IBM 8250 Multiprotocol Intelligent Hub

SA33-0302-02

Management Commands Guide

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page xi.

Third Edition March 1996

The information contained in this manual is subject to change from time to time. Any such changes will be reported in subsequent revisions.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

A form for readers' comments appears at the back of this publication. If the form has been removed, address your comments to:

IBM France
Centre d'Etudes et de Recherches
Service 0798 - BP 79
06610 La Gaude
France

- FAX: (33) 93.24.77.97
- EMAIL: FRIBMQF5 at IBMMAIL
- IBM Internal Use: LGERCF at LGEPROFS
- Internet: rcf_lagaude@vnet.ibm.com

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Parts of information in this guide are reprinted with the permission of 3Com Corporation.

Contents

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send these inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, New York 10594, U.S.A.

Trademark and Service Marks

The following terms, denoted by an asterisk (*), used in this publication, are trademarks or service marks of IBM Corporation in the United States or other countries:

IBM*	AIX NetView/6000	AIXwindows
RISC System 6000	NetView	PS/2
AS/400		

The following terms, denoted by a double asterisk (**), used in this publication, are trademarks of other companies:

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

DEC, DECnet, VT100, and LAT are trademarks of Digital Equipment Corporation.**

OSF/Motif, OSF, and Open Software Foundation are trademarks of the Open Software Foundation.

TriChannel is a registered trademark of 3Com Corporation.**

ProComm is a registered trademark of DATASTORM TECHNOLOGIES, INC.**

DATASTORM is a trademark of DATASTORM TECHNOLOGIES, INC. **

Product Page/Warranties

The following paragraph does not apply to the United Kingdom or to any country where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

Chapter 1. Introduction

This guide provides an alphabetized list of commands for the following 8250 management module versions.

- Ethernet Management Module (EMM) v4.00 *8250 Ethernet Management Module Installation and Operations Guide* (Document Number SA33-0209-1)
- FDDI Management Module (FMM) v2.00 *8250 FDDI Management Module Installation and Operation Guide* (Document Number SA33-0217-1)
- Token Ring Management Module (TRMM) v4.00 *8250 Token Ring Management Module Installation and Operation Guide* (Document Number SA33-0213-4)

Each command is described in detail with examples of its syntax, options, and use. Management commands that only apply to Advanced management module versions are noted.

Intended Audience

Before using this guide, we recommend that you and the network manager/administrator at your site read the Installation and Operation guide that applies to your management module. The Installation and Operation guides describe the functions of the module, provides installation instructions, and defines how to set up the module for operation.

Using 8250 Management

8250 management modules manage 8250 hubs and modules in two ways:

- Terminal-based — Terminal connection to an RS-232 serial port connector
- TELNET — Inband connection to a remote device

You enter management commands at the management prompt on a terminal screen. By default, the management prompt is `8250>`. Refer to the SET TERMINAL PROMPT command in this guide for information on customizing the default management prompt.

The 8250 management modules have an intelligent parser that recognizes 8250 modules.

- If you type an invalid parameter for a module type, the parser backspaces over the invalid parameter. The management module then waits for you to finish 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 displays reiterating the setting, followed by the message 'Command aborted'.

Understanding Command Conventions

You control management modules by entering commands at the management prompt on the terminal screen. Commands are not case-sensitive, that is upper and lower case characters can be used with equal effect, with the exception of the SET COMMUNITY command. The community name that you enter in the command string *is* case-sensitive. For example, *NCS* and *ncs* are different community names.

The following conventions are used in the command descriptions contained in this chapter:

The management prompt is indicated as "`8250>` "

User input is indicated as lowercase courier text. For example `show device` or `set terminal baud`.

A parameter that requires unique or specific user input is indicated by lowercase text surrounded by curly brackets. For example, {new password}.

[ENTER] refers to a carriage return.

Using Terminal Keystroke Functions

In addition to alphanumeric characters, you can use terminal input for the management modules to perform 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 management

module to prompt you for additional information. Terminal keystrokes and their functions are outlined in Table 1-1.

Table 1-1. ***Terminal 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.
Space Bar	Completes a command through *command completion* (refer to next section).
?	Displays the available command options.

Using the Command Completion Feature

Command completion allows the management modules 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:

```
8250> sa
```

Press the Space Bar and the command is completed as follows:

```
8250> save
```

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

Management Commands

Chapter 2 provides an alphabetized list of 8250 Management Module 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 *8250*>. Refer to the SET TERMINAL PROMPT command in Chapter 2 for information on customizing the default management prompt.

Entering Parameters

The management module software has an intelligent parser that recognizes 8250 modules.

- If you enter an invaliid parameter for a module type:

  a. The parser backspaces over the invalid parameter.

  b. The management module 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. A message displays reiterating the setting.

  b. The parser sends a Command aborted message.

Chapter 2. Management Commands

This section provides an alphabetized list of 8250 management commands for the following management modules:

- 8250 Ethernet Management Module (EMM)
- 8250 Token Ring Management Module (TRMM)
- 8250 FDDI Management Module (FMM)

Each description includes:

- Syntax for the command
- Parameter options
- Corresponding terminal responses
- Examples
- Description.

?

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

Format

?
{command} ?

Parameters

none

Examples

The following command displays the list of management commands available under the administrator password. The (?) character does not display on the screen when typed, but is shown in the examples for clarity.

```
8250> ?

bootp
clear
copy
download
logout
maintain
monitor
ping
remote_login
reset
revert
run
save
set
show
telnet
```

Example 2

The following command displays the list of FMM management commands available under the super user login id.

```
8250> save ?   [ENTER]
Possible completions:
   all
   alert
   bootp
   community
   concentrator
   device
   group
   module_port
   schedule
   scripts
   security
   terminal
   tftp
   threshold
```

Description

The ? command is used to list the available management command choices. The ? command can also be used as part of a command to prompt a list of the available command options (called the intelligent completion list).

At *any* point on a command line, type "?" to present a list of available choices. The choices that display are based on the type of management module you are using and the module you are configuring.

For example, to set a module to a network, the completion list only displays the networks that are available for the module: Token Ring, Ethernet, or FDDI.

BOOT

Use the BOOT command to exit maintenance mode and boot the operational code. This command is available only in maintenance mode.

Format

BOOT

Parameters

none

Example

```
>> boot          [ENTER]


8250


Management Module (vx.xx-x),
Copyright (c) 199x IBM Corporation
```

Description

Executing the BOOT command boots the operational code in the Flash EPROM and returns the management module to normal operation.

After the management module boots, you must press [ENTER] to display the password prompt to log in to the management module.

If diagnostics have been disabled (through the SET DEVICE DIAGNOSTICS command), the diagnostics do not execute.

BOOTP

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

Format

BOOTP

Parameters

none

Example

```
8250> bootp [ENTER]
```

Description

Once you initiate BootP, the TRMM transmits a BootP request to the BootP server on its network in order to receive a BootP response. The BootP server first attempts to match the management module MAC address to the MAC address defined in the bootptab file. If the MAC addresses match, the BootP server responds to the BootP request by transmitting the information to the management module.

If the BootP server cannot match the management module MAC address to the MAC address defined in the bootptab file, no action is taken by either the management module or the BootP server.

If the management module current configuration differs from the configuration information contained in the bootp response, the management module will update its configuration as specified in the response.

If addition, if the response contains valid TFTP variables, with a file type set to ASCII, the management module will perform a TFTP to the server IP

address, download the script file as specified by the TFTP filename, and execute this script.

The following BootP information applies to the TRMM only.

BootP can be initiated automatically upon startup or initiated manually with the BOOTP command. Enable the SET BOOTP POWER_UP_MODE command to have the TRMM automatically initiate a BootP request upon startup. Or use the BOOTP command to initiate a BootP request at any time.

If BootP is enabled upon startup of a master TRMM, and the TRMM cannot locate the server on its current network, it will determine to which networks Token Ring modules in the hub are connected (since these are the only available paths to a server). The TRMM will then connect to each of these networks, starting with the next network from the one it is configured, until a BootP server is located (that is, if the TRMM is configured to Token Ring 3, it will assign itself next to Token Ring 4).

If the TRMM is a slave, it will only attempt to locate a BootP server on its current network. If a slave TRMM cannot locate a BootP server on its networks, it displays “No Response.”

Use the SHOW BOOTP command to display the current BootP configuration settings. Use the CLEAR BOOTP command to clear the BootP result.

A sample bootptab file is shown below. This file is created on the BootP server. Comments are entered after the pound sign (#).

```
#/ect/bootptab: database for bootp server (/ect/bootpd)
#Blank lines and lines beginning with '#' are ignored.
#
#Legend:
#
# first field – host name
#
#   hd – home directory
#   bf – bootfile
#   cs – cookie servers
#   ds – domain name servers
#   gw – gateways
#   ha – hardware address
#   ht – hardware type
#   im – impress servers
#   ip – host IP address
#   lg – log servers
#   lp – LPR servers
#   ns – IEN-116 name servers
#   rl – resource location protocol servers
#   sm – subnet mask
#   tc – template host (points to similar host entry)
#   to – time offset (seconds)
#   ts – time servers
#
#   IBM Vendor specific definitions:
#
#   T140 – TFTP server file name
#   T141 – TFTP server file type
#     0x01 = FLASH
#     0x02 = BOOT
#     0x03 = ASCII
#   T142 – TFTP server IP address

IBM 5200M:ip=151.104.12.125:ht=ieee802:ha=100f10f0c68:\
sm=0xffffff00:gw=0x97680c01
0x97680c02:T140="/dhome/davies/script3":\
T141=0x03:T142=0x97680C12
```

CLEAR ARP_TABLE

Use the CLEAR ARP_TABLE command to clear the Address Resolution Table contained in the TRMM.

Format

CLEAR ARP_TABLE

Parameters

none

Example

```
8250> clear arp_table  [ENTER]
Arp table cleared.
```

Description

The CLEAR ARP_TABLE command enables you to clear the entire ARP table when ring configuration changes are made. The ARP table entries time out if not updated within 20 minutes.

Address Resolution Protocol matches a station's IP Address to its physical MAC address. Once the TRMM learns this information, it automatically stores this information in the ARP table. The TRMM accesses this table when sending out IP packets (for example, Ping, Telnet, SNMP), and inserts the appropriate destination address into the frame.

You should clear the ARP table if you change a station's IP configuration (for example, interfaces, IP Address), or if you experience difficulty in communicating with a station. Once the table is cleared, the TRMM 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.

CLEAR BOOTP RESULT

Use the CLEAR BOOTP RESULT command to clear the result of the last BootP operation.

Format

CLEAR BOOTP RESULT

Parameters

none

Example

```
8250> clear bootp result [ENTER]
BootP result cleared.
```

Description

The CLEAR BOOTP RESULT command enables you to clear the result of the last BootP operation performed on the TRMM to which you are connected.

CLEAR COMMUNITY

Use the CLEAR COMMUNITY command to clear an entry from the community table.

Format

CLEAR COMMUNITY {index}

Parameters

{index} = 1 through 10 or all

Example

```
8250> clear community 5       [ENTER]
Community 5 cleared.
```

Description

The CLEAR COMMUNITY command deletes an entry from the community table. Use the SHOW COMMUNITY command to verify the index number of the community entry you want to delete.

CLEAR COUNTER

Use the CLEAR COUNTER command to reset to zero all management module counters or a specific group of management module counters.

Format

CLEAR COUNTER {group}

Parameters

{group} = all
device (default if you press ENTER)
module (slot)
network
port {slot.port or slot.all}
station {mac_address or all}

Examples

Example 1

```
8250> clear counter station 10-00-f1-0f-0c-63 [ENTER]
Counters cleared for MAC Address: 10-00-f1-0f-0c-63
```

Example 2

```
8250> clear counter port 3.6   [ENTER]
Counters cleared for port 3.6.
```

Description

The CLEAR COUNTER command clears the statistical counters for the specified group. Use the SHOW COUNTER command to review current network and per-port statistics prior to clearing them.

CLEAR EVENT_LOG

Use the CLEAR EVENT_LOG command to erase the information in the FMM event log after you have either viewed or printed the information.

Format

CLEAR EVENT_LOG

Parameters

none

Example

```
8250> clear event_log       [ENTER]
Event log is cleared.
```

Description

This command erases the information in the FMM event log. Refer to the SHOW EVENT_LOG command to display the contents of the event log.

CLEAR GROUP

Use the CLEAR GROUP command to remove one port, all ports on a specific module, or all ports from a group.

Format

CLEAR GROUP {group} port {slot.port}

Parameters

{group} = all
group1
group2
group3
group4
group5
group6
group7
group8

{slot} = 1 through 17
all
non_existing

{port} = 1 through 32 or all

Examples

Example 1

This example shows how to clear group4 of all ports.

```
8250> clear group group4 port all    [ENTER]

Port 4.9 cleared from group4.
Port 4.10 cleared from group4.
Port 4.12 cleared from group4.
```

Example 2

This example shows how to clear group7 of all the ports associated with modules that have been removed from the hub (non-existing ports).

```
8250> clear group group7 port non_existing   [ENTER]
```

Description

This command and its options enable you to clear one port or many ports from a specific group. In addition, you may also clear a group of all ports associated with a module(s) that has been removed from the hub.

You may want to use the SHOW GROUP command to display the ports in a group before clearing the group.

CLEAR HOST

Use the CLEAR HOST command to clear a specific host entry or all host names from the host table.

Format

CLEAR HOST {index}

Parameters

{index} = 1 through 20
all

Example

The following command clears the first entry in the host name table:

```
8250> clear host 1    [ENTER]
Host 1 name cleared.
```

Description

This command allows you to clear the host table of a specific host entry or all host entries.

CLEAR LOGIN

Use the CLEAR LOGIN command to clear a specific login entry or all login entries from the login table.

Format

CLEAR LOGIN {index}

Parameters

{index} = 1 through 10
all

Example

The following command clears the first entry in the login table:

```
8250> clear login 1    [ENTER]
Login 1 cleared.
```

Description

This command allows you to clear the login table of a specific login entry or all login entries.

CLEAR LOG EVENT_LOG/TRAP_LOG

Use the CLEAR LOG EVENT_LOG/TRAP_LOG command to erase the information in the TRMM event or trap log.

Format

CLEAR LOG EVENT_LOG/TRAP_LOG

Parameter

none

Example

The following command clears the TRMM fatal system error log:

```
8250> clear log event_log   [ENTER]
Event log is cleared.
```

Description

This command clears the TRMM log of fatal system errors (event log) or system messages (trap log).

CLEAR LOG SYSTEM_EVENT

Use the CLEAR LOG SYSTEM_EVENT command to erase the information in the EMM system event log after you have either viewed or printed the information.

Format

CLEAR LOG SYSTEM_EVENT

Parameters

none

Example

```
8250> clear log system_event       [ENTER]
System event log is cleared.
```

Description

This command erases the information in the system event log. Refer to the SHOW LOG SYSTEM_EVENT command to display the contents of the system event log.

CLEAR RMON ALARM

Use the CLEAR RMON ALARM command to clear entries from the RMON alarm control table.

Format

CLEAR RMON ALARM {index}

Parameters

{index} = 1 through 10
all

Example

The following command clears all alarms from the RMON alarm control table:

```
8250> clear rmon alarm all   [ENTER]

Entry 1 cleared.
```

Description

This command clears entries in the RMON alarm table created by either an RMON application or by using the SET RMON ALARM command. Use the SHOW RMON ALARM CONTROL ALL command to display a list of entries.

CLEAR RMON EVENT

Use the CLEAR RMON EVENT command to clear entries from the RMON event control table.

Format

CLEAR RMON EVENT {index}

Parameters

{index} = 1 through 10
all

Example

The following command clears all events from the RMON control table:

```
8250> clear rmon event all    [ENTER]

Entry 1 cleared.
Entry 2 cleared.
Entry 3 cleared.
Entry 4 cleared.
```

Description

This command clears entries in the RMON event table created by either an RMON application or by using the SET RMON EVENT command. Use the SHOW RMON EVENT CONTROL ALL command to display a list of entries.

CLEAR RMON HOST

Use the CLEAR RMON HOST command to stop data collection for, and clear entries from, the RMON host control table.

Format

CLEAR RMON HOST {index}

Parameters

{index} = 1 through 10
all

Example

The following command stops host table data collection and clears the first entry from the RMON host table:

```
8250> clear rmon host 1 [ENTER]
Entry 1 cleared.
```

Description

This command clears entries in the RMON host table created by either an RMON application or by using the SET RMON HOST command. Use the SHOW RMON HOST CONTROL ALL command to display a list of entries.

CLEAR RMON MATRIX

Use the CLEAR RMON MATRIX command to stop data collection for, and clear entries from, the RMON matrix control table.

Format

CLEAR RMON MATRIX {index}

Parameters

{index} = 1 through 10
all

Example

The following command stops matrix table data collection and clears the first entry from the RMON matrix table:

```
8250> clear rmon matrix 1 [ENTER]
Entry 1 cleared.
```

Description

This command clears entries in the RMON matrix table created by either an RMON application or by using the SET RMON MATRIX command. Use the SHOW RMON MATRIX CONTROL ALL command to display a list of entries.

CLEAR RMON RINGSTATION

Use the CLEAR RMON RINGSTATION command to stop data collection for, and clear entries from, the RMON ringstation control table.

Format

CLEAR RMON RINGSTATION {index}

Parameters

{index} = 1 through 10
all

Example

The following command stops ringstation data collection and clears all entries from the RMON ringstation control table:

```
8250> clear rmon ringstation all    [ENTER]
Entry 1 cleared.
```

Description

This command clears entries in the RMON ringstation table created by either an RMON application or by using the SET RMON RINGSTATION command. Use the SHOW RMON RINGSTATION CONTROL ALL command to display a list of entries.

CLEAR RMON STATISTICS

Use the CLEAR RMON STATISTICS command to stop data collection for, and clear entries from, one of the statistics control tables.

Format

CLEAR RMON STATISTICS {statistic} {index}

Parameters

{statistic} = mac_layer
promiscuous
sourcerouting

{index} = 1 through 10
all

Example

The following command stops data collection for, and clears all entries from, the RMON source routing control table:

```
8250> clear rmon statistics sourcerouting all [ENTER]
```

Description

This command clears entries in the RMON statistics table created by either an RMON application or by using the SET RMON STATISTICS command. Use the SHOW RMON STATISTICS CONTROL ALL command to display a list of entries. The parameters are as follows:

Parameter	Description
mac_layer	Specifies the MAC layer control table for this operation.

Parameter	Description
promiscuous	Specifies the promiscuous control table for this operation.
sourcerouting	Specifies the source routing control table for this operation.

CLEAR RMON TOPN_HOSTS

Use the CLEAR RMON TOPN_HOSTS command to stop data collection for, and clear entries from, the RMON TopN Hosts control table.

Format

CLEAR RMON TOPN_HOSTS {index}

Parameters

{index} = 1 through 10
all

Example

The following command stops TopN Hosts table data collection and clears the first entry from the RMON TopN Hosts table:

```
8250> clear rmon topn_hosts 1 [ENTER]
Entry 1 cleared.
```

Description

This command clears entries in the RMON TopN Hosts table created by either an RMON application or by using the SET RMON TOPN_HOSTS command. Use the SHOW RMON TOPN_HOSTS CONTROL ALL command to display a list of entries.

CLEAR SCHEDULE

Use the CLEAR SCHEDULE command to clear one or all script entries from the schedule.

Format

CLEAR SCHEDULE {schedule number}

Parameters

{schedule number} = 1 through 20
all

Example

```
8250> clear schedule all   [ENTER]

Schedule 1 cleared.
Schedule 2 cleared.
Schedule 3 cleared.
Schedule 4 cleared.
Schedule 5 cleared.
Schedule 6 cleared.
Schedule 7 cleared.
Schedule 8 cleared.
Schedule 9 cleared.
Schedule 10 cleared.
Schedule 11 cleared.
Schedule 12 cleared.
Schedule 13 cleared.
Schedule 14 cleared.
Schedule 15 cleared.
Schedule 16 cleared.
Schedule 17 cleared.
Schedule 18 cleared.
Schedule 19 cleared.
Schedule 20 cleared.
```

Description

This command clears one or all script entries from the schedule.

CLEAR SCRIPT

Use the CLEAR SCRIPT command to clear one or all eight scripts.

Format

CLEAR SCRIPT {script number}

Parameters

{script number} = 1 through 8
all

Example

```
8250> clear script 1    [ENTER]
Script 1 cleared.
```

Description

This command allows you to clear a specific script or all eight scripts.

CLEAR SECURITY AUTOLEARN

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

If using an EMM, note that only the Advanced EMM supports security for Ethernet modules other than the 8250 10BASE-T Security Module. All versions of the EMM (Starter, Basic, and Advanced) support the Security Module.

Format

CLEAR SECURITY AUTOLEARN {slot.port} MAC_ADDRESS {MAC address}

Parameters

{slot} = 1 through 17
all

{port} = 1 through 12 or all

{MAC address} = nn-nn-nn-nn-nn-nn

Example

The example shown clears the MAC address 08-00-87-01-a7-b2 from the Autolearning database that is associated with port 3 on the Security Module in slot 7.

```
8250> clear security autolearn 7.3 mac_address
08-00-87-01-a7-b2 [ENTER]

Port 07.03 address 08-00-87-01-a7-b2 cleared from autolearning
area.
```

Description

This command enables you to clear a port's associated MAC address from the Autolearning database.

Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for information on the Security Module features.

CLEAR SECURITY INTRUDER_LIST

Use the CLEAR SECURITY INTRUDER_LIST command to clear the security Intruder list.

If using an EMM, note that only the Advanced EMM supports security for Ethernet modules other than the 8250 10BASE-T Security Module. All versions of the EMM (Starter, Basic, and Advanced) support the Security Module.

Format

CLEAR SECURITY INTRUDER_LIST

Parameters

none

Example

The example shown below clears the Intruder list.

```
8250> clear security intruder_list     [ENTER]
Security Intruder List cleared.
```

Description

This command clears the Intruder list of all security intrusion information. The Intruder list maintains information regarding the 10 most recent security intrusion attempts.

Refer to the SHOW SECURITY INTRUDER_LIST command for a complete description of the Intruder list.

CLEAR SECURITY PORT MAC_ADDRESS

Use the CLEAR SECURITY PORT MAC_ADDRESS command to clear a MAC Address, or MAC Addresses from a specific port, all ports on a specific module, or all ports on all modules in the hub.

When using an EMM, note that only the Advanced EMM supports security for all Ethernet modules including the 8250 10BASE-T Security Module. However, the Starter and Basic EMM only supports security for the Security Module.

Format

CLEAR SECURITY PORT {slot.port} MAC_ADDRESS {mac address}

Parameters

{slot} = 1 through 17
all

{port} = 1 through 12
all

{mac address} = n-n-n-n-n-n
all (default)

Example

The example shown clears the MAC Address 07-34-24-02-0F-00 from all ports on the module in slot 7.

```
8250> clear security port 7.all mac_address
07-34-24-02-0F-00   [ENTER]

Port 07.all security MAC address 07-34-24—02-0F-00 cleared.
```

Description

This command enables you to clear the assigned security MAC addresses from the specified ports. Cleared addresses are no longer considered authorized.

Security Mode is not automatically disabled when you delete a port's MAC address. Thus, a port may not have a MAC address associated with it yet still have security enabled. In this case, any end station attached to that port is deemed “unauthorized.” Always disable Security Mode for a port that does not have an assigned MAC address.

CLEAR TFTP RESULT

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

Format

CLEAR TFTP RESULT

Parameters

none

Example

```
8250> clear tftp result   [ENTER]
Tftp result cleared.
```

Description

This command enables you to clear the TFTP Result field from the SHOW TFTP command display. The TFTP Result field reports a CLEAR status after the field is cleared.

Clear the TFTP Result field before you begin a download so you can check the status of the download once it has been completed.

CLEAR THRESHOLD

Use the CLEAR THRESHOLD command to remove one or all threshold entries from the threshold table.

Format

CLEAR THRESHOLD {index}

Parameters

{index} = 1 through 10
all

Example

```
8250> clear threshold 3    [ENTER]
Threshold 3 cleared.
```

Description

The CLEAR THRESHOLD command enables you to clear one or all threshold entries from the threshold table.

To verify that you are removing the correct entries, issue the SHOW THRESHOLD command prior to clearing threshold entries from the threshold table.

COPY SCRIPT

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

Format

COPY SCRIPT {script number} TO {script number}

Parameters

{script number} = 1 through 8

Example

```
8250> copy script 1 to 2   [ENTER]
Script 1 copied to script 2.
```

Description

The COPY SCRIPT command enables you to copy the contents of one script to another script (including the script name), thus creating a new script or overwriting an existing script.

DOWNLOAD INBAND

Use the DOWNLOAD INBAND command to load new software onto the management module Boot or Flash EPROM, or onto FDDI media modules.

Refer to the appropriate management module manual for complete information on performing a download.

Format

DOWNLOAD INBAND

Parameters

none

Example

```
8250> download inband      [ENTER]
```

Refer to the appropriate management module installation and operation guide for complete instructions and information on downloading software.

Description

This command should be used only when a new Upgrade Distribution Kit (UDK) diskette is issued from IBM Corporation. When a UDK is available, you should update *all* management modules in your network.

Part of the inband download procedure involves configuring TFTP (Trivial File Transfer Protocol) parameters. Refer to the SET TFTP FILE_NAME, SET TFTP FILE_TYPE, and SET TFTP SERVER_IP_ADDRESS commands in this chapter for information on using TFTP.

Warning: When performing downloads in a configuration using the TRMM copper trunks to connect the hub to external stations, the ring is segmented. The ring is segmented for approximately one minute between the stations directly connected to the hub and the stations connected to the hub through the external trunks. Avoid this type of configuration if constant ring integrity is required. Instead, use repeaters for trunk connections.

Note that the management module traffic statistic collection and display features are disabled during a download. These features are restarted automatically after the download completes successfully.

Any network function (for example, Ping, Telnet) that attempts to communicate with a management module will not succeed until the download completes successfully and the management module re-initializes.

Note: An Automatic Update Service (AUS) is available from IBM whereby you are notified directly from IBM when new UDK releases are available.

DOWNLOAD OUT_OF_BAND

Use the DOWNLOAD OUT_OF_BAND command to load new software from a IBM UDK diskette onto a management module, or to FDDI media modules. This command is available only through maintenance mode, indicated by the >> prompt. You must be logged in to the management module before a download can be executed.

Format

DOWNLOAD OUT_OF_BAND {parameter}

Parameters

boot (updates software on the Boot EPROM)
flash (updates software on the Flash EPROM)

Example

```
>> download out_of_band flash        [ENTER]
```

Refer to the appropriate management module installation and operation guide for complete instructions and information on downloading software.

Description

This command is available only through maintenance mode. It should be used only when a new Update Distribution Kit (UDK) diskette is issued from IBM Corporation. When a UDK is available, you should update *all* management modules in your network.

Note that the management module traffic statistic collection and display features are disabled during a download. These features are restarted automatically after the download completes successfully.

Also, any network function (for example, Ping, Telnet) that attempts to communicate with a management module will not succeed until the download completes successfully and the management module re-initializes.

Warning: When performing downloads in a configuration using the TRMM copper trunks to connect the hub to external stations, the ring is segmented. The ring is segmented for approximately one minute between the stations directly connected to the hub and the stations connected to the hub through the external trunks. This type of configuration should be avoided if constant ring integrity is required. Instead, use repeaters for trunk connections.

Note that you will need the IBM Universal Code Download Kit (Feature Code 3150) in order to initiate the download process.

Note: An Automatic Update Service (AUS) is available from IBM whereby you are notified directly from IBM when new UDK releases are available.

LOGOUT

Use the LOGOUT command to logout from either a remote or local management module session.

Format

LOGOUT

Parameters

none

Examples

Example 1

Logging out from a local management module:

```
8250> logout      [ENTER]
Bye
```

To log back in, press Enter and you will be prompted for a password.

```
Password:
```

Example 2

Logging out from a remote connection:

```
82502> logout          [ENTER]
8250>
Remote session completed
```

Description

This command enables you to log out from either a remote or local management module session. You must SAVE or REVERT recent configuration changes before logging out of the device.

If you are logged into the local management module (the management module to which the terminal is connected) issuing the LOGOUT command ends the session.

If you are logged into a remote management module or other device and issue the LOGOUT command, the terminal connection to the remote device is broken and is reconnected to the local management module.

Note: If a modem is connected and the HANGUP command is enabled, issuing the LOGOUT command also disconnects the modem.

MAINTAIN

Use the MAINTAIN command to enter maintenance mode. Maintenance mode allows you to download new software to the management module through the DOWNLOAD OUT_OF_BAND command.

Format

MAINTAIN

Parameters

none

Example

```
8250> maintain        [ENTER]
```

To enter maintenance mode, enter the administrator password at the prompt as shown below.

```
Enter administrator password:
```

Enter the administrator password (which does not display on the screen) and the following information and prompt is displayed:

```
8250>

8250 Management Module (vx.xx)
Copyright 199x IBM Corporation
>>
```

Description

Once you have accessed maintenance mode you can execute the DOWNLOAD and BOOT commands, discussed earlier in this chapter.

Note: You cannot enter this command if you are connected to a remote management module through the TELNET command.

Management modules do not track network statistics when in maintenance mode. Also, any network function (for example, Ping, Telnet) that attempts to communicate with a management module will not succeed until you enter the BOOT command to re-initialize the management module.

MONITOR

Use the MONITOR command to view ongoing error statistics. The statistics are reported periodically at the time interval that you specify. Note that some of the group options are only available with the Advanced TRMM.

Format

MONITOR {interval} {group} {value} {option}

Parameters

{interval} = 0:05 through 30:00 (default of 5:00 if you press ENTER)

{group} = device (default if you press ENTER)
- module
- network traffic distribution
  - errors
- port {slot.port} error
- station {mac address} errors

TRMM Advanced Only

{group} = network traffic distribution
- port {slot.port} traffic
  - errors
- station {mac address}
  - {all}
- station {mac address} traffic
- top_errors {option}
- top_receivers {option}
- top_senders {option}

{value} = all
- number of stations (maximum 18)

{option} = by_frames
- by_mac_address
- by_octets

Examples

Example 1

This example displays Token Ring network statistics every two minutes for port 1 on the Token Ring module in slot 14.

```
8250> monitor 2:00 port 14.1    [ENTER]

Slot 14, Port 1    MAC Address 10-00-f1-0f-0c-6f

ERROR COUNTERS:
        Line Errors:                          0
        Burst Errors:                         0
        Address/Frame Errors:                 0
        Lost Frame Errors:                    0
        Receive Congestion Errors:            0
        Frame Copy Errors:                    0
        Token Errors:                         0


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

Example 2

This example displays Ethernet network statistics every two minutes.

```
8250> monitor 2:00 network         [ENTER]


Delta of counters for ETHERNET_1 on 06 Mar 94:

Network   Frames   Bcast     CRC Err  AlignErr  Collisions
Time      Octets   Mcast  TooLongErr          Remote/Local
     Utilization          Error Rate        Collision Rate
_____________________________________________________________

ETHERNET_1  11689    326           0       0             0
14:01:48  1599714   2363           0                     0
              2%                  0%                    0%
_____________________________________________________________
```

Example 3

This example displays FDDI network statistics every 5 seconds.

```
8250> monitor 0:05 network          [ENTER]


Network: FDDI_1              Time: 09:36:57
Ring State: ring_op          Utilization: 0 %

_____________________________________________________________

Frames                      Errors               Tokens
      55                         0                   523734857
       0/sec                       0/sec
1138752/sec
                                 0%
Ringops:          1                Frame Error Ratio:        0
Beacons:          0                Lost:                     0
                                   Late:                     0

_____________________________________________________________

This Station

Frames Copied: 2911                Transmitted:           5824
Path Tests:       0                TvxExpires:               0
_____________________________________________________________
```

Description

This command displays statistics for the group specified in the command line. The display is updated periodically based on the number of minutes and seconds you assign. Press any key to discontinue this process and return to the management prompt.

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

Note: When using the MONITOR command to display statistics for Token Ring networks, extra entries with erroneous station addresses may display. These entries are caused by ring error conditions (for example, line errors, burst errors), which are a result of normal ring events (for example, stations inserting onto the ring).

When using command completion to specify the ALL option in the MONITOR command line, you must type at least 'al' or specify 'all' in order for the TRMM to recognize the ALL option. Otherwise, the TRMM assumes the 'a' indicates the beginning of a MAC address.

PING

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

Format

PING {ip address or name} {number of Ping requests}

Parameters

{ip_address} = Internet Protocol Address in the format n.n.n.n

{name} = name of the IBM remote device
(EMM and FMM option only)

{number} = number of packets to be returned
(1 through 255, default is 1 packet)

Examples

Use the following command to verify whether a TRMM with the ip_address 133.8.9.60 is active by having it send you 2 return packets:

```
8250> ping ip_address 133.8.9.60 2  [ENTER]

Starting ping, resolution of displayed time is 10 milli-sec
64 bytes from 151.104.25.141: icmp_seq=0. time=20. ms

Number transmitted=1 Number received=1 Percent loss=0
Total time=20 Minimum time=20 Maximum time=20 Average time=20.
```

Description

This command sends <n> number of ICMP (Internet Control Message Protocol) packets to the specified device, and requests that the device send back the exact number of packets (where **n** is the number you specify in the *number* option).

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

REMOTE_LOGIN

Use the REMOTE_LOGIN command to log into an EMM or other manageable IBM device on the network and manage it from a remote terminal.

Format

REMOTE_LOGIN {device identifier}

Parameters

{device identifier} = ip_address - Internet Protocol address
mac_address - 6-byte Ethernet address
name -name of the IBM remote device

Examples

Example 1

Log into the EMM with the mac_address 08-00-8F-00-00-10.

```
8250> remote_login mac_address 08-00-8F-00-00-10    [ENTER]
Password:
```

Example 2

Log into the EMM with the ip_address 127.33.7.6 :

```
8250> remote_login ip_address 127.33.7.6 [ENTER]
Password:
```

Example 3

Log into the EMM with the name TP007:

```
8250> remote_login name TP007       [ENTER]
Password:
```

Description

Use the REMOTE_LOGIN command and the address or name of the remote EMM (or other manageable IBM device) to which you want to connect. You must be connected to a local EMM before you can issue this command.

Once you are logged into a remote device, you must enter the correct password for that device. From that point on all the commands you issue are for that device. Therefore, if you remotely log into a Midnight Bridge unit, you must use the bridge commands to modify or view statistics for the bridge.

During the time the connection is active to the remote device, the message "This device is now being remotely managed by {Ethernet Address}" displays on a terminal connected to the remote device.

Remote connections are lost when executing commands that interrupt EMM operations (for example, RESET DEVICE or DOWNLOAD).

Use the LOGOUT command to remove the connection from the remote device and return to the local EMM.

Note: You can log in remotely (using Telnet or Remote_Login) to only one management module at a time. That is, in order to establish a remote connection to second device, you must first log out of the initial device.

If you are having trouble logging into a remote device, make sure the device is on the same network (segment) or that it is bridged to that segment. The REMOTE_ LOGIN IP ADDRESS command works if the IP address is on the same IP network as the EMM.

RESET CONCENTRATOR

Use the RESET CONCENTRATOR command to reboot the hardware and software (cold boot) of the 8250 Multiprotocol Intelligent Hub. This command resets the hub and all the modules.

Format

RESET CONCENTRATOR

Parameters

none

Example

```
8250> reset concentrator       [ENTER]

8250>

8250 Management Module (vx.xx)
Copyright (c) 199x IBM Corporation.
```

Description

The RESET CONCENTRATOR command performs a hardware reset of the hub and all the modules. Diagnostic routines execute (if enabled) and traffic forwarding is interrupted briefly. Once the reset is complete, you must log back in to the management module to issue any other commands.

Note that you must save or revert unsaved changes before this command executes.

RESET DEVICE

Use the RESET DEVICE command to reset the management module to which you are connected.

Format

RESET DEVICE

Parameters

none

Example

```
8250> reset device      [ENTER]

8250 Management Module (vx.xx)
Copyright (c) 199x IBM Corporation.
```

Press [ENTER] to get the password prompt and then enter the password to continue.

```
Password:
```

Description

This command is used to reset the management module to which you are connected. You must save or revert unsaved changes before this command will execute.

Warning: When performing resets to a management module in a configuration using the TRMM copper trunks to connect the hub to external stations, the ring becomes segmented. The ring is segmented for approximately one minute between the stations directly connected to the hub and the stations connected to the hub through the external trunks. This type of configuration should be avoided if constant ring integrity is required. Instead, use repeaters for trunk connections.

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.

Format

RESET MASTERSHIP

Parameters

none

Example

```
8250> reset mastership [ENTER]
Resigning
```

Description

This command causes a master management module election for that hub. The management module with the highest mastership priority setting becomes master. You set the management module mastership priority value using the SET MODULE MASTERSHIP_PRIORITY command.

You can issue this command from either a slave or master management module. If you are connected to the master management module, the message “Resigning” displays when you issue this command. When connected to a slave management module, the message “Requesting Master resign” displays when you issue this command.

Note: IBM recommends that the module you designate to be master of the hub be set to priority level 10.

Mastership election completion time is dependent on a management module's mastership priority setting. A management module with a mastership priority value of 10 takes less than 10 seconds to complete a mastership election. A management module with a mastership of one, however, takes about 90 seconds to complete a mastership election.

IBM recommends setting a master management module to 10 and slave management modules to mastership priority values of 7, 8, or 9 to facilitate the election process.

RESET MODULE

Use the RESET MODULE command to perform a hardware reset of a module. Use this command only if a module is not functioning properly.

Format

RESET MODULE {slot}

Parameters

{slot} = 1 through 17

Example

```
8250> reset module 6       [ENTER]
Resetting module 6.
```

Description

The RESET MODULE command allows you to reset a specific module in the hub. A 17-slot hub contains 17 slots, numbered sequentially from left (# 1) to right (# 17). A 6-slot hub contains 6 slots, numbered sequentially from top (# 1) to bottom (# 6). The module specified in the RESET command line is reset to its last configuration.

Note: You cannot reset the management module to which you are logged into, or the Controller Module, using this command. To reset the management module, use the RESET DEVICE command. To reset the Controller Module, use the RESET CONCENTRATOR command. This command resets all modules including the Controller module.

RESET POWER_SUPPLY

Use the RESET POWER_SUPPLY command to switch over from a backup power supply back to the primary supply in an 8250 Multiprotocol Intelligent Hub.

Format

RESET POWER_SUPPLY

Parameters

none

Example

```
8250> reset power_supply         [ENTER]
Resetting power supply...
8250>
8250 Management Module (vx.xx-x)
Copyright (c) 199x IBM Corporation.
```

Press [ENTER] to make the password prompt display.

```
Password:
```

Enter your password to continue.

Description

The RESET POWER_SUPPLY command is used when the hub is working off the backup power supply and you have replaced a faulty primary power supply. This command causes the hub to switch to the primary power supply.

If the primary power supply is absent, or if the hub is already powered from the primary power supply, the switchover to the primary power supply will not take place.

You must save or revert unsaved changes before this command executes.

Warning: A power supply switchover performs a warm boot which causes the hub and all modules (except for the Controller Module) to reset. Once the reset is complete, you must log back into the management module to issue further commands.

REVERT

Use the REVERT command to return to the configuration settings that were in effect as of the last save.

Format

REVERT {group}

Parameters

{group} = alert
all
bootp
community
concentrator
device
group
host
login
module_port
schedule
scripts
security
terminal
tftp
threshold

Examples

Example 1

```
8250> revert device            [ENTER]
Reverting device configuration
```

Example 2

```
8250> revert all             [ENTER]
Reverting alert configuration
Reverting community configuration
Reverting concentrator configuration
Reverting device configuration
Reverting group configuration
Reverting host configuration
Reverting login configuration
Reverting module and port configuration
Reverting schedule configuration
Reverting script configuration
Reverting security configuration
Reverting terminal configuration
Reverting tftp configuration
Reverting threshold configuration
```

Description

The REVERT command allows you to return to the last configuration value settings saved. For example, if you specify REVERT ALERT, any SET ALERT changes you made (after the last SAVE) are abandoned. In addition, REVERT ALERT only affects the ALERT option (all other groups are unchanged).

As a result of issuing the REVERT ALL command, previous configuration values saved are restored.

RUN SCRIPT

Use the RUN SCRIPT command to execute a specific script file.

Format

RUN SCRIPT {script number}

Parameters

{script number} = 1 through 8

Description

This command executes a specific script file. Use the SHOW SCRIPT command to display a script configuration.

SAVE

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

Format

SAVE {group}

Parameters

{group} = alert
all
bootp
community
concentrator
device
group
host
login
module_port
schedule
scripts
security
terminal
tftp
threshold

Examples

Example 1

Use the SAVE ALL command to save *all* of the latest hub configuration values established for an EMM by the SET command.

```
8250> save all           [ENTER]

Saving alert configuration
Saving bootp configuration
Saving community configuration
Saving concentrator configuration
Saving device configuration
Saving group configuration
Saving host configuration
Saving login configuration
Saving module and port configuration
Saving schedule configuration
Saving script configuration
Saving security configuration
Saving terminal configuration
Saving tftp configuration
Saving threshold configuration
```

Example 2

Use the SAVE MODULE_PORT command to save the latest configuration values set for modules and ports in the hub.

```
8250> save module_port          [ENTER]

Saving module and port configuration
```

Example 3

Use the SAVE COMMUNITY command to save any changes made to the community table established by the SET COMMUNITY command.

```
8250> save community           [ENTER]

Saving community configuration
```

Description

Parameter values established by the SET command are effective immediately but are not permanently saved. Use the SAVE command to permanently save these values. Only saved values are in effect after resetting the hub.

Issuing the SAVE ALL command saves all of the latest hub configuration values established by the SET command for alert, community, hub, device, group, module_port, security, terminal, tftp, and threshold parameters.

The SAVE ALERT, SAVE COMMUNITY, SAVE CONCENTRATOR, SAVE DEVICE, SAVE GROUP, SAVE MODULE_PORT, SAVE SECURITY, SAVE TERMINAL, SAVE TFTP, and SAVE THRESHOLD commands allow you to save the values set for the specific category without affecting the other category settings.

Note: Issuing the SAVE ALL or SAVE MODULE_PORT command on a master TRMM automatically saves all module and port configuration information to any slave TRMMs in the hub.

SET

The SET command enables you to change configuration values.

Format

SET {parameter}

Parameters

{parameter} = alert
bootp
clock
community
concentrator
counter
device
group
host
login
module
port
rmon
schedule
script
security
terminal
tftp
threshold
trunk

Description

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.

SET ALERT

Use the SET ALERT command to enable or disable the notification of an alert statement from the management module to the designated trap receiver (for example, SNMP workstation) for certain network occurrences. Use this command to enable or disable alert displays on the terminal screen.

Format

SET ALERT {alert type} {setting}

Parameters

{alert type} = authentication
change
console_display
hello
port_filter (FMM only)
port_up_down
screen
script

{setting} = disable
enable
filter (port_up_down option only)

Examples

Example 1

The following example prevents alerts from being sent when a script executes.

```
8250> set alert script disable      [ENTER]
Alert SCRIPT set to DISABLE.
```

Example 2

The following example enables the notification of an alert for any configuration or variable change made to the hub.

```
8250> set alert change enable      [ENTER]
Alert CHANGE set to ENABLE
```

Example 3

The following example disables the display of trap messages to the connected terminal for an EMM (for FMM or TRMM, use the console_display option).

```
8250> set alert screen disable    [ENTER]
Alert screen set to disable.
```

Description

You can configure the management module to send an alert to the trap receiver (for example, SNMP-based management workstation) when any of the following four system events occur:

authentication - A user tries to access the management module and their IP Address or community name is not valid for the attempted read or write operation.

change - A configuration change is made to this hub.

hello - An existing management module is reset or a new management module is installed in the hub. The alert is sent once every minute until a valid SNMP PDU (Protocol Data Unit) is received or for up to 4 hours and 15 minutes, at which time it shuts off automatically.

script - A trap is only sent to the console when a script executes.

The default setting is disabled for all four of these options.

You may also enable or disable the display of trap messages to the local screen by using the **screen** option as shown in Example 3. The default setting for alert screen is enabled. Note, however, that Slot Up and Slot Down traps *are* transmitted even if the set alert screen feature is disabled.

When *enabled*, the **port_up_down** alert type enables the management module to generate port up and port down traps for all ports.

When *disabled*, the **port_up_down** alert type prevents the management module from generating port up and port down traps for all ports.

When *filtered*, the **port_up_down** alert type enables the management module to generate port up and port down traps as defined in each port's alert setting. This setting is specified by the SET PORT ALERT command.

When *enabled*, the **port_filter** alert type enables the FMM to generate port up and port down traps when the port alert filter setting is also enabled. (The port alert filter setting is specified by the SET PORT ALERT_FILTER command.)

When *disabled*, the **port_filter** alert type has no effect on the FMM and port up and port down traps are always sent.

Note: Your SNMP-based workstation must be designated as the trap receiver through the community table (SET COMMUNITY command) for the traps to be sent to the appropriate location.

SET BOOTP POWER_UP_MODE

Use the SET BOOTP POWER_UP_MODE command to enable the TRMM to initiate a BootP request upon startup of the TRMM.

Format

SET BOOTP POWER_UP_MODE {mode}

Parameters

{mode} = disable (default after initial startup of TRMM)
enable (default when TRMM is first installed)

Example

The following command example enables a bootp request upon startup of the TRMM.

```
8250> set bootp power_up_mode enable [ENTER]
BootP power_up_mode set to ENABLED.
```

Description

This command allows you to define whether the TRMM initiates a BootP request upon startup or does not initiate a BootP request.

SET BOOTP SERVER_IP_ADDRESS

Use the SET BOOTP SERVER_IP_ADDRESS command to define the BootP server IP address to which the TRMM should send the BootP request.

Format

SET BOOTP SERVER_IP_ADDRESS {ip address}

Parameters

{ip address} = n.n.n.n

Example

The following command specifies the TRMM use the IP address 127.3.6.58 to send its BootP request.

```
8250> set bootp server_ip_address 127.3.6.58 [ENTER]
BootP IP address set to 127.3.6.58.
```

Description

This command enables you to define the BootP server IP address to which the TRMM should send its BootP request. If you do not specify an IP address, the TRMM sends out the request to the broadcast address.

SET CLOCK

Use the SET CLOCK command to set the real time clock to establish a starting time, date, and day.

Format

SET CLOCK {time} {date} {day}

Parameters

{time} = hh:mm
{date} = yy/mm/dd
{day} = day of week

Example

The following example sets the internal clock to *05:53 AM,* for *Sunday*, *March 6th, 1994*.

```
8250> set clock 05:53 94/03/06 sunday [ENTER]
Clock set to 05:53 Sun 06 March 94
```

Description

You generally set the internal clock only once, at the time you install the management module into your hub. The clock has its own battery and keeps time even if power fails. You must reset the clock during a leap year or during daylight savings time.

The acceptable values for hours are 0 to 23 and the values for minutes are 0 to 59. Note that the clock information is saved automatically once it is set.

SET COMMUNITY

Use the SET COMMUNITY command to create entries in the community table for management stations that will receive traps from, or be able to change values for, a specified management module.

Format

SET COMMUNITY {community} {IP Address} {access}

Parameters

{community} = community name or all

{IP Address} = Internet Protocol Address (in the format n.n.n.n) or all

{access} = all, oldall, oldtrap, read_oldtrap, read_only, read_trap, read_write, trap

Examples

Example 1

The following example creates the community table entry called **admin** and specifies that this workstation has read_write access to the specified management module, and that it will receive all traps from the management module.

```
8250> set community admin 2.13.34.24 all      [ENTER]
Community set.
```

Example 2

The following example gives the workstation with IP address 12.36.58.17 the name **super**, and enables the person who uses the workstation read and write access to the specified management module.

```
8250> set community super 12.36.58.17 read_write [ENTER]
Community set.
```

Example 3

The following example creates the community table entry called **public** and specifies that workstations have read only access to the management module.

```
8250> set community public all read_only    [ENTER]
Community set.
```

Description

This command enables you to create a new entry in the community table. Each community is granted the access you specify in the {access} option to the agent (management module) information. The access attributes are:

trap access access - The IP Address you specify receives alerts from the management module based on the IBM MIB-II.

read_write access - The IP Address you specify can display and modify information about the management module.

read_trap access - The IP Address you specify can display information about the management module and receive alerts based on the IBM MIB-II.

read_only access - The IP Address you specify can display information about the management module.

all access -The IP Address you specify has read_write and trap access to the management module.

oldtrap access - The IP Address you specify will receive alerts from the EMM based on the IBM MIB I.

read_oldtrap access - The IP Address you specify can display information about the EMM and it will receive alerts based on the IBM MIB I.

oldall access - The IP Address you specify has read_write and trap access to the EMM based on the IBM MIB I.

Note: When you use the IP Address entry of **all**, you cannot use **trap**, **read_trap**, or **all** access.

The three “old” trap attributes should be used when sending traps to workstations using the IBM MIB I variables.

All the non-"old" trap attributes should be used when sending traps to workstations using the IBM MIB II variables.

You can enter up to 10 community table entries with names of up to 15 characters in length. Note that the community name is case-sensitive so that *HUB* and *hub* are different community names.

Refer to the SHOW COMMUNITY command to view entries in the existing community table and the CLEAR COMMUNITY command to delete a community table entry.

SET CONCENTRATOR PLATFORM

Use the SET CONCENTRATOR PLATFORM command to educate the management module as to the hub platform in which it is installed.

Format

SET CONCENTRATOR PLATFORM {hub type}

Parameters

{hub type} = 8250-006
8250-006_FT
8250-017 (default)

Example

```
8250> set concentrator platform 8250-006 [ENTER]
Platform set to 6-Slot.
```

Description

This command allows you to specify the platform, 6-Slot or 17-Slot 8250 Multiprotocol Intelligent Hub, in which your management module is installed.

Note that there is not a separate option for a 6-Slot Hub containing an Hidden Controller Module. The Hidden Controller informs the management module that it is installed in a 6-Slot Hub.

To make the platform selection permanent, issue the SAVE CONCENTRATOR command. Use the SHOW CONCENTRATOR command to display the platform information.

SET COUNTER PORT_STATISTICS

The SET COUNTER PORT_STATISTICS command improves network statistics reporting by allowing you to control whether or not the TRMM collects port statistics.

Format

SET COUNTER PORT_STATISTICS {mode}

Parameters

{mode} = disable (default)
enable

Example

The following command enables port statistics on the TRMM:

```
8250> set counter port_statistics enable [ENTER]
Port statistics enabled.
```

Description

If you disable the Counter Port Statistics feature, the TRMM does not collect port statistics (the default). If you enable the Counter Port Statistics feature, the TRMM collects port statistics.

Note: Collecting port statistics affects network statistics reporting.

To save the SET COUNTER PORT_STATISTICS setting permanently, enter the SAVE ALL or SAVE MODULE_PORT command. The SHOW COUNTER PORT_STATISTICS command allows you to display the current setting for the SET COUNTER PORT_STATISTICS command. There is no SNMP support for the Counter Port Statistics feature.

SET DEVICE BEACON_RECOVERY

Use the SET DEVICE BEACON_RECOVERY command to enable or disable beacon recovery.

Format

SET DEVICE BEACON_RECOVERY {mode}

Parameters

{mode} = disable
enable (default)

Example

The following command disables beacon recovery.

```
8250> set device beacon_recovery disable    [ENTER]
Beacon recovery disabled.
```

Description

The Beacon Recovery feature must be enabled to allow the TRMM to perform beacon recovery. This feature should only be disabled as a troubleshooting tool to prevent rings from "healing themselves" before the problem or faulty device can be isolated.

Note: If Beacon Recovery is disabled, the BCN LED does *not* light when the ring is beaconing.

SET DEVICE BEACON_TIMEOUT

The SET DEVICE BEACON_TIMEOUT command enables you to define a time limit that the TRMM uses to keep a port disabled during beaconing.

Format

SET DEVICE BEACON_TIMEOUT {time}

Parameters

{time} = 1 to 100 seconds

Example

The following command sets the beacon timeout to 20 seconds.

```
8250> set device beacon_timeout 20    [ENTER]
Beacon timeout set to 20 seconds.
```

Description

Because the Beacon Timeout value is not stored in the permanent storage of the TRMM, you must reconfigure the value if the TRMM is reset. The time limit is based upon the timeout value. The default value is 10 seconds.

To display the current Beacon Timeout value, use the SHOW DEVICE command. There is no SNMP support for the Beacon Timeout feature.

SET DEVICE BEACON_TRUNK_RETRY

The SET DEVICE BEACON_TRUNK_RETRY command allows you to configure the number of times the TRMM re-enables trunks disabled due to beaconing conditions.

Format

SET DEVICE BEACON_TRUNK_RETRY {value}

Parameters

{value} = 0 to 255

Example

The following command sets the number of beacon revovery retries to 10:.

```
8250> set device beacon_trunk_retry 10    [ENTER]
Beacon trunk retry set to 10.
```

Description

By default, the beacon recovery algorithm causes the TRMM to re-enable trunks that have been disabled during the beacon recovery process. After the TRMM has tried twice to re-enable trunks, one of the following conditions exists:

- Beaconing is resolved and trunks remain enabled.
- Beaconing is still present on the ring and trunks remain disabled.

If a trunk remains disabled after beacon recovery completes, the TRMM checks the Beacon Trunk Retry value. If the value is greater than 0, the TRMM re-enables the trunk. If the beaconing condition is resolved, the trunk remains enabled and the TRMM does not perform any other beacon recovery actions.

If beaconing recurs as a result of the TRMM re-enabling the trunk, the TRMM re-enters the beacon recovery algorithm and decrements the Beacon Trunk Retry value by 1.

To save the Beacon Trunk Retry value, use the SAVE ALL or SAVE DEVICE command. The Beacon Trunk Retry setting is reported in the SHOW DEVICE command display. There is no SNMP support for this feature.

SET DEVICE CONTACT

Use the SET DEVICE CONTACT command to enter contact information, such as a service contact's name, location, company, and telephone number.

Format

SET DEVICE CONTACT

Parameters

none

Example

```
8250> set device contact         [ENTER]
Enter one line of text:
>
```

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

```
>Network Admin, IBM Engineering Support
Contact changed.
```

Description

You can enter one line of free formatted text of up to 78 alpha-numeric characters.

To make the change permanent, issue the SAVE DEVICE command. Use the SHOW DEVICE command to display the current contact information.

SET DEVICE DEFAULT_GATEWAY

Use the SET DEVICE DEFAULT_GATEWAY command to set the IP Address of the gateway that should be used when the management module does not recognize the receiver address on the local network.

This command also enables you to specify a secondary default gateway for TRMM only.

Format

SET DEVICE DEFAULT_GATEWAY {ip address} {network} {gateway}

Parameters

{ip address} = Internet Protocol Address (in the format n.n.n.n)

{network} = Token Ring	Ethernet
all	all
isolated	isolated
token_ring_1	network_1
token_ring_2	network_2
token_ring_3	network_3
token_ring_4	
token_ring_5	
token_ring_6	
token_ring_7	

TRMM only
{gateway} = primary
secondary

Example

This command sets the gateway with the IP address 131.05.08.58 to be the primary default gateway for Token Ring 3.

```
8250> set device default_gateway 131.05.08.58 token_ring_3
primary

Device primary default gateway changed.
```

Description

The 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. The default gateway is useful when sending management module alert packets to a management workstation that is on a different network.

For TRMM and EMM, the network option enables you to set a unique gateway for each of the possible networks on the hub backplane.

The isolated option enables you to isolate the management module from the backplane, but still communicate through the TRMM Ring In/Ring Out ports.

If the primary default gateway malfunctions, the TRMM uses the IP address of the secondary gateway as defined.

Note: You must reset the management module for the new default gateway to take effect.

SET DEVICE DIAGNOSTICS

Use the SET DEVICE DIAGNOSTICS command to enable or disable diagnostics during startup (or reboot) of the management module.

Format

SET DEVICE DIAGNOSTICS {setting}

Parameters

{setting} = disable
enable

Examples

Example 1

```
8250> set device diagnostics enable     [ENTER]
DIAGNOSTICS option enabled.
```

This command causes diagnostics to run during reset of the management module.

Example 2

```
8250> set device diagnostics disable    [ENTER]
DIAGNOSTICS option disabled.
```

This command disables diagnostics during system reset of the management module.

Description

This command allows you to enable or disable diagnostics from running during system reboot. Disabling diagnostics saves time during reboot of the management module, but does not confirm the operation of the module.

The factory setting for this command is ENABLE.

When a TRMM with diagnostics enabled and an EMM reside in the same hub and the hub is reset or a power cycle occurs, the TRMM may not

become master, even if it has a higher mastership priority setting. To avoid this situation, issue the SET DEVICE DIAGNOSTICS DISABLED command. If you do not issue this command, the administrator must instead issue the RESET MASTERSHIP command after the diagnostics are completed in order to have the TRMM assume mastership.

SET DEVICE DIP_CONFIGURATION

Use the SET DEVICE DIP_CONFIGURATION command to select whether you want media modules in the hub to boot up under the software settings you configured using the SET command, or boot up under the dip switch values as they are set on the modules.

Format

SET DEVICE DIP_CONFIGURATION {setting}

Parameters

{setting} = disable
enable

Example

Issue the following command to have media modules operate from the management module configuration settings rather than the module dip switch settings:

```
8250> set device dip_configuration disable      [ENTER]
DIP CONFIGURATION option disabled.
```

Description

This command allows you to select whether you want media modules in the hub to:

- Boot up under the software settings you configured using the SET command
- Boot up under the dip switch values as they are set on the modules.

The factory setting is DISABLE. This allows the modules to boot up using the software values you specify.

SET DEVICE IP_ADDRESS

Use the SET DEVICE IP_ADDRESS command to set the Internet Protocol address for the management module.

Format

SET DEVICE IP_ADDRESS {ip address} {network}

Parameters

{ip address} = Internet Protocol address (in the format n.n.n.n)

{network} = Token Ring
- all
- isolated
- token_ring_1
- token_ring_2
- token_ring_3
- token_ring_4
- token_ring_5
- token_ring_6
- token_ring_7

Ethernet
- all
- network_1
- network_2
- network_3

Examples

Example 1

This command assigns the same IP address to all Token Ring networks in a hub.

```
8250> set device ip_address 151.05.31.60 all [ENTER]
Device ip_address changed.
```

Example 2

This command sets Ethernet network 1 to IP Address 122.36.58.117.

```
8250> set device ip_address 122.36.58.117 ethernet_1 [ENTER]
Device ip_address changed.
```

Description

IBM factory-sets the management module with the IP address 127.0.0.1. This command allows you to establish the correct IP address for your management module.

Management modules use Internet Protocol addresses as defined by the Internet family. Ensure these numbers are unique to your network.

Enter the internet address as n.n.n.n. (four decimal numbers). Each number can be assigned a value from 0 to 255, which represent a class A, B, or C Internet Protocol address.

The TRMM isolated option enables you to isolate the management module from the backplane, but still communicate through the Ring In/Ring Out ports.

Note: You must reset an FMM or EMM in order for the new IP address to take effect. Once you change the IP Address, connection to the old IP Address is lost. Therefore, it is recommended that you immediately reset the management module when you change the IP Address.

Use the SAVE DEVICE command to make the change permanent. Use the SHOW DEVICE command to display the current IP address.

SET DEVICE LOCATION

Use the SET DEVICE LOCATION command to describe the physical location of the 8250 Multiprotocol Intelligent Hub.

Format

SET DEVICE LOCATION

Parameters

none

Example

```
8250> set device location         [ENTER]
Enter one line of text:
>
```

Type in the physical location of your hub.

```
>Building J3, Floor 3, Wiring Closet   [ENTER]
Location changed.
```

Description

You can enter one line of free format text of up to 78 alphanumeric characters to specify the location of your 8250 hub.

Use the SAVE DEVICE command to make the location change permanent. Use the SHOW DEVICE command to display the location information.

SET DEVICE MONITOR_CONTENTION

Use the SET DEVICE MONITOR_CONTENTION command to enable or disable the TRMM from active monitor contention.

Format

SET DEVICE MONITOR_CONTENTION {setting}

Parameters

{setting} = disable
enable (default)

Example

```
8250> set device monitor_contention   [ENTER]
Device monitor_contention disabled.
```

Description

This command only has an effect if issued before the TRMM opens onto a ring. When the TRMM is already on the ring, setting this command has no effect, even if the active monitor changes.

The TRMM will participate in active monitor contention when this command is enabled. If disabled, the TRMM will not participate in active monitor contention.

Note that the TRMM may still become the active monitor even if this parameter is disabled. This may occur if the TRMM is the first station to detect the need for monitor contention and it has the highest MAC address on the ring *or* no other adapters are configured for active monitor contention.

Likewise, the TRMM may not become the active monitor even if this parameter is enabled. This may occur if another adapter with a higher MAC address attempts to become active monitor first.

If the TRMM is the active monitor, this status will be reported to the right of the TRMM entry in the SHOW NETWORK_MAP TOKEN_RING LOGICAL display.

The monitor contention setting for the TRMM is reported in the SHOW DEVICE display.

Issue the SAVE DEVICE command to make a setting change permanent.

SET DEVICE NAME

Use the SET DEVICE NAME command to assign the management module a name so that, in addition to an IP address, the management module can be addressed uniquely.

Format

SET DEVICE NAME {device name}

Parameters

{device name} = name up to 31 characters

Example

```
8250> set device name 8250        [ENTER]
Device name changed.
```

Description

You may use any format to enter a device name up to 31 alphanumeric characters. To make identification of the management module easier, assign the device name and the terminal prompt for the management module to the same name.

It is also recommended that you assign a unique name to *each* management module.

To make the name change permanent, issue the SAVE DEVICE command. Use the SHOW DEVICE command to display the name information.

SET DEVICE PASSWORD

Use the SET DEVICE PASSWORD command to establish a system administrator and user password for the EMM.

Format

SET DEVICE PASSWORD {group}

Parameters

{group} = administrator
user

Examples

Example 1

```
8250> set device password administrator [ENTER]
```

You are prompted as follows:

```
Enter current administrator password:{enter password} [ENTER]
New password:                    {enter new password} [ENTER]
Verify:                          {enter new password} [ENTER]

Administrator password changed.
```

Example 2

```
8250> set device password user        [ENTER]
```

You are prompted as follows:

```
Enter current administrator password: {enter password}[ENTER]
```

Enter the current administrator password because only the system administrator is authorized to establish the user password.

```
New password:               {enter new user password} [ENTER]
Verify:                     {enter new user password} [ENTER]

User password changed.
```

Description

The EMM provides password protection to control access to commands and information. Passwords may contain up to 15 alphanumeric characters. For security reasons, they are not shown when being entered.

The administrator password gives the system administrator read and write access to all management module commands. The user password provides access to read only commands that allow the user to view status, get help, clear counters, and log out.

Note that the new passwords are effective immediately. You will not be prompted for a password until you log out and then try to log in again. You must issue the SAVE DEVICE command to save the new passwords permanently.

SET DEVICE RESET_MASTERSHIP

Use the SET DEVICE RESET_MASTERSHIP command to force all management modules in the hub into an election process upon powerup of an FMM in that hub.

Format

SET DEVICE RESET_MASTERSHIP {setting}

Parameters

{setting} = disable
enable

Example

The following command example forces all management modules in the hub into an election process upon powerup of an FMM in that hub.

```
8250> set device reset_mastership enable      [ENTER]
Reset mastership option enabled.
```

Description

When SET DEVICE RESET_MASTERSHIP is enabled, the FMM initiates a mastership election upon initial startup and subsequent resets. Initially, the default for this command is “disable.”

This command does not guarantee that the FMM will be elected master. Use the SET MODULE MASTERSHIP PRIORITY command, as described later in this chapter, to set the appropriate priority levels.

SET DEVICE SUBNET_MASK

Use the SET DEVICE SUBNET_MASK command to specify the subnetwork mask for your class of Internet device.

Format

SET DEVICE SUBNET_MASK {mask} {network}

Parameters

{mask} = hexadecimal byte

{network} =	Token Ring	Ethernet
	all	all
	isolated	network_1
	token_ring_1	network_2
	token_ring_2	network_3
	token_ring_3	
	token_ring_4	
	token_ring_5	
	token_ring_6	
	token_ring_7	

Example

To set the subnetwork mask for a class C device for all seven Token Ring networks, enter the following command:

```
8250> set device subnet_mask FF.FF.FF.00 all  [ENTER]
Device subnet mask changed.
```

Description

This command enables you to specify the subnetwork mask for your type of Internet class. In general, the subnetwork mask is the group of common characters on the left of the IP Address (Network ID). The host address is the group of unique characters on the right (Host ID).

On the TRMM, the isolated option enables you to isolate the management module from the backplane, but still communicate through the Ring In/Ring Out ports.

Note: You must reset the management module for the new subnet mask to take effect.

SET DEVICE TRAP_RECEIVE

Use the SET DEVICE TRAP_RECEIVE command to designate the management module as a trap receiver for other SNMP devices on the network.

Format

SET DEVICE TRAP_RECEIVE {setting}

Parameters

{setting} = disable
enable

Example

```
8250> set device trap_receive enable   [ENTER]
Device trap receive enabled.
```

Description

By enabling traps to be sent to your management module, you can track changes and errors from all hubs.

In order for the management module to receive traps, you must add the IP Address of the designated receiver to the community table of all other SNMP devices with trap access.

To make the Trap Receive setting permanent, use the SAVE DEVICE command. Use the SHOW DEVICE command to display the Trap Receive setting.

SET DOWNLOAD NETWORK

Use the SET DOWNLOAD NETWORK command to specify the Ethernet network on which the inband download will occur. This command is used in conjunction with the SET TFTP commands in order to configure the EMM for an inband download. This command can only be issued from maintenance mode.

Format

SET DOWNLOAD NETWORK {network}

Parameters

{network} = 1
2
3

Example

The following command specifies that network 1 be used for the inband download.

```
>> set download network 1     [ENTER]
Download network changed.
```

Description

This command enables you to specify the Ethernet network to be used for inband download when issued from maintenance mode (using version 2.0 or greater BOOT PROMs).

Starter and Basic EMMs support inband downloads only from maintenance mode. Advanced EMM supports inband downloads from the command line and from maintenance mode.

The Download Network setting is saved automatically once you press [ENTER]. Use the SHOW DOWNLOAD command from Maintenance Mode to display the network information.

The SET DOWNLOAD NETWORK command can also be used if a download to flash EEPROM becomes corrupted (for example a power surge occurs during the download).

To recover from a power surge, enter maintenance mode, issue the SET DOWNLOAD NETWORK and SET TFTP commands, and start the download.

SET GROUP MODE

Use the SET GROUP MODE command to enable or disable all of the ports in a specific group. Port groups are supported by the TRMM Advanced.

Format

SET GROUP {group} MODE {setting}

Parameters

{setting} = disable
enable

Example

The following example disables all of the ports associated with group_4.

```
8250> set group group_4 mode disable [ENTER]

Port 04.09 set to DISABLED.
Port 04.10 set to DISABLED.
Port 04.12 set to DISABLED.
```

Description

This command allows you to enable or disable all ports associated with a specific group. You may want to issue the SHOW GROUP command to display the ports in the group before enabling or disabling the ports. This step ensures that you are modifying the correct port group.

SET GROUP NAME

Use the SET GROUP NAME command to define a group name for port group (for example, other than group1, group2). Port groups are supported by the TRMM Advanced.

Format

SET GROUP {group number} NAME {name}

Parameters

{group} = group1
group2
group3
group4
group5
group6
group7
group8

{name} = character string up to 16 characters

Example

The following example renames group1 to Eng1.

```
8250> set group group1 name Eng1 [ENTER]
Group1 named to Eng1.
```

Description

This command allows you to rename a defined port group to a more easily identified group name. The group name can be a maximum of 16 characters. When entering Group commands, the group is identified as the group name you define, not by the group number. For example, if you rename Group1 to Eng1, when you type the SET GROUP MODE command, you must specify Eng1 as the group name.

SET GROUP NETWORK

Use the SET GROUP NETWORK command to assign a group of port-switchable ports to a backplane network. Port groups are supported by the TRMM Advanced only.

Format

SET GROUP {group} NETWORK {network}

Parameters

{group} = group1
group2
group3
group4
group5
group6
group7
group8

{network} = token_ring_1...token_ring_7
isolated

Example

The following example sets ports in group1 to token_ring_1 .

```
8250> set group group1 network token_ring_1 [ENTER]
Group1 set to token_ring_1.
```

Description

Use the SET GROUP NETWORK command to assign a group of port-switchable ports to a backplane network. This command works with port-switching Token Ring modules only. Use the SHOW GROUP command to view a list of port group assignments.

SET GROUP PORT

Use the SET GROUP PORT command to define which ports are associated with a specific group. Port groups are supported by the TRMM Advanced only.

Format

SET GROUP {group} PORT {slot.port}

Parameters

{group} = group1
group2
group3
group4
group5
group6
group7
group8

{slot} = 1 through 17

{port} = 1 through 32 or all

Example

The following example sets port 1 on the module in slot 5 to group1.

```
8250> set group group1 port 5.1 [ENTER]
Port 5.1 set to group1
```

Description

This command enables you to assign ports to a specific group. You can assign ports individually, or all ports on a module, to a specific group. Once the port groups are established, you may then issue the SET GROUP MODE command to enable or disable a group.

SET HOST

Use the SET HOST command to assign host names to IP addresses. Using SET HOST allows you to use the name *or* the IP address to identify a device. This command is available for the TRMM and FMM only.

Format

SET HOST {name} {ip address}

Parameters

{name} = name you want to assign to the device
(maximum 24 characters)

{ip address} = IP address of the device you are naming

Example

The following command assigns the name “FMM20" to the FMM with IP address 151.104.7.77.

```
8250> set host FMM20 151.104.7.77 [ENTER]
Host name-ip address set.
```

Description

A host name can consist of any combination of a maximum of 24 alphanumeric characters, but must begin with a letter.

To make the list of host names permanent, use the SAVE HOST command. Use the SHOW HOST command to display the list of host names.

SET LOGIN

Use the SET LOGIN command to add users to, and change passwords for the FMM or TRMM command interface. You must be logged in as super user to use this feature to create new logins. In addition, you must have super user access to modify your own or another user's password.

Format

SET LOGIN {selection}

Parameters

{selection} = administrator
password
access super_user
user

Example

The following command allows a super user to establish a new administrator name and password.

```
8250> set login administrator    [ENTER]
```

You are prompted as follows:

```
Enter current session password for user “current user name” :{enter
password} [ENTER]

Enter Login Name: {enter name you select} [ENTER]

Enter Login Password: {enter new password} [ENTER]
Verify - re-enter password: {re-enter new password} [ENTER]

Login successfully entered.
```

Description

The FMM or TRMM allows you to configure up to 10 “users,” in any combination of access levels. The FMM provides three levels of user access:

- **User Level** - Allows the user to display information about network configuration and operation (except community table information).

- **Administrator Level** - Allows the user to perform all user-level tasks, as well as configure 8250 modules and ports.
- **Super-User Level** - Allows the user to perform administrator- and user-level tasks, as well as:
  - enter maintenance mode
  - add and change passwords
  - configure hub IP address information
  - configure community tables.

The FMM or TRMM also allows more than one user at a time to log into the command interface. The only limitation is that only one user with write privileges (for example, super_user or administrator) can log in at one time. If a second administrator or super user tries to log in, that user gains access to user-level (read) functions only. Up to four remote (Telnet) sessions can be established at one time.

Note: To modify the password for another user, you must use the CLEAR LOGIN command to first clear the entire login. Then you must re-enter the entire login.

Login names can contain up to 15 characters, but cannot include blanks. Passwords also can include up to 15 characters or they can be blank (by pressing [ENTER]). The default login name is `system` with no password (null). This login provides super user access.

Newly set passwords are effective immediately. You are not prompted for a password until you log out and then try to log in again. You must issue the SAVE LOGIN command for the new passwords to be permanently saved. Use the SHOW LOGIN command to display a list of currently used login names.

SET MODULE AUTOPARTITION_THRESHOLD

Use the SET MODULE AUTOPARTITION_THRESHOLD command to tell the management module the number of collisions to allow on an Ethernet module before automatically partitioning a port.

Format

SET MODULE {slot} AUTOPARTITION_THRESHOLD {threshold}

Parameters

{slot} = 1 through 17

{threshold} = 31_collisions
63_collisions
127_collisions
255_collisions

Example

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

```
8250> set module 7 autopartition_threshold 63_collisions
[ENTER]

Auto-partition threshold set to 63 COLLISIONS.
```

Description

Autopartition threshold tells network management how many collisions to allow before automatically partitioning a port. 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 partition, 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.

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 20-Port Token Ring Module.

Format

SET MODULE {slot} CABLE_IMPEDANCE {impedance}

Parameters

{slot} = 1 through 17

{impedance} = 100ohm
150ohm

Example

```
8250> set module 1 cable_impedance 100ohm     [ENTER]
Cable impedance set to 100 OHM.
```

Description

This command enables you to set the impedance level for the T20MS-RJ45S Token Ring module lobe ports. Unshielded cable is usually 100 ohms and shielded cable is usually 150 ohms.

SET MODULE CONNECTOR_NETWORK

Use the SET MODULE CONNECTOR_NETWORK command to assign a connector to a network. This command is available for the 24-Port 10BASE-T Module.

Format

SET MODULE {slot} CONNECTOR_{connector}_NETWORK {network}

Parameters

{slot} = 1 through 17

{connector} = 1 or 2

{network} = ethernet_1
ethernet_2
ethernet_3
isolated_1
isolated_2

Example

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

```
8250> set module 7 connector_1_network ethernet_3 [ENTER]
Module 7 connector 1 network ID set to ETHERNET 3.
```

Description

The 24-Port 10BASE-T Module provides bank-level configuration flexibility using the 8250 Multiprotocol Intelligent Hub's unique TriChannel architecture. You can assign either of the two 50-pin connectors, or the entire module, to any of three networks (or isolated) on the 8250 Multiprotocol Intelligent Hub backplane.

For example, 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.

SET MODULE CROSSOVER

Use the SET MODULE CROSSOVER command to enable or disable crossover mode for port 8 of 8250 Ethernet 10BASE-T Modules (E08MS-RJ45S).

Format

SET MODULE {slot} CROSSOVER {setting}

Parameters

{slot} = 1 through 17

{setting} = disable
enable

Example

```
8250> set module 1 crossover enable  [ENTER]
Crossover set to ENABLED.
```

Description

Enabling crossover mode allows you to connect port 8 of the 8250 10BASE-T module directly to a 10BASE-T transceiver. This is the default setting for all 10BASE-T ports.

Disabling crossover mode allows you to connect port 8 of the 8250 10BASE-T module directly to any port on another 10BASE-T module or 10BASE-T Hub.

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

SET MODULE LOCALLY_ADMINISTERED_ADDRESS

Use the SET MODULE LOCALLY_ADMINISTERED_ ADDRESS command to change all 6 bytes of the factory-set MAC address to a local setting.

Format

SET MODULE {slot} LOCALLY_ADMINISTERED_ ADDRESS {MAC address}

Parameters

{slot} = 1 through 17

{MAC address} = n-n-n-n

Example

```
8250> set module 12 locally_administered_address 48-03-e3-8f-02-00

MAC address changed; Reset device for change to take effect.
```

Description

The local MAC address can be entered using a management command or through SNMP. If the MAC address entered is a broadcast address or if the locally administered bit is not 1, the command aborts.

Once you issue the SET MODULE LOCALLY_ADMINISTERED_ADDRESS command, you must reset the TRMM in order for the new MAC address to take effect.

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 8250 Ethernet 10BASE-FB Modules.

Format

SET MODULE {slot} LOW_LIGHT_WARNING {setting}

Parameters

{slot} = 1 through 17

{setting} = disable
enable

Example

```
8250> set module 1 low_light_warning enable  [ENTER]
Low-light warning set to ENABLED.
```

Description

A low light condition does not affect network operation. Long link distances may cause a low light condition. It is a good idea to 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 management module. Once the network is running successfully, there is less need for this type of detection.

You may wish to disable the low light detection in situations where you are aware that the light level is low, and would prefer not to have a blinking status indicator signaling the condition.

SET MODULE MAC_ADDRESS_TYPE

Use the SET MODULE MAC_ADDRESS_TYPE command to specify the TRMM's MAC address as either the factory default (burned_in) or as user-defined (locally_administered).

Format

SET MODULE {slot} MAC_ADDRESS_TYPE {setting}

Parameters

{slot} = 1 through 17

{setting} = burned_in (default)
locally_administered

Example

The following example defines the TRMM MAC address as the factory default MAC address.

```
8250> set module 7 mac_address_type burned_in  [ENTER]
Mac address set to burned_in.
```

Description

This command allows you to specify the TRMM's MAC address as either the factory default MAC address or the user-defined MAC address.

This command will be rejected if the MAC address specified as the TRMM's MAC address is 0-0-0-0-0-0.

Issue the SHOW MODULE VERBOSE command to display a TRMM's MAC address.

You must reset the TRMM for a new MAC address to take effect.

SET MODULE MAC_PATH

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

Format

SET MODULE {slot} MAC_PATH {setting}

Parameters

{slot} = 1 through 17

{setting} = primary
secondary

Example

The following example establishes a secondary backplane path for an FDDI module in slot 10.

```
8250> set module 10 mac_path secondary     [ENTER]
Mac path set to secondary.
```

Description

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 (that is A-to-A connection and B-to-B connections).

SET MODULE MASTER_NETWORK

Use the SET MODULE MASTER_NETWORK command to define the network a slave TRMM will be assigned to in the event it becomes the master TRMM.

Format

SET MODULE {slot} MASTER_NETWORK {network}

Parameters

{slot} = 1 through 17

{network} = isolated
token_ring_1
token_ring_2
token_ring_3
token_ring_4
token_ring_5
token_ring_6
token_ring_7
no_change (default)

Example

This example defines network token_ring_3 as the network to which the slave TRMM in slot 6 will be configured in the event it becomes the master TRMM:

```
8250> set module 6 master_network token_ring_3  [ENTER]
Master network for 06 set to token_ring_3.
```

Description

This command allows you to assign a network for a slave TRMM. The slave will be configured for this network in the event it becomes the master TRMM.

The slave TRMM will assign itself to the specified network only when it transitions from being a slave to being a master. It will not use this network assignment after an election process or after a module reset.

If the network is specified as 'no_change', no change is made to the slave TRMM's network assignment when the slave becomes master.

SET MODULE MASTERSHIP_PRIORITY

Use the SET MODULE MASTERSHIP_PRIORITY command to establish the mastership priority of your management modules.

Format

SET MODULE {slot} MASTERSHIP_PRIORITY {priority}

Parameters

{slot} = 1 through 17

{priority} = 1 through 10

Example

This example sets the mastership priority level for the module in slot 6 to level 1.

```
8250> set module 6 mastership_priority 1  [ENTER]
Mastership priority set to 1.
```

Description

This command allows you to assign a priority level to your management modules. It is recommended that you set the management module to the highest priority level (10). All other management modules in the hub then become slaves. If there is a tie between priority levels of management modules in the same hub, the election for a master is arbitrary.

The management module with the highest priority is elected as a master for that hub. A master management module has configuration control, management responsibilities, and fault detection capabilities for the entire hub. A slave module can only listen to its own network activity.

Management modules are factory-set at priority level 10. Priority levels may be set from 1 through 10, with 10 having the highest priority access.

Mastership election completion time is dependent on a management module's mastership priority setting. A management module with a

mastership priority value of 10 takes less than 10 seconds to complete a mastership election. A management module with a mastership of 1, however, will take about 90 seconds to complete a mastership election. IBM recommends setting a master management module to 10 and slave management modules to mastership priority values of 7, 8, or 9 to facilitate the election process.

The MASTER MGT LED on the front panel of the management module lights green when that module is master.

Note: This command only sets the mastership priority. You must issue the RESET MASTERSHIP command to force an election to have another management module take over as master.

SET MODULE MODULE_BYPASS

Use the SET MODULE MODULE_BYPASS command to insert or bypass Token Ring MAU Modules in a ring.

Format

SET MODULE {slot} MODULE_BYPASS {ring status}

Parameters

{slot} = 1 through 17

{ring status} = bypass
insert

Example

```
8250> set module 5 module_bypass insert     [ENTER]
Module 5 INSERTED.
```

Description

Use this command to insert T08MS-RJ45S Token Ring Modules into the ring to which the Ring In and Ring Out cables are connected, or to bypass the module in a ring.

When you bypass the module, traffic still goes through the Ring In and Ring Out ports on the module, but does not travel to the eight media ports.

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. Therefore, you must use this command to insert the module into the ring. Refer to the specific Token Ring Installation Guide for more information on insert and bypass mode.

SET MODULE NETWORK

Use the SET MODULE NETWORK command to assign a particular module to a network.

Format

SET MODULE {slot} NETWORK {network}

Parameters

{slot} = 1 through 17

{network} = ethernet_1 token_ring_1 fddi_1
ethernet_2 token_ring_2 fddi_2
ethernet_3 token_ring_3 fddi_3
isolated token_ring_4 fddi_4
token_ring_5 isolated
token_ring_6
token_ring_7
isolated

Examples

Example 1

This command assigns the module in slot 1 to Token Ring network 3.

```
8250> set module 1 network token_ring_3 [ENTER]
Module 1 network id set to TOKEN_RING_3.
```

Example 2

The following command assigns the module in slot 5 to Token Ring network 1.

```
8250> set module 5 network token_ring_1 [ENTER]
Module 5 network id set to TOKEN_RING_1.
```

Description

You may assign each module to one of the selected networks that are available for the module type (Token Ring, 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 bridged. Each isolated module forms its own segment that isolates the traffic on that module from all other modules in the hub.

When you switch Token Ring modules from one ring to another ring, the rings are momentarily joined. To avoid this situation, switch the modules to isolated before switching them to another ring. This situation does not adversely affect the ring, nor does it have any effect on user applications.

To protect against unauthorized users, the management module automatically isolates a new module when the new module is installed.

ON modules that are network-selectable per port, refer to the SET PORT NETWORK command.

If you change the management module from one network to another, all network statistics are cleared to zeros.

Note: If you change a TRMM network assignment and the new network is on a different IP network (that is, the old and new Token Ring networks are separated by a router), then any stations attached through the front panel Ring-In and Ring-Out ports must be configured with new IP addresses.

SET MODULE PER_PORT_COUNTERS_CONNECTOR

Use the SET MODULE PER_PORT_COUNTERS_CONNECTOR command to select the 12-port connector for which you want the management module to gather port-by-port counter statistics. This command is only available for the 24-Port 10BASE-T Module.

Format

SET MODULE {slot} PER_PORT_COUNTERS_CONNECTOR {connector}

Parameters

{slot} = 1 through 17

{connector} = 1
2

Example

The following example enables the management module to gather statistics for connector 1 on the 24-Port Module in slot 7.

```
8250> set module 7 per_port_counters_connector 1 [ENTER]
Module 7 port counters set to CONNECTOR 1.
```

Description

This command enables you to select the 12-port connector for which you want the management module to gather port-by-port counter statistics. When you select a connector, network management monitors the other connector collectively, reporting statistics for all 12 ports as a single “port”, which displays as port 13.

The MONITOR PORT and SHOW COUNTER PORT {slot.port} commands function normally for the connector you select. If you ask for information on a port that is not being monitored individually, network management displays summed statistics along with instructions for getting more information on the port you selected.

Note: Changing which connector you are monitoring clears all statistics counters. Use the CLEAR COUNTER PORT command to erase any extraneous statistics gathered during the switchover.

SET MODULE PROBE_MODE

Use the SET MODULE PROBE_MODE command to enable RMON probe mode on the TRMM.

Format

SET MODULE {slot} PROBE_MODE {mode}

Parameters

{slot} = 1 through 17

{mode} = enable
disable

Example

The following command enables TRMM RMON probe mode:

```
8250> set module 7 probe_mode enable      [ENTER]
Probe Mode enabled.
```

Description

Table 2-1 shows which TRMM statistics information is available when you enable or disable RMON probe mode.

Table 2-1. Effect on Counters When Enabling and Disabling RMON Probe Mode

TRMM Version v4.0 Counters	Is Counter Available When RMON Probe Mode Is...?	
	Enabled	**Disabled**
Mac_layer Stats	Yes	No
Promiscuous Stats	Yes	No

Table 2-1. Effect on Counters When Enabling and Disabling RMON Probe Mode (Continued)

TRMM Version v4.0 Counters	Is Counter Available When RMON Probe Mode Is...?	
	Enabled	**Disabled**
Host	Yes	No
Host TopN	Yes	No
Matrix	Yes	No
Event	Yes	Yes
Alarm	Yes	Yes
Ring Station	Yes	No
Ring Station Order	Yes	No
Ring Station Config	Yes	No
Source Routing	Yes	No
Show Counter/Monitor Device	Yes	Yes
Show Counter/Monitor xxx Error	Yes	Yes
Show Counter/Monitor xxx Traffic	No	Yes
Show Counter/Monitor top_errors ...	No	Yes
Show Counter/Monitor top_senders ...	No	Yes
Show Counter/Monitor top_receivers ...	No	Yes

Note: Because most TRMM-specific traffic collection is disabled when using probe mode, thresholds that trigger based on these counters will no longer work.

SET MODULE RING_SPEED

Use the SET MODULE RING_SPEED command to set the module to operate at a transmission rate of 4 Mbps or 16 Mbps to match the ring speed of a Token Ring network.

Format

SET MODULE {slot} RING_SPEED {ring speed}

Parameters

{slot} = 1 through 17

{ring speed} = 4mbps
16mbps

Example

```
8250> set module 5 ring_speed 16mbps       [ENTER]
Ring Speed set to 16 MBPS.
```

Description

This command enables you to set the module to operate at a transmission rate of 4 Mbps or 16 Mbps to match the network ring speed. This setting determines the ring speed for *all* ports on the module.

SET PORT ACTIVE_CONNECTOR

Use the SET PORT ACTIVE_CONNECTOR command to activate the correct connector for the media (UTP or STP) you are using on the 8250 Token Ring Bridge Module.

Format

SET PORT {slot.2} ACTIVE_CONNECTOR {media}

Parameters

{slot} = 1 through 17

{media} = DB9 (default)
RJ45

Example

The following example assumes the Token Ring Bridge Module in slot 11 is using unshielded twisted pair cable. In this case, set the port 2 connector to RJ45.

```
8250> set port 11.2 active_connector RJ45    [ENTER]
Port 11.02 active connector set to RJ45.
```

Description

Use the SET PORT ACTIVE_CONNECTOR command to activate the proper connector for the media you are using.

The front panel of the 8250 Token Ring Bridge Module provides connections for either unshielded (UTP) or shielded twisted pair (STP) connections. UTP cable attaches using an RJ-45 connector. STP cable attaches using a DB-9 connector.

The setting for this command is saved automatically once issued. It is not necessary to issue the SAVE command. Consequently, the REVERT command cannot be used. You must re-issue the SET command to change the setting.

SET PORT ALERT

Use the SET PORT ALERT command to enable or disable port up/down trap generation for a specific port. This command works in conjunction with the SET ALERT PORT_UP_DOWN FILTER command (it does not matter in which order you issue these two commands).

Format

SET PORT {slot.port} ALERT {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 24

{setting} = disable (default)
enable

Examples

The following example disables the notification of a port up or port down alert for port 2 on the module in slot 6.

```
8250> set port 6.2 alert disable      [ENTER]
Port Alert set to DISABLED
```

Description

This command allows you to allow enable or disable port up/down trap generation on a per-port basis from the management module to each designated trap receiver.

Once the SET PORT ALERT command has been enabled for a port, you must issue the SET ALERT PORT_UP_DOWN FILTER command to allow or prevent port up and port down traps to be transmitted from the management module to the designated trap receiver.

SET PORT ALERT_FILTER

Use the SET PORT ALERT_FILTER command to enable or disable port up/down trap generation for a specific port. This command works in conjunction with the SET ALERT PORT_FILTER command (it does not matter in which order you issue these two commands). This command applies to the FMM and TRMM only.

Format

SET PORT {slot.port} ALERT_FILTER {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 24

{setting} = disable (default)
enable

Examples

The following example disables the notification of a port up or port down alert for port 2 on the module in slot 6.

```
8250> set port 6.2 alert_filter enable      [ENTER]
Port Alert Filter set to ENABLED
```

Description

This command allows you to enable or disable port up/down trap generation on a per-port basis from the management module to each designated trap receiver.

Once the SET PORT ALERT_FILTER command has been enabled for a port, you must issue the SET ALERT PORT_FILTER command to allow or prevent port up and port down traps to be transmitted from the management module to the designated trap receiver.

SET PORT COLLISION

Use the SET PORT COLLISION command to establish whether normal or alternate collision mode is used for that port on the Ethernet Transceiver Module.

Format

SET PORT {slot.port} COLLISION {mode}

Parameters

{slot} = 1 through 17

{port} = 1 through 3 or all

{mode} = alternate
normal

Example

The following example sets port 3 in slot 6 to normal collision mode.

```
8250> set port 6.3 collision normal      [ENTER]
Collision set to NORMAL.
```

Description

This command enables you to set collision mode to normal or alternate for ports on an Ethernet Transceiver Module. Normal mode is the default setting and it is used primarily with IEEE 802.3 devices and repeaters. Use Alternate mode primarily with non-IEEE 802.3 devices.

Refer to the *8250 Ethernet Transceiver Module Installation Guide* for more information on collision mode and the Ethernet Transceiver module.

SET PORT HALF_STEP

Use the SET PORT HALF_STEP command to establish whether half-step or full-step mode is used for that port on the Ethernet Transceiver Module.

Format

SET PORT {slot.port} HALF_STEP {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 3 or all

{setting} = disable
enable

Example

The following example sets port 2 in slot 7 to full step mode.

```
8250> set port 7.2 half_step disable     [ENTER]
Half_step set to DISABLED.
```

Description

This command enables you to set half-step or full-step mode for ports on an Ethernet Transceiver Module.

Half-step signaling is the default setting and is used primarily with IEEE 802.3 and Ethernet Version 2.0 devices and repeaters.

Full-step signaling is used primarily with non-IEEE 802.3 and earlier Ethernet devices.

Refer to the *8250 Ethernet Transceiver Module Installation Guide* for more information on half-step mode and the Ethernet Transceiver module.

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 8250 Ethernet Port-Switching 10BASE-FB Modules only.

Format

SET PORT {slot.port} HIGH_POWER {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 4 or all

{setting} = disable
enable

Example

```
8250> set port 5.1 high_power enable  [ENTER]
High power optics ENABLED.
```

Description

This command enables 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 this port to certain 10BASE-FB fiber products.

SET PORT LINK_INTEGRITY

Use the SET PORT LINK_INTEGRITY command to enable or disable link integrity for ports on Ethernet 10BASE-T Modules.

Format

SET PORT {slot.port} LINK_INTEGRITY {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 24 or all

{setting} = disable
enable

Example

The following example results in port 1 of the 10BASE-T Module in slot 5 to enable link integrity.

```
8250> set port 5.1 link_integrity enable     [ENTER]
Link integrity set to ENABLED.
```

Description

In general, you should enable link integrity for all ports on your 10BASE-T module to comply with the 10BASE-T standard. You must disable link integrity to connect to older non-10BASE-T equipment. Not all pre-10BASE-T equipment functions with link integrity enabled.

Link integrity must be enabled at both ends or disabled at both ends of the connection. If one end of the connection is different, the port with link integrity enabled will report a link integrity error.

SET PORT LOW_LIGHT_WARNING

Use the SET PORT LOW_LIGHT_WARNING command to enable a warning that displays when the light level received is weak. This command is used with Ethernet 10BASE-FB modules.

Format

SET PORT {slot.port} LOW_LIGHT_WARNING {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 4 or all

{setting} = disable
enable

Example

```
8250> set port 12.1 low_light_warning enable  [ENTER]
Low light warning set to ENABLED.
```

Description

A low light condition does not affect network operation. One reason for receiving a low light condition may be a long link distance. It is a good idea to enable the low light warning during system setup to see if any fiber connections are close to reaching their distance limits. If they are, the port status LED on the fiber module blinks six times to indicate the condition.

Once the network is running, there is less of a need for this type of detection. You may wish to disable the low light detection in situations where you are aware that the light level is low and would prefer not to have a blinking status indicator signaling the condition.

SET PORT MODE ENABLE/DISABLE

Use the SET PORT MODE ENABLE or DISABLE command to turn ports on or off.

Format

SET PORT {slot.port} MODE {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 32 or all

{setting} = disable
enable

Example

The following example disables (turns off) port 2 on the module in slot 6. This port is unusable until it is re-enabled.

```
8250> set port 6.2 mode disable      [ENTER]
Port 6.2 set to DISABLED.
```

Description

The port enable and disable options allow you to turn a single port on or off. You can enable or disable each port on a module by using {*slot*.all}. All ports are factory set to "enable" when shipped.

Note: Once the management module has been installed, all ports of newly installed media modules are automatically disabled for security purposes. You must manually enable these ports through the management module.

SET PORT MODE LOCAL/REMOTE

Use the SET PORT MODE LOCAL or REMOTE command to set an 8250 Terminal Server port to local or remote access.

Format

SET PORT {slot.port} MODE {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 32 or all

{setting} = local
remote

Example

This command sets port 2 on the module in slot 6 to local access where connections can be made to the server through this port.

```
8250> set port 6.2 mode local      [ENTER]
Port 6.2 set to LOCAL.
```

Description

This command enables you to set an 8250 Terminal Server port to local or remote access. When set to local (the default setting), connections can be made to the server through this port (for example, terminals).

When set to remote, connections can be made from the server to an external device (for example, dial-out modems). This command is applicable for 8250 Ethernet Terminal Server Modules only.

SET PORT MODE REDUNDANT/NON_REDUNDANT

Use the SET PORT MODE REDUNDANT or NON_REDUNDANT command to establish redundancy between two ports.

Format

SET PORT {slot.port} MODE {setting} {slot.port}

Parameters

{slot} = 1 through 17

{port} = 1 through 24

{setting} = non_redundant
redundant

Example

The following command establishes port 1 in slot 6 as the primary port and port 3 in slot 6 as the backup.

```
8250> set port 6.1 mode redundant 6.3 [ENTER]

Port 06.01 set to REDUNDANT PRIMARY.
Port 06.03 set to REDUNDANT BACKUP.
```

Description

When you issue the redundancy command for two ports, the first port in the command line becomes the primary link while 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.

Note: Initiating redundancy using a management module could cause a network loop in the unlikely event that:

1. both the management module and the power fail concurrently
2. the network is brought back up using the module dip switch settings
3. the ports of both the primary and redundant links are enabled through the dip switch settings.

To prevent a potential network loop, IBM advises that you disable either the primary or backup port through the dip switch settings, then use the SET PORT MODE command to enable that port.

The Advanced EMM allows you to establish cross-module redundancy. This feature enables you to set ports in different modules as redundant pairs. For example, you can use a fiber port as a primary port and a 10BASE-T port as the backup port. The Starter and Basic EMM do not support cross-module redundancy.

SET PORT MODE REMOTE_DIAGNOSTICS/ NON_REMOTE_DIAGNOSTICS

Use the SET PORT MODE REMOTE_DIAGNOSTICS command to establish redundancy between two ports *and* establish remote diagnostics on these ports. Only use this command when connecting two ports on 10BASE-T modules to a Fault-Tolerant 10BASE-FB Transceiver.

Format

SET PORT {slot.port} MODE {setting} {slot.port}

Parameters

{slot} = 1 through 17

{port} = 1 through 24

{setting} = non_remote_diagnostics
remote_diagnostics

Example

The following command establishes remote diagnostics *and* sets redundancy between ports 5 and 6 in slot 16.

```
8250> set port 16.5 mode remote_diagnostics 16.6     [ENTER]
Port 16.05 and 16.6 REMOTE DIAGNOSTICS ENABLED.
```

Description

This command establishes redundancy between two ports *and* establishes remote diagnostics on these ports. Use this command only when connecting two ports on 10BASE-T modules to a Fault-Tolerant 10BASE-FB Transceiver.

When you establish remote diagnostics between two ports, the first port in the command line becomes the primary link while 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.

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.

Note that 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.

Refer to the *Fault-Tolerant 10BASE-FB Transceiver Installation Guide* for more information and suggested configurations when connecting modules to the Fault-Tolerant Transceiver.

SET PORT MODE REMOTE_FAILURE_SIGNALING

Use the SET PORT MODE REMOTE_FAILURE_SIGNALING command to establish remote failure signaling on redundant FOIRL or 10BASE-FL module links.

Format

SET PORT {slot.port} MODE REMOTE_FAILURE_SIGNALING

Parameters

{slot} = 1 through 17

{port} = 1 through 4

Example

The following command establishes remote failure signaling for port 3 in slot 9.

```
8250> set port 9.3 mode remote_failure_signaling      [ENTER]

Port 09.03 set to REMOTE FAILURE SIGNALING.
```

Description

You can enable Remote Failure Signaling (RFS) for any of the four ports on the FOIRL or 10BASE-FL Module. When you connect two FOIRL or 10BASE-FL 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. RFS is disabled when you disable redundancy on the corresponding port or disable the port itself.

Refer to the *8250 Ethernet FOIRL Module Installation Guide* for more information on RFS mode and the Ethernet FOIRL Module.

Refer to the *8250 Ethernet 10BASE-FL Module Installation Guide* for more information on RFS mode and the Ethernet 10BASE-FL Module.

SET PORT NETWORK

Use the SET PORT NETWORK command to assign a port to a specific network. This command applies to port-switching modules only.

Format

SET PORT {slot.port} NETWORK {network}

Parameters

{slot} = 1 through 17

{port} = 1 through 24 or all

{network} = ethernet_1
ethernet_2
ethernet_3
front_panel
isolated

Examples

Example 1

```
8250> set port 5.2 network ethernet_1_[ENTER]
Port 05.02 network id set to ETHERNET_1
```

This command sets port 2 on the module in slot 5 to network Ethernet 1.

Example 2

```
8250> set port 7.1 network front_panel     [ENTER]
Port 07.01 network id set to FRONT_PANEL
```

This command sets port 1 on the 8250 Ethernet Bridge Module in slot 7 to the AUI port on the front panel.

Example 3

```
8250> set port 4.all network ethernet_2     [ENTER]
Port 04.01 network id set to ETHERNET_2
Port 04.02 network id set to ETHERNET_2
```

This command sets both ports on the 8250 Ethernet Repeater Module in slot 4 to network Ethernet 2.

Description

Ports assigned to the same network form a segment. Ports assigned to different networks are on different segments and cannot communicate unless the networks are bridged. Each isolated port forms its own segment that isolates the traffic on that port from all other modules in the hub. If more than one port on a module is set to isolated, these ports form a segment of their own.

All Ethernet modules are factory-set through the dip switches so that the ports are assigned to channel 1 (Ethernet network 1). Only use the channel setting if your hub is without a management module.

This command applies *only* to modules from IBM that have individual ports that are network-selectable. For modules that are network selectable per module, refer to the SET MODULE NETWORK command.

SET PORT PERSONALITY

Use the SET PORT PERSONALITY command to designate the transmission mode for a port on the FDDI Shielded Twisted Pair Module.

Format

SET PORT {slot.port} PERSONALITY {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 8 or all

{setting} = sddi (default)
tpddi

Example

The following example sets sddi as the transmission mode for port 2 of the FDDI Shielded Twisted Pair Module in slot 8.

```
8250> set port 8.2 personality sddi      [ENTER]
Port Personality set to sddi.
```

Description

The FDDI STP Module supports both the SDDI and TPDDI de facto standards for running FDDI on shielded twisted pair cable. ON a per-port basis, you can designate whether the port is to transmit data using the SDDI or the TPDDI signaling mode. This allows you to connect the module to any vendor device that supports either of the two proposed standards. All ports default to SDDI mode when you first install the FDDI STP Module. You must use SDDI when ports 1 and 2 on the FDDI Shielded Twisted Pair Module are configured as S-type ports.

SET PORT RECEIVE_JABBER

Use the SET PORT RECEIVE_JABBER command to enable or disable Receive Jabber for a port.

Format

SET PORT {slot.port} RECEIVE_JABBER {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 24 or all

{setting} = disable
enable

Example

The following example enables Receive Jabber for port 2 on the Ethernet 50-Pin Module in slot 12.

```
8250> set port 12.2 receive_jabber enable      [ENTER]
Receive Jabber on Port 12.02 set to ENABLED.
```

Description

This command lets you enable or disable Receive Jabber mode for ports. When enabled, if a jabber condition occurs and the transceiver or repeater device fails to halt the condition, Receive Jabber protects the network by disconnecting the link after 10 msecs.

Note: Receive Jabber is set to a default of disabled to conform to the 10BASE-T standard.

SET PORT RING_SPEED

Use the SET PORT RING_SPEED command to set either port on the Token Ring Bridge Module to operate at a transmission rate of 4 or 16 Mbps, depending on the network ring speed.

Format

SET PORT {slot.port} RING_SPEED {setting}

Parameters

{slot} = 1 through 17

{port} = 1 (backplane)
2 (front panel)

{setting} = 4mbps
16mbps

Example

The following example sets port 1 of the Token Ring Bridge Module in slot 5 to 16 Mbps ring speed.

```
8250> set port 5.1 ring_speed 16mbps [ENTER]
Port 5.01 ring speed set to 16mbps.
```

Description

This command enables you to set port 1 or port 2 on the Token Ring Bridge Module to a transmission rate of 4 or 16 Mbps. The setting for this command is saved automatically once issued. It is not necessary to issue the SAVE command. Consequently, you cannot use the REVERT command. You must re-issue the SET command to change the setting.

SET PORT SQE_TEST

Use the SET PORT SQE_TEST command to establish whether SQE Test is enabled or disabled for ports on the Ethernet Transceiver Module.

Format

SET PORT {slot.port} SQE_TEST {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 3 or all

{setting} = disable
enable

Example

The following example enables SQE Test for port 1 in slot 8.

```
8250> set port 8.1 sqe_test enable      [ENTER]
SQE_test on Port 08.01 set to ENABLED.
```

Description

This command lets you enable or disable SQE Test mode for ports on an Ethernet Transceiver Module.

When SQE Test is enabled (the default setting) you can connect this port to most devices, except repeaters.

When SQE Test is disabled you can connect this port to baseband Repeaters and Multiport Transceivers.

Refer to the *8250 Ethernet Transceiver Module Installation Guide* for more information on SQE Test mode and the Ethernet Transceiver Module.

SET PORT SQUELCH

Use the SET PORT SQUELCH command to establish the Squelch Mode as either normal or low for ports on Ethernet 10BASE-T Modules.

Format

SET PORT {slot.port} SQUELCH {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 12 or all

{setting} = low
normal

Example

The following example sets port 1 in slot 5 to a low squelch level.

```
8250> set port 5.1 squelch low      [ENTER]
Squelch set to LOW.
```

Description

The Squelch Mode command allows you to establish the squelch level as either normal or low (sensitive). The squelch level is factory-set to “normal” to conform to the 10BASE-T standard.

When the squelch level is set to low, ports are able to receive weaker signals, allowing longer link distances. You may want to change the level from normal to low for some ports if they experience weak signals. Setting the squelch level to low increases the achievable link distance, but with the added risk of losing packets to impulse noise.

In general, IBM recommends using normal squelch. Ensure that the squelch level at both ends of the link match. If you change the squelch level at the module, you must change the squelch setting at the transceiver also.

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

SET PORT STATION_TYPE

Use the SET PORT STATION_TYPE command to designate a station that does not have a MAC Address (that is, a network analyzer).

Format

SET PORT {slot.port} STATION_TYPE {type}

Parameters

{slot} = 1 through 17

{port} = 1 through 20 or all

{type} = mac_not_present
mac_present (default)

Example

```
8250> set port 3.6 station_type mac_not_present [ENTER]
Station type set to MAC_NOT_PRESENT
```

Description

Stations that assert phantom, but do not have a MAC Address cause problems in the mapping algorithm. To prevent this problem, set the station_type parameter to mac_not_present. This eliminates the stations from the mapping algorithms. Failure to designate a MAC-less station could cause incorrect mapping.

Security settings configured for a port are bypassed when setting the port to a station type of MAC_NOT_PRESENT.

SET PORT TYPE

Use the SET PORT TYPE command to define ports on the FDDI Fiber Module and FDDI Shielded Twisted Pair Module as master or slave ports.

Format

SET PORT {slot.port} TYPE {setting}

Parameters

{slot} = 1 through 17

{port} = 1 through 2

{setting} = master
slave

Example

The following example sets port 1 in slot 7 to be a slave port.

```
8250> set port 7.1 type slave      [ENTER]
Type set to SLAVE.
```

Description

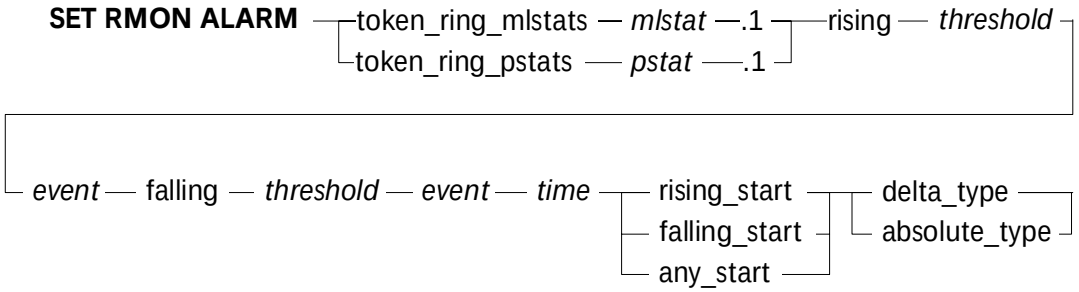
All FDDI Media Module ports default to a Type M (master). Ports 1 and 2 can, however, be designated as Type S (slave) ports. As a slave port, the port can be used to connect to an M port on another FDDI hub. The port can also run as a backup to the master port in redundant configurations. IBM recommends that you designate your S port(s) before enabling the ports on the module.

Note: Ports 3 through 8 operate only as Type M ports. Therefore, the above command is not available for ports 3 through 8. Refer to the appropriate FDDI module manual as needed for additional information on the usage of Type M and Type S ports.

SET RMON ALARM

Use the SET RMON ALARM command to set up an alarm that triggers an event based on the parameters you specify. For additional information on setting up RMON alarms, refer to the *8250 TRMM User's Guide*.

Format



Parameters

Parameter	Description
token_ring_mlstats	Selects the MAC Layer RMON statistics group for this operation.
token_ring_pstats	Selects the Promiscuous RMON statistics group for this operation.

Parameter	Description
mlstat	Specifies a statistic for this operation. *mlstat* can be one of the following: DropEvents Octets Packets RingPurgeEvents RingPurgePackets BeaconEvents BeaconTime BeaconPackets ClaimTokenEvents ClaimTokenPackets NAUNChanges LineErrors InternalErrors BurstErrors ACErrors AbortErrors LostFrameErrors CongestionErrors FrameCopiedErrors FrequencyErrors TokenErrors SoftErrorReports RingPollEvents
pstat	Specifies a statistic for this operation. *pstat* can be one of the following: DropEvents Octets Packets BroadcastPackets MulticastPackets

Parameter	Description
.1	The index number of the TRMM's RMON interface, which is always 1. Append the interface number to the *mlstat* or *pstat* without a space in between. For example: `DropEvents.1`
rising	Introduces the parameters for the rising threshold.
threshold	The statistic value falling below the *threshold* triggers the *event* (see next table row).
event	Index number of the RMON event triggered by the rising threshold. Use the SET RMON EVENT command to create events, and the SHOW RMON EVENTS command to view event index numbers.
falling	Introduces the parameters for the falling threshold.
threshold	The statistic value falling below the *threshold* triggers the *event* (see next table row).
event	Index number of the RMON event triggered by the 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 either by the rising threshold or falling threshold.

Parameter	Description
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 BeaconEvents in an hour:

```
8250> set rmon alarm token_ring_mlstats beaconpackets.1 rising 5 2
falling 1 3 01:00 rising_start delta_type [ENTER]

Entry 2 created.
```

Description

This command allows you to create RMON alarm table entries.

When you have configured an alarm, 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 (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 re-armed 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.

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

SET RMON EVENT {action} {community}

Parameters

{action} = log
log_trap
none
trap

{community} = SNMP community name for trap receivers.

Example

The following command sets up a trap message sent when the BeaconPackets alarm is triggered:

```
8250> set rmon event trap    [ENTER]
Enter one line for event description:
> BeaconPackets Threshold Exceeded!!    [ENTER]
Entry 2 created.
```

Description

When you use this command, the TRMM causes the associated event to occur when triggered by an alarm. You create alarms using the SET RMON ALARM command. The event options are:

- Log — Records the triggered alarm in a log file.
- Trap — Sends a trap to the selected community table.
- Log_Trap — Sends a trap and creates a log entry.
- None — Takes no action. The event is inactive.

SET RMON HOST

Use the SET RMON HOST command to enable host table collection.

Format

SET RMON HOST INTERFACE {index}

Parameters

{index} = interface number you are enabling statistics collection for

Example

The following command enables host table monitoring by the RMON agent:

```
8250> set rmon host interface 1 [ENTER]
Entry 1 created.
```

Description

This command enables RMON host table data collection.

The RMON agent in the TRMM 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.

Note: The TRMM does not collect RMON statistics unless you enable RMON probe mode using the SET RMON PROBE_MODE command.

SET RMON MATRIX

Use the SET RMON MATRIX command to enable collection of RMON Matrix group statistics.

Format

SET RMON MATRIX INTERFACE {index}

Parameters

{index} = interface number you are enabling statistics collection for

Example

The following command enables RMON Matrix group monitoring:

```
ONsemble> set rmon matrix interface 1    [ENTER]
Entry 1 created.
```

Description

The RMON Matrix group collects statistics for each conversation that the RMON agent detects on the network. Normally, the control table contains one entry automatically created at startup. If an entry already exists in the control table, you cannot add a second entry.

SET RMON RINGSTATION

Use the SET RMON RINGSTATION command to enable Ring-Station group monitoring by the RMON agent in the TRMM.

Format

SET RMON RINGSTATION INTERFACE {index}

Parameters

{index} = interface number you are enabling statistics collection for

Example

The following command enables Ring Station group monitoring by the RMON agent:

```
8250> set rmon ringstation interface 1 [ENTER]
Entry 1 created.
```

Description

This command creates an entry in the TRMM RMON ringstation control table. Creating this entry allows the TRMM to collect ringstation statistics.

Note: The TRMM does not collect RMON statistics unless you enable RMON probe mode using the SET RMON PROBE_MODE command.

SET RMON STATISTICS

Use the SET RMON STATISTICS command to enable monitoring by the RMON agent in the TRMM for one of the RMON statistics groups.

Format

SET RMON STATISTICS {group} INTERFACE {index}

Parameters

{group} = mac_layer
promiscuous
sourcerouting

{index} = interface number you are enabling statistics collection for

Example

The following command enables MAC Layer statistics group monitoring by the RMON agent:

```
8250> set rmon statistics mac_layer interface 1 [ENTER]
Entry 1 created.
```

Description

This command enables statistics collection for the indicated RMON group. Use the appropriate SHOW RMON command to view the statistics collected.

Note: The TRMM does not collect RMON statistics unless you enable RMON probe mode using the SET RMON PROBE_MODE command.

SET RMON TOPN_HOSTS

Use the SET RMON TOPN_HOSTS command to enable the collection of RMON Host Top N group statistics by the RMON probe.

Format

SET RMON TOPN_HOSTS {interface} {statistic} {interval}

Parameters

{interface} = 1 (the TRMM has only one interface)

{statistic} = in_octets
in_packets
out_bcasts
out_errors
out_mcasts
out_octets
out_packets

{interval} = period of time you want to monitor the statistic for (*mm:ss*)

Example

The following command enables Host Top N monitoring to rank hosts based on the number of packets sent by each host during a 60-minute interval:

```
ONsemble> set rmon topn_hosts 1 out_packets 60:00
Entry 1 created.
```

Description

Host Top N group statistics collecting works as follows:

1. You create a control table entry specifying the duration of the test interval and the statistic to monitor during that interval.
2. The RMON probe monitors the statistic for the specified interval. During this time the data is not available for viewing.

3. When the interval is complete, the RMON probe ranks the top 10 hosts based on the monitored statistic. You use the SHOW RMON TOPN_HOSTS command to view the data.

   The RMON probe collects no more data for this control table entry.

SET SCHEDULE

Use the SET SCHEDULE command to define the time a specific schedule or all schedules are to run a specific script.

Format

SET SCHEDULE {schedule number} {option}

Parameters

{schedule} = schedule number (1 through 20)
all

{option} = exclude_date (mm/dd)
exclude_day (Sunday - Monday, Weekday, Weekend)
include_date (mm/dd)
include_day (Sunday - Monday, Weekday, Weekend)
mode (enable or disable)
remove_date (mm/dd)
time (hh:mm) - script (script number to execute)

{script number} = 1 through 20
all

Example

The following example defines schedule 1 to run script 3 at 7:00.

```
8250> set schedule 1 time 7:00 script 3 [ENTER]
Schedule 1 set to run script 3 at time 07:00.
```

Description

The SET SCHEDULE command enables you to define the time a specific schedule or all schedules are to run a specific script.

Prior to configuring schedules, issue the SHOW CLOCK command to verify that the TRMM's time and date are correct.

The SET SCHEDULE options include:

Exclude_date (mm/dd) - Overrides the normal schedule by excluding a specific date.

Exclude_day (Sunday - Monday, Weekend, Weekday) - Overrides the normal schedule by excluding a specific day.

Include_date (mm/dd) - Overrides the normal schedule by including a specific date.

Include_day (Sunday - Monday, Weekend, Weekday) - Overrides the normal schedule by including a specific day.

Mode (enable or disable) - Enables or disables one schedule or all schedules.

Remove_date (mm/dd, holiday) - Removes a specific date or day from one schedule or all schedules.

Time (hh:mm) - Defines the time a specific script will be run for one schedule or all schedules. You must also use the SCRIPT option and specify the script number to execute.

SET SCHEDULE HOLIDAY

Use the SET SCHEDULE HOLIDAY command to define the Holiday group which consists of a maximum of 10 entries.

Format

SET SCHEDULE HOLIDAY {option} {date}

Parameters

{option} = include_date (mm/dd)
remove_date (mm/dd)

{date} = month/day (mm/dd)

Example

The following example defines December 25 as a holiday.

```
8250> set schedule holiday include_date 12/25 [ENTER]
Date 12/25 included in HOLIDAY list.
```

Description

The SET SCHEDULE HOLIDAY command enables you to define the day and month of a holiday and include or remove it from the Holiday group.

Once defined, you can use the HOLIDAY option in the SET SCHEDULE {schedule number} INCLUDE_DATE command to have a script execute on the dates specified in the Holiday group. Or, you can specify the EXCLUDE_DATE to exclude all dates in the Holiday group from executing a script.

SET SCHEDULE STARTUP_REPLAY_TIME

Following a reset of the TRMM, use the SET SCHEDULE STARTUP_REPLAY_TIME command to define the amount of time the TRMM will go back and execute scripts.

Format

SET SCHEDULE STARTUP_REPLAY_TIME {time}

Parameters

{time} = hours 1 through 24
since_midnight

Example

The following example causes the TRMM to execute all scripts defined in schedules which were scheduled to run six hours or less from the current time.

```
8250> set schedule startup_replay_time 6   [ENTER]
The startup_replay_time is set to 6 hours.
```

Description

The SET SCHEDULE STARTUP_REPLAY_TIME enables you to define the amount of time the TRMM will go back following a reset and execute scripts.

For example, after a TRMM is reset, if the Startup Replay Time is defined as 6 (hours) and the current time is 8:00 am, the TRMM executes all scripts that have occurred since 2 am.

SET SCHEDULE WEEKDAY

Use the SET SCHEDULE WEEKDAY command to define a group which consists of a maximum of seven entries specifying weekdays.

Format

SET SCHEDULE WEEKDAY

Parameters

{option} = include_day
remove_day

{day} = all
sunday
monday
tuesday
wednesday
thursday
friday
saturday

Example

The following example includes Monday in the Weekday group.

```
8250> set schedule weekday include_day monday [ENTER]
MONDAY included in WEEKDAY variable.
```

Description

The SET SCHEDULE WEEKDAY command enables you to include or remove one day or all days from the Weekday group. Once defined, you can use the WEEKDAY option in the SET SCHEDULE {schedule number} INCLUDE_DAY command to have a script execute on the days specified in the Holiday group. Or, you can specify the EXCLUDE_DAY to exclude all dates in the Weekday group from executing a script.

SET SCHEDULE WEEKEND

Use the SET SCHEDULE WEEKEND command to define a group consisting of a maximum of seven entries specifying weekends.

Format

SET SCHEDULE WEEKEND

Parameters

{option} = include_day
remove_day

{day} = all
sunday
monday
tuesday
wednesday
thursday
friday
saturday

Example

The following example removes Sunday from the schedule.

```
8250> set schedule remove_day sunday [ENTER]
SUNDAY removed from WEEKEND variable.
```

Description

The SET SCHEDULE WEEKEND command enables you to include or remove one day or all days from the Weekend group. Once defined, you can use the WEEKEND option in the SET SCHEDULE {schedule number} INCLUDE_DAY command to have a script execute on the days specified in the Holiday group. Or, you can specify the EXCLUDE_DAY to exclude all dates in the Weekend group from executing a script.

SET SCRIPT DELETE

Use the SET SCRIPT DELETE command to delete a command in a script at the specified line number.

Format

SET SCRIPT {script number} DELETE {line number}

Parameters

{script number} = 1 through 8

{line number} = 1 through 15

Example

The example shown below removes line 6 from script 1.

```
8250> set script 1 delete 6 [ENTER]
Line 6 deleted from SCRIPT 1.
```

Description

The SET SCRIPT DELETE command allows you to delete one command line from a script.

SET SCRIPT INSERT

Use the SET SCRIPT INSERT command to insert new commands into a script at the specified line number.

Format

SET SCRIPT {script number} INSERT {line number}

Parameters

{script number} = 1 through 8

{line number} = 1 through 15

Example

The following example inserts a new line in script 1. The former line 11 moves down to line 12.

```
8250> set script 1 insert 11   [ENTER]
Enter line(s) to insert. Enter a blank line to quit this mode.
```

Description

The SET SCRIPT INSERT command allows you to insert new commands into a script.

SET SCRIPT NAME

Use the SET SCRIPT NAME command to assign a name to a script number.

Format

SET SCRIPT {script number} NAME {name}

Parameters

{script number} = 1 through 8

{name} = maximum of 16 alphanumeric characters

Example

The following example assigns the name engineering1 to script 3.

```
8250> set script 3 name engineering1 [ENTER]
Name set for script 3.
```

Description

The SET SCRIPT NAME command allows you to assign a name for a script number. Use the SHOW SCRIPT command to display the name and other information for a specific script or all scripts.

SET SCRIPT OVERWRITE

Use the SET SCRIPT OVERWRITE command to add a new command to a script at a specified line number to replace the existing command.

Format

SET SCRIPT {script number} OVERWRITE {line number}

Parameters

{script number} = 1 through 8

{line number} = 1 through 15

Example

The following example replaces the command line 1 with a new command in script 3.

```
8250> set script 3 overwrite 1 [ENTER]
Enter line(s) to overwrite. Enter a blank line to quit this
mode.
```

Description

The SET SCRIPT OVERWRITE command allows you to add a new command to a script and replace an existing command.

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 8250 10BASE-T Security Module (E12MSS) only.

Format

SET SECURITY AUTOLEARN {slot.port} CAPTURE

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 12 or all

Example

The following example allows the MAC addresses associated with all ports on the Security Module in slot 3 to be learned by the EMM during Autolearning.

```
8250> set security autolearn 3.all capture  [ENTER]
Autolearn capture done; learned 3 addresses total.
```

Description

Autolearning allows the EMM to continuously monitor network activity and automatically “learn” the valid MAC addresses associated with a port on the Security Module.

Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for detailed information about the Autolearning feature.

SET SECURITY AUTOLEARN DOWNLOAD

Use the SET SECURITY AUTOLEARN DOWNLOAD command to download the contents of the Autolearning database to the specified ports in order for the MAC addresses to be associated with a port.

This command applies to the 8250 10BASE-T Security Module (E12MSS) only.

Format

SET SECURITY AUTOLEARN {slot.port} DOWNLOAD

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 12 or all

Example

The following example initiates a download of the Autolearning database to all 12 ports on the Security Module in slot 3.

```
8250> set security autolearn 3.all download  [ENTER]
Autolearn download done; downloaded 3 addresses total.
```

Description

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.

An EMM allows a maximum of 360 MAC addresses in the Autolearning database per hub. A TRMM allows a maximum of 400 MAC addresses in the Autolearning database per hub.

Because a maximum of four MAC addresses can be associated with one port, only four MAC addresses are downloaded per port. The four MAC addresses with the lowest alpha-numerical values will be downloaded from the Autolearning database to a Security Module port.

The following message is displayed upon completion of the Autolearn Download command (where y indicates the total number of addresses which were copied to a port(s) MAC address table):

```
Autolearn download done; downloaded y addresses total.
```

If a port has more than four MAC addresses in the Autolearning database at the time of the download, the following message displays 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 4 autolearned
addresses.
```

If any MAC address was skipped because the hub limit of 360 addresses was reached, the following message displays upon completion of the Autolearn Download command:

```
Note: the number of autolearned addresses exceeds the hub
limit. Only the first X addresses (as ordered by slot, port,
and addr) were downloaded.
```

When using an EMM, the X is replaced by the EMM hub limit of 360 MAC addresses. When using a TRMM, the X is replaced by the TRMM hub limit of 400 MAC addresses.

Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for detailed information on Autolearning.

SET SECURITY AUTOLEARN MAC_ADDRESS

Use the SET SECURITY AUTOLEARN MAC_ADDRESS command to manually add a MAC address into the Autolearning database. This command applies to the 8250 10BASE-T Security Module (E12MSS) only.

Security for Ethernet modules (other than the 10BASE-T Security Module) is only available with the Advanced EMM. All versions of the EMM (Starter, Basic, Advanced) support the Security Module. The Basic and Advanced TRMM are capable of configuring security for all modules that support security.

Format

SET SECURITY AUTOLEARN {slot.port} MAC_ADDRESS {address}

Parameters

{slot} = 1 through 17 or all
{port} = 1 through 12 or all
{MAC address} = nn-nn-nn-nn-nn-nn

Example

The following example adds the MAC address 07-34-24-02-0F-00 to the Autolearning database and associates it with port 1 on the Security Module in slot 3.

```
8250> set security autolearn 3.1 mac_address 07-34-24-02-0F-00
[ENTER]

Address 07-34-24-02-0F-00 associated with port 03.01 in
Autolearning area.
```

Description

This command enables you to manually add a MAC address to the Autolearning database and specify in the command line to which port you want this MAC address associated.

The address 00-00-00-00-00-00 is invalid for this command.

Use the SHOW SECURITY AUTOLEARN command to display the entries in the Autolearning database.

SET SECURITY AUTOLEARN MASK

Use the SET SECURITY AUTOLEARN MASK command to allow or prevent a port MAC addresses from being learned by the EMM during Autolearning.

This command applies to the 8250 10BASE-T Security Module (E12MSS) only.

Format

SET SECURITY AUTOLEARN {slot.port} MASK {setting}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 12 or all

{setting} = disable
enable

Example

The following example allows the MAC addresses associated with all ports on the Security Module in slot 3 to be learned by the EMM during Autolearning.

```
8250> set security autolearn 3.all mask disable [ENTER]
Port 03.all autolearn mask set to DISABLED.
```

Description

The Autolearn Mask setting allows (disable the mask) or prevents (enable the mask) the EMM from learning MAC addresses for a port during Autolearning. This setting also determines whether the EMM is allowed or prevented from downloading learned MAC addresses to the port.

SET SECURITY PORT ACTION_ON_INTRUSION

Use the SET SECURITY PORT ACTION_ON_INTRUSION command to define the corrective action an EMM is to take when a port (for which Intrusion Control has been defined) experiences a security intrusion attempt.

Format

SET SECURITY PORT {slot.port} ACTION_ON_INTRUSION {action}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 12 or all

{action} = disable_and_trap (default)
disable_only
no_action
trap_only

Example

The following example defines the port action for port 1 on the Security Module in slot 3 to no_action.

```
8250> set security port 3.1 action_on_intrusion
no_action [ENTER]

Port 03.01 action_on_intrusion set to NO_ACTION.
```

Description

The intrusion actions are described below. Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for complete information on the Security Module and its features.

disable_and_trap - Disables the specified port and sends a trap to the EMM console or stations defined in the EMM's community table.

disable_only - Only disables the specified port.

no_action - No action is taken upon an intrusion attempt (although the Security Module stills forces a collision on an intruding packet).

trap_only - Only sends a trap to stations defined in the EMM's community table.

In order for an EMM to log a security intrusion attempt into the Intruder List, you must configure the ACTION_ON_INTRUSION setting for either *disable_and_trap or trap_only*. These settings allow a trap to be sent upon an intrusion, which also logs the entry into the Intruder List.

Refer also to the SHOW SECURITY INTRUDER_LIST command described in this guide for a description of the Intruder List.

SET SECURITY PORT MAC_ADDRESS

Use the SET SECURITY PORT MAC_ADDRESS command to define address-to-port security for ports in your network. These MAC addresses are stored in the port's MAC address table.

Security for Ethernet modules (other than the 10BASE-T Security Module) is only available with the Advanced EMM. All versions of the EMM (Starter, Basic, Advanced) support the Security Module. The TRMM Basic and Advanced are capable of configuring security for all modules that support security.

Format

SET SECURITY PORT {slot.port} MAC_ADDRESS {address}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 24 or all

{address} = nn-nn-nn-nn-nn-nn

Example

The following example associates port 2 in slot 3 with the MAC address 07-34-24-02-0F-00.

```
8250> set security port 3.2 mac_address 07-34-24-02-0F-00
[ENTER]
Security MAC address 07-34-24-02-0F-00 associated with port
03.02.
```

Description

This command enables you to define address-to-port security for ports in your network. You may assign a maximum of four MAC addresses with a specific port. After you define a MAC address for a port, enable the security feature using the SET SECURITY PORT MODE command. From that point on, if the EMM detects a packet that does not contain one of the port's

authorized MAC addresses, it sends an alarm to the EMM console (or management workstation) and disables the port.

The address 00-00-00-00-00-00 is invalid for this command.

Note: You cannot enable the security feature for logical ports (that is, EMM or TRMM ports) or for ports on a protocol other than the one you are using.

Use the SHOW SECURITY AUTOLEARN command to display the entries in the Autolearning database.

SET SECURITY PORT MODE

Use the SET SECURITY PORT MODE command to enable or disable address security for a specific port, all ports on a module, or all ports on all modules in a hub.

Security for Ethernet modules (other than the 10BASE-T Security Module) is only available with the Advanced EMM. All versions of the EMM (Starter, Basic, Advanced) support the Security Module. The TRMM Basic and Advanced are capable of configuring security for all modules that support security.

Format

SET SECURITY PORT {slot.port} MODE {setting}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 24 or all

{setting} = disable
enable

Example

The following example enables security on port 2 in slot 3 of the hub.

```
8250> set security port 3.2 mode enable        [ENTER]
Port 03.2 security mode set to ENABLED.
```

Description

This command enables you to enable or disable security for ports. From that point on, if the EMM detects a packet that does not contain one of the port's authorized MAC addresses, it sends an alarm to the EMM (or management workstation) and disables the port.

The 8250 10BASE-T Security Module provides the flexibility of manually enabling or disabling Security Mode. Security Mode is automatically

enabled for a Security Module port(s) when you issue the SET SECURITY PORT SECURITY_TYPE command. Only the ports specified in the SET SECURITY PORT SECURITY_TYPE command line will have Security Mode enabled.

Security type is automatically configured to *Full* when you issue the SET SECURITY PORT MODE ENABLE command. Only the ports specified in the SET SECURITY PORT MODE ENABLE command line will have security type set to *Full*.

You may enable Security Mode for a port that does not have MAC addresses associated with it. However, each packet received by a port that does not have a valid MAC address assigned to it is treated as an intrusion.

Note: You must disable Security Mode for the EMM to Autolearn MAC addresses for ports that are configured for Security Types Intrusion or Full. If Security Mode is not disabled, the MAC addresses are not autolearned. In addition, the port reports an intrusion. (An intrusion is only reported if the ACTION_ON_INTRUSION is configured to either DISABLE_AND_TRAP or TRAP_ONLY.)

Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for detailed information about the Security Module features.

SET SECURITY PORT SECURITY_TYPE

Use the SET SECURITY PORT SECURITY_TYPE command to define the security type for ports on the 8250 10BASE-T Security Module (E12MSS).

Format

SET SECURITY PORT {slot.port} SECURITY_TYPE {type}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 12 or all

{type} = eavesdropping_only
intrusion_only
full (default)

Example

The following example configures port 2 on the Security Module in slot 3 for the security type eavesdropping_only.

```
8250> set security port 3.2 security_type
eavesdropping_only   [ENTER]

Port 03.02 security mode set to EAVESDROPPING_ONLY.
```

Description

The security types are described briefly on the next page. Refer to the *8250 10BASE-T Security Module Installation and Operation Guide* for complete information on the Security Module and its features.

Eavesdroppping Security - Allows the Security Module to deliver packets only to the end station to which a packet is addressed. This feature prohibits unauthorized end stations from listening (eavesdropping) on packets that are not specifically addressed to them. The *Eavesdropping_only* option defines the security type as eavesdropping only, which does not include Intrusion Control.

Intrusion Control - Allows the Security Module to prevent delivery of packets transmitted from unauthorized stations on the network. If a port receives a packet from its end station which contains an invalid source-address, the Security Module forces a collision. The collision prevents intruding end stations from gaining access to a port and transmitting unauthorized data over the network. The *Intrusion_only* option defines the security type as Intrusion only, which does not include Eavesdropping security. Intrusion Control also provides you with the ability to define on a per-port basis the corrective action an EMM is to take when a port experiences a security intrusion attempt. Refer to the SET SECURITY PORT ACTION_ON_INTRUSION command for information on defining port action.

Full - Defines both Eavesdropping Security and Intrusion Control security features for the specified port.

Note: The SET SECURITY PORT SECURITY_TYPE and the SET SECURITY PORT MODE ENABLE commands work in conjunction with each other. Security type is automatically configured to *Full* when you issue the SET SECURITY PORT MODE ENABLE command. Security Mode is automatically *enabled* when you issue the SET SECURITY PORT SECURITY_TYPE command.

SET TERMINAL AUXILIARY BAUD

Use the SET TERMINAL AUXILIARY BAUD command to set the transmission data rate for communication over the FMM auxiliary port.

Format

SET TERMINAL AUXILIARY BAUD {baud rate}

Parameters

{baud rate} = 300, 1200, 2400, 4800, 9600, 19200, 38400

Example

The following example specifies a rate of 2400 baud for communication over the module's auxiliary port.

```
8250> set terminal auxiliary baud 2400   [ENTER]
Terminal parameter changed.
```

Description

The SET TERMINAL AUXILIARY BAUD command allows you to establish the appropriate baud rate at which the management module receives and transmits data to your terminal or modem. The factory set baud rate on the FMM is 9600. Before connecting a terminal or modem to the FMM, check the baud rate of the designated terminal or modem. A device and the FMM must be set at the same baud rate in order to communicate.

Therefore, once you change the baud rate of your FMM, you will lose connection with the terminal you used to make that change. To resume operation, reconnect the FMM to a device operating under the new baud rate for which the FMM is configured.

Note: When using higher baud rates (19200 and 38400), be sure to enable Xon/Xoff flow control on the terminal.

SET TERMINAL AUXILIARY DATA_BITS

Use the SET TERMINAL AUXILIARY DATA_BITS command to establish the number of data bits for communication over the FMM auxiliary port.

Format

SET TERMINAL AUXILIARY DATA_BITS {data bits}

Parameters

{data bits} = 7 or 8

Example

The following example specifies that seven data bits be used for communication over the FMM auxiliary port.

```
8250> set terminal auxiliary data_bits 7     [ENTER]
Terminal parameter changed.
```

Description

The SET TERMINAL AUXILIARY DATA_BITS command allows you to set the data bits level according to the requirements of the attached device (for example, terminal or modem). The factory default for this command is 8 data bits.

If your terminal or modem and the FMM do not have the same data bit setting, you may not be able to log into the system.

SET TERMINAL AUXILIARY PARITY

Use the SET TERMINAL AUXILIARY PARITY command to establish parity for communication over the FMM auxiliary port.

Format

SET TERMINAL AUXILIARY PARITY {parity}

Parameters

{parity} = even
odd
none

Example

The following example specifies that *even* parity be used for communication over the FMM auxiliary port.

```
8250> set terminal auxiliary parity even   [ENTER]
Terminal parameter changed.
```

Description

The SET TERMINAL AUXILIARY PARITY command allows you to set the parity according to the requirements of the attached device (for example, terminal or modem). The default for this command is *none*.

If your terminal or modem and the FMM do not have the same parity setting you will not be able to log into the system.

SET TERMINAL AUXILIARY STOP_BITS

Use the SET TERMINAL AUXILIARY STOP_BITS command to establish the number of stop bits between characters when communicating over the FMM's auxiliary port.

Format

SET TERMINAL AUXILIARY STOP_BITS {stop bits}

Parameters

{stop bits} = 1 or 2 (default is 2)

Example

The following example identifies that 1 stop bit be used for communication over the FMM auxiliary port.

```
8250> set terminal auxiliary stop_bits 1   [ENTER]
Terminal parameter changed.
```

Description

Stop bits signal the end of a character being received and the beginning of an idle state. The FMM is factory-set to use 2 stop bits when communicating over the auxiliary port.

SET TERMINAL AUXILIARY TERMINAL_TYPE

Use the SET TERMINAL AUXILIARY TERMINAL_TYPE command to define the terminal type you are using with an FMM.

Format

SET TERMINAL AUXILIARY TERMINAL_TYPE {type)

Parameters

{type} = terminal type (maximum of 40 characters)

Example

The following example defines the auxiliary terminal type as a VT100 terminal:

```
8250> set terminal auxiliary terminal_type   [ENTER]
Enter terminal type:   vt100   [ENTER]
Terminal parameter changed.
```

Description

Defining a terminal type is useful when performing an outbound Telnet session. The terminal type is sent to the device which is connected to the FMM during the Telnet session. Defining a terminal type enables the device to send the proper control sequences to the FMM, which are displayed on the FMM's terminal.

SET TERMINAL BAUD

Use the SET TERMINAL BAUD command to set the transmission data rate between your terminal and the management module.

Format

SET TERMINAL BAUD {baud rate}

Parameters

{baud rate} = 300, 1200, 2400, 4800, 9600 (default is 9600)

Example

The following example changes the baud rate to 2400 baud.

```
8250> set terminal baud 2400      [ENTER]
```

Description

The SET TERMINAL BAUD command allows you to establish the appropriate baud rate at which the management module receives and transmits data to your terminal or modem. The default baud rate on the management module is 9600 baud. Check the baud rate of the device before connecting a terminal or modem to the management module.

You must set your device and the management module to the same baud rate in order to communicate.

To connect a terminal or modem that is set to a different baud rate than the management module, change the management module factory default baud rate from 9600 to the new value as follows:

1. Set a terminal to 9600 baud and press [ENTER] to get access to the management module.

2. Issue the SET TERMINAL BAUD command to set the baud rate to your specifications. Once you set this lower rate, you lose your connection to the management module.

3. Remove the terminal connection and connect the device that has the lower baud rate to resume your connection to the management module.

4. Issue the SAVE TERMINAL command to save the new terminal setting.

SET TERMINAL CONSOLE BAUD

Use the SET TERMINAL CONSOLE BAUD command to set the transmission data rate between your terminal and an FMM or TRMM.

Format

SET TERMINAL CONSOLE BAUD {baud rate}

Parameters

{baud rate} = 300, 1200, 2400, 4800, 9600, 19200, 38400
(default is 9600)

Example

This example changes the baud rate to 2400 baud.

```
8250> set terminal console baud 2400      [ENTER]
```

Description

The SET TERMINAL CONSOLE BAUD command allows you to establish the appropriate baud rate at which an FMM or TRMM receives and transmits data to your terminal or modem. The default baud rate on the FMM or TRMM is 9600 baud. Check the baud rate of the device before connecting a terminal or modem to the FMM or TRMM.

Set your device and the FMM or TRMM to the same baud rate in order to communicate.

SET TERMINAL CONSOLE DATA_BITS

Use the SET TERMINAL CONSOLE DATA_BITS command to establish the number of data bits accepted by your terminal when it communicates with an FMM or TRMM.

Format

SET TERMINAL CONSOLE DATA_BITS {data bits}

Parameters

{data bits} = 7 or 8

Example

This command sets the number of data bits to 7.

```
8250> set terminal console data_bits 7     [ENTER]
```

Description

The SET TERMINAL CONSOLE DATA_BITS command allows you to set the data bits level according to your terminal requirements. The factory default value is 8 data bits.

If your terminal or modem and an FMM or TRMM do not have the same data bit setting you will not be able to log into the system.

SET TERMINAL CONSOLE HANGUP

Use the SET TERMINAL CONSOLE HANGUP command to terminate a modem connection from an FMM or TRMM. When this command is enabled and you log out, the modem disconnects automatically.

Format

SET TERMINAL CONSOLE HANGUP {setting}

Parameters

{setting} = disable (default)
enable

Example

```
8250> set terminal console hangup disable     [ENTER]
```

Description

If TERMINAL CONSOLE HANGUP is enabled when you log out of an FMM or TRMM using a modem connection, the modem is automatically disconnected. The modem is also disconnected if this setting is enabled and you leave your terminal unattended for the amount of time established by the terminal TIMEOUT command.

The default value is *disabled*. If this command is disabled, the modem is disconnected only when you manually hang up the modem.

Note: If you fail to hang up the modem connection, an unauthorized user may pick up the last login session.

SET TERMINAL CONSOLE PARITY

Use the SET TERMINAL CONSOLE PARITY command to establish the parity setting to use when communicating between your terminal and an FMM or TRMM.

Format

SET TERMINAL CONSOLE PARITY {parity}

Parameters

{parity} = even
none
odd

Example

```
8250> set terminal console parity even      [ENTER]
```

Description

The SET TERMINAL CONSOLE PARITY command allows you to set the parity according to your terminal requirements. The default value is NONE.

If your terminal or modem and an FMM or TRMM are not set to the same parity, you can not log into the system.

SET TERMINAL CONSOLE STOP_BITS

Use the SET TERMINAL CONSOLE STOP_BITS command to establish the number of stop bits between characters when communicating between your terminal and an FMM or TRMM.

Format

SET TERMINAL CONSOLE STOP_BITS {stop bits}

Parameters

{stop bits} = 1 or 2 (default is 1)

Example

```
8250> set terminal console stop_bits 1        [ENTER]
```

Description

The FMM or TRMM is factory set to 1 stop bit to signal the end of a character being received and to reset the line to an idle state. The SET TERMINAL CONSOLE STOP_BITS command allows you to set the stop bits value to 1 or 2 bits.

SET TERMINAL CONSOLE TERMINAL_TYPE

Use the SET TERMINAL CONSOLE TERMINAL_TYPE command to define the terminal type you are using with an FMM or TRMM.

Format

SET TERMINAL CONSOLE TERMINAL_TYPE {type)

Parameters

{type} = terminal type (maximum of 40 characters)

Example

The following command defines the terminal type as a VT100 terminal:

```
8250> set terminal console terminal_type   [ENTER]
Enter terminal type:   vt100   [ENTER]
Terminal parameter changed.
```

Description

Defining a terminal type is useful when performing an outbound Telnet session. The terminal type is sent to the device which is connected to the FMM or TRMM during the Telnet session. This setting enables the device to send the proper control sequences to the FMM or TRMM, which are displayed on the FMM or TRMM terminal.

SET TERMINAL DATA_BITS

Use the SET TERMINAL DATA_BITS command to establish the number of data bits accepted by your terminal when it communicates with the management module.

Format

SET TERMINAL DATA_BITS {data bits}

Parameters

{data bits} = 7 or 8

Example

This command sets the number of data bits to 7.

```
8250> set terminal data_bits 7     [ENTER]
```

Description

The SET TERMINAL DATA_BITS command allows you to set the data bits level according to your terminal requirements. The factory default value is 8 data bits.

If your terminal or modem and the management module do not have the same data bit setting, you cannot log into the system.

SET TERMINAL HANGUP

Use the SET TERMINAL HANGUP command to terminate a modem connection. When this command is enabled and you log out, the modem is disconnected automatically.

Format

SET TERMINAL HANGUP {setting}

Parameters

{setting} = disable (default)
enable

Example

```
8250> set terminal hangup disable      [ENTER]
```

Description

If TERMINAL HANGUP is enabled when you log out of the management module using a modem connection, the modem is automatically disconnected. The modem is also disconnected if this setting is enabled and you leave your terminal unattended for the amount of time established by the terminal TIMEOUT command.

The default value is *disabled*. If this command is disabled, the modem is disconnected only when you manually hang up the modem.

Note: If you fail to hang up the modem connection, an unauthorized user may pick up the last login session.

SET TERMINAL PARITY

Use the SET TERMINAL PARITY command to establish the parity setting to use when communicating between your terminal and the management module.

Format

SET TERMINAL PARITY {parity}

Parameters

{parity} = even
none
odd

Example

```
8250> set terminal parity even      [ENTER]
```

Description

The SET TERMINAL PARITY command allows you to set the parity according to your terminal requirements. The default value is NONE.

If your terminal or modem and the management module do not have the same parity setting, you cannot log into the system.

SET TERMINAL PROMPT

Use the SET TERMINAL PROMPT command to customize the management prompt that displays on your terminal when connected to a particular management module.

Format

SET TERMINAL PROMPT {prompt}

Parameters

{prompt} = terminal prompt up to 15 characters (default 8250)

Example

This command sets the new prompt for a TRMM to “TRMM1> ”.

```
8250> set terminal prompt TRMM1>      [ENTER]
```

A space is automatically appended to the prompt entered. This causes a space between the angle bracket and the beginning of the command as shown below using the SET command.

```
TRMM1> set
```

Description

The default prompt for all 8250 management modules is “8250> ”. The SET TERMINAL PROMPT command allows you to customize this prompt with a string of 15 alphanumeric characters in length. When using this command, you must include all the characters you want to appear in the new prompt, including the angle bracket (>).

IBM recommends that you make the terminal prompt and the device name the same for each individual management module. If you are remotely connected to a device, the prompt indicates that there is a remote connection established.

SET TERMINAL STOP_BITS

Use the SET TERMINAL STOP_BITS command to establish the number of stop bits between characters when communicating between your terminal and the management module.

Format

SET TERMINAL STOP_BITS {stop bits}

Parameters

{stop bits} = 1 or 2 (default is 1)

Example

```
8250> set terminal stop_bits 1        [ENTER]
```

Description

The management module is factory set to 1 stop bit to signal the end of a character being received and to reset the line to an idle state. The SET TERMINAL STOP_BITS command allows you to set the stop bits value to 1 or 2 bits.

SET TERMINAL TERMINAL_TYPE

Use the SET TERMINAL TERMINAL_TYPE command to define the terminal type you are using.

Format

SET TERMINAL TERMINAL_TYPE {type}

Parameters

{type} = terminal type (maximum of 40 characters)

Example

The following command defines the terminal type as a VT100 terminal.

```
8250> set terminal terminal_type vt100  [ENTER]
Terminal type changed.
```

Description

Defining a terminal type is useful when performing an outbound Telnet session. The terminal type is sent to the device which is connected to the TRMM during the Telnet session. This setting enables the device to send the proper control sequences to the TRMM, which are displayed on the TRMM terminal.

SET TERMINAL TIMEOUT

Use the SET TERMINAL TIMEOUT command to enable the management module to automatically log you out of the system if no typing has been performed at the terminal during a specified period of time.

Format

SET TERMINAL TIMEOUT {minutes}

Parameters

{minutes} = minutes from 1 to 30
0 (zero for no timeout)

Example

This command logs you out of the system if your terminal is unattended for more than 10 minutes.

```
8250> set terminal timeout 10       [ENTER]
```

The following message is displayed if changes are not saved before the timeout occurs:

```
Warning: Unsaved changes.
Bye
```

Unsaved changes remain set, but are lost if the management module is reset. You must re-establish connection to the management module to SAVE the changes.

Description

The SET TERMINAL TIMEOUT command allows you to set the amount of time that your terminal may be unattended before you are logged out of the system. The acceptable values are from 1 to 30 minutes or 0, which means no timeout. The default value is 0.

Once TIMEOUT has been set, you are given that amount of time in which to respond to a screen prompt. If you do not respond within the set

amount of time, the word “Timeout!” is displayed, the terminal beeps, and you are logged out of the system.

The MONITOR command is not interrupted by this command.

Note: If a modem is attached and the HANGUP command is enabled, the modem is also disconnected during a timeout.

SET TFTP FILE_NAME

Use the SET TFTP FILE_NAME command to specify the name of the file to be used for the download.

Format

SET TFTP FILE_NAME {file name}

Parameters

{file name} = full pathname up to 128 characters

Example

The following command specifies that the file **trmf.bin** in the directory **trmmsoft** on the c: drive should be used to perform inband downloads.

```
8250> set tftp file_name  [ENTER]
Enter tftp file name: /trmmsoft/trmf.bin
Tftp file name changed.
```

Description

This command enables you to specify the filename to be used for inband download. It is used in conjunction with the SET TFTP SERVER_IP_ADDRESS and SET TFTP FILE_TYPE commands. The name you enter is free format up to 128 alphanumeric characters. The management module assumes a default pathname of /tftpboot unless otherwise specified.

You must enter the TFTP filename within 10 seconds or the command times out. If this happens, simply re-enter the command.

To set the TFTP filename permanently, use the SAVE TFTP command. Use the SHOW TFTP command to display the TFTP parameter settings.

SET TFTP FILE_TYPE

Use the SET TFTP FILE_TYPE command to specify whether you want to download ascii from a script file, or new boot or flash code. Use this command for inband downloads.

Format

SET TFTP FILE_TYPE {parameter}

Parameters

{parameter} = ascii
boot
flash

Example

The following command specifies that the flash code file is to be used for the inband download.

```
8250> set tftp file_type flash     [ENTER]
tftp file set to flash.
```

Description

This command enables you to specify the file type to be used for inband download. The ASCII option enables you to download a script file. Note that the first line of the script file must be a header containing the following information:

SCRIPT {script name} {script number}. The script name and number are optional, but you must enter SCRIPT in uppercase letters.

The boot code file is used to update the Boot EPROM. The flash code file is used to update the Flash EPROM. This command is used in conjunction with the SET TFTP SERVER_IP_ADDRESS and SET TFTP FILE_NAME commands.

SET TFTP SERVER_IP_ADDRESS

Use the SET TFTP SERVER_IP_ADDRESS command to specify the ip address of the server that contains the download file used for inband download.

Format

SET TFTP SERVER_IP_ADDRESS {ip address}

Parameters

{ip address} = n.n.n.n

Example

The following command specifies the server with the ip address 125.36.58.117 to be used for the inband download.

```
8250> set tftp server_ip_address 125.36.58.117  [ENTER]
Tftp server IP address set.
```

Description

This command enables you to specify the IP address of the server that contains the download file. It is used in conjunction with the SET TFTP FILE_TYPE and SET TFTP FILE_NAME commands.

Use the SHOW TFTP command to display the TFTP parameter settings.

SET THRESHOLD ACTION

Use the SET THRESHOLD ACTION command to define the corrective action the TRMM is to take when a threshold has been exceeded. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} ACTION {action} {script number}

Parameters

{action} = script_only {script number}
script_trap {script number}
trap_only (default)

{index} = 1 through 10
all

Example

The following command allows the TRMM to send a trap when threshold 1 has been exceeded.

```
8250> set threshold 1 action trap_only [ENTER]

Index:                      1
Mode:                       DISABLED
Description:
Action:                     TRAP ONLY: script number N/A
Data Source:                (not initialized)
Threshold Value:            8
Current Value:              —-
Interval:                   6790:15:28
Time Since Last Triggered: (never)
```

Description

This command enables you to define the corrective action a TRMM is to take when a threshold has been exceeded.

The action options include:

Script_only - Instructs the TRMM to run a specific script.

Script_trap - Instructs the TRMM to run a specific script and send a trap to the management workstation.

Trap_only - Instructs the TRMM to send a trap only.

SET THRESHOLD DESCRIPTION

Use the SET THRESHOLD DESCRIPTION command to enter a one-line description of the threshold entry. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} DESCRIPTION {description}

Parameters

{index} = 1 through 10
all

Example

```
8250> set threshold 1 description   [ENTER]


Enter a description for the threshold:
> This threshold is set for network frames. [ENTER]

Description changed.
Index:                      1
Mode:                       Enabled
Description:                This threshold is set for network
                            frames
Action:                     TRAP_ONLY Script number N/A
Data Source:                Network Frames
Threshold Value:            1000
Current Value:              —-
Interval:                   0:01:00
Time Since Last Triggered: (never)
```

Description

This command enables you to enter a one-line description of 40 characters to describe the variable for which thresholding is set.

SET THRESHOLD INTERVAL

Use the SET THRESHOLD INTERVAL command to specify the time interval for which a thresholding entry is to be monitored. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} INTERVAL {interval}

Parameters

{index} = 1 through 10
all

{interval} = hours
minutes
seconds

Example

The following example specifies that the number of network frames at the *end* of each 2-minute interval is subtracted from the number of network frames at the *beginning* of the 2-minute interval. The resulting number is compared to the value specified in the SET THRESHOLD VALUE command to ensure that the threshold has not been exceeded.

```
8250> set threshold 1 interval 2 minutes  [ENTER]

Interval changed.
Index:                      2
Mode:                       Disabled
Description:                This threshold is for network frames
Action:                     TRAP_ONLY Script number N/A
Data Source:                Network Frames
Threshold Value:            1000
Current Value:              —-
Interval:                   00:02:00
Time Since Last Triggered: (never)
```

Description

This command enables you to specify the time interval between thresholding samples. Once a variable is defined and threshold values are set and enabled, the TRMM monitors that variable at the end of each threshold interval.

The minimum interval is five seconds and the maximum is 24 hours.

SET THRESHOLD MODE

Use the SET THRESHOLD MODE command to enable or disable the thresholding feature. This command is available for the Advanced TRMM only.

Format

SET THRESHOLD MODE {index} {setting}

Parameters

{index} = 1 through 10
all

{setting} = disable
enable

Example

The following example enables thresholding for index 3.

```
8250> set threshold 3 mode enable  [ENTER]

Index:                          3
Mode:                           ENABLED
Description:
Action:                         TRAP_ONLY Script number N/A
Data Source:                    Network TOKEN_RING_1 : Frames
Threshold Value:                1000
Current Value:                  —-
Interval:                       0:01:00
Time Since Last Triggered:      (never)
```

Description

This command allows you to enable or disable the thresholding feature for a specific threshold index. You must set all thresholding parameters (that is, variable, value, interval, description) before you can enable the thresholding feature. If you attempt to enable the thresholding feature prior to setting the proper parameters, a warning is displayed instructing you to supply the missing information.

SET THRESHOLD NETWORK

Use the SET THRESHOLD NETWORK command to define the network variable on which to set a threshold. This command also enters the variable as an index entry in the threshold table. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} NETWORK {variable}

Parameters

{index} = 1 through 10
all

{variable} = broadcast_frames
frames
hard_errors
multicast_frames
octets
soft_errors

Example

The following command set a threshold for network frames for index entry 1.

```
8250> set threshold 1 network frames  [ENTER]

Index:                          1
Mode:                           DISABLED
Description:
Action:                         TRAP_ONLY Script number N/A
Data Source:                    Network TOKEN_RING_1 : Frames
Threshold Value:                0
Current Value:                  —-
Interval:                       0:01:00
Time Since Last Triggered:      (never)
```

Description

This command enables you to set a threshold on a network variable and enter this threshold in the threshold table. Descriptions of the network variables are explained in the following table.

Field	Description
Broadcast_frames	The number of frames sent to the broadcast address, which are received by all stations.
Frames	The number of frames on the network.
Hard_errors	The number hard errors on the network. Hard errors are fatal errors that require beacon recovery.
Multicast_frames	The number of multicast frames on the network.
Octets	The number of octets on the network.
Soft_errors	The number of soft errors on the network. Soft errors are errors that are recoverable by the MAC layer protocol. Soft errors include: line errors, burst errors, lost frame errors, ARI/FCI set errors, frame copy errors, receive congestion errors, and token errors.

SET THRESHOLD PORT

Use the SET THRESHOLD PORT command to define the port variable on which to set a threshold. This command also requires you to specify the index number of the variable, which is entered in the threshold table. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} PORT {slot.port} {variable}

Parameters

{index} = 1 through 10
all

{slot} = 1 through 17

{port} = 1 through 20

{variable} = broadcast_frames
errors
frames
multicast_frames
octets

Example

The following command sets a threshold for port frames for port 1 of the module in slot 14 and defines this entry as index 1 in the threshold table.

```
8250> set threshold 1 port 14.1 frames [ENTER]

Index:                       1
Mode:                        DISABLED
Description:
Action:                      TRAP_ONLY Script number N/A
Data Source:                 Port 14.1 : Frames
Threshold Value:             0
Current Value:               —-
Interval:                    0:01:00
Time Since Last Triggered: (never)
```

Description

This command enables you to set a threshold on a port variable and to enter this threshold in the threshold table.

SET THRESHOLD STATION

Use the SET THRESHOLD STATION command to define the station variable on which to set a threshold. This command also enters the variable as an index entry in the threshold table. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} STATION {mac address} {variable}

Parameters

{index} = 1 through 10
all

{mac address} = mac address

{variable} = broadcast_frames
errors
frames
multicast_frames
octets

Example

The following command sets a threshold for station errors for index entry 7.

```
8250> set threshold 7 station 10-00-F1-0F-0C-6F
errors [ENTER]

Index:                        7
Mode:                         DISABLED
Description:
Action:                       TRAP_ONLY Script number N/A
Data Source:                  Station 10-00-f1-0f-0c-6f:Errors
Threshold Value:              2000
Current Value:                —-
Interval:                     0:01:00
Time Since Last Triggered:    (never)
```

Description

This command enables you to set a threshold on a station variable, and enter this threshold in the threshold table.

SET THRESHOLD VALUE

Use the SET THRESHOLD VALUE command to define the threshold value to which the difference between the count at the end of the interval and the count at the beginning of the interval are compared. This command is available for the TRMM Advanced only.

Format

SET THRESHOLD {index} VALUE {value}

Parameters

{index} = 1 through 10

{value} = numeric value

Example

The following command sets a threshold value of 1000. In this example, index 5 is a thresholding entry for network frames, with an interval of 2 minutes.

```
8250> set threshold 5 value 1000 [ENTER]

Index:                          5
Mode:                           DISABLED
Description:
Action:                         TRAP_ONLY Script number N/A
Data Source:                    Network TOKEN RING 1:Frames
Threshold Value:                1000
Current Value:                  —-
Interval:                       0:02:00
Time Since Last Triggered:      (never)
```

Description

This command enables you set the threshold value to which the ending and beginning variable counters are compared.

The above example specifies that the number of network frames at the *end* of every 2-minute interval are subtracted from the number of network frames at the *beginning* of the 2-minute interval. This value is compared to the threshold value specified in the SET THRESHOLD VALUE command. If this number is greater than the defined threshold value, a trap is sent.

SET TRUNK RING_IN/RING_OUT CABLE_MONITOR

Use the SET TRUNK RING_IN CABLE_MONITOR and the SET TRUNK RING_OUT CABLE_ MONITOR commands to enable or disable cable monitor mode on the copper Ring In and/or Ring Out ports on Token Ring modules.

Format

SET TRUNK {slot} RING_IN.{trunk port} CABLE_MONITOR {setting}

SET TRUNK {slot} RING_OUT.{trunk port} CABLE_MONITOR {setting}

Parameters

{slot} = 1 through 17

{trunk port} = 1 or 2 (only required on the T02MS-FIB Module)

{setting} = disable
enable

Examples

Example 1

The following command enables cable monitor mode for the Ring In port of the Token Ring Fiber Repeater Module in slot 5 of the hub.

```
8250> set trunk 5 ring_in.1 cable_monitor enable [ENTER]
Cable Monitor set to ENABLED.
```

Example 2

The following command enables cable monitor mode for the Ring Out port of the MAU Module in slot 3 of the hub.

```
8250> set trunk 3 ring_out cable_monitor enable [ENTER]
Cable Monitor set to ENABLED.
```

Description

Use this command to enable or disable cable monitor mode for the copper Ring In and/or Ring Out ports on Token Ring modules. This mode sets the ports so they wrap the ring to keep it up and running if the module senses a cable fault. For this mode to work, you must use the IBM 43G3873 or 43G3874 cable to connect the hub ports.

Cable monitor mode should be enabled *only* when connecting Ring In and Ring Out ports of Token Ring modules in the same hub. Cable monitor mode should be *disabled* when connecting to non-IBM modules.

Note: Cable Monitor mode can be enabled 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, 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.

SET TRUNK RING IN /RING OUT EXTERNAL_BEACON_RECOVERY

Devices that do not support beacon recovery (for example, IBM 8228) may cause a multi-hub ring to segment at all Ring In and Ring Out 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 management module that the device does not support beacon recovery, and enables the management module to isolate the beaconing device. Failure to designate a device that does not support beacon recovery could cause the entire ring to segment if beaconing occurs on that device.

Format

SET TRUNK {slot} RING_IN {trunk port} EXTERNAL_BEACON_ RECOVERY {setting}

SET TRUNK {slot} RING_OUT {trunk port} EXTERNAL_BEACON_ RECOVERY{setting}

Parameters

{slot} = 1 through 17

{trunk port} = 1 or 2 (only required on the T02MS-FIB Module)

{setting} = exists
non_exists (default)

Examples

In this example, a T02MS-FIB in slot 3 of 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, issue the following command:

```
8250> set trunk 3 ring_in.1 external_beacon_recovery
non_exists [ENTER]

External beacon recovery set to non_exists.
```

Description

When using TRMMs in a multi-hub ring having segments connected to devices that do not support beacon recovery, hubs may segment when a beaconing condition occurs.

When a beaconing condition occurs, TRMMs wrap segments in order to isolate a beaconing device. The TRMMs then unwrap the segments to verify that the beaconing condition is resolved. If a device continues to beacon, the TRMMs wraps the segments permanently, causing the ring to segment.

Designating devices that do not support beacon recovery informs the TRMM of the existence of these devices, thus enabling the TRMM to partition only the beaconing device, rather than the entire ring. Once the trunk connected to the beaconing device has been wrapped, the TRMM unwraps all other segments in the ring and restores ring functionality.

Trunks connected to devices that do perform beacon recovery (for example, 8250 Multiprotocol Intelligent Hubs with TRMMs as master) should have this parameter set to *exists*.

SET TRUNK RING_IN/RING_OUT COMPATIBILITY_MODE

Use the SET TRUNK RING_IN COMPATIBILITY_MODE and the SET TRUNK RING_OUT COMPATIBILITY_ MODE commands to enable or disable IBM 8230 Compatibility Mode on the fiber Ring In or Ring Out trunks on the Token Ring Fiber Repeater Module.

Format

SET TRUNK {slot} RING_IN.1 COMPATIBILITY_ MODE {setting}

SET TRUNK {slot} RING_OUT.1 COMPATIBILITY_ MODE {setting}

Parameters

{slot} = 1 through 17

{setting} = disable
enable

Example

The following commands enable Compatibility Mode for the fiber Ring In and Ring Out trunks of the Token Ring Fiber Repeater Module in slot 3 of the hub.

```
8250> set trunk 3 ring_in.1 compatibility_mode enable
Compatibility mode set to ENABLED.
8250> set trunk 3 ring_out.1 compatibility_mode enable
Compatibility mode set to ENABLED.
```

Description

Use these commands to enable or disable Compatibility Mode on the Token Ring Fiber Repeater Module. When enabled, this mode provides compatibility between the fiber trunks on the Token Ring Fiber Repeater Module and the fiber trunks on an IBM 8230 Controlled Access Unit (CAU).

You must *enable* Compatibility Mode when connecting a Fiber Repeater Module to an IBM 8230 CAU using the fiber Ring In and Ring Out trunks.

You must *disable* Compatibility Mode when connecting the module to another Fiber Repeater Module.

Refer to the appropriate Token Ring Fiber Repeater Module documentation for more information about Compatibility Mode.

SET TRUNK RING_IN/RING_OUT MODE

Use the SET TRUNK RING_IN MODE and the SET TRUNK RING_OUT MODE commands to enable or disable the Ring In and Ring Out ports on Token Ring Modules.

Format

SET TRUNK {slot} RING_IN.{trunk port} MODE {setting}

SET TRUNK {slot} RING_OUT.{trunk port} MODE {setting}

Parameters

{slot} = 1 through 17

{trunk port} = 1 or 2 (only required on the T02MS-FIB Module)

{setting} = disable
enable

Example

The following commands enable the Ring In and Ring Out ports of the TRMM in slot 5 of the hub.

```
8250> set trunk 5 ring_in mode enable       [ENTER]
Trunk 05 ring_in set to ENABLED.
8250> set trunk 5 ring_out mode enable       [ENTER]
Trunk 05 ring_out set to ENABLED.
```

Description

Use these commands to enable or disable the Ring In and Ring Out ports on Token Ring Modules. Enabling the Ring In and Ring Out ports allows you to add a module to the ring.

Refer to the specific Token Ring Installation Guide for more information on Ring In and Ring Out ports.

SET TRUNK RING_IN/RING_OUT MODE REDUNDANT

Use the SET TRUNK RING_IN MODE REDUNDANT and the SET TRUNK RING_OUT MODE REDUNDANT commands to enable or disable trunk fault tolerance on the T02MS-FIB module.

Format

SET TRUNK {slot} RING_IN.{trunk port} MODE {setting}

SET TRUNK {slot} RING_OUT.{trunk port} MODE {setting}

Parameters

{slot} = 1 through 17

{trunk port} = 1 or 2

{setting} = redundant
non_redundant

Example

The following command shows how to establish trunk redundancy on Ring_In.1 between the T02MS-FIB modules in slots 1 and 3:

```
8250> set trunk 1 ring_in.1 mode redundant 3
```

In the example, the module in:

- Slot 1 is the primary trunk and is enabled.
- Slot 3 is the redundant trunk and is disabled.

If the module in slot 1 fails or if the Ring-In trunk fails, the TRMM:

- Enables the redundant trunk on the module in slot 3 (making the module in slot 3 the primary trunk)
- Disables the trunk on the module in slot 1

In addition to enabling the redundant trunk and disabling the primary trunk, the TRMM also performs the following functions to ensure ring integrity. Ring integrity prevents the ring from segmenting.

1. Because the module in slot 3 may not have a valid connection, the TRMM monitors the trunk for 10 seconds.
2. If the trunk has not established a valid connection, the TRMM switches between the primary and redundant trunks every 10 seconds until a valid connection is established.
3. Once the TRMM establishes a valid connection, the trunk remains enabled until a failure condition occurs.

Note: If both the Ring-In and Ring-Out fiber trunks on the module in slot 1 are configured to be redundant with the module in slot 3 and a failure occurs on the Ring-In trunk only, a switchover does not occur.

4. The T02MS-FIB module still performs a wrap on the failed Ring-In trunk to maintain the integrity of the ring.

Description

The TRMM fiber trunk redundancy feature:

- Allows you to configure redundant trunks using the fiber Ring-In and Ring-Out trunks on two different T02MS-FIB modules in a hub
- Provides full redundancy for the T02MS-FIB fiber trunks

You can configure redundancy on one or both of the Ring-In and Ring-Out fiber trunks. Once you establish a redundant trunk, it becomes active only when the primary trunk fails. The TRMM supports trunk redundancy only for modules that reside in the same hub.

Note: If both the Ring-In and the Ring-Out fiber trunks on the same module are configured for redundancy, a switchover occurs only when *both* trunks fail. This feature prevents the ring from segmenting.

Warning: When you configure redundancy using the *Ring-In* fiber trunk of a primary T02MS-FIB module, ensure that you connect the corresponding *Ring-In* fiber trunk of the redundant module to another T02MS-FIB module.

Warning: When you configure redundancy using the *Ring-Out* fiber trunk of a primary T02MS-FIB module, ensure that you connect the corresponding *Ring-Out* fiber trunk of the redundant module to another T02MS-FIB module.

The TRMM protects the network from ring segmentation by preventing you from configuring the Ring-In and Ring-Out fiber trunks on the same T02MS-FIB module to be both primary and redundant. If you attempt to configure one trunk for primary and one trunk for redundancy on the same module (an invalid configuration), an error message displays and the command is aborted.

Refer to the *8250 TRMM User's Guide* for more information on fiber trunk redundancy.

SET TRUNK RING_IN NETWORK_MAP

Use the SET TRUNK RING_IN 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.

Format

SET TRUNK {slot} RING_IN.{trunk port} NETWORK_MAP {setting}

Parameters

{slot} = 1 through 17

{trunk port} = 1 or 2 (only required on the T02MS-FIB Module)

{setting} = external
internal

Example

The following command sets the Ring In port of the TRMM in slot 5 to an internal network map, meaning that this port is connected to another trunk port in the same hub.

```
8250> set trunk 5 ring_in network_map internal       [ENTER]
Network map state set to INTERNAL.
```

Description

Use this command to enable or disable the Network Map feature between copper trunk ports on Ring In ports on Token Ring modules. When two copper trunk ports are connected between two hubs, you must set NETWORK MAP to EXTERNAL. When two copper trunks are connected within a hub (for example, a TRMM to a T08MS-RJ45S), the network map must be configured to Internal so that port to address mapping is correct.

SHOW ALERT

Use the SHOW ALERT command to list the current alert settings for the management module.

Format

SHOW ALERT

Parameters

none

Example

Example 1

The following example displays alert settings for an EMM.

```
8250> show alert        [ENTER]

Alert AUTHENTICATION  set to ENABLED
Alert CHANGE          set to ENABLED
Alert HELLO           set to ENABLED
Alert PORT_UP_DOWN    set to ENABLED
Alert SCREEN           set to ENABLED
```

Example 2

This example displays alert settings for an FMM.

```
8250> show alert [ENTER]

Alert AUTHENTICATION set to ENABLED
Alert CHANGE          set to ENABLED
Alert CONSOLE_DISPLAY set to ENABLED
Alert HELLO           set to ENABLED
Alert PORT_FILTER     set to ENABLED
```

Description

This command displays the current alert settings for the management module. The settings are described in the SET ALERT command section.

SHOW BOOTP

Use the SHOW BOOTP command to display a TRMM's current BootP configuration settings.

Format

SHOW BOOTP

Parameters

none

Example

```
8250> show bootp        [ENTER]

——- BOOTP VARIABLES ——-
BootP Server IP address: 127.36.58.53
BootP Power Up Mode:     enabled
BootP Result:            Okay
```

Description

This command displays the current BootP configuration settings for a TRMM.

SHOW CLOCK

Use the SHOW CLOCK command to display the current time, date, and day.

Format

SHOW CLOCK

Parameters

none

Example

The following command displays the current clock setting.

```
8250> show clock          [ENTER]

Clock is set to 05:53 Sun 6 Mar 94
```

Description

This command displays the current time, date, and day.

SHOW COMMUNITY

Use the SHOW COMMUNITY command to list the current community settings for the management module.

Format

SHOW COMMUNITY

Parameters

none

Example

```
8250> show community        [ENTER]

Index   Community Name   IP Address       Access
_____   ______________   _______________ _________

 1      user1            013.024.038.054  Read
 2      ncs              013.024.035.041  All
 3      super            013.024.043.083  Read
 4      admin            013.024.056.098  Read-Write
 5      [empty]
 6      [empty]
 7      [empty]
 8      [empty]
 9      [empty]
 10     [empty]
```

Description

This command displays the current community settings for the management module.

Note: IP Address 127.0.0.1 refers to all IP addresses that can be reached on the network.

SHOW CONCENTRATOR

Use the SHOW CONCENTRATOR command to display information about the hub.

Format

SHOW CONCENTRATOR

Parameters

none

Example

```
8250> show concentrator       [ENTER]

Concentrator Information:

Concentrator Type: 8250-017

Primary power supply status: NORMAL
Backup power supply status: NORMAL
Temperature sensor status:   NORMAL
```

Description

The information that displays is defined below:

Field	Description
Concentrator Type	Indicates whether this is a 8250-006 (6-slot) or 8250-017 (17-slot) hub.
Primary power supply status (Master management module only)	Indicates normal or faulty status.

Field	Description
Backup power supply status (Master management module only)	Indicates normal or faulty status. If a backup power supply is not present, status = REMOVED.
Temperature status (Master management module only)	Indicates normal or overheated temperature status of the hub.

SHOW COUNTER DEVICE

Use the SHOW COUNTER DEVICE command to report error and traffic statistics for the TRMM to which you are currently connected.

Format

SHOW COUNTER DEVICE

Parameters

none

Example

The following example displays counter statistics for a TRMM.

```
8250> show counter device      [ENTER]

MAC Address 10-00-f1-0f-0c-70
ERROR COUNTERS:
           Line Errors:                    0
           Burst Errors:                   3
           Address/Frame Errors:           0
           Lost Frame Errors:              0
           Receive Congestion Errors:      1
           Frame Copy Errors:              0
           Token Errors:                   0
TRAFFIC COUNTERS:
         Inbound Octets:                1218
         Inbound Unicast Packets:          0
         Inbound Non-Unicast Packets:    367
         Inbound Discarded Packets:        0
         Inbound Error Packets:            0
         Outbound Octets:              16708
         Outbound Unicast Packets:         0
         Outbound Non-Unicast Packets:     0
         Outbound Discarded Packets:       0
         Outbound Error Packets:           0
```

Description

This command displays all counters for the TRMM since the last clear or reset. Error and Traffic counters are described in the following tables. For

similar information on other stations, issue the SHOW COUNTER PORT command.

Negative values are displayed when the error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once the counters are reset, correct values are displayed when a subsequent SHOW COUNTER command is issued.

Error Counters	Description
Line Errors	The line error counter is incremented when: **1)** a frame is repeated or copied, *and* **2)** the Error Detected Indicator is zero in the incoming frame, *and* **3)** one of the following conditions exists: a) a code violation between the starting delimiter and ending delimiter of the frame. b) a code violation in a token. c) a Frame Check Sequence error.
Burst Errors	The burst error counter is incremented when a TRMM detects the absence of transitions for five half-bit times between the starting delimiter and ending delimiter, or the ending delimiter and the starting delimiter.
Address/Frame Errors	The address/frame error counter is incremented when: **1)** a TRMM receives an Active Monitor Present (AMP) MAC frame with the address/frame bits equal to zero, *and* **2)** a Standby Monitor Present (SMP) MAC frame with the address/frame bits equal to zero, *or* more than one SMP MAC frame with the address/frame bits equal to zero, without receiving an intervening AMP MAC frame.

Error Counters	Description
Lost Frame Errors	The lost frame error counter is incremented when a TRMM is in transmit (stripping) mode and fails to receive the end of the frame it transmitted.
Receive Congestion Errors	The receive congestion error counter is incremented when an adapter in repeat mode recognizes a frame addressed to it but has no buffer space available to copy the frame.
Frame Copy Errors	The frame copied error counter is incremented when an adapter in receive/repeat mode recognizes a frame addressed to its specific address but finds the ARI bits not equal to zero. This indicates a possible line hit or duplicate address.
Token Errors	The token error counter is active only in the active monitor station. It is incremented when the active monitor detects an error with the token protocol as follows: **1)** the monitor count bit of a token with nonzero priority equals one. **2)** the monitor-count bit of a frame equals one. **3)** no token or frame is received within a 10 ms window. **4)** the starting delimiter/token sequence has a code violation in an area where code violations must not exist.

Traffic Counters	Description
Inbound Octets	The number of packets received by the TRMM that were specifically sent to the TRMM.
Inbound Unicast Packets	The number of packets specifically addressed to the TRMM.
Inbound Non-Unicast Packets	The number of broadcast packets received by the TRMM.
Inbound Discarded Packets	The number of packets received by the TRMM that were discarded. Packets were good but the TRMM discarded because it lacked buffer space.
Inbound Error Packets	The number of packets received by the TRMM that were corrupted (that is, checksum error).
Outbound Octets	The total number of octets transmitted out of the TRMM, including framing characters.
Outbound Unicast Packets	The total number of packets that higher-level protocols transmitted to a subnet-unicast address, including those that were discarded or not sent.
Outbound Non-Unicast Packets	The total number of packets that higher-level protocols transmitted to a non-unicast (that is, a subnet broadcast or subnet multicast) address, including those that were discarded or not sent.
Outbound Discarded Packets	The number of outbound packets chosen to be discarded though no errors have been detected.
Outbound Error Packets	The number of outbound packets that could not be transmitted because of errors.

SHOW COUNTER MODULE

Use the SHOW COUNTER MODULE command to have the EMM or FMM report statistics for all modules or a specified module that is on the current network.

Format

SHOW COUNTER MODULE {slot}

Parameters

{slot} = 1 through 17 or all

Example

Example 1

The following example displays performance statistics for the Ethernet module in slot 5.

```
8250> show counter module 5      [ENTER]

Non-zero counters for network ETHERNET_1 on 16 Dec 93:

Slot       Frames    Bcast      CRC Err   AlignErr Collisions
Time       Octets    Mcast   TooLongErr                Remote
──────────────────────────────────────────────────────────────

 5          47855     1089            0          1           6
15:23:52 17349711     5510            0
```

Description

When you use this command, all counters are displayed since the last clear or reset. You receive an error message that precedes the display if you specify a module that is on a different network than the master module, or a slot number where no module exists.

The information that displays is defined on the following table.

Column	Description
Slot	Slot number of the module from which statistics are being displayed.
Time	Time the report was run in the format: hour, minutes, and seconds.
Frames	Number of good frames received.
Octets	Number of good octets received (1 BYTE = 1 OCTET = 8 BITS).
Bcast	Number of received Broadcast Destination Address Packets.
Mcast	Number of received Multicast Address Packets.
CRC Err	Number of CRC errors received (not including AlignErr).
TooLongErr	Number of too long errors received (packets greater than 1518 bytes).
AlignErr	Number of alignment errors received. Alignment errors indicate CRC errors that do not end on a byte boundary.
Collisions Remote	Number of collisions a port received over the remote network. This counter counts received fragments.

Example 2

The following example displays statistics for the FDDI module in slot 4.

```
8250> show counter module 4          [ENTER]

Slot        Network    BP_Error_Count     MC_Rcv_Error_Count
Time                   BP_Unlock_Count    MC_Xmt_Error_Count
_____________________________________________________________
4           FDDI_4     0                  1
01:02:03               2                  3
```

Column	Description
Slot	Slot number of the module for which statistics are being reported.
Time	Time (hour, minute, and second) that this information was gathered.
Network	FDDI network to which this module has been assigned.
BP_Error_Count	Number of invalid FDDI symbols received from another FDDI module over the 8250 backplane. Backplane errors are detected and isolated by the FDDI Module.
BP_Unlock_Count	Number of times that the receive clock circuitry on the module failed to recognize a backplane clock and unlocked. Loss of receive clock is detected and isolated by the FDDI Module, which recovers automatically from such errors.
MC_Rcv_Error_Count	Number of receive errors on the FMM Channel (MC).
MC_Xmt_Error_Count	Number of transmit errors on the FDDI Management Channel (MC).

SHOW COUNTER NETWORK

Use the SHOW COUNTER NETWORK command to report error or traffic statistics for the network to which the management module is assigned. The traffic option is available for the TRMM Advanced only.

Format

SHOW COUNTER NETWORK {parameter}

Parameters

{parameter} = errors (default)
traffic distribution (TRMM Advanced only)

Description

The SHOW COUNTER NETWORK command enables you to display error or traffic statistics for the network to which the management module is assigned. All counters are displayed since the last clear or reset.

Examples

Example 1

The following example displays EMM network error statistics.

```
8250> show counter network      [ENTER]
Non-zero counters for network ETHERNET_1 on 15 Nov 93:


Network    Frames   Bcast      CRC Err    AlignErr Collisions
Time       Octets   Mcast   TooLongErr            Remote/Local
──────────────────────────────────────────────────────────────
ETHERNET_1    928      21           0           0        0
13:24:47    74129     129           0                      0
```

Network counter fields are described on the following page.

Column	Description
Network	Network for which the statistics are being displayed.
Time	Time the report was run in the format: hour, minutes, and seconds.
Frames	Number of good frames received.
Octets	Number of good octets received (1 BYTE = 1 OCTET = 8 BITS).
Bcast	Number of received Broadcast Destination Address Packets.
Mcast	Number of received Multicast Address Packets.
CRC Err	Number of CRC errors received (not including AlignErr).
TooLongErr	Number of too long errors received (packets greater than 1518 bytes).
AlignErr	Number of alignment errors received. Alignment errors indicate CRC errors that do not end on a byte boundary.
Collisions Remote	Number of collisions a port received over the remote network. This counter counts received fragments.
Collisions Local	Number of collisions recorded within the local hub on that network. This counter is incremented if two ports receive data simultaneously.

Example 2

This example reports error statistics for the TRMM network.

```
8250> show counter network errors [ENTER]

NETWORK ERRORS:
      Beacon Events:             0
      Ring Purge Recoveries:     1
STATION ERROR TOTALS:
      ISOLATING ERRORS:
      Line Errors:               0
      Burst Errors:              3
      Address/Frame Errors:      0
      NON-ISOLATING ERRORS:
      Lost Frame Errors:         0
      Receive Congestion Errors: 0
      Frame Copy Errors:         0
      Token Errors:              6
```

Error fields are described in the table on the next page.

Negative values are displayed when the error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once the counters are reset, correct values are displayed when a subsequent SHOW COUNTER command is issued.

When using command completion to specify the ALL option in the SHOW COUNTER STATION command line, you must type at least 'al' or specify 'all' in order for the TRMM to recognize the ALL option. Otherwise, the TRMM assumes the 'a' indicates the beginning of a MAC address.

Field	Description
Beacon Events	Number of beacon events on the network.
Ring Purge Recoveries	Number of times the ring has been purged and has recovered to a normal operating state.

Field	Description
Line Errors	The line error counter is incremented whenever: a) A code violation occurs in the frame b) A code violation occurs in the token c) A Frame Check Sequence (FCS) error occurs
Burst Errors	When a station detects the absence of transitions.
Address/Frame Errors	An error with the Address Recognized Indicator (ARI) and/or the Frame Copied Indicator (FCI) and the upstream neighbor is unable to set the ARI/FCI bits in a frame that it has copied.
Lost Frame Errors	Station that transmitted a packet did not receive the same packet completely.
Receive Congestion Errors	Receiving station has no buffer space in which to copy the received frame.
Frame Copy Errors	A packet addressed to a station has already been copied by another station.
Token Errors	A station did not receive a valid token within 10 ms. This counter only increments if the station is active monitor.

Example 3

This example reports traffic statistics for the TRMM network.

```
8250> show counter network traffic distribution [ENTER]
Network Traffic Counters for TOKEN_RING_1 at 16:26 Mon 29 Nov 93
Time since last clear counters: 0:03:07
Frame Distribution Summary:
Non-MAC Frames: Multicast 0   Broadcast    1 Source Routed 2
 Frame Size        Frames                 Octets
18 to    63       0    0.00%             0    0.00%
64 to   127       22   30.56% XXX.       2119   54.07% XXXXX.
128 to  255       0    0.00%             0    0.00%
256 to   511      0    0.00%             0    0.00%
512 to  1023      0    0.00%             0    0.00%
1024 to 2047      0    0.00%             0    0.00%
2048 to  4095     0    0.00%             0    0.00%
4096 to  8191     0    0.00%             0    0.00%
```

```
8192 to 18000     0    0.00%             0    0.00%
      > 18000     0    0.00%             0    0.00%
MAC Frames        50   69.44% XXXXXXX    1800   45.93% XXXXX

Total Frames:           72
Total Octets:         3919
```

The traffic display reports the percentage of non-MAC (that is, normal network traffic) traffic generated on the network. Total percentage of MAC frames generated on the network is reported at the bottom of the command display. MAC frames consists of Token Ring protocol frames. The X(s) and (.)s next to the frame and octet percentages are a visual representation of the percentages rounded up to the next 5%. X equals 10% and (.) equals 5%. From the example above, the first frame counter of 1146 is 33.14%, which equates to XXX. (rounding out 33.13% to 35%).

This means that frames with lengths of 18 to 63 octets make up 33.14% of the traffic currently on the network.

Traffic fields are described in the following table.

Field	Description
Non-MAC Multicast Frames	Number of non-MAC frames that were transmitted to a multicast address.
Non-MAC Broadcast Frames	Number of non-MAC frames that were transmitted to a broadcast address.
Non-MAC Source Routed Frames	Number of source routed frames on the network.
Frames	Number of frames on the network.
Octets	Number of octets on the network.
MAC Frames	Number of MAC frames on the network. MAC frames consist of Token Ring protocol frames.
Total Frames	Number of frames on the network.
Total Octets	Number of octets on the network.

Example 4

This example reports error statistics for the FMM network.

```
8250> show counter network      [ENTER]


Network: FDDI_1              Time: 09:36:57
Ring State: ring_op          Utilization: 0 %

_____________________________________________________________
Frames                      Errors               Tokens
      55                          0                    523734857
       0/sec                      0/sec
1138752/sec
                                  0%

Ringops:               1            Frame Error Ratio:        0
Beacons:               0            Lost:                     0
                                    Late:                   0

_____________________________________________________________
This Station
Frames Copied:      2911            Transmitted:           5824
Path Tests:            0           TvxExpires:               0

_____________________________________________________________
```

Error fields are described in the following table.

Column	Description
Network	Network for which information is being displayed.
Time	Time (hour:minute:seconds) for which the monitoring of these events is taking place.
Frame_Ct	Number of all frames received.
Error_Ct	Number of error frames detected by this FMM MAC.
TvxExpired_Ct	Number of Valid Transmission Timer (TVX) expirations.

Column	Description
Beacon_Ct	Number of beacon frames received by this FMM.
RingOp_Ct	Number of times that the FDDI ring to which this FMM is assigned has re-initialized.
Copied_Ct	Number of frames containing Service Data Units (SDUs) addressed to and successfully copied by this FMM MAC.
Lost_Ct	Errors are detected while this FMM MAC is in the process of receiving a frame or token. A Lost-Ct error prevents complete Protocol Data Unit (PDU) reception.
Late_Ct	Number of Token Rotation Timer (TRT) expirations since a token was received by this FMM MAC or since this FMM MAC was reset.
Trace_Ct	Number of times that this FMM has participated in a trace test.

SHOW COUNTER PORT

Use the SHOW COUNTER PORT command to report error statistics for a specific port or all ports on a module. The traffic option is available for the TRMM Advanced only. This option enables you to also display traffic statistics for one or all ports.

Format

SHOW COUNTER PORT {slot.port} {parameter}

Parameters

{slot} = 1 through 17

{port} = 1 through 24 or all

{parameter} = errors (default)
traffic (TRMM Advanced only)

Description

All counters display values accrued since the last clear or reset. Statistics are only shown for active ports.

Negative values are displayed when Token Ring error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once the counters are reset, correct values are displayed when a subsequent SHOW COUNTER command is issued.

Examples

Example 1

The following example displays port counters for port 2 on the Token Ring module in slot 5.

```
8250> show counter port 5.2 errors  [ENTER]

MAC Address 10-00-f1-0f-0c-60
ERROR COUNTERS:
         Line Errors:               1
         Burst Errors:              0
         Address/Frame Errors:      0
         Lost Frame Errors:         0
         Receive Congestion Errors: 0
         Frame Copy Errors:         0
         Token Errors:              3
```

Token Ring port statistic fields are described in the following table.

Error Counters	Description
Line Errors	The line error counter is incremented when: **1)** a frame is repeated or copied, *and* **2)** the Error Detected Indicator is zero in the incoming frame, *and* **3)** one of the following conditions exists: **a)** a code violation between the starting delimiter and ending delimiter of the frame. **b)** a code violation in a token. **c)** a Frame Check Sequence error.
Burst Errors	The burst error counter is incremented when a TRMM detects the absence of transitions for five half-bit times between the starting delimiter and ending delimiter, or the ending delimiter and the starting delimiter.

Error Counters	Description
Address/Frame Errors	The address/frame error counter is incremented when: **1)** a TRMM receives an Active Monitor Present (AMP) MAC frame with the address/frame bits equal to zero, *and* **2)** a Standby Monitor Present (SMP) MAC frame with the address/frame bits equal to zero, *or* more than one SMP MAC frame with the address/frame bits equal to zero, without receiving an intervening AMP MAC frame.
Lost Frame Errors	The lost frame error counter is incremented when a TRMM is in transmit (stripping) mode and fails to receive the end of the frame it transmitted.
Receive Congestion Errors	The receive congestion error counter is incremented when an adapter in repeat mode recognizes a frame addressed to it but has no buffer space available to copy the frame.

Error Counters	Description
Frame Copy Errors	The frame copied error counter is incremented when an adapter in receive/repeat mode recognizes a frame addressed to its specific address but finds the ARI bits not equal to zero. This indicates a possible line hit or duplicate address.
Token Errors	The token error counter is active only in the active monitor station. It is incremented when the active monitor detects an error with the token protocol as follows: **1)** the monitor count bit of a token with nonzero priority equals one. **2)** the monitor count bit of a frame equals one. **3)** no token or frame is received within a 10-ms window. **4)** the starting delimiter/token sequence has a code violation in an area where code violations must not exist.

The following example displays Ethernet port statistics.

Example 2

```
8250> show counter port 5.2       [ENTER]
Non-zero counters for network ETHERNET_1 on 17 Jun 93:

Slot.Port Frames    Bcast      CRC Err   AlignErr Collisions
Time       Octets    Mcast   TooLongErr                Remote
            LastSourceAddr      Changes          LastErrorAddr
_____________________________________________________________
 5.2         1522       56           0          0           0
12:22:25    92574      337           0
         08-54-6f-01-32-08           5      08-74-04-2c-43-02
```

Ethernet port statistic fields are described in the following table.

Column	Description
Slot.Port	Slot and port for which the statistics are being displayed.
Time	Time the report was run, in hours, minutes, and seconds.
Frames	Number of good frames received.
Octets	Number of good octets received (1 BYTE = 1 OCTET = 8 BITS).
Bcast	Number of received Broadcast Destination Address Packets.
Mcast	Number of received Multicast Destination Address Packets.
LastSourceAddr	Ethernet Address of the last device sending information through this port.
CRC Err	Number of frames with CRC errors (not including AlignErr).

Column	Description
TooLongErr	Number of too long errors received (packets greater than 1518 bytes).
Changes	Number of times the Last Source Address has changed.
AlignErr	Number of frames received with alignment errors. Alignment errors indicate CRC errors that do not end on a byte boundary.
Collisions Remote	Number of collisions a port received over the remote network. This counter counts received fragments.
LastErrorAddr	Value in the source address field of the last packet received in error for this port.

The following example displays FDDI port statistics.

Example 3

```
8250> show counter port 4          [ENTER]

Slot     Network     BP_Error_Count    MC_Rcv_Error_Count
Time                 BP_Unlock_Count   MC_Xmt_Error_Count
_____________________________________________________________
```

FDDI port statistic fields are described in the following table.

Column	Description
Slot.Port	Slot/port number of the module for which statistics are being reported.
Time	Time (hour, minutes, and seconds) that this information was gathered.
Network	FDDI network to which this module has been assigned.

Column	Description
LEM_Count	Link Error Monitor (LEM) Count detects and reports invalid line state transitions. **Range: 0 through 65535** **Note:** Use the MONITOR command to obtain a log of the invalid line state transitions reported over a user-defined period of time.
LEM_Rejects_Count	The Link Error Monitor (LEM) Rejects Count detects and reports the number of times the link has reinitialized as a result of excessive link errors. **Range: 0 through 255** **Note:** Use the MONITOR command to obtain a log of the LEM_Rejects_Count reported over a user-defined period of time.
LER_Estimate	The Link Error Rate (LER) Estimate is the long term average link error rate based upon the current LEM count. The error rate ranges from 15 (good) to 4 (poor); however, the module reinitializes if the LER_Estimate falls below 7. **Note:** Use the MONITOR command to obtain a log of the average link error rate reported over a user-defined period of time.
LCT_Fail_Count	The Link Confidence Test (LCT) verifies the physical link and reports the number of successive link failures detected during the connection process. **Range: 0 through 255** **Note:** Use the MONITOR command to obtain a log of the number of successive link failures reported over a user-defined period of time.

SHOW COUNTER PORT_STATISTICS

Use the SHOW COUNTER PORT_STATISTICS command to determine whether or not the TRMM is currently collecting port statistics.

Format

SHOW COUNTER PORT_STATISTICS

Parameters

none.

Example

The following command shows whether or not port statistics are enabled on the TRMM.

```
8250> show counter port_statistics
Port statistics are ENABLED.
```

Description

Use the SHOW COUNTER PORT_STATISTICS command to determine whether or not the TRMM is currently collecting port statistics. Use the SET COUNTER PORT_STATISTICS command to enable and disable TRMM port statistics collection.

SHOW COUNTER STATION

Use the SHOW COUNTER STATION command to report TRMM error or traffic statistics for one MAC Address or all stations on the network to which the TRMM is assigned. Traffic statistics are available for the TRMM Advanced only.

Format

SHOW COUNTER STATION {station} {parameter}

Parameters

{station} = MAC Address
all
{parameter} = errors (default)
traffic (Advanced TRMM only)

Examples

Example 1

This example displays errors statistics for a specific MAC Address.

```
8250> show counter station 10-00-f1-0f-0c-70 errors [ENTER]

MAC Address 10-00-f1-0f-0c-70
ERROR COUNTERS:
         Line Errors:              1
         Burst Errors:             0
         Address/Frame Errors:     0
         Lost Frame Errors:        0
         Receive Congestion Errors: 0
         Frame Copy Errors:        0
         Token Errors:             3
```

Example 2

This example displays a summary of station traffic statistics for the network to which the TRMM Advanced is assigned.

```
8250> show counter station all traffic   [ENTER]

Station Statistics-sorted byMAC Address-at 12:57 Tue 06 Jul 93

MAC Address         Slot.Port Since Cleared   Frames   Octets
10-00-F1-0F-0C-7A   14.01           0:46:47    403      14508
10-00-F1-0F-0C-6F   11.01           0:46:47    184      6624
10-00-F1-0F-0C-4F   Remote          0:46:47    184      6624
FF-FF-FF-FF-FF-FF   Broadcast       0:46:47    887      31932
```

Description

The SHOW COUNTER STATION command enables you to display error or traffic statistics for stations on the network to which the TRMM is assigned. The error count is cumulative, starting from the time the station was added to the ring. Issue the CLEAR COUNTER command to reset the counters back to 0.

The SHOW COUNTER STATION command display may indicate extra entries with erroneous station addresses. These entries are caused by ring error conditions (for example, line errors, burst errors), which are a result of normal ring events (for example, stations inserting onto the ring).

Negative values are displayed when Token Ring error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once the counters are reset, correct values are displayed when a subsequent SHOW COUNTER command is issued.

Stations that are in the same hub and on the same network as the TRMM display their slot and port numbers.

External refers to a station that is on the same network as the TRMM, but in a different hub.

Remote refers to a station on a different network that is bridged to the network to which the TRMM is assigned. Remote station counters reflect

traffic statistics that only occur on the network to which the TRMM is assigned.

To show counters for stations on another network you must either use the TELNET command to log in to the TRMM monitoring that network or reassign the TRMM to the network you wish to monitor. Refer to the SHOW COUNTER DEVICE command for descriptions of the error counters.

A broadcast or multicast MAC address is identified in the Slot.Port field.

SHOW COUNTER TOP_ERRORS

Use the SHOW COUNTER TOP_ERRORS command to report a summary of TRMM error statistics sorted by the top error senders on the network. This command is available for the TRMM Advanced only.

Format

SHOW COUNTER TOP_ERRORS {group} {value}

Parameters

{group} = by_frames (default)
by mac_address

{value} = all (default at startup)
number of stations (1 through 1000)

Example

This example displays by MAC address the total error frames received by stations on the network.

```
8250> show counter top_errors   [ENTER]
_____________________________________________________________

Station Error Summary-sorted by Top Error Senders - at 07:59
Mon 25 Jan 93
_____________________________________________________________

MAC Address        Slot.Port Time Since Cleared     Frames
                                                  (isolating +
                                                   congestion)
10-00-F1-0F-0C-6F 14.01                0:12:55          4
10-00-F1-0F-0C-60 EXTERNAL             0:13:00          3
08-01-20-0C-9C-78 EXTERNAL             0:12:55          1
```

Description

The SHOW COUNTER TOP_ERRORS command enables you to report a summary of error statistics for all stations, or a specified number of stations on the network by frames or by MAC address. The stations are displayed in order according to the number of errors they have received. The station that has received the most errors is displayed first. Top errors counters include only isolating errors (for example, line burst, access control) and congestion errors.

The SHOW COUNTER TOP_ERRORS command display may indicate extra entries with erroneous station addresses. These entries are caused by ring error conditions (for example, line errors, burst errors), which are a result of normal ring events (for example, stations inserting onto the ring).

Negative values are displayed when Token Ring error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once you reset the counters, correct values are displayed when you issue a subsequent SHOW COUNTER command.

The default for this command at startup is *all*. The default for subsequent SHOW COUNTER TOP_ERRORS commands is the last value requested.

Use the SHOW COUNTER STATION ERROR or SHOW COUNTER PORT ERROR commands to display a more detailed report of the errors for an individual station.

SHOW COUNTER TOP_RECEIVERS

Use the SHOW COUNTER TOP_RECEIVERS command to report a summary of TRMM traffic statistics by frames, MAC address, or octets as received by stations on the network. This command is available for the TRMM Advanced only.

Format

SHOW COUNTER TOP_RECEIVERS {group} {value}

Parameters

{group} = by_frames
by_mac_address
by_octets (default)

{value} = all (default at startup)
number of stations (1 through 1000)

Example

This example displays by MAC address the total traffic statistics received by stations on the network.

```
8250> show counter top_receivers by_mac_address [ENTER]

Station Traffic Statistics-sorted by Top Receivers-at 7:35 Weds 27 Jan 93

MAC Address         Slot.Port Time Since Cleared  Frames   Octets
10-00-F1-0F-0C-60   EXTERNAL           0:1:03      804      438024 56.44%
10-00-F1-0F-0C-5F   REMOTE             0:1:17      397      219117 28.24%
08-01-20-0C-9C-78   EXTERNAL           0:1:27     1189       73561   9.48%
C0-00-FF-FF-FF-FF   Broadcast          0:1:58      887       31932   4.11%
FF-FF-FF-FF-FF-FF   Broadcast          0:2:07      126        9072   1.17%
C0-00-00-00-00-00   Ring Param Server  0:2:19       20        1320   0.17%
10-00-F1-0F-0C-6C   03.06              0:3:18       15        1218   0.16%
C0-00-00-00-00-08   Ring Err Monitor   0:3:31       21        1068   0.14%
c0-00-00-00-00-01   Network Manager    0:5:23       20         720   0.09%
```

Description

The SHOW COUNTER TOP_RECEIVERS command enables you to display a summary of traffic statistics received by all stations or a specified number of stations on the network. The stations are displayed in order by frames, MAC address, or octets according to the amount of traffic they have received.

The SHOW COUNTER TOP_STATIONS command display may indicate extra entries with erroneous station addresses. These entries are caused by ring error conditions (for example, line errors, burst errors), which are a result of normal ring events (for example, stations inserting onto the ring).

Negative values are displayed when Token Ring error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once you reset the counters, correct values are displayed when you issue a subsequent SHOW COUNTER command.

The default for this command at startup is *all*. The default for subsequent SHOW COUNTER TOP_RECEIVERS commands is the last value requested.

Use the SHOW COUNTER STATION TRAFFIC command or the SHOW COUNTER PORT TRAFFIC command to display a more detailed report of the traffic received by an individual station.

SHOW COUNTER TOP_SENDERS

Use the SHOW COUNTER TOP_SENDERS command to report by frames, MAC address, or octets a summary of TRMM traffic statistics transmitted by stations on the network. This command is available for the TRMM Advanced only.

Format

SHOW COUNTER TOP_SENDERS {group} {value}

Parameters

{group} = by_frames
by_mac_address
by_octets (default)

{value} = all (default at startup)
number of stations (1 through 1000)

Example

This example displays the total traffic statistics transmitted by stations on the network.

```
8250> show counter top_senders [ENTER]

Station Traffic Statistics- sorted by Top Senders - at 11:57 Sun 24 Jan 93

MAC Address        Slot.Port Time Since Cleared     Frames Octets
08-01-20-0C-9C-78 EXTERNAL         0:3:06           1567    670316 86.39%
10-00-F1-0F-0C-60 EXTERNAL         0:8:0           91136     65817  8.48%
10-00-F1-0F-0C-5F REMOTE           0:8:27            396     22975  2.96%
10-00-F1-0F-0C-6F 14.01            0:13:00           376     16780  2.16%
09-01-20-0C-0C-60 REMOTE           0:17:33             1        36  0.00%
```

Description

The SHOW COUNTER TOP_SENDERS command reports a summary of traffic statistics transmitted by all stations or a specified number of stations on the network. The stations are displayed in order according to the amount of traffic they have transmitted. The station that has sent the most octets is displayed first.

The SHOW COUNTER TOP_SENDERS command display may indicate extra entries with erroneous station addresses. These entries are caused by ring error conditions (for example, line errors, burst errors), which are a result of normal ring events (for example, stations inserting onto the ring).

The stations are displayed in order by frames, MAC address, or octets according to the amount of traffic they have sent.

Negative values are displayed when Token Ring error frame/octet counters wrap (at two billion plus counts). Issue the appropriate CLEAR COUNTER command to reset the values. Once you reset the counters, correct values are displayed when you issue a subsequent SHOW COUNTER command.

The default for this command at startup is *all*. The default for subsequent SHOW COUNTER TOP_SENDERS commands is the last value requested.

Use the SHOW COUNTER STATION TRAFFIC command or the SHOW COUNTER PORT TRAFFIC command to display a more detailed report of the traffic transmitted by an individual station.

SHOW DEVICE

Use the SHOW DEVICE command to display information about a management module.

Format

SHOW DEVICE

Parameters

none

Example

The following command displays information about a TRMM:

```
8250> show device [ENTER]

IBM T01MS Token Ring Management Module (Advanced-MGT) v4.00-A pSOS+ SNMP

Name:  8250
Location:  Unknown
For assistance contact:
  System Administrator

Boot EPROM Version:  v3.03-A    Size:  256 KBytes
Flash EPROM Version: v4.00-A    Size: 1024 KBytes  DRAM Size: 2048 KBytes
Serial Number:                     Service Date:  95/02/27    Restarts: 152

Network     IP Address       Subnet Mask   Primary Gateway  Secondary Gateway
--------    --------------   -----------   ---------------  -----------------
tr_1     *  151.104.25.141   FF.FF.FF.00   0.0.0.0        * 0.0.0.0
tr_2        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_3        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_4        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
tr_5        151.104.25.141   FF.FF.FF.00   0.0.0.0          0.0.0.0


tr_6        151.104.25.141   FF.FF.FF.00   0.0.0.0          0.0.0.0
tr_7        151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0
isolated    151.104.25.141   FF.FF.FF.00   151.104.25.38    0.0.0.0

MAC Address: 10-00-F1-0F-23-FC
Beacon Trunk Retry:  0 time(s)
Dip Configuration:  DISABLED    Diagnostics:         ENABLED
Trap Receive:       DISABLED    Beacon Recovery:     ENABLED
Monitor Contention: ENABLED     Beacon Timeout:      10 second(s)
```

Description

The information that displays is defined below:

Field	Description
Name	Identification given to the management module.
Location	Physical location of the management module.
For assistance contact	Service contact information.
Boot EPROM Version	Software version number for the Boot EPROM.
Flash EPROM Version	Software version number for the Flash EPROM.
Serial Number	IBM serial number for the management module.
Service Date	Last date (yy/mm/dd) hardware/ software was changed on the management module.
Restarts	Number of system restarts logged.
Interface (TRMM only)	Identifier for the seven Token Ring backplane networks and one isolated network. An asterisk (*) indicates which network is active.
IP Address	Management module Internet Protocol address.
Subnet Mask	Subnetwork mask that is used for that network.

Field	Description
Default Gateway Primary/Secondary (Secondary is TRMM only)	Address of the gateway that is used when the destination cannot be found on the local network. An asterisk (*) indicates the active gateway.
MAC Address	Management module MAC address.
Dip Configuration	System boots the modules using the dip switch settings or the software settings.
Diagnostics	Indicates if diagnostics are run when reset.
Trap Receive	Setting for the trap receive feature.
Beacon Recovery (TRMM only)	Setting for the beacon recovery feature.
Reset Mastership	Indicates if the FMM is set to receive traps from other agents on the network.
Monitor Contention (TRMM only)	Indicates if the TRMM participates in active monitor contention.

SHOW DOWNLOAD

Use the SHOW DOWNLOAD command to display the value defined for performing an inband download to an EMM. This command is available only when running an EMM in Maintenance Mode.

Format

SHOW DOWNLOAD

Parameters

none

Example

```
>> show download       [ENTER]
—- Download Variables —-
Download Network:    1
```

Description

The information that displays shows the number of the network that is used for inband download from Maintenance Mode (using EMM version 2.0 or greater BOOT PROMs). It is used in conjunction with the SET TFTP SERVER_IP_ADDRESS and SET TFTP FILE_NAME commands.

Use the SET DOWNLOAD command from Maintenance Mode to modify the network that is used to download new software to an EMM from the TFTP Server.

SHOW EVENT_LOG

Use the SHOW EVENT_LOG command to display the values in the FMM system event log.

Format

SHOW EVENT_LOG

Parameters

none

Example

```
8250> show event_log      [ENTER]

Display of Last Error - Flash Version: vx.xx

Crash Date/Time: 05:53 Sun 6 Mar 94
Date/Time:       06:17 Mon 7 Mar 94
   -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   personal computer = 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 .......

8250>
```

Description

When the management module detects an error, it records important information about the failure in the system event log and then resets the management module. The message “Fatal Error: See system event log! Call IBM Customer Service” and the trap that caused the fatal error, displays on the terminal connected to the affected management module when the module resets. The message remains on the screen until you display the system event log. In addition, the IBM fatal error (8) is sent to the trap receiver (as defined in the community table).

Use the SHOW EVENT_LOG command to display the system event log after receiving a fatal error. Record the system event information in a file (or to a printer) and call IBM Customer Support to diagnose why the management module failed.

You may want to use the CLEAR EVENT_LOG command to erase the information in the log once you have viewed or printed it.

The log example on the previous page contains the line: `Ack Date/Time`. This displays the date and time that the contents of the system event log were acknowledged with the SHOW EVENT_LOG command.

SHOW GROUP

Use the SHOW GROUP command to display the Token Ring ports associated with a specific group. The Port Group feature is available with the Advanced TRMM only.

Format

SHOW GROUP {group}

Parameters

{group} = all
group1
group2
group3
group4
group5
group6
group7
group8

Example

The following example displays all of the ports associated with all groups.

```
8250> show group all [ENTER]

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]
```

Description

This command enables you to displays the Token Ring ports defined in a specific group or all groups.

SHOW HOST

Use the SHOW HOST command to display the FMM or TRMM host table.

Format

SHOW HOST

Parameters

none

Example

```
8250> show host       [ENTER]
    Index Host Name                IP Address
     -------------                 ----------
         1 saba                     151.104.56.20
         2 eng1                     151.3.6.58
         3 mkt                      151.2.2.27
         4 finance                  151.12.23.6
         5 education                151.102.17.4
         6 support                  151.102.16.5
         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]
```

Description

This command displays the FMM or TRMM host table.

SHOW LOGIN

Use the SHOW LOGIN command to display the FMM or TRMM login table.

Format

SHOW LOGIN

Parameters

none

Example

```
8250> show login        [ENTER]
    Login Table:
Index   Login Name     Access         Active Sessions
-----   -----------     -------         ----------------

    1   system          Local Super User     1
    2   lynnl           Super User           0
    3   mkt             User                 0
    4   education       Administrator        0
    5   finance         User                 0
    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           Local Super User      1 days 04:07:19
```

Description

This command displays the FMM or TRMM login table.

SHOW LOG EVENT_LOG

Use the SHOW LOG EVENT_LOG command to display the values in the system event log.

Format

SHOW LOG EVENT_LOG

Parameters

none

Example

The following command displays the event log:

```
8250> show log event_log              [ENTER]
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

D=11111111 0000023D 00000000 00000000 00000000 00000000 00000000
Vector = 20020494   personal computer = 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 .......
```

Description

This command displays the system event log after receiving a fatal error. Record the system event information in a file (or to a printer) and call IBM Technical Support to determine why the TRMM failed.

SHOW LOG SYSTEM_EVENT

Use the SHOW LOG SYSTEM_EVENT command to display the values in the EMM system event log.

Format

SHOW LOG SYSTEM_EVENT

Parameters

none

Example

```
8250> show log system_event     [ENTER]

Display of Last Error - Flash Version: vx.xx

Crash Date/Time: 05:58 Sat 6 Mar 93
Date/Time:       06:17 Sun 7 Mar 93

   -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   personal computer = 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 .......

8250>
```

Description

When the management module detects an error, it records important information about the failure in the system event log and then resets the management module. The message “Fatal Error: See system event log! Call IBM Customer Service”, and the trap that caused the fatal error displays on the terminal connected to the affected management module when the module resets. The message remains on the screen until you display the

system event log. In addition, the IBM fatal error (8) is sent to the trap receiver (as defined in the community table).

Use the SHOW LOG SYSTEM_EVENT command to display the system event log after receiving a fatal error. Record the system event information in a file (or to a printer) and call IBM Customer Support to diagnose why the management module failed.

You may want to use the CLEAR LOG SYSTEM_EVENT command to erase the information in the log once you have viewed or printed it.

The log example on the previous page contains the line: `Ack Date/Time`. This displays the date and time that the contents of the system event log were acknowledged with the SHOW LOG SYSTEM_EVENT command.

SHOW LOG TRAP_LOG

Use the SHOW LOG TRAP_LOG command to display the log entries for the most recently sent traps.

Format

SHOW LOG TRAP_LOG

Parameters

none

Example

The following command displays a list of nonfatal system traps:

```
8250> show log trap_log     [ENTER]

-------------------TRAP 1 ----------------------------


Message received from this device on 15:43 Mon 24 Jul 95:

Enterprise:                IBM
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
```

Description

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 TRMM is reset or if power is lost to the TRMM.

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.

SHOW MODULE

Use the SHOW MODULE command to display settings for all of the modules currently installed in your hub.

Format

SHOW MODULE {slot} {option}

Parameters

{slot} = 1 through 17 or all

{option} = verbose
no_verbose (default if you press ENTER)

Examples

Example 1

This example uses the verbose option to display detailed settings of the TRMM in slot 3.

```
8250> show module 3 verbose    [ENTER]

Slot  Module           Version Network       General Information
----  ---------------- ------- ------------- ------------------
*03   T01MS-MGT        v4.00-A TOKEN_RING_1  Master Management Module

T01MS-MGT: 8250 Token Ring Management Module

Mastership Priority:                    10
Station Address:                        10-00-f1-0f-23-fc
Locally Administered Address:           00-00-00-82-08-00
MAC Address Type:                       BURNED-IN
Ring Speed:                             16 MBPS
Network Status:                         OKAY
RMON Probe Mode:                        ENABLED
Master Network:                         NO_CHANGE
Active MAC Address:                     10-00-f1-0f-23-fc
Interface Number:                       1
```

Example 2

This example shows the type and location of all modules installed in the hub. The asterisk (*) displayed on slot 7 indicates the TRMM that you are currently logged into.

```
8250> show module all    [ENTER]

Slot  Module       Version   Network         General Information
----  -------      -------   -------         --------------------
01    C00NS-RCTL   vx.x        N/A           Active Fault-Tolerant Cntrl
03    T20MS-RJ45S  vx.x      TOKEN_RING_1
05    T20MS-RJ45S  vx.x      TOKEN_RING_2
07*   T01MS-MGT    vx.x      TOKEN_RING_1    Master Management Module
011   T02MS-FIB    vx.x      TOKEN_RING_2
```

Description

This command displays information for all of the modules currently installed in your hub. The verbose option is used only when you SHOW a single module in the hub. This option gives more detailed information about the software and dip switch settings for the module.

For more details about modules that are network-settable per port, use the SHOW PORT command.

SHOW NETWORK_MAP

Use the SHOW NETWORK_MAP command to display a topology of the Ethernet, Token Ring or FDDI networks currently configured in the hub.

Format

SHOW NETWORK_MAP {protocol}

Parameters

{protocol} = Ethernet = all
mac_address
module
port

Ethernet Sort Order
by_frames
by_mac_address
by_octets
by_port
by_time

fddi
token_ring - logical
mac_address
physical
port

Examples

Example 1

For Ethernet, this command displays the source addresses for each frame received on a per-port basis. It can contain up to 1024 addresses and it maintains a frame count indicator (not a true frame count) per address. Use [CTRL-C] to end the display and return to the command line. The following example displays a network map for port 1 on the Ethernet module in slot 6. The information that displays on the Ethernet screen is defined below.

```
8250> show network_map ethernet port 6.1      [ENTER]

Network Map for network ETHERNET_1 on 08 Nov 93:
Note: Frames and Octets are indicators, not real counters.

Port   MAC Address        Frames   Octets    Time Since Seen
_____  _________________  ______   ______    _______________
06.01  00-00-3C-00-14-66  1        130       0d 0h 16m 52s
06.01  08-00-20-07-41-3C  2        128       0d 0h 42m 2s
06.01  02-60-8C-0C-A4-6D  1        128       0d 0h 36m 25s
```

Column	Description
Slot.Port	Indicates the slot and port number of the statistics being displayed.
MAC Address	The Ethernet source address received by this port on this network.
Frames	An estimated count of the number of frames generated by this address.
Octets	An estimated count of the number of octets generated by this address.
Time Since Seen	The amount of time since this address was seen on this port.

Example 2

For FDDI modules, this command is used to display the physical ring topology of the FDDI networks currently configured in the hub. For each network, the modules which comprise that network, and their respective upstream and downstream slots, are displayed along with the module's status. The following example displays a network map for all FDDI modules in the hub. The information that displays is defined below.

```
8250> show network_map fddi     [ENTER]

Slot     Status    Upstream_Slot     Downstream_Slot
_____________________________________________________
12       OKAY      16                14
14       OKAY      12                16
```

Column	Description
Slot	Indicates the slot numbers of the modules which comprise each FDDI network.
Status	Under normal operating conditions, OKAY is displayed. PARTIAL FAIL is reported if a partial hardware failure is detected.
Downstream Slot	Identifies the hub slot number for the adjoining module on the ring. This field identifies the module to which the specified FDDI Module will pass the token.
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 3

For Token Ring modules, this command shows the physical links between ports on all connected Token Ring modules in the hub.

The information displayed by this command is defined on the next page. Press Ctrl-C together to end the display and return to the command line.

```
8250> show network_map token_ring physical  [ENTER]

Physical wiring map for modules in TOKEN_RING_1:

 Upstream       Connection       Downstream
 Slot ID        Type             Slot ID
 --------       ----------       -----------

 External       Fiber            7
 7              Copper           3
 3              Copper           7
 7              Backplane        8
 8              Backplane        6
 6              Copper           External
```

Example 4

Use the SHOW NETWORK_MAP TOKEN_RING LOGICAL command to display information about ring topology and identify which port is the active monitor.

```
8250> show network_map token_ring logical   [ENTER]

Token Ring Logical Map

MAC Address            Slot        Port

10-00-f1-0f-0c-63      7            1
10-00-90-28-4d-52      3           20 <- Active Monitor
10-00-90-28-30-e0      3           10
08-00-20-10-61-4d      3            1
```

Column	Description
Upstream Slot ID	Identifies the hub slot number for the adjoining module on the ring. This field identifies the module passing the token to the specified Token Ring Module.
Connection Type	Specifies the 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	Identifies the hub slot number for the adjoining module on the ring. This field identifies the module to which the specified Token Ring module will pass the token.

If the connection type is fiber, the upstream and downstream slot ID will be “external”. If the connection type is copper, the upstream and downstream slot ID may be “external”. External means that the connection could be

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.

SHOW NETWORK_PATHS

Use the SHOW NETWORK_PATHS command to display a list of the logical network assignments, and their corresponding physical backplane path connection.

Format

SHOW NETWORK_PATHS {protocol}

Parameters

{protocol} = all
ethernet
fddi
token_ring

Example

```
8250> show network_paths all    [ENTER]

Physical Path      Logical Network
_____________      _______________

ETHERNET_PATH_1    ETHERNET_1
ETHERNET_PATH_2    in use
ETHERNET_PATH_3    ETHERNET_3

— More —

TR_PATH_1          in use
TR_PATH_2          in use
TR_PATH_3          in use
TR_PATH_4          in use
TR_PATH_5          available
TR_PATH_6          available
TR_PATH_7          TOKEN_RING_1
TR_PATH_8          available
TR_PATH_9          available
TR_PATH_10         in use
TR_PATH_11         in use
TR_PATH_12         TOKEN_RING_1
```

```
TR_PATH_13          in use
TR_PATH_14          in use
TR_PATH_15          in use


FDDI_PATH_1         FDDI_1
FDDI_PATH_2         in use
FDDI_PATH_3         in use
FDDI_PATH_4         in use
FDDI_PATH_5         in use
FDDI_PATH_6         in use
FDDI_PATH_7         FDDI_1
FDDI_PATH_8         in use
```

Description

This command displays a list of the logical network assignments and their corresponding physical channel (backplane path) connection. The term ETHERNET_PATH corresponds to the channel, that is, ETHERNET_PATH_2 is channel 2.

The term “in use” means that another protocol's network assignment has canceled out the availability of the path for use. And the term “available” means that the path is available for that protocol.

Network data paths are assigned dynamically by the management module, and are allocated and de-allocated according to changes in the network.

Refer to Chapter 1 in the appropriate management module guide for an explanation of network path allocation.

SHOW PORT

Use the SHOW PORT command to display the mode and status of all ports or a specified port.

Format

SHOW PORT {slot.port} {option}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 32

{option} = no_verbose - Default if you press Enter
verbose

Examples

(separate examples for each protocol on the pages that follow)

Description

This command displays the port configurations indicating the port number, mode, status, and network assignment for the ports. When applicable, general information also displays. As shown in the examples to follow, the verbose option provides detailed information about the software and DIP switch settings for the modules.

Examples

Example 1 for Ethernet

The following example displays a summary status of all ports in the hub.

```
8250> show port all            [ENTER]

Port Display for Module E04PS-FIB:

Port  Mode       Status        Network      General Information
──────────────────────────────────────────────────────────────
03.01 ENABLED    OKAY          ETHERNET_2
03.02 DISABLED   LINK FAILURE  ETHERNET_2
03.03 ENABLED    OKAY          ETHERNET_1
03.04 DISABLED   LINK FAILURE  ETHERNET_1
— More —

Port Display for Module E08MS-RJ45S:

05.01 ENABLED    OKAY          ETHERNET_2
05.02 DISABLED   OKAY          ETHERNET_2
05.03 ENABLED    OKAY          ETHERNET_2
05.04 DISABLED   LINK FAILURE  ETHERNET_2
05.05 ENABLED    OKAY          ETHERNET_2
05.06 DISABLED   OKAY          ETHERNET_2
05.07 ENABLED    LINK FAILURE  ETHERNET_2
05.08 DISABLED   LINK FAILURE  ETHERNET_2

Port Display for Module E02PS-AUIF:

06.01 PRIMARY    OKAY         ETHERNET_2 Active; Buddy 06.02
06.02 BACKUP     OKAY         ETHERNET_2 Standby; Buddy 06.01
```

Example 2 for Ethernet

The following example displays a detailed status for a specific Ethernet port.

```
8250> show port 8.1 verbose    [ENTER]

Port Display for Module E02PS-AUIF:

Port  Mode      Status     Network        General Information
──────────────────────────────────────────────────────────────
08.01 ENABLED   OKAY       ETHERNET_2

Alert:                   ENABLED
Port Connector:          FEMALE AUI
Network Dip Setting:     ETHERNET_2
Mode Dip Setting:        ENABLED
```

The information that can be displayed in the Status column of the port configuration report is defined below.

Status Display	Indicates
Okay	The port is operating properly.
Link Failure	The port is not receiving a good signal. The possible causes: a cable break or lost connection.
RX Jabber	A jabber condition was detected on the link and the port was shut down. When the jabber condition is resolved, the port comes back up automatically.
Remote Link Failure	The remote port is not receiving a good signal from the port.
Remote Jabber	A jabber condition exists at the remote side of the link and the port has been shut down by the remote transceiver.
Invalid Data	Invalid data is being detected by the receiver.
Low Power	A fiber signal has been received at the low end of the power range. This condition does not shut down the port.
Fatal Error	An error has occurred in the module that makes it inoperable.
Partition	The port has been partitioned because 31 consecutive collisions have been received. No more traffic can be received by this port until the condition that caused the partition is cleared.

Example 1 for Token Ring

```
8250> show port 6.all verbose        [ENTER]

Port Display for Module T02MS-FIB :

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
```

The information that can be displayed in the Status column of the reports is defined below.

Status Display	Indicates
Okay	Port is operating properly.
Link Failure	Port is not receiving a good signal. The possible causes: a cable break or lost connection.
Fatal Error	Error has occurred in the module making 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	Phantom current is not detected at the Token Ring port because the station is powered down, no station is attached, a cable fault has occurred, or because the adapter card removed itself from the ring.

Example 1 for FDDI

The following command string displays a summary status, as shown in the example below, for all ports on the designated module.

```
8250> show port 8.all       [ENTER]

Port Display for Module F08MS-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 FDDI

The following command string displays a detailed status, as shown in the example below, for a specific FDDI port.

```
8250> show port 3.2 verbose          [ENTER]

Port Display for Module F08MS-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
```

The information that can be displayed in the Status and General Information columns of these reports is defined below.

Column	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 whether 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).

Column	Description
Network	Specifies the network to which the module is assigned.

General Information	The following information can be reported through this field:
	`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 Customer Support.)
	`Bad Bypass/Remote Port`
	(This error occurs only when the FMM boots up. See Technical Assistance in Chapter 6 in the *8250 FDDI Management Module Installation and Operation Guide*.)
	Note: Withholding M-M identifies an illegal configuration. **PCM Break State** may mean there is a hardware failure with the module.

SHOW RMON ALARM CONTROL

Use the SHOW RMON ALARM CONTROL command to view entries in the RMON alarm control table. For information on RMON control tables, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON ALARM CONTROL {index}

Parameters

{index} = index
all

Example

The following command shows alarm 1:

```
8250> show rmon alarm control        [ENTER]

RMON Alarm Control Information:

Index Interval            Sample Type Owner
----- ------------------- ----------- ----------------
    1 0 day(s) 01:00:00   Delta       system

Monitored Variable              : TokenRingMLStatsRingPurgePackets.1
Current Value                   : 0
Rising  Threshold / Event       : 5 / 3
Falling Threshold / Event       : 0 / 4
```

Description

This command displays entries in the RMON alarm control table.

SHOW RMON DISTRIBUTION DATA

Use the SHOW RMON DISTRIBUTION DATA command to display a graph showing the percentage of network traffic for each packet size.

Format

SHOW RMON DISTRIBUTION PROMISCUOUS DATA {index}

Parameters

{index} = index
all

Example

The following command displays RMON distribution statistics:

```
8250> show rmon distribution promiscuous data all [ENTER]

RMON Token Ring Distribution:

Distribution for index 1:

                    0%         25%        50%        75%        100%

Packet Size         |          |          |          |          |  Packets

-------------------------------------------------------------------------

18   to 63          | *********                                 | 10903
64   to 127         | ************************                  | 27837
128  to 255         |                                           | 288
256  to 511         | ****                                      | 4663
512  to 1023        |                                           | 690
1024 to 2047        |                                           | 0
2048 to 4095        |                                           | 0
4096 to 8191        |                                           | 0
8192 to 18000       |                                           | 0
Greater Than 18000  |                                           | 0
```

Description

This command displays a graph showing the percentage of network traffic for each packet size.

SHOW RMON EVENT CONTROL

Use the SHOW RMON EVENT CONTROL command to display entries from the RMON event control table. For information on RMON control tables, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON EVENT CONTROL {index}

Parameters

{index} = index
all

Example

The following command shows all events in the event control table:

```
8250> show rmon event control all     [ENTER]

RMON Event Control Information:

Index Type             Community        Time Since Sent     Owner
----- ---------------- ---------------- ------------------- --------
    1 Log              (None)           Not Triggered       monitor

Description: Internal log events

    2 Log and Trap      traps           Not Triggered       monitor

Description: MIB II events

    3 Log               public          Not Triggered       system

Description: RingPurgePackets limit exceeded!

    4 None              public          Not Triggered       system

Description: Re-arming RingPurgePackets alarm.
```

Description

This command displays entries from the RMON event control table.

SHOW RMON HOST CONTROL

Use the SHOW RMON HOST CONTROL command to view the RMON host control table. RMON control tables are used to configure RMON operation. For information on RMON control tables, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON HOST CONTROL {index}

Parameters

{index} = index
all

Example

The following command displays the RMON host control table:

```
8250> show rmon host control 1 [ENTER]
RMON Host Control Information:

Index Data Source     Table Size  Last Delete Time    Owner
----- --------------- ----------- ------------------- -------
    1 Interface 1              13 No Deletions        monitor
```

Description

This command displays the RMON host control table. RMON control tables are used to configure RMON operation.

SHOW RMON HOST DATA

Use the SHOW RMON HOST DATA command to display data from the RMON Host table. For information on RMON Host group data, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON HOST DATA {index} {order}

Parameters

{index} = index
all

{order} = all
all by_creation_order
all by_host_address
host_address *mac address*

Example

The following command displays RMON host statistics for one MAC address:

```
8250> show rmon host data 1 host_address 0-0-1a-24-0-0 [ENTER]

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
```

Description

This command displays RMON host data in the order you specify. The options are as follows:

Parameter	Description
all by_creation_order	Lists hosts by the order in which the RMON agent in the TRMM detected them.
all by_host_address	Lists hosts by numerical MAC address order.
host_address *mac address*	Displays host data for the specified MAC address.

SHOW RMON LOG DATA

Use the SHOW RMON LOG DATA command to display entries from the RMON event log. For information on RMON log data, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON LOG DATA {index}

Parameters

{index} = index
all

Example

The following command shows all events in the event control table:

```
8250> show rmon log data all [ENTER]

RMON Event Log Display:

Event Index 3
Index 1
Time 07 Dec 94 10:38:13

Alarm 1 rising 18 >= 1
```

Description

This command shows the result of any RMON event you create that sends its output to LOG. See the SET RMON EVENT command for more information.

SHOW RMON MATRIX CONTROL

Use the SHOW RMON MATRIX CONTROL command to view the RMON Token Ring matrix control table.

Format

SHOW RMON MATRIX CONTROL [index}

Parameters

{index} = index
all

Example

The following command displays the RMON matrix control table:

```
8250> show rmon matrix control 1  [ENTER]

RMON Matrix Control Information:

Index Data Source      Table Size Last Delete Time    Owner
----- ---------------- ---------- ------------------- ---------------

    1 Interface 3               0 No Deletions        system
```

Description

This command displays control table entries created by your RMON application or by using the SET RMON MATRIX Command. RMON control tables are used to configure RMON operation. For information on RMON control tables, refer to the *8250 TRMM User's Guide.*

SHOW RMON MATRIX DATA

Use the SHOW RMON MATRIX DATA command to display data for the RMON Matrix group. For information on RMON Matrix group data, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON MATRIX DATA {index} {sort order}

Parameters

{index} = index
all

{sort order} = by_destination_address
by_source_address
involving mac_address

Example

The following command displays RMON matrix entries ordered numerically by destination MAC address:

```
8250> show rmon matrix data 1 by_destination_address[ENTER]

RMON Matrix display for Interface 1 :

Source Address                  : 11-22-33-44-55-66
Destination Address             : 11-22-33-44-55-66
Index                           : 1
Packets                         : 2
Octets                          : 36
Errors                          : 0

Source Address                  : 11-22-33-44-55-66
Destination Address             : c0-00-00-00-00-02
Index                           : 1
Packets                         : 4
Octets                          : 248
Errors                          : 0

Source Address                  : 11-22-33-44-55-66
Destination Address             : c0-00-00-00-00-10
Index                           : 1
Packets                         : 2
Octets                          : 84
Errors                          : 0

Source Address                  : 11-22-33-44-55-66
Destination Address             : c0-00-ff-ff-ff-7f
Index                           : 1
Packets                         : 393
Octets                          : 12576
Errors                          : 0

End of Matrix Table.
```

Description

This command shows a record of conversations between hosts on your system.

SHOW RMON RINGSTATION CONTROL

Use the SHOW RMON RINGSTATION CONTROL command to view the RMON Token Ring Ring-Station control table.

Format

SHOW RMON RINGSTATION CONTROL [index}

Parameters

{index} = index
all

Example

The following command displays the RMON Ring Station control table:

```
8250> show rmon ringstation control all [ENTER]

RMON Ring Station Control Table:

Index                          : 1
Table Size                     : 6
Active Stations                : 6
Ring State                     : 1
Beacon Sender                  : 00-00-00-00-00-00
Beacon NAUN                    : 00-00-00-00-00-00
Active Monitor                 : 10-00-5a-7a-a6-b3
Order Changes                  : 1
Owner                          : monitor
```

Description

This command displays control table entries created by your RMON application or by using the SET RMON RINGSTATION Command. RMON control tables are used to configure RMON operation. For information on RMON control tables, refer to the *8250 TRMM User's Guide.*

SHOW RMON RINGSTATION DATA

Use the SHOW RMON RINGSTATION DATA command to display data from the RMON Token Ring Ring-Station group. For information on RMON Token Ring Ring-Station group data, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON RINGSTATION DATA {index} {order}

Parameters

{index} = index
all

{order} = all
order
host_address *mac address*

Examples

The following command displays RMON Ring Station statistics for one MAC address:

```
8250> show rmon ringstation data 1 host_address 0-0-0-0-10-40
[ENTER}

RMON Ring Station Group:

Index                          : 1
Mac Address                    : 00-00-00-00-10-40
Last NAUN                      : 00-00-00-00-00-00
Station Status                 : 2
Last Enter Time                : 06 Dec 94 16:16:02
Last Exit Time                 : 06 Dec 94 16:16:02
Duplicate Address              : 0
In Line Errors                 : 0
Out Line Errors                : 0
Internal Errors                : 0
In Burst Errors                : 0
Out Burst Errors               : 0
AC Errors                      : 0
Abort Errors                   : 0
Lost Frame Errors              : 0
Congestion Errors              : 0
Frame Copied Errors            : 0
Frequency Errors               : 0
Token Errors                   : 0
```

```
In Beacon Errors                : 0
Out Beacon Errors               : 0
Insertions                      : 0
```

The following example shows the order of MAC addresses in a ring containing two stations:

```
8250> show rmon ringstation data 1 order [ENTER]
RMON Ring Station Order:

Index                           : 1
Order Index                     : 1
Mac Address                     : 10-00-f1-0f-3a-e0


Index                           : 1
Order Index                     : 2
Mac Address                     : 00-00-30-80-ef-b3


End of Table
```

Description

This command displays RMON host data in the order you specify. The options are as follows:

Parameter	Description
all	Lists all ring stations.
order	Lists ring stations in token-passing order.
host_address *mac address*	Lists ring station data for the specified MAC address.

SHOW RMON STATISTICS CONTROL

Use the SHOW RMON STATISTICS CONTROL command to view the RMON Statistics group control tables.

Format

SHOW RMON STATISTICS {type} CONTROL {index}

Parameters

{type} = mac_layer
promiscuous
sourcerouting

{index} = index number or all

Example

The following command displays the RMON MAC Layer control table:

```
8250> show rmon statistics mac_layer control 1 [ENTER]

RMON Token Ring Mac Layer Statistics Control Table:

Index  Data Source                    Owner
-----  -----------                    -----
    1  Interface 1                    monitor
```

Description

This command shows the RMON control table entries for RMON statistics created by an RMON application or by using the SET RMON STATISTICS command. RMON control tables are used to configure RMON operation. For information on RMON control tables, refer to the *8250 TRMM User's Guide*.

SHOW RMON STATISTICS DATA

Use the SHOW RMON STATISTICS command to display data from RMON Statistics groups.

Format

SHOW RMON STATISTICS {type} DATA {index}

Parameters

{type} = mac_layer
promiscuous
sourcerouting

{index} = index number or all

Example

The following command displays Source Routing group statistics:

```
8250> show rmon statistics sourcerouting data 1 [ENTER]
RMON Token Ring Source Routing Statistics:
Ring Number                      : 1
In Frames                        : 0
Out Frames                       : 0
Through Frames                   : 0
All Routes Broadcast Frames      : 0
Single Routes Broadcast Frames   : 2
In Octets                        : 0
Out Octets                       : 0
Through Octets                   : 0
All Routes Broadcast Octets      : 0
Single Routes Broadcast Octets   : 420
Local LLC Frames                 : 85533
1 Hop Frames                     : 0
2 Hop Frames                     : 0
3 Hop Frames                     : 0
4 Hop Frames                     : 0
5 Hop Frames                     : 0
6 Hop Frames                     : 0
7 Hop Frames                     : 0
8 Hop Frames                     : 0
More Than 8 Hops Frames          : 0
```

Description

This command displays data collected for the group you have selected. For information on RMON Statistics group data, refer to the *8250 TRMM User's Guide*.

SHOW RMON TOPN_HOSTS CONTROL

Use the SHOW RMON TOPN_HOSTS CONTROL command to view the RMON Token Ring Host Top N control table.

Format

SHOW RMON TOPN_HOSTS CONTROL [index}

Parameters

{index} = index
all

Example

The following command displays the RMON Host Top N control table:

```
8250> show rmon topN_hosts control
Enter index: 1

RMON Host Top N Control Information :

-------------------------------------------------------------------

TopN Index Duration            Requested Size   Rate Base
---------- ------------------- ---------------- ----------------
     1     0 day(s) 00:30:00                10 Output Packets

Host Index Start Time          Granted Size     Owner
---------- ------------------- ---------------- ----------------
     1     26 Mar 96 17:25:56               10 system

-------------------------------------------------------------------
```

Description

This command displays control table entries created by your RMON application or by using the SET RMON TOPN_HOSTS Command. RMON control tables are used to configure RMON operation. For information on RMON control tables, refer to the *8250 TRMM User's Guide.*

SHOW RMON TOPN_HOSTS DATA

Use the SHOW RMON TOPN_HOSTS DATA command to display data for the RMON Host Top N group. For information on RMON Host Top N group data, refer to the *8250 TRMM User's Guide*.

Format

SHOW RMON TOPN_HOSTS DATA {data index}

Parameters

{data index} = rank of host among the top data entries collected, or all

Example

The following command displays data for all 10 hosts:

```
8250> show rmon topN_hosts data all   [ENTER]

RMON Host Top N Display for Interface 1 :
Index Address           Input Packets
----- ----------------- ------------------------
   1  c0-00-ff-ff-ff-ff                      1258
   2  c0-00-00-00-00-02                       755
   3  c0-00-00-00-00-10                       315
   4  11-22-33-44-55-66                       314
   5  c0-00-ff-e7-32-8b                        79
   6  c0-00-00-12-14-02                        60
   7  34-00-29-ef-c0-10                        42
   8  9a-22-33-44-55-66                        22
   9  9a-22-33-00-00-02                         0
  10  34-00-29-00-00-10                         0
```

Description

This command shows the top 10 entries for a any RMON TOPN_HOSTS DATA collected. The data index tells the command which control table entry you want to view data for. The data index lets you view data for a particular host on the list. To view data for all hosts, select all.

SHOW SCHEDULE

Use the SHOW SCHEDULE command to display schedule information for all schedules or a specific schedule.

Format

SHOW SCHEDULE {schedule}

Parameters

{schedule} = all
schedule_index
holiday
startup_replay_time
weekday
weekend

Example

The following example displays all current schedule information.

```
8250> show schedule all [ENTER]

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
```

Description

This command displays schedule information for all schedules or a specific schedule. A plus (+) next to a date indicates the date is included in the schedule. A minus (-) indicates a date is excluded from the schedule.

SHOW SCRIPT

Use the SHOW SCRIPT command to display information about a specific script or all scripts.

Format

SHOW SCRIPT {script number} {option}

Parameters

{script number} = all
1 through 8

{option} = no_verbose
verbose

Example

The following example displays script information for all eight scripts.

```
8250> show script all [ENTER]

Script Number           Script Name
    1                   eng
    2                   sales3
    3                   tech.pubs
    4                   (No Name Assigned)
    5                   (No Name Assigned)
    6                   finance1
    7                   finance2
    8                   sales1
```

Description

This command displays script information on a specific script or all scripts. The 'verbose' option displays the list of commands in the script(s).

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.

Format

SHOW SECURITY AUTOLEARN {slot.port}

Parameters

{slot} = 1 through 17

{port} = 1 through 12

Example

The following example displays the Autolearning database entries for the ports on the 8250 10BASE-T Security Module in slot 3.

```
8250> show security autolearn 3.all [ENTER]


Autolearned Addresses for Module E12MS-TELCOS 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 4
security addresses autolearned for it. Only the first 4
addresses per port (as ordered by MAC address) will be
downloaded; extraneous addresses are marked in the display
above with an asterisk.
```

Description

A single asterisk (*) marks entries for a port that exceeds the maximum of four MAC addresses per port. A double asterisk (**) marks entries that have exceeded the hub capacity of 360 MAC addresses. Entries that exceed the 360 maximum (that is, the 361st entry and greater) will not be downloaded.

If your hub is near full capacity, or if you have ports connected to bridges, you may wish to perform two or more Autolearn Captures, which may prevent these ports from exceeding the EMM limit of 360 MAC addresses per hub or the TRMM limit of 400 MAC address per hub.

Use the CLEAR SECURITY AUTOLEARN MAC_ADDRESS command to clear a MAC address or all MAC addresses for a specified port, all ports on a module, or all ports on all modules in the hub.

SHOW SECURITY INTRUDER_LIST

Use the SHOW SECURITY INTRUDER_LIST command to display information regarding the 10 most recent security intrusions.

Format

SHOW SECURITY INTRUDER_LIST

Parameters

none

Example

The following example displays the intruder list.

```
8250> show security intruder_list [ENTER]

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
```

Description

This command displays information regarding the 10 most recent security intrusion attempts. The display includes the port that experienced the intrusion, 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, and whether the management module automatically disabled the port.

Use the CLEAR SECURITY INTRUDER_LIST command to clear all entries from the Intruder list.

The Intruder list contains a maximum of 10 entries. Therefore, when the Intruder list contains 10 entries and a new entry is added, the oldest entry is cleared automatically.

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.

When using an EMM to define or show security, only the EMM Advanced supports the security feature. However, all versions of the EMM (Starter, Basic, Advanced) support the 8250 10BASE-T Security Module.

Format

SHOW SECURITY PORT {slot.port} {option}

Parameters

{slot} = 1 through 17 or all

{port} = 1 through 24 or all

{option} = no_verbose
verbose

Example

Example 1

The following example displays security information for all ports on the 8250 10BASE-T Security Module in slot 3.

```
Security Display for Module E12MSS in Slot 3:

Port   Mode       MAC Addresses   General Information
----   --------   -------------   -------------------

3.01   DISABLED   NONE            ETHERNET_1
3.02   DISABLED   NONE            ETHERNET_1
3.03   DISABLED   NONE            ETHERNET_1
3.04   DISABLED   NONE            ETHERNET_1
```

Example 2

The following example displays all security information for the 8250 10BASE-T Security Module in slot 17.

```
8250> show security port 17.all    [ENTER]

Security Display for Module E12MSS in Slot 17 :
Port   Mode        MAC Addresses       General Information
———-   ————-       ——————————————-   ——————————————————-
17.01  DISABLED    17-01-01-01-01-01   ETHERNET_1
17.02  EAVESDROP   NONE                ETHERNET_1
17.03  INTRUSION   01-02-03-04-05-06   ETHERNET_1
                   01-02-03-04-05-07
17.04  FULL        NONE                ETHERNET_1
17.05  FULL        NONE                ETHERNET_1
17.06  FULL        NONE                ETHERNET_1
17.07  FULL        NONE                ETHERNET_1
17.08  FULL        03-02-01-00-09-08   ETHERNET_1
                   03-02-01-00-09-09
17.09  FULL        NONE                ETHERNET_1
17.10  FULL        NONE                ETHERNET_1
17.11  FULL        NONE                ETHERNET_1
17.12  DISABLED    NONE                ETHERNET_1
```

Description

This command displays security information for a specific port, all ports on a module, or all ports on all modules in a hub.

SHOW TERMINAL

Use the SHOW TERMINAL command to display the terminal parameter values.

Format

SHOW TERMINAL

Parameters

none

Example

```
8250> show terminal        [ENTER]

Terminal Session Parameters:
  Prompt:       8250>
  Timeout time: 0

Console Port Parameters:
  Baud:         9600
  Data bits:    8
  Parity:       NONE
  Stop bits:    2
  Hangup:       DISABLED
  Terminal:     VT100
```

Description

These parameters are described in detail in the SET TERMINAL section.

SHOW TFTP

Use the SHOW TFTP command to display the TFTP parameters.

Format

SHOW TFTP

Parameters

none

Example

```
8250> show tftp   [ENTER]

- - - - - TFTP Variables - - - - -

TFTP Server IP Address:     151.36.58.117
TFTP File Name:             TRMMf.bin
TFTP File Type:             flash
TFTP Result:                OKAY
```

Description

This command displays the TFTP parameters that were set using the SET TFTP FILE_NAME, SET TFTP FILE_TYPE, and SET TFTP SERVER_IP_ADDRESS commands.

The information that displays is defined below.

Field	Description
TFTP Server IP Address	Address of the server that contains the download file.
TFTP File Name	Name of the file that is downloaded to this TRMM.
TFTP File Type	Type of file to be downloaded (Flash or Boot).
TFTP Result	Status of the last download.

SHOW THRESHOLD

Use the SHOW THRESHOLD command to display one or all threshold entries in the threshold table. Only the Advanced TRMM supports thresholding.

Format

SHOW THRESHOLD {index}

Parameters

{index} = all
1 through 10

Examples

Example 1

The following example displays all threshold entries.

```
8250> show threshold all              [ENTER]

                    Threshold   Current
Index   Mode        Value       Value     Data Source
-----   --------    -----       -------   ------------------------------
1       ENABLED     7000        —-        Network TOKEN_RING_1 : Octets
2       ENABLED     9000        15000     Port 14.1 : Broadcast Frames
3       DISABLED    5000        10000     Port 14.1 : Frames
4       DISABLED                0         Network TOKEN_RING_1 : Errors
5       CLEARED                 0         (not initialized)
6       ENABLED     3500        5000      Port 14.1 : Broadcast Frames
7       ENABLED     30          50        Station 10-00-f1-0f-0c-6f:Errors
8       DISABLED                0         Port 14.1 : Multicast Frames
9       DISABLED                0         Network TOKEN_RING_1:Frames
10      CLEARED                 0         (not initialized)
```

Example 2

The following example displays threshold information for threshold entry 1.

```
8250> show threshold 1  [ENTER]

Index:                          1
Mode:                           ENABLED
Description:                    Set for TR1 Network Frames
Data Source:                    Network TOKEN_RING_1: Frames
Threshold Value:                7000
Current Value:                  —-
Interval:                       0:01:00
Time Since Last Triggered:      (never)
```

Description

The SHOW THRESHOLD command enables you to display one or all threshold entries from the threshold table.

SHOW TRUNK

Use the SHOW TRUNK command to display the status of the trunk connections of 8250 Token Ring Modules and 8250 FDDI Modules.

Format

SHOW TRUNK {slot} {parameter} {option}

Parameters

{slot} = 1 through 17 or all

{parameter} = all

ring_in.{trunk port}
ring_out.{trunk port}

backplane_in
backplane_out

{option} = no_verbose (default if you press ENTER)
verbose

Example

```
8250> show trunk 1 ring_in.1 verbose     [ENTER]

Trunk Display for Module T02MS-FIB :

Slot Trunk      Mode     Status       Network       General Information
---- ---------- -------- ------------ ------------- -----------------
 01  RING_IN.1  PRIMARY  OKAY         TOKEN_RING_2  Active ; Buddy: 02

Trunk Type:                           FIBER
Trunk Connector:                      FIBER
Trunk Wrap State:                     UNWRAPPED
Trunk Mode Dip Setting:               ENABLED
Compatibility Mode Setting:           DISABLED
Compatibility Mode Dip Setting:       DISABLED
External Beacon Recovery:             NON_EXISTS
```

Description

Use this command to display the status of the trunk connections of 8250 Token Ring Modules and 8250 FDDI Modules.

SMT_GET ACCESS

Use the SMT_GET ACCESS command to display the current access for a remote station. This command is available for FMM only.

Format

SMT_GET ACCESS

Parameters

none

Example

```
8250> smt_get access     [ENTER]
SMT Access: permissive.
```

Description

The SMT standard describes a mechanism by which an SMT station can get and set SMT operational parameters for a remote SMT station. These Get and Set operations are sent from one station to another using PMF (Parameter Management Frames) over the network.

Once SMT access has been specified (see SMT_SET ACCESS later in this chapter), use the SMT_GET ACCESS command to display the current status.

For additional information, refer to the Station Management (SMT) standard for FDDI.

SMT_GET MAC_TIMERS

Use the SMT_GET MAC_TIMERS command to display current values for all MAC-related timers for an FMM.

Format

SMT_GET MAC_TIMERS

Parameters

none

Example

```
8250> smt_get mac_timers      [ENTER]

FDDI MAC Operations Group Timers

Treq                165.007
Tneg                 15.827
Tmax                170.000
TvxValue              3.420
Tmin                    4.014
```

Description

As shown in the above example, this command displays a current status of all MAC-related timers, where:

Treq = the station's bid for the Target Token Rotation Time (TTRT).

Tneg = the negotiated TTRT for all stations on the ring. Note that Tneg is only valid if the ring is operational.

Tmax = the station's upper boundary for the TTRT. If TTRT is greater than Tmax, then this station will not be able to enter the ring.

TvxValue = the reinitialization threshold. If no activity is detected on the ring (that is, no frames or tokens) for the time given to TVX, then this station forces a re-initialization of the ring.

Tmin = the station's lower boundary for the TTRT. If TTRT is less than Tmin, then this station will not be able to enter the ring.

SMT_GET PATH_TIMERS

Use the SMT_GET PATH_TIMERS command to display current values for all path-related timers. This command is available for FMM only.

Format

SMT_GET PATH_TIMERS

Parameters

none

Example

```
8250> smt_get path_timers      [ENTER]

FDDI Path Class Configuration Group

Trace MaxExpiration                7000.0
TVXLowerBound                       3.420
T MaxLowerBound                      170.000
```

Description

As shown in the above example, this command displays a current status of all path-related timers, where:

Trace MaxExpiration - Maximum amount of time this station has to complete the Trace process.

TVXLowerBound - Reinitialization threshold. If no activity is detected on the ring (that is, no frames or tokens) for the time given to TVX, then this station forces a reinitialization of the ring.

T MaxLowerBound - Station's upper boundary for the TTRT. If TTRT is greater than Tmax, then this station cannot enter the ring.

SMT_GET USER_DATA

Use the SMT_GET USER_DATA command to display any information stored through the SMT_SET USER_DATA command. This command is available for FMM only.

Format

SMT_GET USER_DATA {data}

Parameters

{data} = user-defined data

Example

```
8250> smt_get user_data       [ENTER]
User_Data: “                          ”
```

Description

This command reports information stored through the SMT_SET USER_DATA command.

SMT_SET ACCESS

Use the SMT_SET ACCESS command to manage the use of SMT commands from an external SMT workstation.

Format

SMT_SET ACCESS {setting}

Parameters

{setting} = restrictive
permissive

Example

Example 1

The following command enables an external SMT workstation to issue both SMT GET and SMT SET commands.

```
8250> smt_set access permissive      [ENTER]
SMT access set to permissive.
```

Example 2

The following command restricts the use of SMT commands from an external SMT workstation.

```
8250> smt_set access restrictive      [ENTER]
SMT access set to restrictive.
```

Description

The SMT_Set Access command enables you to prevent or allow a remote SMT station to set operational parameters for a local station. Setting SMT access to “restrictive” prevents all remote stations from changing any parameter. Setting SMT access to “permissive” allows any remote station on the ring to change any parameters.

SMT_SET MAC_TMAX

Use the SMT_SET MAC_TMAX command to specify the maximum value supported by this station when bidding for the TTRT. This command is available for FMM only.

Format

SMT_SET MAC_TMAX {number}

Parameters

{number} = between 10.4860 and 1342.1777 milliseconds
(167.77216 is the default if you press [ENTER])

Example

```
8250> smt_set mac_tmax 173.15      [ENTER]
Timer set to 173.15 milliseconds.
```

Description

This command allows you to specify the maximum value allowed by this station when bidding for the ring's Target Token Rotation Time (TTRT).

SMT_SET MAC_TMIN

Use the SMT_SET MAC_TMIN command to specify the minimum value supported by this station when bidding for the TTRT. This command is available for FMM only.

Format

SMT_SET MAC_TMIN {number}

Parameters

{number} = between 0 and 5.24288 milliseconds
(4.01408 is the default if you press [ENTER])

Example

```
8250> smt_set mac_tmin 4.15      [ENTER]
Timer set to 4.15 milliseconds.
```

Description

This command requires that you specify the minimum value supported by this station when bidding for the ring's Target Token Rotation Time (TTRT).

SMT_SET MAC_TREQ

Use the SMT_SET MAC_TREQ command to specify the Treq value to be used for the bidding process to determine a TTRT for the ring. This command is available for FMM only.

Format

SMT_SET MAC_TREQ {number}

Parameters

{number} = between 0 and 1342.1777 milliseconds
(165.00736 is the default if you press [ENTER])

Example

```
8250> smt_set mac_treq 165.8       [ENTER]
Timer set to 165.8 milliseconds.
```

Description

Treq sets the station's bid for the Target Token Rotation Time (TTRT). The station with the lowest Treq wins this bidding process. The lowest Treq value then becomes the TTRT, which is shared by all stations on the ring. The smaller the TTRT, the faster each station's response time (however the station will have less time to transmit data). The larger the TTRT, the slower the response time (however the station will have a longer time to transmit data).

SMT_SET PATH_TVX

Use the SMT_SET PATH_TVX command to specify the TVX timer for the path. This command is available for FMM only.

Format

SMT_SET PATH_TVX {number}

Parameters

{number} = between 0.02048 and 5.24288 milliseconds
(3.42016 is the default if you press [ENTER])

Example

```
8250> smt_set path_tvx 4.4    [ENTER]
Timer set to 4.4 milliseconds.
```

Description

This command allows you to specify the TVX timer for the path.

The TVX timer determines the length of time a ring remains inactive (no token or frames seen by the MAC) before the MAC reinitializes the ring. This timer should be greater than 3.4 milliseconds and less than the Target Token Rotation Time (TTRT).

SMT_SET USER_DATA

Use the SMT_SET USER_DATA command to store information about your FMM.

Format

SMT_SET USER_DATA {user data}

Parameters

{user data} = 32-byte string

Example

```
8250> smt_set user_data engineering  [ENTER]
User_Data changed to “engineering”
```

Description

This command allows you to store a 32-byte string of ASCII data. You may want to use this command to uniquely identify the FMM.

TELNET

Use the TELNET command to log in to any management module, or any other device on the network and communicate from a remote terminal. Only one Telnet session to or from a management module is allowed at a time, except for TRMM, which allows up to four incoming sessions.

Format

TELNET {ip address} {telnet port}

Parameters

{ip address} = Internet Protocol address
n.n.n.n

{telnet port} = integer (for the 8250 Ethernet Terminal Server Module only)

Example

The following command Telnets into a device using its IP address.

```
8250> telnet 127.36.58.7 [ENTER]
```

Some management module versions will require that you press Enter after the connection is established in order to initiate the password prompt.

```
Password: password   [ENTER]
```

Description

Use the TELNET command and the IP address of the remote management module (or other device supporting TELNET) to which you want to connect. Once you are logged in to the remote device, enter the correct password for that device.

Use the LOGOUT command to remove the connection from the remote device and return to the local management module.

Refer to the following suggestions if you are having trouble establishing a Telnet session:

- Make sure the device is on the same network (segment) or that it is bridged or routed to that segment. Use the PING command to test the connection.
- If you attempt to establish a Telnet session to a device that already has a Telnet session in progress, the second Telnet request (and subsequent requests) is placed into a queue. This request remains in the queue until the first Telnet session is removed, or it times out after 4 to 5 minutes elapse.
- If you establish and remove multiple Telnet sessions (for example, three) within 4 minutes, the fourth Telnet attempt may not be successful. Retry until the session establishes successfully.
- If you cannot establish a Telnet session with a Token Ring device, it may be because the device is experiencing receive congestion errors. Resolve the receive congestion errors before attempting to establish another Telnet session.

Note: You can remotely log in to (using TELNET or Remote_Login) only one management module at a time. That is, in order to establish a remote connection to a second device, you must first log out of the initial device.