Manageable Media Conversion Center

LM C1600A

#33070
CAUTION: RJ connectors are NOT INTENDED FOR CONNECTION TO THE PUBLIC TELEPHONE NETWORK. Failure to observe this caution could result in damage to the public telephone network.

Compliance Information
UL Listed
C-UL Listed (Canada)
CISPR/EN55022 Class A

FCC Regulations
This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at the user's own expense.

Canadian Regulations
This digital apparatus does not exceed the Class A limits for radio noise for digital apparatus set out on the radio interference regulations of the Canadian Department of Communications.

European Regulations
Warning
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Copyright Restrictions
© 1998 Black Box Corporation
All rights reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical – without written permission from Black Box Corporation.

Trademark Notice
All registered trademarks and trademarks are the property of their respective owners.
# Table of Contents

Preface .................................................. iii

1 INTRODUCTION ........................................ 1.1

1.1 The 16-Slot Media Conversion Center ............ 1.2
   Media-Converter Slide-in-Modules ............... 1.3
   Optional Management Module .................. 1.3
   Power Supply Module(s) ...................... 1.3

1.2 The 16-Slot Media Conversion Center in the Network . 1.4

1.3 Connectors, Indicators, and Switches .......... 1.5

1.4 Optional SNMP Management .................... 1.6

2 SITE PLANNING ....................................... 2-1

3 INSTALLATION ....................................... 3.1

3.1 Unpacking LMC1600A Equipment ................. 3.2

3.2 Installing Optional Redundant Power Supply Module in LMC1600A Chassis .......................... 3.3

3.3 Installing Optional Management Module in LMC1600A Chassis .......................... 3.4

3.4 Installing One or More Media Converter Slide-in-Module(s) in LMC1600A Chassis ................ 3.5

3.5 Installing the LMC1600A in Rack or on Table ...... 3.6
   Standard 19-Inch Rack Installation ............ 3.6
   Table-Top Installation ...................... 3.7

3.6 Connecting Media Converter Slide-In-Modules to Network ........................................ 3.7

3.7 Connecting Management Module to Command-Line Interface ........................................ 3.8
# LMC1600A

## 3.8 Connecting Management Module to Network Management Station

## 3.9 Powering the LMC1600A

## 3.10 Using Command-Line Interface to Set IP Parameters

## 3.11 Optionally Using SNMPc™ at NMS to Monitor LMC1600A Status

## 4 Operation

4.1 Using Status LEDs

4.2 Using the Command-Line Interface

4.3 Using SNMP

## 5 Maintenance

5.1 Fault Isolation and Recovery

5.2 Hardware Replacement Procedures

5.3 Firmware Upgrades

## Appendix

Appendix A. Media Conversion Center Technical Specifications

Appendix B. Null Modem Cable Specifications

Appendix C. Introduction to SNMP in the LMC1600A

Appendix D. SNMP Glossary

Appendix E. Messages at Command-line Interface

## Index
Preface

This user's guide is intended for the network administrator responsible for installing, configuring, using, and maintaining a Black Box Corporation 16-Slot Media Conversion Center. A working knowledge of local area network (LAN) operations, including familiarity with communications protocols used on interconnected LANs, is assumed.
1 INTRODUCTION

The modular, scalable Black Box Corporation 16-Slot Media Conversion Center (LMC1600A) allows the network administrator to select from among Black Box Corporation Media Converter Slide-in-Modules, to install the Media Converter Slide-in-Modules in the powered LMC1600A chassis, and then to connect various network media, at a central wiring location, through the Media Converter Slide-in-Modules.

If an SNMP Management Module is installed in the LMC1600A, the network administrator also can use a remote Network Management Station to monitor the status of the LMC1600A and of any installed Media Converter Slide-in-Modules.

As network conditions change, the network administrator can add or swap Media Converter Slide-in-Modules, can install a redundant Power Supply Module (if not originally configured and factory installed) and/or can install the SNMP Management Module (if not originally configured and factory installed).

This introduction to the LMC1600A 16-Slot Media Conversion Center provides:

1.1 The 16-Slot Media Conversion Center .......................... 1-2
1.2 The 16-Slot Media Conversion Center in the Network .... 1-4
1.3 Connectors, Indicators, and Switches ...................... 1-5
1.4 Optional SNMP Management .............................. 1-6
1.1 The 16-Slot Media Conversion Center

The Black Box Corporation LMC1600A 16-Slot Media Conversion Center chassis provides installation space for up to sixteen Media Converter Slide-in-Modules, up to two Power Supply Modules, and one SNMP Management Module, as shown in the cut-out top view below:

NOTE: Media Converter Slide-in-Modules, Power Supply Modules, and Management Modules are all hot-swapable.
MEDIA CONVERTER SLIDE-IN-MODULES

Selectable Media Converter Slide-in-Modules installed in slots at the front of the Media Conversion Center allow the network administrator to connect various network media.

NOTE: Refer to the documentation that comes with each Media Converter Slide-in-Module for connector and LED indicator information specific to that Media Converter Slide-in-Module.

POWER SUPPLY MODULE(S)

A Power Supply Module, installed at the back of the Media Conversion Center before shipment, supplies power to installed Media Converter Slide-in-Modules and to the optional SNMP Management Module. An optional redundant Power Supply Module also can be installed at the back of the Media Conversion Center.

OPTIONAL MANAGEMENT MODULE

An optional Management Module that can be installed at the back of the Media Conversion Center, with an LMC1600A SNMP MIB, allows the network administrator to monitor the Media Conversion Center and installed Slide-In-Modules status using SNMP network management.
1.2 The 16-Slot Media Conversion Center in the Network

Using Media Converter Slide-in-Modules installed in the 16-Slot Media Conversion Center, the network administrator can connect various network media at a central wiring location.

As new media are added to the network, the network administrator installs new Media Converter Slide-in-Modules to support the changed network requirements.
1.3 Connectors, Indicators, and Switches

Connectors

AC power connectors are located on the Power Supply Module(s) installed at the back of the Media Conversion Center.

A serial port for accessing the command-line interface and an Ethernet port, through which the Management Module communicates with a remote Network Management Station (NMS), are available at the Management Module installed at the back of the Media Conversion Center.

NOTE: Connectors to network media are located on each Media Converter Slide-In-Module installed at Media Conversion Center front.

Switches

Power ON/OFF switches are located on each Power Supply Module installed at the Media Conversion Center back.

A reset switch is located on the Management Module installed at the back of the Media Conversion Center.

Power Modules Indicators

Power and In Use Power Supply Module LED indicators are located at the front of the Media Conversion Center.

NOTE: A Power LED indicator also is located on each Power Supply Module installed at the back of the Media Conversion Center.

Management Module Indicators

Power, Link, RX (receive) and TX (transport) Management Module LED indicators are located at the front of the Media Conversion Center.

NOTE: Network management indicators located on the Management Module installed at the back of the Media Conversion Center loosely mirror the network management indicators located on the front of the Media Conversion Center.
1.4 **Optional SNMP Management**

The 16-Slot Media Conversion Center provides an optional SNMP Management Module with an installed LMC1600A SNMP MIB to enable SNMP network management from a remote Network Management Station (NMS).

A command-line interface at a terminal or terminal emulator attached to the Management Module allows the network administrator to configure IP addresses during the initial installation and to monitor the LMC1600A using messages displayed at the command-line interface.

A Telnet option over the network also is available for access to the Management Module.
2 SITE PLANNING

The site for the 16-Slot Media Conversion Center must provide the following:

- AC power outlet for each Power Supply Module in the 16-Slot Media Conversion Center
- Adequate ventilation
- Standard environmental conditions
- Isolation from electrical noise, including radio transmitters and broadband amplifiers, motors, high power electrical lines, or fluorescent light fixtures.

Additionally:

- Twisted pair cables should not run in the same conduit with power line cables
- Phone lines should be separated from data cables
- Flat or “silver satin” wires should not be used.
3 INSTALLATION

Direction is provided in the pages that follow for the steps required to install the LMC1600A 16-Slot Media Conversion Center:

3-1 Unpacking the LMC1600A Equipment ................. 3-2
3-2 Installing Optional Redundant Power Supply in LMC1600A ... Chassis ........................................ 3-3
3.3 Installing Optional Management Module in LMC1600A ...... Chassis ........................................ 3-4
3.4 Installing One or More Media Converter Slide-in-Module(s) in LMC1600A Chassis ........................................ 3-5
3.5 Installing the LMC1600A in Rack or on Table ............ 3-6
3.6 Connecting Media Converter Slide-In-Modules to Network .3-7
3.7 Connecting Command-Line Interface to Management Module .. ............................................ 3-8
3.8 Connecting Network Management Station to Management Module ............................................ 3-9
3.9 Powering the LMC1600A ........................................ 3-10
3.10 Using Command-Line Interface to Set IP Parameters .3-11
3.11 Optionally Using SNMPc™ at NMS to Monitor Status .3-12
### 3.1 Unpacking LMC1600A Equipment

Use the following list to verify the shipment:

<table>
<thead>
<tr>
<th>Item</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-Slot Media Conversion Center: LMC1600A with Power Cord</td>
<td>LMC1600A</td>
</tr>
<tr>
<td>User's Guide</td>
<td>33070</td>
</tr>
<tr>
<td>Redundant Power Supply Module</td>
<td>LMC1600-PS (optional)</td>
</tr>
<tr>
<td>Management Module</td>
<td>LMC1600-MM (optional)</td>
</tr>
<tr>
<td>Black Box Corporation SNMP graphical display software for Win95</td>
<td>SNMPc (optional)</td>
</tr>
<tr>
<td>One or more selectable Media Converter Slide-in- Modules</td>
<td>LMC160x</td>
</tr>
</tbody>
</table>
3.2 Installing Optional Redundant Power Supply Module in LMC1600A Chassis

WARNING: Do NOT connect the Power Supply Module to AC power before installing completely in the 16-Slot Media Conversion Center (steps 1-5, below). Failure to observe this caution could result in equipment damage and/or personal injury or death.

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Power Supply Module in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Power Supply Module.

To install the Redundant Power Supply Module in the LMC1600A chassis:

1. Carefully place LMC1600A on table or other flat, stable surface.
2. Locate Redundant Power Supply Module installation slot on back of LMC1600A.
3. Remove Redundant Power Supply Module protective plate from installation slot by removing two screws that secure plate to back of LMC1600A.
4. Carefully slide Redundant Power Supply Module into installation slot, aligning Redundant Power Supply Module with installation guides:
   NOTE: Ensure that the Redundant Power Supply Module is firmly seated against the backplane.
5. Carefully rotate panel fastener screws (PROVIDED WITH POWER SUPPLY MODULE) clockwise to secure.
3.3 Installing Optional Management Module in LMC1600A Chassis

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Management Module in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Management Module.

To install the Management Module in the LMC1600A chassis:

1. Carefully place LMC1600A on table or other flat, stable surface.
2. Locate Management Module installation slot on back of LMC1600A.
3. Remove Management Module protective plate from installation slot by removing two screws that secure plate to back of LMC1600A.
4. Carefully slide Management Module into installation slot, aligning the Management Module with the installation guides. NOTE: Ensure that the Management Module is firmly seated against the backplane.
5. Carefully rotate panel fastener screws clockwise to secure.
3.4 Installing One or More Media Converter Slide-in-Module(s) in LMC1600A Chassis

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Media Converter Slide-in-Module(s) in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Media Converter Slide-in-Module(s).

To install the Media Converter Slide-in-Module in the LMC1600A chassis:

1. Carefully place the LMC1600A on table or other flat, stable surface.
2. Locate sixteen (16) Media Converter Slide-in-Module installation slots at the front of the LMC1600A.
   NOTE: Media Converter Slide-in-Modules can be installed in any installation slot, in any order.
3. Remove Media Converter Slide-in-Module protective plate from selected installation slot by removing two (2) screws that secure plate to front of LMC1600A.
   NOTE: Ensure that the Media Converter Slide-in-Module is firmly seated against the backplane.
5. Install one (1) panel fastener screw (PROVIDED WITH SLIDE-IN-MODULE) and carefully rotate clockwise to secure.
6. Repeat steps 3 through 5 for additional Slide-In Media-Converter Modules.
3.5 Installing the LMC1600A in Rack or on Table

CAUTION: Do not allow air intake vents at bottom of Media Conversion Center to become blocked. Failure to observe this caution could result in equipment damage or failure.

3.5.1 Standard 19-Inch Rack Installation

WARNING: Mount the Media Conversion Center chassis evenly and securely in the rack. Failure to observe this caution could allow the Media Conversion Center to fall, resulting in equipment damage and possible injury to personnel.

NOTE: Installation bracket mounting screws are provided with the 16-Slot Media Conversion Center unit. Rackmount screws and clip nuts are NOT provided with the 16-Slot Media Conversion Center unit.

To install the 16-Slot Media Conversion Center in a standard 19-inch rack:

1. Locate six (6) installation bracket screws (PROVIDED) for each 16-Slot Media Conversion Center to be installed.
2. Align universal mounting bracket against side of Media Conversion Center chassis so that three (3) chassis installation holes are visible through four (4) universal mounting bracket installation holes and so that bracket surface to be attached to 19-inch site rack is flush with front of chassis.
3. Using Phillips screwdriver, install three (3) screws through mounting bracket into side of 16-Slot Media Conversion Center.
4. Repeat steps 2 and 3 for second mounting bracket.
5. Locate four (4) screws and optional clip-nuts (NOT PROVIDED) for each 16-Slot Media Conversion Center to be installed.
6. Carefully align 16-Slot Media Conversion Center at secure and level position between the 19-inch site rack mounting rails.
7. Install two (2) screws through right front bracket into right site rack mounting rail and two (2) screws through left front bracket into left site rack mounting rail, using clip nuts to secure if necessary.
3.5.2 Table-Top Installation

The 16-Slot Media Conversion Center can be placed on a table, shelf or other flat, secure surface in a well-ventilated environment.

3.6 Connecting Media Converter Slide-In-Modules to Network

NOTE: Connect network cables ONLY to Media Converter Slide-In-Module connectors within the same protocol (such as Ethernet-to-Ethernet, Fast Ethernet-to-Fast Ethernet, ATM-to-ATM). Failure to observe this caution will cause data transfer to fail.
3.7 Connecting Management Module to Command-Line Interface

NOTE: Network management can be configured ONLY if an optional Management Module has been installed in the 16-Slot Media Conversion Center.

NOTE: The serial port cable is attached directly to a DTE device through a null modem cable. Refer to the Appendix for the cable configuration.

To connect the SNMP Management Module to the Command-Line Interface:

1. Locate the correct DB9 serial port cable with female DB9 connector.
2. Attach the DB9 serial port female cable connector to the male DB9 serial port connector on the Media Conversion Center.
3. Attach the other end of the DB9 serial port cable to an ASCII terminal or terminal emulator.

NOTE: The 16-Slot Media Conversion Center uses the following serial port parameter values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>baud</td>
<td>9600</td>
</tr>
<tr>
<td>stop bits</td>
<td>1</td>
</tr>
<tr>
<td>data bits</td>
<td>8</td>
</tr>
<tr>
<td>parity</td>
<td>NONE</td>
</tr>
</tbody>
</table>

Using methods appropriate to the attached terminal, verify that the serial port parameters of the attached terminal match the 16-Slot Media Conversion Center port parameter values. If necessary, modify the attached terminal port parameter values.
3.8 Connecting Management Module to Network Management Station

NOTE: Black Box Corporation provides a vendor disk with a MIB that can be used with any SNMP application and with a graphical display intended to be used on a remote PC on which SNMPc™ software from Castle Rock Computing has been installed. If other SNMP applications are preferred, contact Black Box Corporation for direction.

To connect the SNMP Management Module to the remote Network Management Station:

1. Locate correct network cable with male RJ-45 connector.
2. Attach male RJ-45 connector to Media Conversion Center Management Module.
3. Attach other end of cable to a network hub.
4. Locate second network cable.
5. Attach second network cable to the network hub.
6. Attach other end of cable to the remote Network Management Station.
3.9 Powering the LMC1600A

To power the 16-Slot Media Conversion Center:

1. At 16-Slot Media Conversion Center back, locate the power receptacle on the Power Supply Module.
2. Plug hub (female) end of power cord into 16-Slot Media Conversion Center power receptacle.
3. Plug outlet (male) end of power cord into correct voltage AC rack or wall socket.
4. Repeat steps 1 through 3 for second Power Supply Module, if installed.
5. Press the Power Supply Module ON/OFF switch to the 1 position.
6. Verify that POWER LED on Power Supply Module is illuminated.
7. Repeat steps 5 through 6 for second Power Supply Module, if installed.
8. At 16-Slot Media Conversion Center front, verify that POWER LED(s) is/are illuminated.
9. If applicable, at 16-Slot Media Conversion Center front, verify that Management Module POWER LED is illuminated.
3.10 Using Command-Line Interface to Set IP Parameters

NOTE: Internet protocol (IP) network parameters must be set if the 16-Slot Media Conversion Center is to be managed using SNMP or ICMP.

After the terminal or terminal emulator has been attached to the LMC1600A and the LMC1600A has been reset, a command-line prompt comes up at the attached terminal or terminal emulator:

MCC16> _

Set the IP, netmask, and gateway addresses.

NOTE: If the private community name has been changed from “private”, use the correct name when entering the su command.

At the command line prompt, type and enter:

MCC16> su=private

[su]MCC16> set ip=<ip address (in the format: nnn.nnn.nnn.nnn)>

NOTE: Every time you enter an IP configuration command, MCC-1600 validates ALL IP parameter and reports any problems found.

[su]MCC16> set netmask=<mask (in the format: nnn.nnn.nnn.nnn)>

[su]MCC16> set gateway=<gateway address (in the format: nnn.nnn.nnn.nnn)>

Optionally change the community names.

At the command line prompt, type and enter:

[su]MCC16> set public=<public community name>

[su]MCC16> set private=<private community name>

Save the network configuration.

To save the network configuration, type and enter:

[su]MCC16> save
3.11 Optionally Using SNMPc™ at NMS to Monitor LMC1600A Status

NOTE: Black Box Corporation provides a vendor disk with a MIB and graphical display that can be used on a remote Network Management Station built on a PC on which SNMPc™ software from Castle Rock Computing is installed. Refer to the installation material in the Castle Rock SNMPc™ documentation to learn the hardware and software requirements of this NMS.

To install and use Black Box Corporation graphical display SNMP software at the remote Network Management Station:

1. Obtain and install hardware and software required to run the remote Network Management Station and then install SNMPc™ software, including the vendor disk from Black Box Corporation.
2. Ensure that the 16-Slot Media Conversion Center is powered ON.
3. At the remote SNMPc™ Network Management Station, start the SNMPc™ application.

NOTE: Refer to the Castle Rock SNMPc™ documentation for detailed direction for using SNMPc™ to “build a network map” on the display screen that includes an icon identifying the 16-Slot Media Conversion Center and then to bring up a “near-real-time” graphic display of the LMC1600A with installed Media Converter Slide-In-Modules.
IMPORTANT NOTE: The default private community name for the MCC-1600 is “private”. The default private community name assigned to a node by SNMPc is “netman”. If this difference is not resolved, the MCC-1600 security functions will NOT allow SET operations through SNMPc.

Choose one of three ways to resolve this issue:

1. Change the MCC-1600’s private community name to “netman” by issuing a “set private=netman” command at the command-line interface. Use the “save” command to save this change.

2. Before the SNMPc map is created, change the default private community name that SNMPc assigns to new map nodes:
   - Select “Edit” from the main SNMPc menu
   - Select “Node Defaults...” from the menu
   - Click on the “Comm...” button
   - Change the “Set” community name to “private”
   - Click “OK”.
   - Click “OK” AGAIN.

3. After the SNMPc map is created, change the private community name that SNMPc uses with an affected MCC-1600
   - Single click the MCC-1600 in the map window.
   - Select “Edit” from the main SNMPc menu
   - Select “Edit Object...” from the menu
   - Click on the “Comm...” button
   - Change the “Set” community name to “private”
   - Click “OK”.
   - Click “Change”
4. OPERATION

Daily operation of the LMC1600A 16-Slot Media Conversion Center requires no network administrator activity except occasionally monitoring status LED indicators.

The physical status LED indicators on the 16-Slot Media Conversion Center and on installed Media Converter Slide-In-Modules are used to monitor an unmanaged 16-Slot Media Conversion Center.

The 16-Slot Media Conversion Center can be managed using an SNMP MIB provided with the Management Module. An optional Black Box Corporation SNMPc™ graphical display at a remote Network Management Station (NMS) can be used to monitor status LED indicators on a managed 16-Slot Media Conversion Center AND status LED indicators on all Media Converter Slide-In-Modules installed in the managed LMC1600A.

NOTE: Management can be configured ONLY if an optional Management Module has been installed in the 16-Slot Media Conversion Center.

Status and trace messages available at a command-line interface also can be used to monitor a managed 16-Slot Media Conversion Center.

Direction is provided in the pages that follow for monitoring the LMC1600A 16-Slot Media Conversion Center:

4-1 Using Status LEDs .................................................. 4-2
4-2 Using the Command-Line Interface .......................... 4-3
4.3 Using SNMP .......................................................... 4-9
4.1 Using Status LEDs

4.1.1 Media Conversion Center LED Indicators

**Power Module Indicators**

*Power* and *In Use* Power Supply Module LED indicators located at the front of the Media Conversion Center whether Power Supply #1 and/or Power Supply #2 is installed in the Media Conversion Center and which power supply is powering the Media Conversion Center.

**NOTE:** A Power LED indicator also is located on each Power Supply Module installed at the back of the Media Conversion Center.

**Management Module Indicators**

*Power, Link, RX (receive)* and *TX (transmit)* Management Module LED indicators located at the front of the Media Conversion Center indicate that the Media Conversion Center Management Module is powered, that a network link is established, and that the Media Conversion Center Management Module is either receiving or transmitting network data.

**NOTE:** Network management indicators located on the Management Module installed at the back of the Media Conversion Center loosely mirror the network management indicators located on the front of the Media Conversion Center.

4.1.2 Media Converter Slide-In-Module LED Indicators

Refer to the User's Guides that come with each Media Converter Slide-In-Module to interpret the LED indicators for that module.
4.2 Using the Command-Line Interface

The LMC1600A interface, analogous to a Unix shell, permits the network administrator to display status messages and also to display and to alter various network settings, including IP parameters.

4.2.1 Connecting Terminal to Management Module

The management command-line interface is accessible via a terminal or terminal emulator attached to the RS-232 serial port on the Media Conversion Center Management Module.

NOTE: The serial port cable will be attached directly to a DTE device through a null modem cable. Refer to the Appendix for the null modem cable configuration.

1. Locate the correct DB9 serial port cable with female DB9 connector.
2. Attach the DB9 serial port female cable connector to the male DB9 serial port connector on the Media Conversion Center.
3. Attach the other end of the DB9 serial port cable to an ASCII terminal or terminal emulator.

NOTE: The 16-Slot Media Conversion Center uses the following serial port parameter values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>baud</td>
<td>9600</td>
</tr>
<tr>
<td>stop bits</td>
<td>1</td>
</tr>
<tr>
<td>data bits</td>
<td>8</td>
</tr>
<tr>
<td>parity</td>
<td>NONE</td>
</tr>
</tbody>
</table>

Using methods appropriate to the attached terminal, verify that the serial port parameters of the attached terminal match the 16-Slot Media Conversion Center port parameter values. If necessary, modify the attached terminal port parameter values.
4.2.2 Commands at the Command-Line Interface

Commands available at the command-line interface include:

? or help

Displays the list of currently available commands. When in super-user mode (see the su command) privileged commands are available.

clear or cls

Clears the screen.

get[=oid]

Performs an SNMP GET operation on the local MIB database, using the given object ID (OID). The OID is expressed numerically, and must be fully specified. If ‘=oid’ is omitted, the ending OID of the last successful GET/GETNEXT/SET command is used. Examples: “GET=1.3.6.1.2.1.1.3.0” Get current sysUptime value. “GET” Get sysUptime value again.

gnext[=oid]

Performs an SNMP GETNEXT operation on the local MIB database, using the given object ID (OID). GET/GETNEXT/SET command is used. This command behaves in a way similar to the GET command, except that the OID need not be fully specified, since it displays the data associated with the “next higher” OID, rather than an exact OID.

gn

A shorthand command equivalent to “GETNEXT”. No OID parameter is accepted, i.e. “GN=1.3.6” is not valid.

memtest

Executes a thorough DRAM diagnostic, as contrasted with the spot-check that is executed at system startup.

ping[=nnn.nnn.nnn.nnn]

Sends an ICMP ECHO message to the specified IP address. If no IP address is specified, the last valid IP address specified on a ‘ping’ command is used. The system transmits the ECHO message and acknowledges the command to the console. Note the sequence number and message ID contained in the console acknowledgement. These values are also displayed when incoming ECHO REPLy messages are reported, allowing the user to match ECHO REPLy messages with transmitted ECHO messages. The IP address specified with this command will be saved when a save command is issued.
4 OPERATION

|rping| Toggles repetitive pinging. The `rping` command transmits an ICMP echo message once per second until the rping command is issued again. Prior to issuing this command, a destination IP address must be supplied by issuing a ping command with a legal IP destination. The state of this command will be saved when a save command is issued.

| save| This command saves many of the parameters set by the other commands in this section to FLASH memory. Once saved, the settings persist through rebooting and power cycling. Saved settings can be overwritten at any time by issuing another save command.

| set=oid,type,value| Perform an SNMP SET operation on the local MIB database, using the given OID, type and value. The OID is expressed numerically and must be fully specified. If an asterisk (*) is specified in the place of the OID, the ending OID of the last successful GET/GETNEXT/SET command is used. Type = data type associated with variable being set, using: “INTEGER”, “STRING”, “IP”. Value = the data to be assigned to the SNMP MIB variable.

| set gateway=nnn.nnn.nnn.nnn| Sets the gateway IP address, i.e. the address of the station to which the management card transmits all datagrams with destinations that are not on the local subnet. This setting will be lost at the next reboot or power cycle unless the save command is issued.

| set ip=nnn.nnn.nnn.nnn| Sets the IP address of this management card. This setting will be lost at the next reboot or power cycle unless the save command is issued.

| set netmask=nnn.nnn.nnn.nnn| Sets the subnet mask that the management card will use when transmitting datagrams. This setting will be lost at the next reboot or power cycle unless the save command is issued.
Commands at the Command-Line Interface

**set private=private community name**  Sets the private community name. This community name must be used in all SNMP SET requests transmitted to the management card, and is also the password used to initiate super-user mode at the command line interface (see the su= command). The default private community name is “private”. This setting will be lost at the next reboot or power cycle unless the save command is issued.

**set public=public community name**  Sets the public community name. This community name must be used in all SNMP GET and GETNEXT requests transmitted to the management card. The default public community name is “public”. This setting will be lost at the next reboot or power cycle unless the save command is issued.

**set tntrip=nnn.nnn.nnn.nnn**  Sets the TELNET Remote IP address.

**set tntripmask=nnn.nnn.nnn.nnn**  Sets the TELNET Remote IP mask.

Together, these two commands allow the network administrator to control which stations are permitted to access the Management Module via TELNET.

**EXAMPLES:**

RIP=aaa.bbb.ccc.ddd
MASK=255.255.255.255 TELNET
connections accepted only from station
aaa.bbb.ccc.ddd

RIP=aaa.bbb.ccc.ddd
MASK=255.255.255.0 TELNET
connections accepted only from subnet
aaa.bbb.ccc.0

RIP=0.0.0.0 MASK=0.0.0.0 TELNET
connections accepted from any station.

**NOTE:**

Super User mode must be in effect. (See SU command.)

Changes made during TELNET session take effect at logout.
4  OPERATION

**show**  Displays configuration and status information.

**sql=length**  This command allows the maximum Length (in bytes) of the Serial output Queue to be set. This queue holds text data waiting to be displayed on the console. When a large value is used, the chances of display data being dropped due to high backlog are reduced, but system performance can be seriously degraded under peak loads. Values that are too small may cause erratic display behavior, such as incomplete displays and failure to display a prompt. Range: 200 to 65335. Default: 1200.

**su=private community name**  Initiates super user mode. In this mode, privileged operations (such as save) are available.

**su**  Terminates super user mode.

**tm=mask**  Sets trace mask to the hexadecimal value specified.

The mask is always entered and displayed in hex, and is the combination of all of the currently selected traces - which are each represented by a single bit. The default mask is 101h - checksum + ICMP errors.
### Commands at the Command-Line Interface

**xr**

Initiates firmware update into management card. This process allows updated software to be loaded into the management card. To update the software, 1) obtain the newest compatible version from Black Box Corporation, 2) attach the management card’s serial port to a terminal emulator that supports the XMODEM/CRC (256 byte blocks) protocol, 3) issue the XR command, and 4) initiate a “Send” or “Upload” command from the terminal emulator to send the new software to the management card.

**CAUTION:** If the 'write' phase is interrupted or fails for any reason, the LMC1600A management card will be damaged and will require servicing from Black Box Corporation. Using a battery-backed uninterruptible power supply is highly recommended.

**CAUTION:** This software cannot check to make sure that the software that is downloading is compatible with the hardware into which the software is loaded. Incorrect software changes may damage the management card necessitating factory service. If you have any doubts, contact Black Box Corporation for assistance before starting.

**CAUTION:** Firmware update may cause all saved settings to be lost.
4.3 **Using SNMP**

Optionally use SNMP management software at a remote Network Management Station to monitor the LMC1600A and installed Slide-In-Modules.

A Telnet option over the network also is available for access to the Management Module. **NOTE:** One and only one Telnet connection to the Management Module is permitted.

**NOTE:** SNMPc™ software from Castle Rock Computing can be installed at a PC-based SNMP Network Management Station to monitor a real-time BitView emulation of the LMC1600A and all installed Slide-In-Modules. SNMPc™ menu-selectable dialogue boxes also are available for monitoring the network installation. Refer to the SNMPc™ documentation from Castle Rock Computing, Inc.
5 MAINTENANCE

Maintenance direction provided in this section for the LMC1600A Media Conversion Center includes:

5.1 Hardware Replacement Procedures ................. 5-4
5.2 Firmware Upgrades .................................. 5-8
5.1 Hardware Replacement Procedures

WARNING: The 16-Slot Media Conversion Center contains no user-serviceable parts. DO NOT, UNDER ANY CIRCUMSTANCES, open and attempt to repair 16-Slot Media Conversion Center equipment. Failure to observe this warning could result in personal injury or death from electrical shock.

NOTE: Failure to observe the above warning will immediately void any warranty.

5.1.1 Replacing Media Converter Slide-In-Module

CAUTION: Wear a grounding device and observe electrostatic discharge precautions when installing Media Converter Slide-in-Module(s) in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Media Converter Slide-in-Module(s).

NOTE: The Media Converter Slide-in-Modules are hot-swappable.

To replace a Media Converter Slide-in-Module in the LMC1600A chassis:

1. Remove Media Converter Slide-in-Module to be replaced by rotating and removing one (1) screw that secures Slide-in-Module to LMC1600A chassis front and sliding Media Converter Slide-In-Module from LMC1600A chassis.

2. Carefully slide replacement Media Converter Slide-in-Module into installation slot.

   NOTE: Ensure that the Media Converter Slide-in-Module is firmly seated against the backplane.

5.1.2 Replacing Power Supply Module

**CAUTION:** Wear a grounding device and observe electrostatic discharge precautions when installing Power Supply Module in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Power Supply Module.

To replace a Power Supply Module in the LMC1600A chassis:

1. Disconnect outlet end of power cord from AC wall socket.
2. At Media Conversion Center back, disconnect power cord from power receptacle of Power Supply Module to be replaced.
3. Remove Power Supply Module to be replaced by rotating and removing two (2) screws that secure Power Supply Module to LMC1600A chassis front and sliding Power Supply Module from LMC1600A chassis.
4. Carefully slide replacement Power Supply Module into installation slot, aligning Power Supply Module with installation guides:
   
   **NOTE:** Ensure that the Power Supply Module is firmly seated against the backplane.
5. Secure Power Supply Module by carefully rotating installation screws clockwise.
6. Connect power cord to Power Supply Module power receptacle.
7. Connect power cord to AC wall socket.
8. Press Power Supply Module ON/OFF switch to the 1 position.
9. Verify that POWER LED at front of 16-Slot Media Conversion Center is illuminated.
5.1.3 Replacing Power Supply Module Fuse

**CAUTION: Replace fuse only with same size and rating. Failure to observe this caution could result in equipment damage.**

To replace a Power Supply Module fuse:

1. Disconnect outlet end of power cord from AC wall socket.
2. At Media Conversion Center back, disconnect power cord from Power Supply Module power receptacle.
3. From inside edge of power receptacle, insert small flat blade screwdriver into groove on front inside edge of fuseholder and carefully pry fuse holder (with installed fuse) from Power Supply Module.
4. Rotate fuse holder to display fuse.
5. Carefully remove fuse from fuse holder.
6. Install **SAME SIZE AND RATING** replacement fuse in fuse holder.
   **NOTE:** Snap fuse holder into place.
8. Connect power cord to Power Supply Module power receptacle.
9. Connect power cord to AC wall socket.
10. Verify that POWER LED at front of 16-Slot Media Conversion Center is illuminated.
5.1.4 Replacing Management Module

**CAUTION:** Wear a grounding device and observe electrostatic discharge precautions when installing Management Module in the 16-Slot Media Conversion Center. Failure to observe this caution could result in damage to, and subsequent failure of, the Management Module.

NOTE: The 16-Slot Media Conversion Center Management Modules are hot-swappable.

To replace a 16-Slot Media Conversion Center Management Module in the LMC1600A chassis:

1. At Media Conversion Center back, remove Management Module to be replaced by rotating and removing two screws that secure Management Module to back of LMC1600A and sliding Management Module from LMC1600A chassis.

2. Carefully slide replacement Management Module into installation slot, aligning the Management Module with the installation guides.
   
   NOTE: Ensure that the Management Module is firmly seated against the backplane.

5.2 Firmware Upgrades

To upgrade the firmware:

1. Obtain new firmware by contacting Black Box Corporation Technical Support.

CAUTION: The MCC-1600 software cannot check to make sure that the firmware you are downloading is compatible with your hardware. (Firmware files are NOT automatically extracted from ZIP files.) INCORRECT FIRMWARE DOWNLOADS WILL DAMAGE THE MANAGEMENT MODULE, NECESSITATING FACTORY SERVICE. If in doubt, abort this process and contact Black Box Corporation for assistance.

2. Initiate the MCC-1600 end of X-modem transfer by entering the following two commands at the MCC-1600 command-line prompt:

   MCC16> su=private

   [su] MCC16> xr

CAUTION: Do not transfer a ZIP file. UnZIP the ZIP file and transfer the binary file contained in the ZIP file. Failure to observe this caution will cause equipment damage.

3. Enter terminal-emulator specific commands to initiate the terminal emulator end of the X-modem transfer. This will cause the file to be transferred. When file transfer is complete, the new code will be written into flash memory and the Management Module will reboot.

CAUTION: IF THE 'WRITE' PHASE IS INTERRUPTED OR FAILS FOR ANY REASON, THE LMC1600A MANAGEMENT MODULE WILL BE DAMAGED AND MUST BE RETURNED TO TRANSITION NETWORKS FOR SERVICE. Use of a battery-backed uninterruptible power supply is HIGHLY recommended.

NOTE: Firmware update may cause all saved settings to be lost.
APPENDIX A. Media Conversion Center Technical Specifications

Dimensions

- **Chassis**: 17" x 14" x 3.5" (430 mm x 356 mm x 89 mm)
- **Media Converter Modules**: 3" x 1" x 4.7"
- **Power Supply Modules**: 7.5" x 2.7" x 7.8"
- **Management Module**: 5.3" x 0.8" x 7.7"

Shipping Weight

- **Chassis**: 12 Lbs

Universal Power Supply

- **Input Range**: 85 to 265 VAC at 47 to 63 Hz. Rated at 110 watts maximum.
- **NOTE**: Power supply modules supply +12VDC at 9A Max. Only one power supply module provides power to the chassis and installed modules; the second power supply is used if the first fails.

<table>
<thead>
<tr>
<th>TN P/N</th>
<th>Requirement</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>3344</td>
<td>120 volts, 60 hertz</td>
<td>USA/Canada/Mexico</td>
</tr>
<tr>
<td>3344</td>
<td>100 volts, 50-60 hertz</td>
<td>Japan</td>
</tr>
<tr>
<td>3347</td>
<td>230 volts, 50 hertz</td>
<td>Europe</td>
</tr>
<tr>
<td>3348</td>
<td>240 volts, 50 hertz</td>
<td>Australia</td>
</tr>
<tr>
<td>3349</td>
<td>240 volts, 50 hertz</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>

Environment

- **Temperature**: 0-50°C (32° to 122° F)
- **Humidity**: 10-90%, non condensing
- **Altitude**: 0-10,000 feet

Approvals

- UL listed EN 60950; FCC & CISPR class A; CE Mark

Warranty

- Lifetime
APPENDIX B. Null Modem Cable Specifications

DB9 cable is used for connecting a terminal or terminal emulator to the Media Conversion Center Management Module to access the command-line interface.

The table below shows the pin assignments for the DB9 cable.

<table>
<thead>
<tr>
<th>Function</th>
<th>Mnemonic</th>
<th>Pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier Detect</td>
<td>CD</td>
<td>1</td>
</tr>
<tr>
<td>Receive Data</td>
<td>RXD</td>
<td>2</td>
</tr>
<tr>
<td>Transmit Data</td>
<td>TXD</td>
<td>3</td>
</tr>
<tr>
<td>Data Terminal Ready</td>
<td>DTR</td>
<td>4</td>
</tr>
<tr>
<td>Signal Ground</td>
<td>GND</td>
<td>5</td>
</tr>
<tr>
<td>Data Set Ready</td>
<td>DSR</td>
<td>6</td>
</tr>
<tr>
<td>Request To Send</td>
<td>RTS</td>
<td>7</td>
</tr>
<tr>
<td>Clear To Send</td>
<td>CTS</td>
<td>8</td>
</tr>
</tbody>
</table>

25 Pin RS-232 Null Modem Cable

- Chassis Ground 1 ________ 1 Chassis Ground
- Transmit Data 2 ________ 3 Receive Data
- Receive Data 3 ________ 2 Transmit Data
- Request To Send 4 [ ] 4 Request To Send
- Clear To Send 5 [ ] 5 Clear To Send
- Data Terminal Ready 6 20 Data Terminal Ready
- Data Set Ready 8 6 Data Set Ready
- Carrier Detect 8 6 Carrier Detect
- Data Terminal Ready 20 8 Carrier Detect
- Signal Ground 7 ________ 7 Signal Ground
APPENDIX C. Introduction to SNMP in the LMC1600A

NOTE: A protocol is a set of rules that governs data transmission and reception. The Simple Network Management Protocol (SNMP) is an Internet protocol (as are protocols such as the Transmission Control Protocol (TCP) and Internet Protocol (IP)). SNMP was developed in the mid-1980s as an interim response to communication barriers encountered among different types of networks. Formally specified in a series of related Request for Comment (RFC) documents, SNMP is becoming the de facto Internet network management standard.

SNMP is a protocol that defines network communication between a Managed Device (such as the LMC1600A) and the network administrator at a Network Management Station. The SNMP protocol uses simple Operations on a set of variables on the managed device (called instances of Managed Objects) to allow the network administrator to monitor and to control the managed device from a remote location.

Managed Device A managed device is a hardware unit with embedded SNMP software (including a Management Information Base (MIB) – the set of managed objects on that managed device – and an agent – the software that monitors the data in the MIB) connected to a network with SNMP management available. NOTE: An LMC1600A with installed Media Converter Modules, AND with an installed Management Module, is a single managed device.

Network Management Station (NMS) A network management station (NMS) is a high-end workstation, also connected to the network, that provides SNMP network management application software and a user interface. NOTE: An optional network management application and user interface for the LMC1600A are provided by SNMPc™ software from CastleRock Computing installed on a network Windows™ PC.

SNMP Operations SNMP is a simple request-response protocol with four defined operations: GET, GET-NEXT, SET, and TRAP. To monitor (read) the managed device, the network administrator initiates, through the user interface to the network management application on the NMS, the GET and GET-NEXT operations on selected called instances of managed objects (variables) in the managed device MIB. To control (write) the managed device, the network administrator initiates, through the user interface to the network management application on the NMS, the SET operation on selected instances of managed objects in the managed device MIB. The SNMP agent on the managed device initiates the TRAP operation to alert the network administrator, through the user interface to the network management application on the NMS, of instances of MIB-defined asynchronous events on the managed device.

Managed Objects Managed objects are the types of information on a managed device that can be identified and collected by SNMP agent software and that can be made available to the network administrator through the user interface on the NMS. Managed objects can be scalar (a single object instance – such as the LMC1600A network IP address) or tabular (related instances – such as the various LED displays on a Media Converter Module installed in the LMC1600A).
The Management Information Base (MIB) is the set of managed objects on a managed device and is depicted as an abstract tree with unnamed root, as shown in the diagram.

Managed objects are depicted as nodes in the MIB tree. Object identifiers (object IDs, or OIDs) for the managed objects use a machine-independent format (a subset of the Abstract Syntax Notation 1 (ASN.1)) to uniquely identify each managed object in the MIB tree. NOTE: Abstract notation allows communication among diverse networks.

OIDs in the ASN.1 syntax are represented by a structured series of positive integers, each separated by a period, that “follows” a MIB path to uniquely identify a managed object. (MIB development is particularly active in the portion of the International Organization for Standardization (ISO) branch represented by object identifier 1.3.6.1 and dedicated to the Internet community.)

The current Internet-standard MIB (known as MIB-II, with OID 1.3.6.1.2.1) is a MIB module typically supported by all SNMP agents on TCP/IP enabled devices or systems. MIB-II contains 171 objects grouped by protocol (including TCP, IP, UDP, SNMP), with other identifiers, including system (1) and interfaces (2). This MIB file contains a description of the object hierarchy on the managed device, as well as the OID, syntax and access privileges for each variable in the MIB.

The network administrator can use an OID: 1.3.6.1.2.1.1 to identify MIB-II “system description” data to an SNMP agent. The network administrator also can use the associated label, `sysDescr`, to identify the same data to the SNMP agent, since the SNMP agent uses the MIB-II object identifier: 1.3.6.1.2.1.1= `sysDescr` to translates the label to the corresponding OID.

Vendors define private branches to include instances of their products. The Black Box Corporation private chassis MIB is represented by the object identifier 1.3.6.1.4.1.868 and includes objects such as “chassis” (for the LMC1600A), identified in ASN.1 notation by OID 1.3.6.1.4.1.868.2.4 with the associated label "mcc16ComIpAddr" (the LMC1600A IP address), which is identified in ASN.1 notation by OID 1.3.6.1.4.1.868.2.4.2.1.1.4.
The following is a complete listing of the Black Box Corporation' LMC1600A MIB:

1.3= org
1.3.6= dod
1.3.6.1= internet
1.3.6.1.2= mgmt
1.3.6.1.2.1= mib-2
1.3.6.1.2.1.1= system
1.3.6.1.2.1.1.1= sysDescr
1.3.6.1.2.1.1.2= sysObjectID
1.3.6.1.2.1.1.3= sysUpTime
1.3.6.1.2.1.1.4= sysContact
1.3.6.1.2.1.1.5= sysName
1.3.6.1.2.1.1.6= sysLocation
1.3.6.1.2.1.1.7= sysServices
1.3.6.1.4= private
1.3.6.1.4.1= enterprises
1.3.6.1.4.1.868= transition
1.3.6.1.4.1.868.1= productld
1.3.6.1.4.1.868.1.4= chassisProdslld
1.3.6.1.4.1.868.1.4.1= chassisSlotTypes
1.3.6.1.4.1.868.1.4.1.1= chSmC20p
1.3.6.1.4.1.868.1.4.1.1.1= ceTbtFrl03Id
1.3.6.1.4.1.868.1.4.1.1.2= ceCxTbt04Id
1.3.6.1.4.1.868.1.4.1.1.3= ceCxFrl04Id
1.3.6.1.4.1.868.1.4.1.1.5= cfSmMm05Id
1.3.6.1.4.1.868.1.4.1.1.24= cfSmMm04Id
1.3.6.1.4.1.868.1.4.1.1.28= cfdCdo1ld
1.3.6.1.4.1.868.1.4.1.1.29= cbrCfo1ld
1.3.6.1.4.1.868.1.4.1.1.30= ce100BtxFrl03Id
1.3.6.1.4.1.868.1.4.1.1.31= mc20pemptyld
1.3.6.1.4.1.868.1.4.2= products
1.3.6.1.4.1.868.2= chassis
1.3.6.1.4.1.868.2.4= card
1.3.6.1.4.1.868.2.4.1= slotM c20p
1.3.6.1.4.1.868.2.4.1.1= ceTbtFrl03Table
1.3.6.1.4.1.868.2.4.1.1.1= ceTbtFrl03Entry
1.3.6.1.4.1.868.2.4.1.1.1.1= ceTbtFrl03ld
1.3.6.1.4.1.868.2.4.1.1.1.2= ceTbtFrl03FiberRecv
1.3.6.1.4.1.868.2.4.1.1.1.3= ceTbtFrl03FiberLink
1.3.6.1.4.1.868.2.4.1.1.1.4= ceTbtFrl03TPRecvc
1.3.6.1.4.1.868.2.4.1.1.1.5= ceTbtFrl03TPLink
1.3.6.1.4.1.868.2.4.1.1.1.6= ceTbtFrl03Power
1.3.6.1.4.1.868.2.4.1.1.2= ceCxTbt04Table
1.3.6.1.4.1.868.2.4.1.1.2.1= ceCxTbt04Entry
1.3.6.1.4.1.868.2.4.1.1.2.1.1= ceCxTbt04ld
1.3.6.1.4.1.868.2.4.1.1.2.1.2= ceCxTbt04Jabber
1.3.6.1.4.1.868.2.4.1.1.2.1.3= ceCxTbt04CoaxRecv
1.3.6.1.4.1.868.2.4.1.1.2.1.4= ceCxTbt04TPRecvc
1.3.6.1.4.1.868.2.4.1.1.2.1.5= ceCxTbt04TPLink
1.3.6.1.4.1.868.2.4.2.1.1.8 = mcc16ComPS1InUse
1.3.6.1.4.1.868.2.4.2.1.1.9 = mcc16ComPS2Power
1.3.6.1.4.1.868.2.4.2.1.1.10 = mcc16ComPS2InUse
1.3.6.1.4.1.868.2.4.2.1.2 = mcc16Ver1
1.3.6.1.4.1.868.2.4.2.1.2.1 = mcc16SlotTable
1.3.6.1.4.1.868.2.4.2.1.2.1.1 = mcc16SlotEntry
1.3.6.1.4.1.868.2.4.2.1.2.1.1.1 = mcc16Index
1.3.6.1.4.1.868.2.4.2.1.2.1.1.2 = mcc16DeviceType
APPENDIX D. SNMP GLOSSARY

ARP  
Address Resolution Protocol  Method for determining Ethernet address from IP address.

binding  
See ‘variable binding.’

flash  
Memory that retains its contents when power is disconnected.

MIB  
Management Information Base. The types, names, and OID tree structure of a group of SNMP variables. Manifested in software on the managed network entity and in a text document for the managing station. [The objects that are available in a managed system. The information is represented in Abstract Syntax Notation 1 (ASN.1)]

ICMP  
Internet Control Message Protocol. A set of information, error, and control messages used on IP networks. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

IP  
Internet Protocol. A network layer protocol whose primary responsibility is routing.

Object Id  
A “name” for a particular piece of SNMP data. For example, a GET operation on the object id “1.3.6.1.2.1.1.1.0” returns a string describing the managed system. This same OID is used for every system that supports the system description variable. The dotted numeric value is used instead of a simple text name so that a tree structure can be implied in the name.

OID  
Object ID  See above.

g et  
An SNMP ‘read’ operation in which the data associated with a specific, exact object id is returned.

getnext  
An SNMP ‘read’ operation where the data returned is the data associated with the object id that is numerically ‘next.’ e.g. a GETNEXT operation on the object id 1.3.6.1.2.1.1.1.0 would return the Object ID 1.3.6.1.2.1.1.2.0 and the data associated with it.

PDU  
Protocol Data Unit. An SNMP operation encoded for network transmission.

Protocol  
The formal set of rules on coding, formatting and timing of inputs and outputs between communicating devices.

set  
An SNMP ‘write’ operation.

SNMP  
Simple Network Management Protocol An application layer protocol that allows remote management of networked devices.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMI</td>
<td>Structure of Management Information.</td>
</tr>
<tr>
<td>UDP</td>
<td><strong>User Datagram Protocol.</strong> A connectionless transport layer protocol used in IP networks; provides an end-to-end interface for use by applications. This protocol carries SNMP as a payload, and is carried as a payload by IP.</td>
</tr>
<tr>
<td>variable binding</td>
<td>A subsection of a PDU. A variable binding contains an Object ID and the data value associated with that Object ID.</td>
</tr>
<tr>
<td>XMODEM/CRC</td>
<td>A protocol commonly used to transfer files across an RS-232 link.</td>
</tr>
</tbody>
</table>
APPENDIX E. Messages at Command-line Interface

Messages that might be displayed at the command-line interface are listed in alphabetical order.

Each message provides an explanation of the probable source of the message and, where indicated, suggested corrective action in response to the message.

ARP: no response from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. It indicates that the management card has abandoned (due to timeout) an attempt to determine the Ethernet address of the station it was asked to communicate with. Possible causes: 1) The destination station is down or does not exist 2) the subnet mask is set incorrectly 3) Ethernet communications have been disrupted. This message is printed only when the appropriate traces are enabled via the “TM=mask” command.

ARP: REQUEST from nnn.nnn.nnn.nnn/nn nn nn nn nn nn for nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. It indicates that another station (whose IP and Ethernet addresses are indicated at the beginning of the message) is attempting to determine the Ethernet address of the management card via Address Resolution Protocol (ARP). The management card answers each ARP request with a message containing the requested information. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.

ARP: REQUEST sent for nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface or in response to a console command. It indicates that the management card has transmitted an Address Resolution Protocol (ARP) packet in an attempt to determine the Ethernet address of the station whose IP address is noted at the end of the message. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.

ARP: RESPONSE from: nnn.nnn.nnn.nnn=nn nn nn nn nn nn to: nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the management card has (via ARP) successfully determined the Ethernet address of the station whose IP address is noted at the beginning of the message. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.
Indicates a latent software defect or a hardware failure in the Ethernet controller. Call Black Box Corporation for assistance.

**Command only available in super-user mode. Enter ‘SU=’**

This message is a response to a console command. You have entered a privileged command without first entering super-user mode. The privileged command is rejected. Enter “SU =” followed by the private community name, and then re-enter the command that caused the error.

**Community name changed. Use SAVE command to make permanent.**

Response to a console command. The public or private community name was changed via the “PUBLIC=new-public” or “PRIVATE=new-private” commands. This message warns you that the changes made will be lost the next time the management card is reset, rebooted, or power cycled - unless they are saved in FLASH memory as suggested.

**[Count]**

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that one of the Ethernet controller’s internal counters has overflowed. This message can be ignored or disabled via the “TM =mask” command.

**CPU ADDRESS ERROR, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn**

This unsolicited message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

**<D>**

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An incoming Ethernet packet was discarded because the receive queue was full, i.e. Ethernet packets are arriving more quickly than they can be processed. This may occur occasionally (during periods of peak network load) without indicating a problem. However, if the message cannot be explained by heavy Ethernet traffic and it repeats more than a few times a minute or system operation is impaired, call Black Box Corporation for assistance. To eliminate these messages, use the “TM =mask” command to disable the traces.

**DMA ADDRESS ERROR, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn**

This unsolicited message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.
DOWNLOAD: Format of downloaded file is incorrect. Firmware update aborted.
DOWNLOAD: Please reset the Management Module.

This message indicates that the signature at the end of the transferred file was incorrect, i.e. the file you are attempting to transfer is not a valid firmware module. The update process is aborted and the management module is halted as a precaution. Note that if you obtained new firmware in .ZIP format, you must unzip it before transferring it to the management module.

DOWNLOAD: Invalid internal checksum. x=nnn, c=nnn Firmware update aborted.
DOWNLOAD: Please reset the Management Module.

The checksum calculated after the end of the XMODEM transfer did not compare correctly. Note that this probably does not indicate a problem with the XMODEM transfer into the management module. Instead, this probably indicates that the source firmware file you are attempting to transfer is corrupted. The update process is aborted and the management module is halted as a precaution.

DOWNLOAD: Press the ESC key to continue

This message is a response to the “XR” console command. This message is printed periodically after a firmware update attempt, under the assumption that the terminal emulator will fail to display console traffic it thinks is part of the XMODEM transfer. Waiting for an ESC before printing any final messages reduces somewhat the chances that your terminal emulator will mask them. When you see this message, press ESC and the XMODEM termination message(s) will be displayed.
DOWNLOAD: XMODEM/CRC receive error: tttt
DOWNLOAD: Rebooting

Response to the “XR” console command. The XMODEM /CRC transfer failed. The last XMODEM/CRC error is displayed. Values for tttt include:

“Timeout” - Timeout waiting for data
“Serial” - low level serial transmission error
“Protocol” - Unimplemented protocol, i.e. not XMODEM/CRC
“EOT” - Received End Of Text from remote
“Canceled” - Received CANCEL from remote
“Retries - EOT” - too many retries on EOT
“Retries - C” - too many retries on C.
“Retries - Receive” - too many retries on receive. This is the code that will be displayed if the management card never sees any attempt by the terminal emulator to start the transfer.

“Unexpected packet number” - packet received out of sequence.
“Last Packet resent” - duplicate packet discarded
“Bad CRC” - Data was corrupted in transit
“Not start of packet” - Expected SOT, STX or EOT
“Not ACK” - Expected ACK or NAK
“Received max # bytes” - received packet too big

To resolve this problem, check the following:
1) Is serial cable configured correctly, in good condition, and plugged in firmly? NOTE: Issuing console commands and receiving appropriate responses indicates null-modem cable is wired correctly.
2) Is XMODEM/CRC protocol used for the transfer? This protocol uses a 16 bit CRC with 128 byte data blocks. Neither original XMODEM (8 bit checksums with 128 byte data blocks) nor XMODEM-1K (16 bit CRCs with 1024 byte data blocks) is supported. NOTE: Many terminal emulator implementations use XMODEM/CRC but describe it as “XMODEM.”
3) Is the transmitting station fast enough? Place the code on a local hard disk and use that copy as the source for your XMODEM/CRC transfer.

DOWNLOAD: XMODEM/CRC receive success, nnn bytes!
DOWNLOAD: FLASH ‘WRITE’ phase beginning. DO NOT INTERRUPT!

This message is a response to the “XR” console command. The XMODEM/CRC transfer was successful. This message is your “last chance” to abort the firmware update operation. When this message is displayed, you have approximately seven seconds left before the write begins (assuming that your terminal emulator displays it immediately when it is transmitted). If the write is interrupted, the management card will be damaged.

ERROR: Invalid configuration checksum. All saved values ignored.

This is a system startup message. The management card has disabled its network interface as a safety precaution. The user should (at a minimum) enter an IP address (via the “SET IP=ip” command), a subnet mask (via the “SET NETMASK=mask” command), and a gateway address (via the “SET GATEWAY=ip” command), then enter the “SAVE” command. This message may indicate a latent software defect or a hardware failure. If the message persists or recurs after performing the suggested corrective action, call Black Box Corporation for assistance.
ETH: ERROR, This version of the driver cannot run on this hardware revision.

The Ethernet driver has determined that it is definitely incompatible with the hardware version it is attempting to run on. The ethernet driver is disabled. A software update is required to correct this problem. Contact Black Box Corporation technical support.

ETH: Can’t transmit. Reason=nn ttttt

This unsolicited message is printed periodically as applications attempt to transmit Ethernet packets. All outgoing Ethernet traffic has been halted. One or more reason code bits (nn) are expanded to text (ttttt).

“Software incompatible with hardware.” Contact Black Box Corporation technical support for assistance.

“Invalid IP/Netmask/Gateway configuration.” Local IP address, subnet mask, and/or default gateway are improperly configured. Further explanation of the configuration error will be provided by other messages. For more information, see console commands “SET IP=nnn.nnn.nnn.nnn”, “Softwre Shutdown.” Resets the Management Module. Contact Black Box Corporation if the message persists.

“Link Down.” Indicates a problem with the link to the Management Module.

“Hardware initialization failed.” Verify that the management card is properly connected to an active 10Base-T Ethernet port. Power cycle the management card. If message persists, contact Black Box Corporation technical support.

ETH: Invalid frame type, len=0xnnnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the protocol type field of an incoming Ethernet II frame is not recognized, or the frame is not a valid Ethernet II frame. This usually indicates the presence on the local Ethernet segment of broadcast traffic that the management card is not programmed to interpret. The only supported types are ARP and IP over Ethernet II. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.

ETH: Unsupported protocol 0xnnnn

See “ETH: Invalid frame type, len=0xnnnn”

ETH: Warning, unknown model identifier.

This is a system startup message. The Ethernet driver does not recognize the model identifier of the hardware it is attempting to run on. This probably indicates that the software is older than the hardware. The driver attempts to continue, but correct operation cannot be guaranteed. A software update is required to eliminate this message. Contact Black Box Corporation technical support.
ETHERNET INITIALIZATION FAILED

This unsolicited message is displayed when an unusual hardware or software condition is detected. An attempt to initialize the Ethernet controller failed. Power cycle the management card. If the message persists, call Black Box Corporation for assistance.

ETHERNET RESET FAILED

See "ETHERNET INITIALIZATION FAILED"

FLASH: Erase verify failed. $nnnn$ invalid words.

This message is a response to a console command. This message indicates a hardware failure or latent software defect. Retry the operation. If the message persists, call Black Box Corporation for assistance.

FLASH: Function not implemented.

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.

FLASH: Illegal return code.

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.

FLASH: Illegal target address range

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.

FLASH: ROM starting address is not on sector boundary.

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.

FLASH: Saving configuration, please wait up to one minute...

This message is a response to a console command. The management card is saving its configuration to flash (i.e. non-volatile) memory. If this operation is interrupted, the saved configuration will be invalid and the management card will be unable to access the network (e.g. it will be unable to respond to SNMP requests) until IP parameters are re-entered. In this case, media conversion functions continue normally. The primary purpose of the SAVE operation is to make sure that the appropriate network parameters (i.e. IP address, subnet mask, and gateway address) are automatically available should the management card be rebooted for any reason, though other parameters are saved as well.

FLASH: Source data does not fit in specified target range.

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.
FLASH: This version of the software does not support flash.

This message is a response to a console command. This message indicates a latent software defect. Call Black Box Corporation for assistance.

FLASH: Write complete.

This message is a response to a console command. An attempt to save data or code in FLASH (i.e. non-volatile) memory was successful.

FLASH: Write verify failed. nnnn invalid words.

This message is a response to a console command. This message indicates a hardware failure or latent software defect. Retry the operation. If the message persists, call Black Box Corporation for assistance.

GENERAL ILLEGAL INSTRUCTION, SP=nnnnnnnnn PC=nnnnnnnnn SR=nnnnnnnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

[h=nnnn]

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. The Ethernet interface has failed. Call Black Box Corporation for assistance.

ICMP: DESTINATION UNREACHABLE message received from nnn.nnn.nnn.nnn (ignored)
ICMP: code=tttttt

Where ttttt is “NETWORK UNREACHABLE,” “HOST UNREACHABLE,” “PROTOCOL UNREACHABLE,” “PORT UNREACHABLE,” “FRAGMENTATION REQUIRED and DF SET,” or “SOURCE ROUTE FAILED.”

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A gateway or host has determined that a datagram sent by the management card cannot be delivered. Frequently, this is due to an invalid IP address or a router, firewall or host configuration problem. A numeric value for ttttt indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: ECHO message received from nnn.nnn.nnn.nnn, id=nnn seq=nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The named station is PINGing the management card. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.
ICMP: ECHO REPLY message received from nnn.nnn.nnn.nnn, id=nnn seq=nnn

Displayed in response to a packet that arrived at the Ethernet interface. A PING response was received. Note the identification and sequence numbers; similar numbers are displayed when the PING packet is transmitted. The values can be used to match transmissions with responses. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: INFORMATION REQUEST message received from nnn.nnn.nnn.nnn (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This probably means that another host is attempting to find out what network it is on. The incoming ICMP message is ignored, since the management card does not support the INFORMATION service. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: INFORMATION REPLY message received from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message should never be displayed, since the management card does not support the INFORMATION service. If the message persists, call Black Box Corporation for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: invalid checksum, perhaps from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming ICMP message was invalid. This is usually due to the corruption of the datagram in transit. Note that the source address displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.

ICMP: PARAMETER PROBLEM message received from nnn.nnn.nnn.nnn
(ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A datagram sent by the management card was discarded by the named host. This message indicates that a message was corrupted in transit, or that an incompatibility exists between the networking code in the management card and the networking code in the named station. If the message persists, call Black Box Corporation for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.
ICMP: REDIRECT message received from nnn.nnn.nnn.nnn (ignored)
ICMP: code=ttttt recommended gateway=nnn.nnn.nnn.nnn

Where ttttt is "REDIRECT for NETWORK", "REDIRECT for HOST", or "REDIRECT for NETWORK and TOS".
This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is sent by the 'from ip' gateway when multiple gateways are attached to the local subnet and the management card is using a less-than-ideal gateway to reach its destination host. Since the management card does not support the use of multiple gateways, the only guaranteed way to eliminate this message is to place the management card on a subnet with only one gateway. If this is not possible, the management card’s gateway address can be changed to match the recommended gateway - though this will probably result in more redirect messages from the new gateway. Note that if the gateway that sent the redirect message conforms to standards, it will forward the data transmitted by the management card to the correct gateway and the messages can simply be disabled or ignored. A numeric value for ttttt indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: ROUTER ADVERTISEMENT message received from nnn.nnn.nnn.nnn (ignored)
ICMP: ROUTER SOLICITATION message received from nnn.nnn.nnn.nnn (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. These messages are displayed when ICMP Router Discovery messages are received. The management card does not support ICMP Router Discovery. The incoming ICMP messages are ignored. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 1256, ICMP Router Discovery Messages, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: SOURCE QUENCH message received from nnn.nnn.nnn.nnn (ignored)
This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Due to congestion, the named gateway or host is requesting that the management card slow the flow of datagrams. Since the management card almost never transmits unsolicited datagrams, this message is ignored. This message is printed only when the appropriate traces are enabled via the "TM=mask" command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.
ICMP: TIME EXCEEDED message received from nnn.nnn.nnn.nnn (ignored)
ICMP: code=tttt

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A datagram sent by the management card was not delivered due to timeout in transit.

When ttttt is “TTL EXPIRED IN TRANSIT” this means that a gateway saw a Time-To-Live value of zero - probably indicating a routing loop or other network configuration error. Note that the management card assigns the maximum legal Time-To-Live value to each outgoing datagram.

When ttttt is “REASSEMBLY TIMER EXPIRED” this means that datagram fragment reassembly timed out at the destination host, which is caused by 1) the loss of one or more of the fragments in transit, 2) a short reassembly timer at the destination host, or 3) an extremely slow network path.

A numeric value for ttttt indicates that the code is not recognized, usually due to the use of proprietary codes. Contact the vendor of the transmitting station for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: TIMESTAMP message received from nnn.nnn.nnn.nnn (ignored)

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The incoming ICMP message is ignored, since the management card does not support the TIMESTAMP service. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL. This message does not indicate an error condition. No corrective action is required.

ICMP: TIMESTAMP REPLY message received from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message should never be displayed, since the management card does not support the TIMESTAMP service. If the message persists, call Black Box Corporation for assistance. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For more information, see RFC 792, Internet Control Message Protocol, available via anonymous FTP from NIC.DDN.MIL.

ICMP: UNKNOWN TYPE 0xnn message received from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that an unknown ICMP message was received. Some network vendors transmit proprietary types and codes in ICMP messages. If the message persists, contact the vendor of the transmitting station for assistance, or contact Black Box Corporation if you are reasonably sure the type is not proprietary. If system operation is not impaired, then no corrective action is required. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. For information on possible new ICMP messages see the RFC collection, available via anonymous FTP from NIC.DDN.MIL.
Illegal character

This message is a response to a console command. A non-printable character (outside the range 20h to 7Eh) was seen in a community name entered from the console.

Illegal length. 1-30 characters required.

This message is a response to a console command. Re-enter the console command, making sure that the community name entered falls within the given bounds. No white space is permitted anywhere in the command.

Illegal register read nnnn nnnn nnnn
Illegal register write nnnn nnnn nnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect. Call Black Box Corporation for assistance.

ILLEGAL SLOT INSTRUCTION, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

Incorrect password.

This message is a response to a console command. The correct “SU=password” password is the same as the private community name. The default is “private”. If you have forgotten your private community name and are unable to retrieve it from your Network Management Station, call Black Box Corporation for assistance.

*** Invalid IP address: ttttt

This message is a response to a console command. An invalid local or gateway IP address was entered. An IP address must be entered as “a.b.c.d” where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the address 0.0.0.0 is entered for a local IP address (but not for a gateway address). It is not possible to use this address as a local or gateway IP address.

*** Invalid subnet mask: ttttt

This message is a response to a console command. An invalid subnet mask was entered. The subnet mask must be entered as “a.b.c.d” where a, b, c, and d are decimal integers from 0 to 255. A further requirement for the subnet mask is that it consist of a single region of all ‘1’ bits at the most-significant end and a single region of ‘0’ bits at the least significant end (i.e. no ‘1’ bit is permitted to the right of any ‘0’ bit, and no ‘0’ bit is permitted to the left of any ‘1’ bit). No white space is permitted anywhere in the command.
IP: Incoming datagrams with invalid checksums are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a datagram with an invalid IP checksum is received, and for every 256 such datagrams after that. Unless this message is displayed frequently, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

IP: Incoming datagram fragment from nnn.nnn.nnn.nnn discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the transmitting station (identified by its IP address) or a gateway along the way has split the message into fragments. The management card does not support IP fragmentation or reassembly, so the traffic is discarded. Fragmentation is usually triggered by a message that is too large to fit into the Maximum Transmission Unit (MTU) of one of the networks it must pass through. Large messages are created when a network management application attempts to perform a GET or a SET operation on a large number of variables at once; try splitting such requests up. Another possible cause is that the message passed through a non-Ethernet network with a small MTU. If possible, route the traffic around this network. This message is printed only when the appropriate traces are enabled via the “TM=mask” command.

IP: Incoming fragmented datagrams are being discarded.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a IP datagram fragment is received, and for every 256 datagram fragments after that. See also “IP: Incoming datagram fragment from nnn.nnn.nnn.nnn discarded”

IP: Invalid IP checksum, possibly from nnn.nnn.nnn.nnn
IP: checksum calculated=nnnn transmitted=nnnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming IP datagram was invalid. This is usually due to the corruption of the datagram in transit. Note that the address displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. Unless this message is displayed frequently or system operation is impaired, no corrective action is required. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

IP: Unsupported protocol 0xnn from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The datagram is addressed to a protocol not supported by the management card. For example, if another station attempts to establish a TCP connection with the management card, this message will be displayed since the management card does not support TCP. Supported protocols: ICMP, UDP. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.
IP: Warning, no default gateway address specified. dest=nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The management card has been asked to transmit a packet to a destination that is not on the same subnet as its own IP address, but no gateway address has been configured (via the “SET GATEWAY=ip” command). The management card will attempt to locate the destination station on the local Ethernet segment without using a gateway - this process almost always fails. This message is printed when any traces (including the default traces) are enabled via the “TM=mask” command.

Local IP=nnn.nnn.nnn.nnn Gateway IP=nnn.nnn.nnn.nnn Subnet mask=nnn.nnn.nnn.nnn

This message is a response to a console command. The network configuration settings currently in use are shown. These settings are not necessarily compatible or correct, and have not necessarily been saved. Once the settings have been proven to work, they should be saved to non-volatile memory via the “SAVE” command.

MCC16>

This is a prompt that indicates that the management card’s command line interface is ready for another non-privileged command. To enter privileged commands, first enter the “SU=private” command.

Memory test failed at nnnnnnnn

This is a system startup message. The DRAM test encountered an error. Power cycle the system. If the message persists, contact Black Box Corporation for assistance.

New trace mask = nnnnnnnn

This message is a response to a console command. The trace mask was successfully changed. For more information, see the description of the “TM=mask” command.

NON-MASKABLE INTERRUPT, SP=nnnnnnnn PC=nnnnnnnn SR=nnnnnnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

[Overflow nn]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that the controller’s receive buffer has overflowed. The Ethernet controller is reset as a precaution. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the “TM=mask” command.
PING: invalid destination IP address.

This message is a response to a console command. This indicates a syntax error in the entry of an IP address. Enter "PING=a.b.c.d" where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the IP address 0.0.0.0 is entered. It is not possible to ping this invalid address.

PING: pinging nnn.nnn.nnn.nnn, id=nnn seq=nnn

This message is a response to a console command. This message is displayed each time a ICMP ECHO packet is transmitted, i.e. once when a "PING" command is entered, and multiple times if the "RPING" command is entered. Note the identification and sequence numbers. They may be compared with those displayed when responses are received.

[Reset]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that the controller has entered the reset state or that the controller’s receive buffer has overflowed. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the "TM=mask" command.

[rr:no buffer nnnn]

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. An incoming Ethernet packet was discarded due to lack of memory. The number is the byte count of the packet, in hex. If this trace message occurs frequently, it indicates one of the following: 1) Excessive network traffic directed at the management card: 1a) Simultaneous SNMP requests from a large number of Network Management Stations 1b) Inadequate flow control - i.e. a station is continuously transmitting and not waiting for responses 1c) excessive broadcast traffic on the network segment. 2) Memory depletion due to excessive console output traffic Or, 3) a latent software defect or hardware failure. To eliminate these messages, use the “TM=mask” command to disable the traces.

RTL ISR=nn

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. The Ethernet controller caused an interrupt. Additional normal-completion indications may follow: “[Remote DMA complete]” “[TX ok]” “[RX ok]” “<get: b=nn-c=nn>”.

E.14

LMC1600A
This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. This unsolicited message is displayed when an unusual hardware or software condition is detected. The Ethernet controller was reset by software in response to a perceived error condition. Check the Ethernet segment to which the management card is attached for unusual conditions, such as a jabbering station. If operation of the management module is not impaired, it is likely that the condition was triggered by a peak in network traffic, in which case the message should be ignored or disabled via the "TM=mask" command.

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. A packet was extracted from the Ethernet receive queue. To eliminate these messages, use the "TM=mask" command to disable the traces. This message does not indicate an error condition. No corrective action is required.

This advanced debug message should be displayed only when debug traces have been enabled at the advice of Black Box Corporation technical support. The unsolicited message is displayed when an unusual condition is detected by the Ethernet controller and indicates one of the following: 1) A packet with an invalid CRC was received. 2) A frame alignment error occurred. 3) A packet was missed (probably due to a peak in network load). The Ethernet controller is reset as a precaution. To eliminate this message, use the "TM=mask" command to disable the traces.

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Decode of an incoming PDU failed. The PDU was discarded. ttttt provides a reason: “memory allocation failed” usually triggered by heavy network traffic and/or heavy console traffic. Unless this message is displayed frequently or system operation is impaired, no corrective action is required. “parent decode failed” occurs as SNMP attempts to clean up after an earlier error. Can be ignored.

The remaining messages indicate a malformed or incompatible incoming message:
“Alignment failure” the expected length of some element of the message does not match the actual length.
“invalid integer” an integer with a size other than 1, 2, or 4 bytes was received.
“null OID” an Object ID had zero sub-identifiers.
“illegal OID” indicates that a sub-identifier in an Object ID had more than 28 data bits.
“invalid length” a octet string had zero data length, or a NULL had non-zero data length.
“undefined tag” an element of the message could not be identified.
SNMP: berdecode - Tag nnnn not defined

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the management card received an SNMP PDU that it could not decode. If the message persists, call Black Box Corporation for assistance.

SNMP: berfree - tag nnnn not implemented

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a latent software defect. Call Black Box Corporation for assistance.

SNMP: beroutput - unimplemented tag nnnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the management card received an SNMP PDU that it could not decode. If the message persists, call Black Box Corporation for assistance.

SNMP: Cannot process request. Reason: tttt

This message is a response to a console command. The GET/GETNEXT/SET operation entered from the console could not be processed for the given reason. Check the MIB document for the variable you are attempting to access to make sure the Object ID you are entering is correct, and (for SET operations) that you understand the type and range of the variable correctly. Note that the appropriate security information is automatically supplied for all GET/GETNEXT/SET operations initiated from the console. The console must be in super-user mode before a SET operation is permitted. For values of tttt, see message “SNMP: Error ‘ttttt’ error_index=nnn on request from nnn.nnn.nnn.nnn”

SNMP: Community is not OCTET STRING in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Decode of incoming PDU failed

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A variety of causes are possible, e.g. malformed SNMP message, out of memory, etc. Usually, this message is accompanied by other more specific messages, if the appropriate traces are enabled.

SNMP: dumpbertree - tag nnnn not implemented

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a latent software defect. Call Black Box Corporation for assistance.
SNMP: Error ‘ttttt’ error_index=nnn on request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The management card was unable to process an incoming SNMP request for the stated reason. The error index indicates which of the (possibly many) variable bindings (i.e. individual sub-requests) in the incoming message caused the error. Values for ttttt include:

“noError” Theoretically impossible. If this message is displayed, contact Black Box Corporation for assistance.
“tooBig” An incoming message or the response to that message was too large for the management card to handle. If this message persists, contact Black Box Corporation for assistance.
“noSuchName=ttttt” A request was received for an Object ID that is not supported by the management card, or the community name in the request is invalid. Make sure the correct community names and MIBs are loaded into the managing station.
“badValue” An incoming SET request had a variable binding with an SMI data type incompatible with that of the variable being changed (e.g. “sysName” cannot be set to an integer), or the data was excessively large.
“readOnly” A SET request message attempted to change an item that is read-only in the current MIB view. (i.e. the data item is read-only in all MIB views, or the public community string was used for a SET operation on a read-write data item.)
“genErr” One of the following: 1) An incoming message contained an integer that was 3 bytes long or 5 or more bytes long 2) An incoming message contained an unrecognized BER data type. 3) Memory allocation failed while processing an SNMP message. 4) An incoming message contained an excessively long Object ID.

SNMP: Error displaying SNMP message

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. Probably indicates a low-memory condition during the display of “outgoing SNMP” traces.

SNMP: Error index is not 0 in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Error index is not INTEGER in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Error status is not 0 in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates a malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.
SNMP: Error status is not INTEGER in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Extra data in variable binding in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: GET id=nnnn ind=nnnn ttttt nnn.nnn.nnn...

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. It indicates that a variable binding is being processed by SNMP. The message that immediately follows shows the data associated with the binding. Note that one trace message is printed per binding; the id=nnnn given allows the user to determine which bindings were grouped in a single PDU. The text string tttt, if present, indicates an error code returned during processing of the binding. The remainder of the line is the object ID requested in the binding. This message is printed only when the appropriate traces are enabled via the “TM=mask” command.

SNMP: getlen - unimplemented tag nnnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates that the management card received an SNMP PDU that it could not decode. If the message persists, call Black Box Corporation for assistance.

SNMP: GETNEXT id=nnnn ind=nnnn ttttt nnn.nnn.nnn...

See “SNMP: GET id=…”

SNMP: Individual variable binding SEQUENCE missing in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Internal error, invalid MIB structure

This is a system startup message. This message indicates a latent software defect. Call Black Box Corporation for assistance.

SNMP: Invalid oid tttt

This message is a response to a console command. A numeric Object ID with at least three sub-identifiers was expected (e.g. “1.3.6”). For GET and SET operations, a fully specified OID is required, i.e. all indices (for tables) or a trailing “.0” (for scalars) must be specified.

SNMP: Invalid OID tag in variable binding in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.
SNMP: Memory allocation error

This message is a response to a console command. Insufficient memory was available to process the request, usually due to a peak in system activity. Retry the operation. If the message persists, call Black Box Corporation for assistance.

SNMP: Outer variable binding SEQUENCE missing in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: PDU from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An SNMP message has arrived from the IP address noted. If enough memory is available, a decode of the message will be displayed. This message is displayed only if the appropriate traces are enabled via the TM = command.

SNMP: PDU to nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. An SNMP message is being transmitted to the IP address noted. If enough memory is available, a decode of the message will be displayed. This message is displayed only if the appropriate traces are enabled via the TM = command.

SNMP: Request ID is not INTEGER in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: SET id=nnnn ind=nnnn ttttt nnn.nnn.nnn...

See “SNMP: GET id=...”

SNMP: SNMP PDU is not SEQUENCE in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: system reset performed via SNMP from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The management card has been ordered (via an SNMP “SET” operation) to save all settings into FLASH (as if the SAVE command had been entered from the console) and reboot itself.

SNMP: Variable binding value is constructed in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.
SNMP: Version is not INTEGER in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Unrecognized request tag nnn in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message indicates an malformed incoming PDU. If the message persists, call Black Box Corporation for assistance.

SNMP: Version is not V1 in request from nnn.nnn.nnn.nnn

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. A remote network management system (identified by its IP address) has attempted to communicate with the management card using a version of SNMP SMI other than V1. This version of the management card’s software supports only SMI V1.

[su] MCC16>

This is a prompt that indicates that the management card’s command line interface is ready for another super-user command. To return to non-privileged mode, enter the “SU” command.

Super-user mode off.

This message is a response to a console command. Super-user mode was disabled via the “SU” command. The default command set has been restored.

Super-user mode on.

This message is a response to a console command. Super-user mode was enabled via the “SU =password” command. Additional privileged commands are now available. See the help menu.

TRANSMIT TIMEOUT

This unsolicited message is displayed when an unusual hardware or software condition is detected. The Ethernet controller did not confirm completion of a transmit command. This may indicate a hardware failure. Power cycle the management card. If the message persists, call Black Box Corporation for assistance.

<TX>

This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. An Ethernet transmit attempt was made. To eliminate these messages, use the “TM =mask” command to disable the traces.
This is an advanced debug message that should only be displayed when debug traces have been enabled at the advice of Black Box Corporation technical support. This unsolicited message is displayed when an unusual condition is detected by the Ethernet controller. This message indicates that a transmit attempt was aborted due to excessive collisions. The Ethernet controller is reset as a precaution. To eliminate this message, use the “TM=mask” command to disable the traces.

**UDP: Incoming datagrams with invalid checkssums are being discarded.**

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. This message is displayed the first time a datagram with an invalid UDP checksum is received, and for every 256 such datagrams after that. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

**UDP: Invalid UDP checksum, possibly from nnn.nnn.nnn.nnn port nnnn**
**UDP: checksum calculated=nnnn transmitted=nnnn ln=nn**

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The checksum of an incoming UDP datagram was invalid. This is usually due to the corruption of the datagram in transit. Note that the address and port displayed may be incorrect due to this corruption. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. Excessive occurrences may indicate physical layer network problems resulting in packet corruption.

**UDP: Unsupported destination port nnn from nnn.nnn.nnn.nnn**

This unsolicited message is displayed in response to a packet that arrived at the Ethernet interface. The datagram is addressed to a service not supported by the management card. For example, if another station attempts to communicate with the UDP TFTP service on the management card, this message will be displayed since the management card does not support TFTP. The only supported port is SNMP. This message is printed only when the appropriate traces are enabled via the “TM=mask” command. This message does not indicate an error condition. No corrective action is required.

**UNEXPECTED EXCEPTION, SP=nnnnnnnn PC=nnnnnnnnn SR=nnnnnnnn**

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

**Usage: PING=nnn.nnn.nnn.nnn**

This message is a response to a console command. This indicates a syntax error in the entry of a PING command. Enter “PING” to use the last valid PING address provided, or “PING=a.b.c.d” where a, b, c, and d are decimal integers from 0 to 255. No white space is permitted anywhere in the command. This message is also displayed when the command form “PING” is entered but no valid IP address has been entered via a previous “PING=a.b.c.d”. This message is also displayed when the IP address 0.0.0.0 is entered. It is not possible to ping this address.
Use the SAVE command to make the current configuration permanent.

This message is a response to a console command. The configuration has changed since the last restart of the management card. The changes made will be lost the next time the management card is reset, rebooted, or power cycled - unless they are saved in FLASH memory as suggested. You must first enter super-user mode by entering the “SU=password” command to make the SAVE command accessible.

USER BREAK, SP=nnnnnnnnn PC=nnnnnnnnn SR=nnnnnnnnn

This unsolicited message is displayed when an unusual hardware or software condition is detected. This message indicates a latent software defect or a hardware failure. Call Black Box Corporation for assistance.

WARNING: Gateway IP address is undefined. (Use SET GATEWAY= command)

This message can be displayed at system startup and whenever the management card's IP parameters are changed via console command. The default value for the management card's gateway IP address is 0.0.0.0, which is invalid. A gateway IP address must be assigned to the management card before it can communicate with any station that is not on the same logical IP subnetwork.

WARNING: Local IP address is undefined. (Use SET IP= command)

This message can be displayed at system startup and whenever the management card's IP parameters are changed via console command. The default value for the management card's IP address is 0.0.0.0, which is invalid. An IP address must be assigned to the management card before it can be accessed via a management station.

WARNING: Local IP nnn.nnn.nnn.nnn and gateway IP nnn.nnn.nnn.nnn are not on the same subnet under subnet mask nnn.nnn.nnn.nnn

This message can be displayed at system startup and whenever the management card's IP parameters are changed via console command. This message indicates that the gateway is not on a locally attached network (i.e. the 'network' bits in the local IP address are not the same as the corresponding bits in the gateway address) and is therefore unreachable. This probably means that there has been an error configuring the local IP address, the gateway address, or the subnet mask. The most likely result of this is that all IP datagrams not destined for stations on the local subnet will be lost. To fix this problem, choose a local IP address, a gateway IP address, and a subnet mask that are compatible, and enter them into the system via the “SET IP=ip”, “SET GATEWAY=ip”, and/or “SET NETMASK=mask” commands, then enter the “SAVE” command to make the changes permanent.
WARNING: Saved configuration settings missing or corrupt.

This is a system startup message. This message is normal on a new management card or (sometimes) on a management card whose firmware has been updated. When this message appears, the management card’s network interface is disabled. The user should (at a minimum) enter an IP address (via the “SET IP=ip” command), a subnet mask (via the “SET NETMASK=mask” command), and a gateway address (via the “SET GATEWAY=ip” command), then enter the “SAVE” command. If this procedure does not eliminate the message, call Black Box Corporation for assistance.

WARNING: Subnet mask is undefined. (Use SET NETMASK= command)

This message can be displayed at system startup and whenever the management card’s IP parameters are changed via console command. The default value for the management card’s subnet mask is 0.0.0.0, which is invalid. A subnet mask must be assigned to the management card before it can communicate with any station that is not on the same logical IP subnetwork.

```
nnnnnnnnn=nnnn
nnnnnnnnnn==nnnn
```

This is an advanced debug message that should be displayed only when debug traces have been enabled at the advice of Black Box Corporation technical support. These messages show I/O operations to the Ethernet chip. At the left is the I/O address being read/written, the second number is the value being read (==) or written (=). To eliminate these messages, use the “TM=mask” command to disable the traces.
Trace Masks (TM = command)

The mask is always entered and displayed in hex, and is the combination of all of the currently selected traces - which are each represented by a single bit. The default mask is hex 101 - checksum + ICMP errors

Trace masks other than the default are not recommended for use except on the specific advice of Transition Networks technical support. They may impair the management card’s operation due to the large amount of console output they can cause if the network segment is carrying even light traffic. This is particularly true for traces from group 2, which, on a busy network, can overflow the management card’s console queue in a fraction of a second. Note that when the console output queue (which holds roughly 30 lines of text by default) is full, new console messages are discarded without notice.

Group 1

00000001 - Errors on incoming IP, ICMP or UDP datagram headers: invalid checksum, or (unsupported) fragmentation.
00000004 - ARP - locally and remotely initiated exchanges
00000008 - ARP - locally initiated exchanges
00000010 - Ethernet packets discarded due to receive queue full or memory depletion
00000020 - Errors reported by the Ethernet controller
00000100 - Incoming ICMP error indications
00000200 - Incoming ICMP request/response messages other than ECHO/ECHO REPLY
00000400 - Incoming ICMP ECHO (i.e. PING) messages (reporting of outgoing ECHO and incoming ECHO REPLY messages cannot be disabled)
00001000 - Report each SNMP GET binding and the result.
00002000 - Report each SNMP GETNEXT binding and the result.
00004000 - Report each SNMP SET binding and the result.

Group 2

01000000 - Dump all outgoing SNMP PDUs to the console.
10000000 - Reads/writes to registers on Ethernet controller
20000000 - Ethernet ISR, transmit, receive routines
40000000 - Packets ‘not for us,’ e.g. a broadcast to a UDP port the management card does not implement
80000000 - Dump all incoming SNMP PDUs to the console.
INDEX

A

About SNMP in the LMC1600A C.1
About the LMC1600A 1.1

B

BitView emulation 4.9

C

Command-Line Interface 1.6, 3.8, 4.3, E.1
 Commands 4.4
  getnext[=oid] 4.4
  get[=oid] 4.4
  memtest 4.4
  ping 4.4
  rping 4.5
  save 4.5
  set gateway=nnn.nnn.nnn.nnn 4.5
  set ip=nnn.nnn.nnn.nnn 4.5
  set netmask=nnn.nnn.nnn.nnn 4.5
  set private 4.6
  set public 4.6
  set tntrip 4.6
  set tntripmask 4.6
  set=oid,type,value 4.5
  show 4.7
  su 4.7
  tm=mask 4.7
  xr 4.8
  Installing 3.1
  Introduction 1.6
  Messages E.1

Using 4.3
Connectors, LMC1600A 1.5

F

Fault Isolation 5.2
Fault Isolation and Recovery Table 5.2
Firmware, LMC1600A, Upgrading 5.8
Fuse (Power Supply Module), Replacing 5.6

I

Indicators, LED 1.5
Installation 3.1, 3.13
 Connecting Management Module to Command-Line Interface 3.8
 Connecting Management Module to Network Management Station 3.9
 Connecting Media Converter Slide-In-Modules to Network 3.7
 Installing One or More Media Converter Slide-In-Module(s) in LMC1600A Chassis 3.5
 Installing Optional Management Module in LMC1600A Chassis 3.4
 Installing Optional Redundant Power Supply Module in LMC1600A Chassis 3.3
 Installing the LMC1600A in Rack or on Table 3.6
  Rack Installation 3.6
  Table-Top Installation 3.7
 Powering the LMC1600A 3.10
 Unpacking LMC1600A Equipment 3.2
 Using Command-Line Interface to Set IP Parameters 3.11
 Using SNMPc™ at NMS to Monitor Status 3.12
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction 1.1, 1.3</td>
<td>1.2</td>
</tr>
<tr>
<td>Media Conversion Center 1.2</td>
<td></td>
</tr>
<tr>
<td>Connectors, Indicators, and Switches 1.5</td>
<td></td>
</tr>
<tr>
<td>In the Network 1.4</td>
<td></td>
</tr>
<tr>
<td>Management Module, Optional 1.3</td>
<td></td>
</tr>
<tr>
<td>Media-Converter Slide-in-Modules 1.3</td>
<td></td>
</tr>
<tr>
<td>Power Supply Module(s) 1.3</td>
<td></td>
</tr>
<tr>
<td>SNMP Management 1.6</td>
<td></td>
</tr>
<tr>
<td>IP Parameters, Setting 3.11</td>
<td>3.1</td>
</tr>
<tr>
<td>L</td>
<td></td>
</tr>
<tr>
<td>LED Indicators 1.5, 4.2</td>
<td></td>
</tr>
<tr>
<td>LMC1600A Chassis, Installing 3.6</td>
<td>3.6</td>
</tr>
<tr>
<td>Rack Installation 3.6</td>
<td></td>
</tr>
<tr>
<td>Table or Shelf Installation 3.6</td>
<td></td>
</tr>
<tr>
<td>LMC1600A Object ID Tree C.3</td>
<td></td>
</tr>
<tr>
<td>LMC1600A, internal view 1.2</td>
<td></td>
</tr>
<tr>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Management Module 3.8</td>
<td>3.8</td>
</tr>
<tr>
<td>Connecting to Command-Line Interface 3.8</td>
<td></td>
</tr>
<tr>
<td>Connecting to Network Management Station 3.9</td>
<td></td>
</tr>
<tr>
<td>Management Module, Optional 1.3</td>
<td></td>
</tr>
<tr>
<td>Management Module, Replacing 5.7</td>
<td></td>
</tr>
<tr>
<td>Managing Media Conversion Center, Introduction 1.6</td>
<td></td>
</tr>
<tr>
<td>Media Conversion Center Installation 3.1</td>
<td></td>
</tr>
<tr>
<td>Media Conversion Center Maintenance 5.1</td>
<td></td>
</tr>
<tr>
<td>Media Conversion Center, Introduction 1.1</td>
<td></td>
</tr>
<tr>
<td>Media Converter Slide-in-Module(s), Installing 3.5</td>
<td>3.5</td>
</tr>
<tr>
<td>Media Converter Slide-in-Module, Replacing 5.4</td>
<td></td>
</tr>
<tr>
<td>Media-Converter Slide-in-Modules 1.3</td>
<td></td>
</tr>
<tr>
<td>Messages at Command-line Interface E.1</td>
<td></td>
</tr>
<tr>
<td>MIB Tree C.2</td>
<td></td>
</tr>
<tr>
<td>MIBs and Object Identifiers C.2</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>Network Management 1.6</td>
<td>1.6</td>
</tr>
<tr>
<td>Null Modem Cable Specifications B.1</td>
<td></td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>Object ID Tree C.3</td>
<td></td>
</tr>
<tr>
<td>OIDs C.2</td>
<td></td>
</tr>
<tr>
<td>Operation, Media Conversion Center</td>
<td></td>
</tr>
<tr>
<td>Using Status LEDs 4.2</td>
<td></td>
</tr>
<tr>
<td>Using the Command-Line Interface 4.3</td>
<td></td>
</tr>
<tr>
<td>Commands 4.4</td>
<td></td>
</tr>
<tr>
<td>Terminal Connection 4.3</td>
<td></td>
</tr>
<tr>
<td>Operations, SNMP C.1</td>
<td></td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>Power Specifications A.1</td>
<td>1.1</td>
</tr>
<tr>
<td>Power Supply Module, Installing 3.3</td>
<td>3.3</td>
</tr>
<tr>
<td>Power Supply Module, Replacing 5.5</td>
<td>5.5</td>
</tr>
<tr>
<td>Power Supply Modules, Introduction 1.3</td>
<td>1.3</td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Rack Installation 3.6</td>
<td>3.6</td>
</tr>
</tbody>
</table>
Redundant Power Supply Module, Installing 3.3
Replacing 5.4
  Management Module 5.7
  Media Converter Slide-In-Modules 5.4
  Power Supply Module 5.5
  Power Supply Module Fuse 5.6

S
Setting IP Parameters 3.11
Simple Network Management Protocol C.1
Site Planning 2.1
SNMP 4.9
SNMP GLOSSARY D.1
SNMP Parameters, Setting 3.11, 3.13
SNMP, Introduction C.1
SNMPc™ 4.9
SNMPc™, Optional 3.12
Specifications, Media Conversion Center A.1
Specifications, Power Input A.1
Status LEDs 1.5, 4.2
Switches 1.5

T
Table, Fault Isolation and Recovery 5.2
Table-Top Installation 3.7
Telnet 1.6, 4.9
TM = command E.24
Trace Masks E.24

X
xr, Using for Firmware Upgrade 5.8