Status:                  OKAY
Line Current Status:                     OKAY
Path Current Status:                     OKAY
Path Current Width:                      STS
M/S/L Speed (bps):                       155
M/S/L Admin Status:                      ENABLED
M/S/L Oper Status:                       UP
M/S/L Last Change:                       <timestamp>

Path Speed (bps):                        155
Path Admin Status:                       ENABLED
Path Oper Status:                        UP
Path Last Change:                        <timestamp>
```

See the ATM Backbone SwitchModule User Guide *for definition of terms and additional information.*

SHOW TERMINAL

Use the SHOW TERMINAL command to display the terminal parameter values for either the Console or Auxiliary port.

Format

show terminal

Example

The following command displays terminal settings for the Console and Auxiliary ports:

```
CB5000> show terminal

Terminal Session Parameters:
  Prompt        CB5000>
  Timeout time:0

Console Port Parameters:
  Baud:         9600
  Data bits:    8
  Parity:       NONE
  Stop bits:    2
  Hangup:       DISABLED
  Mode:         COMMAND LINE
  Terminal:     VT100

Auxiliary Port Parameters:
  Baud:         9600
  Data bits:    8
  Parity:       NONE
  Stop bits:    2
  Hangup:       DISABLED
  Mode:         COMMAND LINE
  Terminal:     VT100
```

Related Command

SET TERMINAL

SHOW TFTP

Use the SHOW TFTP command to display TFTP parameter values.

Format

show tftp

Example

The following command displays TFTP values:

```
CB5000> show tftp

--- TFTP Variables: ---

TFTP Server IP Address: 127.0.0.1
TFTP File Name:         image
TFTP Result:            OKAY
```

TFTP Result	Definition
CLEAR	User cleared the previous value in this field (CLEAR TFTP command).
TRANSFER IN PROGRESS	TFTP file transfer is in progress.
OKAY	TFTP file transfer completed successfully.
UNDEFINED TFTP ERROR	Undefined TFTP error.
FILE NOT FOUND	The TFTP server could not find the file.
ACCESS ERROR	The TFTP server could not access the file.
DISK FULL	Upload error only.
NO RESPONSE FROM SERVER	The TFTP server did not respond to the request.
INVALID DOWNLOAD KEY	The download key entered as part of a licensed software upgrade is invalid.
FEPROM ERASE ERROR	The hub receiving the download reported an error. Retry the download. If the error recurs, the hub requires servicing.
FEPROM PROGRAM ERROR	The hub receiving the download reported an error. Retry the download. If the error recurs, the hub requires servicing.
TFTP TRANSFER ERROR	An error occurred during the transfer. Retry the download.
DOWNLOAD DECODE ERROR	The file on the server may be corrupt.
DOWNLOAD FAILED	The download failed. Retry the download.
CRC ERROR	The download failed. Retry the download.
FILE TOO LARGE FOR MEMORY	An incorrect file was specified.
GATEWAY UNREACHABLE	The hub received was unable to communicate with the default gateway. Make sure the default gateway IP address is set correctly (SHOW DEVICE command). Make sure the default gateway is operating correctly.
MODULE TYPE INCORRECT	You specified an incorrect module type for the file you are trying to download.
FILE TYPE INCORRECT	You specified an incorrect file.
TIMEOUT WAITING FOR PKT	An error occurred on the network. Retry the download.

Related Commands SET TFTP FILE_NAME
SET TFTP SERVER_IP_ADDRESS

SHOW TR_SURROGATE CRS_STATION

Use the SHOW TR_SURROGATE CRS_STATION command to show CRS station configuration values.

Format

show tr_surrogate ——— *slot*.**2** ——— **crs_station**

slot.**2**	The slot ID for the module that you is selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command shows CRS station information for the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 crs_station

Configuration Report Server Ring Station Data for MAC address
08-00-8e-d0-00-c9
of Network TOKEN_RING_1
------------------------------------------------------------------------
Station Status: Active
Mfg. Adapter Address:08-00-8e-d0-00-c9
NAUN Address:   10-00-04-38-2b-52
Functional Address:00-00-00-18
Group Address:  ff-ff-ff-ff
Microcode Level:000001c1e3f1f4c2f340
Microcode Status:100000900000
Product Id:     20202020202020202020202020202020
Function Class Mask:7b7f
Max. Token Priority:0003
Physical Location:00000000
```

Field	Definition
Station Status	Active — Station inserted in the ring and capable of responding to CRS requests. Inactive — Station incapable of responding to CRS requests or participating in beacon functions.
Mfg. Adapter Address	Burned-in adapter address assigned by the adapter manufacturer.
NAUN Address	Address of the station's Nearest Active Upstream Neighbor (NAUN) in the ring. All zeros indicates that the ring station is inactive.
Functional Address	Functional address information for this ring station. This information is used to identify ring station functions.
Group Address	Group Address used in the Report Ring Station Address and the Report Ring Station Attachments MAC frame.
Microcode Level	Microcode level of the station.
Microcode Status	Current state of the sending station's microcode.
Product Id	Unique identifier that indicates which hardware product the ring station is.

Field	Definition
Function Class Mask	Identifier for the functional classes that the station is able to transmit.
Max. Token Priority	Maximum token priority this station is allowed to set.
Physical Location	Physical location of the ring station.

Related Command SET TR_SURROGATE

SHOW TR_SURROGATE CRS_STATUS

Use the SHOW TR_SURROGATE CRS_STATUS command to show CRS surrogate status information.

Format

show tr_surrogate ——— *slot*.**2** ——— **crs_status**

slot.**2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command shows the CRS status of the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 crs_status

Configuration Report Server Status Data for Network TOKEN_RING_1
-----------------------------------------------------------------
CRS Traps:      ENABLED
NAUN Changes:   0
Active Monitor Changes:0
Tx Forward Strip Status:0000
```

Field	Definition
CRS Traps	Indicates if the CRS function has been configured to report Ring Topology Change traps. Use the SET TR_SURROGATE CRS_STATUS CRS_TRAPS command to change this setting.
NAUN Changes	Displays a count of the total number of NAUN changes on the ring segment since CRS was activated.
Active Monitor Changes	Displays a count of the total number of Active Monitor changes on the ring segment since CRS was activated.
Tx Forward Strip Status	Displays the strip status of the Transmit-Forward Frame.

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE REM_ERROR_MAC_ FRAME

Use the SHOW TR_SURROGATE REM_ERROR_MAC_FRAME command to show the contents of the REM error MAC frame. The REM Error MAC Frame Table displays information used to build a trap that describes the Neighbor Notification and Active Monitor Error portions of the Forward MAC Frame Error trap. The agent builds this trap and forwards it to the Network Management System. Use the SHOW TR_SURROGATE REM_ERROR_MAC_FRAME command to show information about the most-recently received Error MAC Frame.

Format

show tr_surrogate ——— *slot*.**2** —— **rem_error_mac_frame**

slot.**2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command shows the REM error MAC frame for the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 rem_error_mac_frame

Ring Error Monitor Error MAC Frame Trap Data for Network TOKEN_RING_1
-----------------------------------------------------------------------
Station Address 00-00-00-00-00-00
Station NAUN Address00-00-00-00-00-00
Station Physical Location00000000
Last Neighbor Notification Address00-00-00-00-00-00
Monitor Error Code0000
```

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE REM_ISOLATING

Use the SHOW TR_SURROGATE REM_ISOLATING command to show REM Isolating Table information. The REM Isolating Table lists information in the isolating table for the downstream station of a fault domain.

Format

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.
all	Shows all REM isolating information.
index	Shows the indicated entry from the REM Isolating Table.

Example

The following command shows the REM isolating table for the TR-NMC in slot 3.2:

```
CB5000> show tr_surrogate 3.2 rem_isolating 1
Ring Error Monitor Isolating Error Data for Entry 1, Network
TOKEN_RING_3
-------------------------------------------------------------------
Station Address 10-00-5a-b1-6b-3c
Impending Soft Error Threshold Exceeded   FALSE
Excessive Soft Error Threshold Exceeded   FALSE
Station Error Weight  3
Station NAUN Address  00-01-68-50-06-2e
Station Physical Location 00000000
```

Field	Description
Station Address	Lists the MAC address of the station associated with the accumulated error weight.
Impending/Excessive Soft Error Threshold Exceeded	Indicates whether the station with the isolating MAC address is in a weight-exceeded (excessive) or pre-weight exceeded (impending) condition.
Station Error Weight	Lists the calculated error weight of this station in the Isolating Table. The default is zero.
Station NAUN Address	Lists the address of the Nearest Active Upstream Neighbor of the station.
Station Physical Location	Gives the physical location of the receiving ring station of the fault domain.

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE REM_LAST_BEACON

Use the SHOW TR_SURROGATE REM_LAST_BEACON command to show information on the REM last received beacon. The REM Beacon Data Trap Table displays information used to build a trap that describes the beacon type, physical location, and fault domain of a beaconing station. Use the SHOW TR_SURROGATE REM_LAST_BEACON command to show information about the most-recently detected beacon condition on the ring.

Format

show tr_surrogate ——— *slot.***2** ——— **rem_last_beacon**

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command shows the REM last beacon received by the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 rem_last_beacon

Ring Error Monitor Last Received Beacon Data for Network
TOKEN_RING_1
-------------------------------------------------------------------
Beacon Type                    Signal Loss
Station Address                00-ff-00-00-00-00
Station NAUN Address           00-00-ff-00-00
Station Physical Location      00012345
Beacon Recovery Status         None Left
```

Field	Description
Beacon Type	Indicates the type of beacon that occurred on the ring. The options are: ■ Recovery Mode Set ■ Signal Loss ■ Token Not Claimed ■ Token Claimed ■ Invalid — Is displayed when there has not been a beacon recorded
Station Address	If the ring is beaconing currently, this field displays the address of the station transmitting beacon frames.
Station NAUN Address	Displays the Nearest Active Upstream Neighbor of the station transmitting beacon frames. This station is also referred to as the upstream station in the beacon fault domain.
Station Physical Location	Displays the physical location of the beaconing station.

Field	Description
Beacon Recovery Status	Indicates which stations in the beacon domain have been removed from the ring as part of the beacon recovery process. The options are: ■ None Left — No stations have been removed. ■ Beaconing Station Left — Only the station transmitting beacon frames has left the ring. ■ NAUN Station Left — Only the Nearest Active Upstream Neighbor station has left the ring. ■ Both Stations Left — Both the beaconing station and the NAUN have left the ring. ■ Invalid — No beaconing event recorded currently.

Related Command SET TR_SURROGATE

SHOW TR_SURROGATE REM_LAST_SOFT_ ERROR

Use the SHOW TR_SURROGATE REM_LAST_SOFT_ERROR command to show the contents of the REM Last Received Soft Error Table. The REM Last Received Soft Error Table primarily provides information to SNMP network managers. Because the information is designed to create a particular trap, it contains only the state of the stations at the time the Ring Error Monitor received the Soft Error Report MAC frame.

Use the SHOW TR_SURROGATE REM_LAST_SOFT_ERROR command to show information about the most-recent soft error on the ring.

Format

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command shows REM Last Soft Error received data for the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 rem_last_soft_error

Ring Error Monitor Last Received Soft Error Data for Network
TOKEN_RING_1
-------------------------------------------------------------------
Line Errors:                    0
Internal Errors:                0
Burst Errors:                   0
AC Errors:                      0
Abort Delimiters:               0
Lost Frame Errors:              0
Receiver Congestion Errors:     2
Frame Copied Errors:            0
Frequency Errors:               0
Token Errors:                   0
```

Field	Description
Line Errors	Indicates the number of line errors reported in the last Soft Error Report MAC Frame.
Internal Errors	Indicates the number of internal errors reported in the last Soft Error Report MAC Frame. The counter is incremented when the ring station recognizes a recoverable internal error.
Burst Errors	Indicates the number of burst errors reported in the last Soft Error Report MAC Frame. The counter is incremented when the ring station detects the absence of transitions for 5 half-bit times.
AC Errors	Indicates the number of AC errors reported in the last Soft Error Report MAC Frame. The counter is incremented when the ring station receives an AMP or SMP with the AC = b '00' without first receiving an AMP frame.
Abort Delimiters	Indicates the number of 'abort delimiter transmitted' errors reported in the last Soft Error Report MAC Frame. The counter is incremented when the ring station transmits an abort delimiter.

Field	Description
Lost Frame Errors	Indicates the number of lost frame errors reported in the last Soft Error Report MAC Frame.
Receiver Congestion Errors	Indicates the number of receiver congestion errors reported in the last Soft Error Report MAC Frame. Receiver congestion errors indicate that incoming frames are arriving faster than the receiver can accommodate them.
Frame Copied Errors	Indicates the number of frame copied errors reported in the last Soft Error Report MAC Frame.
Frequency Errors	Indicates the number of frequency errors reported in the last Soft Error Report MAC Frame.
Token Errors	Indicates the number of token errors reported in the last Soft Error Report MAC Frame.

Related Command SET TR_SURROGATE

SHOW TR_SURROGATE REM_SOFT_ERROR

Use the SHOW TR_SURROGATE REM_SOFT_ERROR command to show a count of REM non-isolating soft error data. The REM Soft Error Statistics table provides a cumulative count of non-isolating soft error counters.

Format

show tr_surrogate ——— *slot.***2** ——— **rem_soft_error**

*slot.***2**	The slot ID for the module that you selected for the operation. The number can be from 1 through 17. The subslot is always 2.

Example

The following command shows REM soft error data for the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 rem_soft_error

Ring Error Monitor Total Soft Error Data for Network TOKEN_RING_1
------------------------------------------------------------------------
Lost Frame Errors:                          0
Receiver Congestion Errors:                 0
Frame Copied Errors:                        0
Token Errors:                               0
Table Full Conditions:                      0
Minimum Decrement Exceeded Conditions:      0
Receiver Congestion Table-Full Conditions: 0
```

Field	Description
Lost Frame Errors	Total lost frames reported to the REM.
Receiver Congestion Errors	Total receive congestion errors reported to the REM. Receive congestion errors may indicate that the TR-NMC is being overloaded by incoming traffic.
Frame Copied Errors	Total frame copied errors reported to the REM.
Frequency Errors	Total frequency errors reported to the REM.
Token Errors	Total token errors reported to the REM.
Table Full Conditions	Total table full conditions reported by the REM.
Minimum Decrement Exceeded Conditions	Total number of times that the REM attempted to set its decrement value below the minimum value allowed.
Receiver Congestion Table-Full Conditions	Total number of receiver congestion table full conditions reported by the REM.

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE REM_STATUS

Use the SHOW TR_SURROGATE REM_STATUS command to show which REM groups are enabled.

Format

show tr_surrogate ——— *slot.***2** —— **rem_status**

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command displays the current REM Status Table:

```
CB5000> show tr_surrogate 11.2 rem_status

Ring Error Monitor Status Data for Network TOKEN_RING_1
-------------------------------------------------------------------
REM Traps:                          DISABLED
Weight Exceeded Traps:              DISABLED
PreWeight Exceeded Traps:           DISABLED
Receiver Congestion Traps:          DISABLED
NonIso Threshold Exceeded Traps:    DISABLED
Forward Frames Traps:               DISABLED
Ring Line Error Data:               DISABLED
Ring Internal Error Data:           DISABLED
Ring Burst Error Data:              DISABLED
Ring AC Error Data:                 DISABLED
Ring Abort Xmitted Error Data:      DISABLED
Ring Lost Frames Error Data:        DISABLED
Ring Receiver Congestion Data:      DISABLED
Ring Frame Copied Data:             DISABLED
Ring Frequency Error Data:          DISABLED
Ring Token Error Data:              DISABLED
Auto Line Error Data:               DISABLED
Auto Internal Error Data:           DISABLED
Auto Burst Error Data:              DISABLED
Auto AC Error Data:                 DISABLED
Auto Abort Xmitted Error Data:      DISABLED
Auto Lost Frames Error Data:        DISABLED
Auto Receiver Congestion Data:      DISABLED
Auto Frame Copied Data:             DISABLED
Auto Frequency Error Data:          DISABLED
Auto Token Error Data:              DISABLED
Ring State:                         Normal
Reset:
Reset Complete
```

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE REM_THRESHOLD_ EXCD

Use the SHOW TR_SURROGATE REM_THRESHOLD_EXCD command to show information about the most-recently detected threshold exceeded condition. The REM Non-Isolating Threshold Exceeded Table displays information used to build a trap that describes the soft error counter that has been exceeded.

Format

show tr_surrogate ——— *slot.***2** —— **rem_threshold_excd**

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command displays information about the most-recently detected threshold exceeded condition for the TR-NMC in slot 11.2:

```
CB5000> show tr_surrogate 11.2 rem_threshold_excd

Ring Error Monitor Non-Isolating Threshold Exceeded Data for Network
TOKEN_RING_1
-------------------------------------------------------------------
Lost Frame Errors:                              0
Receiver Congestion Errors:                     0
Frame Copied Errors:                            0
Frequency Errors:                               0
Token Errors:                                   0
Table Full Conditions:                          0
Minimum Decrement Exceeded Errors:              0
Receiver Congestion Table-Full Conditions:      0
```

Related Command

SET TR_SURROGATE

SHOW TR_SURROGATE SURR_STATUS

Use the SHOW TR_SURROGATE SURR_STATUS command to assess the current state of a TR-NMC's REM and CRS servers.

Format

show tr_surrogate ——— *slot.***2** ——— **surr_status**

*slot.***2**	The slot ID for the module that you selected for the operation. The slot number can be from 1 through 17. The subslot is always 2.

Example

The following command displays the surrogate status for the TR-NMC in slot 6.2:

```
CB5000> show tr_surrogate 6.2 surr_status

Surrogate Status Data for Network TOKEN_RING_1
------------------------------------------------------------------
Surrogate Admin Status:       DISABLED
Port Mac Address:             00-00-00-00-00-00
Ring Segment:                 0000
Ring Utilization:             0.0%
REM Admin Status:             DISABLED
REM Oper Status:              Idle
CRS Admin Status:             DISABLED
CRS Oper Status:              Idle
```

Field	Description
Surrogate Admin Status	Indicates whether or not the Token Ring Surrogate features (REM and CRS) are enabled or disabled.
Port Mac Address	Identifies the port MAC address of the server functions. This address, together with the Ring Segment number, identifies the surrogate location.
Ring Segment	Identifies the ring segment for which the server in the Port MAC address maintains management information. You can set this value using the SET TR_SURROGATE SURR_STATUS command.
Ring Utilization	Gives the calculated percentage use of the ring the server resides on.
REM Admin Status	Indicates if the REM function is enabled for the Token Ring interface associated with the port MAC address. You can change this setting using the SET TR_SURROGATE SURR_STATUS SURR_ADMIN or the SET TR_SURROGATE SURR_STATUS REM_ADMIN command.
REM Oper Status	Indicates the current operational state of the REM for this interface. The options are: ■ Active — REM function operating. ■ Idle — REM function not operating currently. This means that either the surr_admin or the rem_admin status is set to disable. ■ Initializing — REM function being activated. ■ Initialization failed — REM function could not start. ■ Unavailable — REM function not implemented on this device. ■ Terminating — REM function currently being halted.

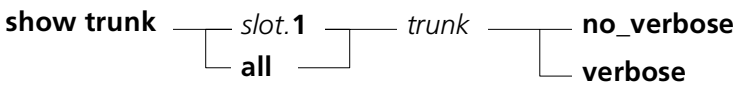
Field	Description
CRS Admin Status	Indicates if the CRS function is enabled for the Token Ring interface associated with the port MAC address. You can change this setting using the SET TR_SURROGATE SURR_STATUS SURR_ADMIN or the SET TR_SURROGATE SURR_STATUS CRS_ADMIN command.
CRS Oper Status	Indicates the current operational state of the CRS for this interface. The options are: ■ Active — CRS function operating. ■ Idle — CRS function not operating currently. This means that either the surr_admin or the crs_admin status is set to disable. ■ Initializing — CRS function being activated. ■ Initialization failed — CRS function could not start. ■ Unavailable — CRS function not implemented on this device. ■ Terminating — CRS function currently being halted.

Related Command SET TR_SURROGATE

SHOW TRUNK

Use the SHOW TRUNK command to display the status of Ring-In/Ring-Out connections.

Format



slot.**1**	Selects the hub slot (1 through 17) for this operation.
trunk	Selects the trunk for this operation. The trunk port setting is required only on fiber repeater modules. ring_in.*port* ring_out.*port* backplane_in backplane_out
no_verbose	Displays summary information. no_verbose is the default selection.
verbose	Displays extended trunk information.

Example

The following command displays trunk information on the module in slot 3:

```
CB5000> show trunk 3.1 ring_in verbose
Trunk Display for Module 5208M-TP:
Slot  Trunk     Mode     Status      Type   General Information
-------------------------------------------------------------------
03    RING_IN  ENABLED  NO SQUELCH    COPPER  Trunk is down

Trunk Connector:RJ45S
Trunk Mode Dip Setting:ENABLED
Cable Monitor:  DISABLED
Cable Monitor Dip Setting:ENABLED
Network Map State:INTERNAL
```

Status	Definition
OKAY	Trunk is operating properly.
NO PHANTOM	Port is not connected to an operating trunk port.
NO SQUELCH	The trunk does not detect a signal from a remote Ring-In/Ring-Out device.
BEACON WRAPPED	Trunk is wrapped because the device connected to the trunk caused a beaconing condition. While the trunk is wrapped, the trunk software checks the trunk every 30 seconds and unwraps when the remote device is ready.

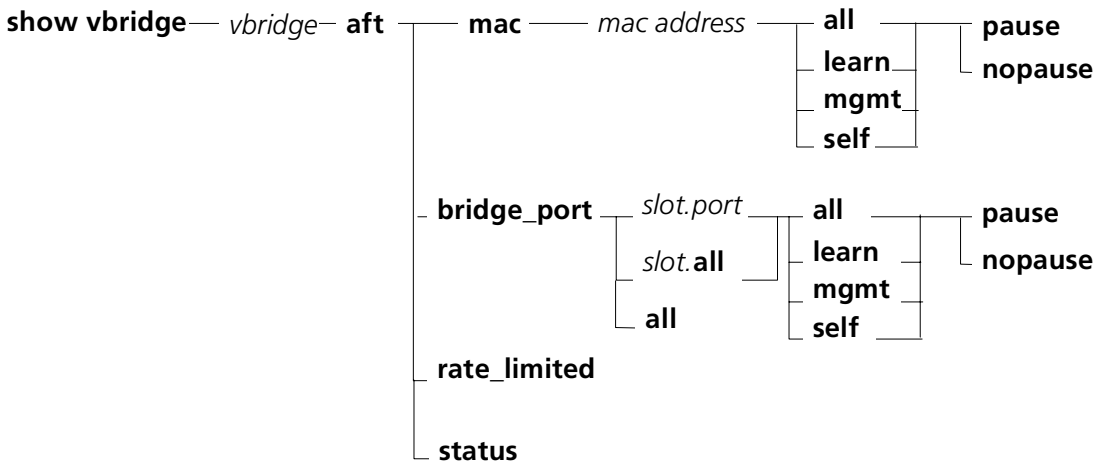
Related Command

SET TRUNK RING_IN/RING_OUT

SHOW VBRIDGE AFT

Use the SHOW VBRIDGE AFT command to display user-created filters and learned entries in the address table.

Format



vbridge	The virtual bridge (1 through 256) about which you want to display information. You must enter the number of a defined virtual bridge.
mac	Displays address table entries relating to a MAC address or set of MAC addresses.
mac address	The MAC address entry about which you want to display information: Enter the MAC address in hexadecimal format.
bridge_port	Displays address table entries relating to a bridge port or set of bridge ports. ■ *slot.port* *slot* is 1 through 17. *port* is 1 through 24. The command displays all entries in the virtual bridge address table associated with this bridge port. ■ *slot*.**all** *slot* is 1 through 17. The command displays all entries in the virtual bridge address table associated with all bridge ports on this SwitchModule.
rate_limited	Displays address table entries that have rate limiting enabled.
status	Displays the number of learned entries, user-created (mgmt) entries, and entries pertaining to the SwitchModule.
all	Displays address table entries for all MAC addresses in the virtual bridge.
learn	Displays address table entries the SwitchModule has learned.
mgmt	Displays user-configured address table entries.
self	Displays entries pertaining to the SwitchModule.
pause	Displays information in sections, pausing until you press the spacebar to continue the display.
nopause	Displays information all at once, without pausing for you to press the spacebar. Use this option when dumping information to a log file.

Example 1 The following commands display status information for the virtual bridge 1 address table:

```
CB5000> show vbridge 1 aft status

Address Forwarding Status of VBridge 1
------------------------------------------------------------------------
                         Current      Peak          TimeStamp
------------------------------------------------------------------------
Learned Entries:            8           14          05:33 13 Oct 99
Mgmt Entries:            1981         1981          09:37 13 Oct 99
Self Entries:               7            7          09:37 13 Oct 99
```

Example 2 The following command displays information about MAC address entries in the virtual bridge 1 address table:

```
CB5000> show vbridge 1 aft mac all
------------------------------------------------------------------------
Entry VBridge  MAC_Address       Port   Type   Persist Source_Check
------------------------------------------------------------------------
 1    1        08-00-8f-11-19-a0 CPU    SELF   NOAGE    DISABLE
 2    1        08-00-8f-11-19-ac CPU    SELF   NOAGE    DISABLE
 3    1        ff-ff-ff-ff-ff-ff CPU    SELF   NOAGE    DISABLE
```

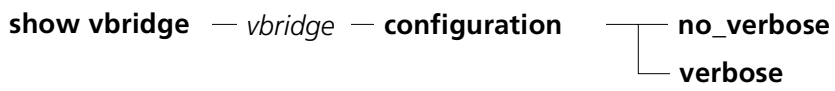
Example 3 The following command displays entries in the address table that consist of a MAC address associated with any bridge port in slot 13:

```
CB5000> show vbridge 1 aft bridge_port 13.all
------------------------------------------------------------------------
Entry VBridge  MAC_Address       Port   Type   Persist  Source_Check
------------------------------------------------------------------------
 1    1        00-00-86-20-a8-1b 13.1   LEARN  AGE      DISABLE
 2    1        00-50-04-95-32-ac 13.1   LEARN  AGE      DISABLE
 3    1        00-80-3e-7c-41-f2 13.1   LEARN  AGE      DISABLE
 4    1        00-c0-4f-39-67-dd 13.1   LEARN  AGE      DISABLE
 5    1        08-00-20-21-b9-95 13.1   LEARN  AGE      DISABLE
 6    1        08-00-20-8a-0a-4e 13.1   LEARN  AGE      DISABLE
 7    1        08-00-8f-30-04-6f 13.1   LEARN  AGE      DISABLE
 8    1        10-00-5a-fa-52-76 13.1   LEARN  AGE      DISABLE
```

SHOW VBRIDGE CONFIGURATION

Use the SHOW VBRIDGE CONFIGURATION command to display information about virtual bridges on CoreBuilder 5000 SwitchModules.

Format



vbridge	The virtual bridge (1 through 256) about which you want to display information. You must enter the number of a defined virtual bridge.
no_verbose	Displays: ■ Virtual bridge number ■ Virtual bridge identifier ■ Number of ports assigned to the virtual bridge ■ Spanning Tree state ■ General information (such as name) If you do not enter the VERBOSE option, NO_VERBOSE is the default.
verbose	Displays the information shown by the NO_VERBOSE option, plus Spanning Tree parameters for the virtual bridge.

Example

The following command displays configuration information about virtual bridge 25:

```
CB5000> show vbridge 25 configuration verbose

VBridge   Bridge Identifier      Ports       Spanning Tree  General Information
-------   --------------------------       -------------  ---------------
     25   80-00-08-00-8f-11-1a-5a2 DISABLED  vbridge_25

Interface Number:                   NONE
Interface Mode:                     N/A
Aging Time:                         300
Learned Entry Discards:             0
Spanning Tree Priority:             32768
Spanning Tree Bridge Max Age:       20.00
Spanning Tree Bridge Forward Delay: 15.00
Spanning Tree Bridge Hello Time:    2.00
Spanning Tree Hold Time:            1.00
Spanning Tree Max Age:              20.00
Spanning Tree Hello Time:           2.00
Spanning Tree Forward Delay:        15.00
Designated Root:                    80-00-08-00-8f-11-1a-5a
Root Cost:                          0
Root Port:                          0
Topology Changes:                   0
Time Since Topology Changed:        667395.26
```

SHOW VBRIDGE IGMP_SNOOPING BRIDGE_PORT

Use the SHOW VBRIDGE IGMP_SNOOPING BRIDGE_PORT command to display all the IP addresses that are in the IGMP cache and are associated with the specified bridgeport.

Format

show vbridge — *vbridge* — **igmp_snooping** — **bridge_port** — *slot.port*

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.
slot.port	Identifies the slot and port for this operation.

Example

The following command displays all the IP addresses that are in the IGMP Snooping cache for Vbridge 25 located in slot 8:

```
CB5000> show vbridge 25 igmp_snooping bridge_port 8.1

Entry  VBridge  IP_Address     MAC_Address         Port
------ -------- -------------- -----------------   ------
1       1       224.0.0.35     01-00-5e-00-00-23   8.1
2       1       224.0.0.139    01-00-5e-00-00-8b   8.1
```

Related Commands

SHOW VBRIDGE IGMP_SNOOPING IP BRIDGE_PORT
SHOW VBRIDGE IGMP_SNOOPING ROUTER_PORTS

SHOW VBRIDGE IGMP_SNOOPING IP

Use the SHOW VBRIDGE IGMP_SNOOPING IP command to display all the ports associated with the specified IP address.

Format

show vbridge — *vbridge* — **igmp_snooping** — **ip** — *xx.xx.xx.xx*

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.
xx.xx.xx.xx	The specific IP address for which you want to display all the associated ports.

Example

The following command displays IGMP Snooping port information about virtual bridge 25 at IP address 111.12.13.14:

```
CB5000> show vbridge 25 igmp_snooping ip 111.12.13.14

Entry   Vbridge   IP_Address     MAC_Address          Port
------- --------  -------------  -----------------    -----
1       1         111.12.13.14   01-00-5e-00-00-23    2.1
2       2         111.12.13.14   01-00-5e-00-00-23    2.2
```

Related Commands

SHOW VBRIDGE IGMP_SNOOPING IP ALL
SHOW VBRIDGE IGMP_SNOOPING IP BRIDGE_PORT
SHOW VBRIDGE IGMP_SNOOPING MAC
SHOW VBRIDGE IGMP_SNOOPING MAC ALL

SHOW VBRIDGE IGMP_SNOOPING IP ALL

Use the SHOW VBRIDGE IGMP_SNOOPING IP ALL command to display all IP addresses and MAC addresses, and their associated ports in the IGMP Snooping cache.

Format

show vbridge — *vbridge* — **igmp_snooping** — **ip** — **all**

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.

Example

The following command displays IGMP Snooping information about virtual bridge 25:

```
CB5000> show vbridge 25 igmp_snooping ip all

Entry   Vbridge     IP_Address     MAC_Address          Port
------- ---------  -------------- -------------------- ----
1       1          224.0.0.35     01-00-5e-00-00-23    2.3
2                                                      3.5
3                                                      5.7
4       1          224.0.0.139                         2.1
5                                                      5.2
```

Related Commands

SHOW VBRIDGE IGMP_SNOOPING IP BRIDGE_PORT
SHOW VBRIDGE IGMP_SNOOPING IP
SHOW VBRIDGE IGMP_SNOOPING MAC
SHOW VBRIDGE IGMP_SNOOPING MAC ALL

SHOW VBRIDGE IGMP_SNOOPING IP BRIDGE_PORT

Use the SHOW VBRIDGE IGMP_SNOOPING IP BRIDGE_PORT command to display all the ports associated with the specified IP address.

Format

show vbridge – *vbridge* – **igmp_snooping** – **ip** – *xx.xx.xx.xx* – **bridge_port** – *slot.port*

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.
xx.xx.xx.xx	The specific IP address for which you want to display all the associated IGMP Snooping ports.
slot.port	Identifies the specific slot and port for this operation.

Example

The following command displays all the IGMP Snooping ports associated with virtual bridge 25 at IP address 111.12.13.14:

```
CB5000> show vbridge 25 igmp_snooping ip 111.12.13.14 bridge_port 2.1

Entry      Vbridge   IP_Address     MAC_Address           Port
-------    ---------  -------------------------------    -----
1          1         111.12.13.14   01-00-5e-00-00-23     2.1
2          2         111.12.13.14   01-00-5e-00-00-23     2.2
```

Related Commands

SHOW VBRIDGE IGMP_SNOOPING IP
SHOW VBRIDGE IGMP_SNOOPING IP ALL
SHOW VBRIDGE IGMP_SNOOPING MAC
SHOW VBRIDGE IGMP_SNOOPING MAC ALL

SHOW VBRIDGE IGMP_SNOOPING MAC

Use the SHOW VBRIDGE IGMP_SNOOPING MAC command to display a MAC address, its IP address and its associated ports in the IGMP Snooping cache.

Format

show vbridge — *vbridge* — **igmp_snooping** — **mac** — *xx.xx.xx.xx.xx.xx*

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.
xx.xx.xx.xx.xx.xx	The specific MAC address for which you want to display associated IGMP Snooping ports.

Example

The following command displays all the IGMP Snooping ports for virtual bridge 1 at MAC address 01.00.5e.00.00.23:

```
CB5000> show vbridge 1 igmp_snooping mac 01.00.5e.00.00.23

Entry   Vbridge     IP_Address      MAC_Address          Port
------- ---------   --------------- -------------------- -----
1       1           224.0.0.35      01-00-5e-00-00-23    2.1
2       1           224.0.0.139     01-00-5e-00-00-23    2.1
```

Related Command

SHOW VBRIDGE IGMP_SNOOPING MAC ALL

SHOW VBRIDGE IGMP_SNOOPING MAC ALL

Use the SHOW VBRIDGE IGMP_SNOOPING MAC ALL command to display all MAC addresses, their IP addresses and their associated ports in the IGMP Snooping cache.

Format

show vbridge — *vbridge* — **igmp_snooping** — **mac** — **all**

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.

Example

The following command displays all the IGMP Snooping ports for virtual bridge 1:

```
CB5000> show vbridge 1 igmp_snooping mac all

Entry   Vbridge     IP_Address      MAC_Address          Port
------- ---------   -------------- ------------------- -----
1       1           224.0.0.35     01-00-5e-00-00-23   2.1
2                                                       3.5
3                                                       5.7
4       1           224.0.0.139    01-00-5e-00-00-8b   2.1
5                                                       5.2
```

Related Command

SHOW VBRIDGE IGMP_SNOOPING MAC

SHOW VBRIDGE IGMP_SNOOPING ROUTER_PORTS

Use the SHOW VBRIDGE IGMP_SNOOPING ROUTER_PORTS command to display all the ports that are designated as router ports in the IGMP Snooping cache.

Format

show vbridge — *vbridge* — **igmp_snooping** — **router_ports**

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.

Example

The following command displays all the ports that are designated as router ports for virtual bridge 1:

```
CB5000> show vbridge 1 igmp_snooping router_ports

Entry   Vbridge   Port
------- --------- ------
1       1         2.1
2       1         3.5
3       1         7.5
4       1         7.8
```

Related Command

SHOW VBRIDGE IGMP_SNOOPING BRIDGE_PORT

SHOW VBRIDGE IGMP_SNOOPING STATUS

Use the SHOW VBRIDGE IGMP_SNOOPING STATUS command to display information about IGMP Snooping on a specified Vbridge.

Format

show vbridge — *vbridge* — **igmp_snooping** — **status**

vbridge	The virtual bridge (1 through 240) about which you want to display information. You must enter the number of a defined virtual bridge.

Example

The following command displays information about IGMP Snooping on virtual bridge 1:

```
CB5000> show vbridge 1 igmp_snooping status

IGMP Snooping                              ENABLED
IGMP Querying                              ENABLED
Port Aging Time                            300
Querier IP Address                         151.104.2.1
Querier State                              Listening
Querier Listening Time (seconds)           30
Querier Interval (seconds)                 125
Sent Query Packets                         200
Group Aging Time (seconds)                 300
```

Related Commands

SHOW VBRIDGE IGMP_SNOOPING IP
SHOW VBRIDGE IGMP_SNOOPING IP ALL
SHOW VBRIDGE IGMP_SNOOPING BRIDGE_PORT
SHOW VBRIDGE IGMP_SNOOPING MAC
SHOW VBRIDGE IGMP_SNOOPING MAC ALL
SHOW VBRIDGE IGMP_SNOOPING ROUTER_PORTS

TELNET

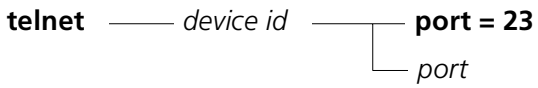
Use the TELNET command to log in to any DMM, or any other target device on the network that supports TELNET.

Use the LOGOUT command to terminate a connection to a remote DMM and return to the local management hub.

If you are having trouble establishing a TELNET session, make sure the target device is on, or bridged or routed to, the same ring as the management hub. You can use the PING command to test if the target device is currently reachable over the network.

You can remotely log in to only one management hub at a time. Before you use TELNET to connect to a second target device, log out of the first target device.

Format



device id	IP address or host name of the device with which you are making a TELNET connection. Enter the address as a series of four decimal bytes separated by periods. For example, 192.122.19.4. You can use host names from the host table in place of IP addresses. Refer to the descriptions for SHOW HOST and SET HOST.
port	Integer identifying the port. The default is 23, which is the TELNET port on most target devices.

Example

The following command establishes a TELNET session with a device with IP address 127.36.58.7 through the default TELNET port (23):

```
CB5000> telnet 127.36.58.7
```

UPLOAD IN_BAND DEVICE CONFIGURATION

Use the UPLOAD IN_BAND DEVICE CONFIGURATION command to save the current configuration of a hub to a file. This configuration file can later be downloaded.

Before you use the UPLOAD IN_BAND command:

- Use the SET TFTP FILE_NAME command to specify the name of the file to save the configuration to.
- Use the SET TFTP SERVER_IP_ADDRESS command to specify the IP address of the TFTP server.

Format

upload in_band device configuration

Example

The following command saves the configuration in the file HUB1CON, previously specified with the SET TFTP FILE_NAME command:

```
CB5000> upload in_band device configuration
This operation will overwrite the file HUB1CON.
Do you wish to continue? (y/n): y
```

Related Commands

DOWNLOAD INBAND
SET TFTP FILE_NAME
SET TFTP SERVER_IP_ADDRESS

A TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site
- 3Com Bulletin Board Service (3Com BBS)
- 3Com Facts℠ Automated Fax Service

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site enter this URL into your Internet browser:

http://www.3com.com/

This service provides access to online support information such as technical documentation and software library, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

This interactive tool contains technical product information compiled by 3Com expert technical engineers around the globe. Located on the World Wide Web at **http://knowledgebase.3com.com**, this service gives all 3Com customers and partners complementary, round-the-clock access to technical information on most 3Com products.

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

- Hostname: **ftp.3com.com**
- Username: **anonymous**
- Password: **<your Internet e-mail address>**

You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

3Com Bulletin Board Service

The 3Com BBS contains patches, software, and drivers for 3Com products. This service is available through analog modem or digital modem (ISDN) 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	Up to 14,400 bps	61 2 9955 2073
Brazil	Up to 28,800 bps	55 11 5181 9666
France	Up to 14,400 bps	33 1 6986 6954
Germany	Up to 28,800 bps	4989 62732 188
Hong Kong	Up to 14,400 bps	852 2537 5601
Italy	Up to 14,400 bps	39 2 27300680

Country	Data Rate	Telephone Number
Japan	Up to 14,400 bps	81 3 5977 7977
Mexico	Up to 28,800 bps	52 5 520 7835
P.R. of China	Up to 14,400 bps	86 10 684 92351
Taiwan, R.O.C.	Up to 14,400 bps	886 2 377 5840
U.K.	Up to 28,800 bps	44 1442 438278
U.S.A.	Up to 53,333 bps	1 847 262 6000

Access by Digital Modem

ISDN users can dial in to the 3Com BBS using a digital modem for fast access up to 64 Kbps. To access the 3Com BBS using ISDN, call the following number:

1 847 262 6000

3Com Facts Automated Fax Service

The 3Com Facts automated fax service provides technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3Com Facts using your Touch-Tone telephone:

1 408 727 7021

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers technical telephone support services. To find out more about your support options, please the 3Com technical telephone support phone number at the location nearest you.

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

Here is a list of worldwide technical telephone support numbers:

Country	Telephone Number	Country	Telephone Number
Asia Pacific Rim			
Australia	1 800 678 515	P.R. of China	10800 61 00137 or
Hong Kong	800 933 486		021 6350 1590
India	+61 2 9937 5085	Singapore	800 6161 463
Indonesia	001 800 61 009	S. Korea	
Japan	0031 61 6439	From anywhere in S. Korea:	00798 611 2230
Malaysia	1800 801 777	From Seoul:	(0)2 3455 6455
New Zealand	0800 446 398	Taiwan, R.O.C.	0080 611 261
Pakistan	+61 2 9937 5085	Thailand	001 800 611 2000
Philippines	1235 61 266 2602		
Europe			
From anywhere in Europe, call:	+31 (0)30 6029900 phone +31 (0)30 6029999 fax		
Europe, South Africa, and Middle East			
From the following countries, you may use the toll-free numbers:			
Austria	0800 297468	Netherlands	0800 0227788
Belgium	0800 71429	Norway	800 11376
Denmark	800 17309	Poland	00800 3111206
Finland	0800 113153	Portugal	0800 831416
France	0800 917959	South Africa	0800 995014
Germany	0800 1821502	Spain	900 983125
Hungary	00800 12813	Sweden	020 795482
Ireland	1800 553117	Switzerland	0800 55 3072
Israel	1800 9453794	U.K.	0800 966197
Italy	1678 79489		
Latin America			
Argentina	AT&T +800 666 5065	Mexico	01 800 CARE (01 800 2273)
Brazil	0800 13 3266	Peru	AT&T +800 666 5065
Chile	1230 020 0645	Puerto Rico	800 666 5065
Colombia	98012 2127	Venezuela	AT&T +800 666 5065
North America	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876-3266		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

To obtain an authorization number, call or fax:

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+65 543 6500	+65 543 6348
Europe, South Africa, and Middle East	+31 30 6029900	+31 30 6029999
Latin America	1 408 326 2927	1 408 326 3355
From the following countries, you may call the toll-free numbers; select option 2 and then option 2:		
Austria	0800 297468	
Belgium	0800 71429	
Denmark	800 17309	
Finland	0800 113153	
France	0800 917959	
Germany	0800 1821502	
Hungary	00800 12813	
Ireland	1800 553117	
Israel	1800 9453794	
Italy	1678 79489	
Netherlands	0800 0227788	
Norway	800 11376	
Poland	00800 3111206	
Portugal	0800 831416	
South Africa	0800 995014	
Spain	900 983125	
Sweden	020 795482	
Switzerland	0800 55 3072	
U.K.	0800 966197	
U.S.A. and Canada	1 800 NET 3Com (1 800 638 3266) Enterprise Customers: 1 800 876 3266	1 408 326 7120 (not toll-free)

3Com Corporation LIMITED WARRANTY

CoreBuilder® 5000 Distributed Management Module

HARDWARE

3Com warrants to the end user ("Customer") that this hardware product will be free from defects in workmanship and materials, under normal use and service, for one (1) year from the date of purchase from 3Com or its authorized reseller.

3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, 3Com may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. 3Com warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

SOFTWARE

3Com warrants to Customer that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from 3Com or its authorized reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation under this express warranty shall be, at 3Com's option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable 3Com published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with 3Com's published specifications or user manual.

THIS 3COM PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD-PARTY SOFTWARE, THE USE OF WHICH IS GOVERNED BY A SEPARATE END USER LICENSE AGREEMENT. THIS 3COM WARRANTY DOES NOT APPLY TO SUCH THIRD-PARTY SOFTWARE. FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE.

YEAR 2000 WARRANTY

See the 3Com Year 2000 Web site at http://www.3com.com/products/yr2000.html

OBTAINING WARRANTY SERVICE

Customer must contact a 3Com Corporate Service Center or an Authorized 3Com Service Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from 3Com or its authorized reseller may be required. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number or User Service Order (USO) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. Responsibility for loss or damage does not transfer to 3Com until the returned item is received by 3Com. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after 3Com receives the defective product.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

Dead- or Defective-on-Arrival. In the event a product completely fails to function or exhibits a defect in materials or workmanship within the first forty-eight (48) hours of installation but no later than thirty (30) days after the date of purchase, and this is verified by 3Com, it will be considered dead- or defective-on-arrival (DOA) and a replacement shall be provided by advance replacement. The replacement product will normally be shipped not later than three (3) business days after 3Com's verification of the DOA product, but may be delayed due to export or import procedures. The shipment of advance replacement products is subject to local legal requirements and may not be available in all locations. When an advance replacement is provided and Customer fails to return the original product to 3Com within fifteen (15) days after shipment of the replacement, 3Com will charge Customer for the replacement product, at list price.

INCLUDED SERVICES:

Telephone Support, with coverage for basic troubleshooting only, will be provided for ninety (90) days from the date of purchase, on a commercially reasonable efforts basis. Please refer to the Technical Support appendix in the Getting Started Guide for telephone numbers.

3Com's Web and Bulletin Board Services provide 3Knowledgebase, bug tracking, documentation, release notes, and some software maintenance releases at no charge.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the State of California, U.S.A., excluding its conflicts of laws principles and excluding the United Nations Convention on Contracts for the International Sale of Goods.

3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA 95052-8145
(408) 326-5000