SpectraCast®
DTMX5000

IP Gateway
Installation and Operation Manual

Part Number MN/DTMX5000.IOM Revision 1

SpectraCast®

DTMX5000

IP Gateway
Installation and Operation Manual

Comtech EFData is an ISO 9001
Registered Company.

Part Number MN/DTMX5000.IOM
Revision 1
September 11, 2000

Comtech EFData, 2114 West 7th Street, Tempe, Arizona 85281 USA, (480) 333-2200, FAX: (480) 333-2161.

Customer Support

Contact the Comtech EFData Customer Support Department for:

- Product support or training
- Information on upgrading or returning a product
- Reporting comments or suggestions concerning manuals

A Customer Support representative may be reached at:

Comtech EFData
Attention: Customer Support Department
2114 West 7th Street
Tempe, Arizona 85281 USA

(480) 333-2200 (Main Comtech EFData Number)
(480) 333-4357 (Customer Support Desk)
(480) 333-2161 FAX

or, E-Mail can be sent to the Customer Support Department at:

service@comtechefdata.com

Contact us via the web at www.comtechefdata.com.

1. To return a Comtech EFData product (in-warranty and out-of-warranty) for repair or replacement:

2. Request a Return Material Authorization (RMA) number from the Comtech EFData Customer Support Department.

3. Be prepared to supply the Customer Support representative with the model number, serial number, and a description of the problem.

4. To ensure that the product is not damaged during shipping, pack the product in its original shipping carton/packaging.

5. Ship the product back to Comtech EFData. (Shipping charges should be prepaid.)

For more information regarding the warranty policies, see Warranty Policy, p. xii.

Table of Contents

Figures

Tables

Overview of Changes to Previous Edition

This revision supersedes part number MN/DTMX5000 Rev. 0 dated June 9, 2000.

A summary of the changes made for Rev. 1 includes:

General	Updated company name and revision level/date
Chapter 1	Updated photograph and graphics
Chapter 3	Updated General parameters
	Updated 3.2 Editing CFG.INI parameters
	Updated 3.2.1 General Parameters
	Added 3.2.1.9 Gateway Description section
	Updated 3.2.2 Network parameters
	Updated 3.2.2.5 Transportation
	Deleted 3.2.10 Multicast Key Period
	Updated 3.2.3 CCU Parameters
	Updated 3.2.4 DVB Mapping Parameters
	Updated 3.3 SNMP Parameters
	Updated 3.5 Maintenance Parameters
	Updated 3.5.1 Description of Maintenance Parameters

About this Manual

This manual provides installation and operation information for the Comtech EFData DTMX5000 IP Gateway. This is a technical document intended for earth station engineers, technicians, and operators responsible for the operation and maintenance of the DTMX5000 IP Gateway.

Conventions and References

Cautions and Warnings

CAUTION indicates a hazardous situation that, if not avoided, may result in minor or moderate injury. CAUTION may also be used to indicate other unsafe practices or risks of property damage.

WARNING indicates a potentially hazardous situation that, if not avoided, could result in death or serious injury.

Metric Conversion

Metric conversion information is located on the inside back cover of this manual. This information is provided to assist the operator in cross-referencing English to Metric conversions.

Recommended Standard Designations

Recommended Standard (RS) Designations have been superseded by the new designation of the Electronic Industries Association (EIA). References to the old designations are shown only when depicting actual text displayed on the screen of the unit (RS-232, RS-485, etc.). All other references in the manual will be shown with the EIA designations (EIA-232, EIA-485, etc.) only.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Reporting Comments or Suggestions Concerning this Manual

Comments and suggestions regarding the content and design of this manual will be appreciated. To submit comments, please contact the Comtech EFData Customer Support Department.

EMC Compliance

EN55022 Compliance

This equipment meets EN55022.

This is a Class A product. In a domestic environment, it may cause radio interference in which the user may be required to take adequate measures.

Federal Communications Commission (FCC)

Note: All cables shall be shielded.

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 provided reasonable protection against harmful interference when the equipment is operated in a commercial environment.

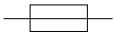
This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case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

European Low Voltage Directive

The following information is applicable for the European Low Voltage Directive (EN60950):

<HAR>	Type of power cord required for use in the European Community.
	CAUTION: Double-pole/Neutral Fusing ACHTUNG: Zweipolige bzw. Neutralleiter-Sicherung

International Symbols:

	Alternating Current.
	Fuse.
	Safety Ground.
	Chassis Ground.

Note: For additional symbols, refer to “Cautions and Warnings” listed earlier in this preface.

Warranty Policy

This Comtech EFData product is warranted against defects in material and workmanship for a period of one year from the date of shipment. During the warranty period, Comtech EFData will, at its option, repair or replace products that prove to be defective.

For equipment under warranty, the customer is responsible for freight to Comtech EFData and all related custom, taxes, tariffs, insurance, etc. Comtech EFData is responsible for the freight charges **only** for return of the equipment from the factory to the customer. Comtech EFData will return the equipment by the same method (i.e., Air, Express, Surface) as the equipment was sent to Comtech EFData.

Limitations of Warranty

The foregoing warranty shall not apply to defects resulting from improper installation or maintenance, abuse, unauthorized modification, or operation outside of environmental specifications for the product, or, for damages that occur due to improper repackaging of equipment for return to Comtech EFData.

No other warranty is expressed or implied. Comtech EFData specifically disclaims the implied warranties of merchantability and fitness for particular purpose.

Exclusive Remedies

The remedies provided herein are the buyer's sole and exclusive remedies. Comtech EFData shall not be liable for any direct, indirect, special, incidental, or consequential damages, whether based on contract, tort, or any other legal theory.

Disclaimer

Comtech EFData has reviewed this manual thoroughly in order that it will be an easy-to-use guide to your equipment. All statements, technical information, and recommendations in this manual and in any guides or related documents are believed reliable, but the accuracy and completeness thereof are not guaranteed or warranted, and they are not intended to be, nor should they be understood to be, representations or warranties concerning the products described. Further, Comtech EFData reserves the right to make changes in the specifications of the products described in this manual at any time without notice and without obligation to notify any person of such changes.

If you have any questions regarding your equipment or the information in this manual, please contact the Comtech EFData Customer Support Department.

1 Chapter 1. INTRODUCTION

This chapter provides a general description of the DTMX5000 IP Gateway, herein after referred to as, “the DTMX5000” or “Gateway.”

1.1 Introduction

The DTMX5000 IP Gateway (Figure 1-1) provides a high-speed connection between a network and a satellite or cable DVB channel. The DTMX5000 is compliant with DVB MPE standard EN 301.192. (See Appendix A.)

Figure 1-1. The DTMX5000

1.2 Description

On the input-side, the DTMX5000 connects to two 10/100 BaseT Local Area Networks (LANs). To ensure security and support high availability, the DTMX5000 has two separate 10/100 BaseT Network Interface Cards (NICs).

Transportation NIC	Data from this NIC can only be forwarded to the DVB channel. This NIC can be connected to an unsecured network (such as the Internet).
Control and Management NIC	Connected to a secured network.

The DTMX5000 links to a DVB modulator for the Single Channel per Carrier (SCPC) transmissions, or to a DVB Multiplexer (Mux), connected to a QPSK modulator in the case of Multiple Channels per Carrier (MCPC) transmissions. The DTMX5000 environment is shown in Figure 1-2.

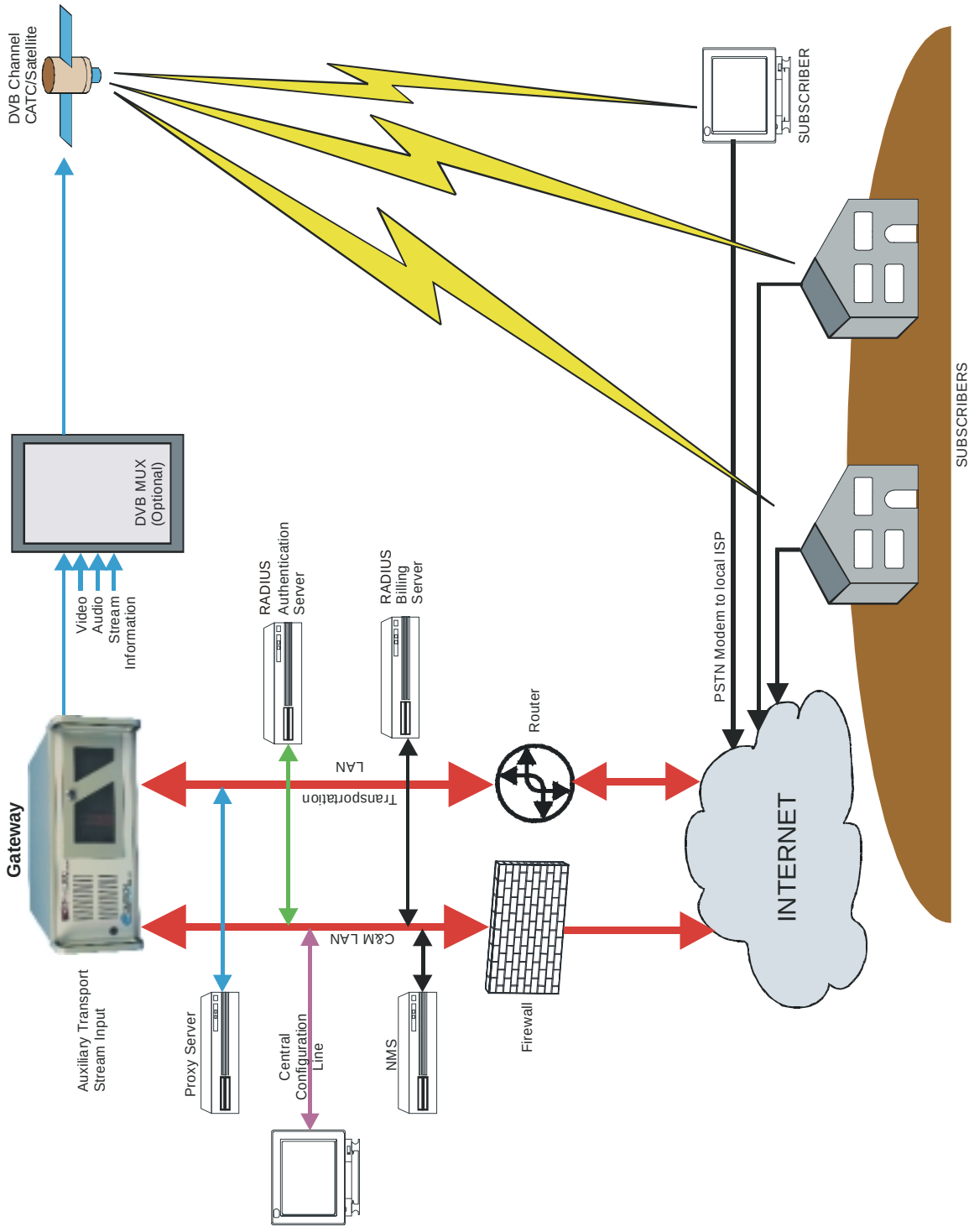


Figure 1-2. DTMX5000 Environment

1.2.1 Proxy Servers

At data request, the requested packet is routed to the proxy server. The proxy server acts as an intermediary between the final destination and the subscriber. The proxy server retrieves the data from its cache or the Internet, and returns the requested data to the subscriber via the DTMX5000.

1.2.2 Central Configuration Unit

The Central Configuration Unit (CCU) can control the DTMX5000. The CCU is an application running on a Windows NT™ station at the hub. This application monitors subscriber's activities, selects the proxy server for each session, maintains the routing table on the proxy table server, and interacts with external billing and authentication systems. (See Appendix B.)

As the subscriber logs On, the CCU notifies the DTMX5000 of the subscriber's:

- Quality of Server (QoS)
- Group Identification (ID)
- Encryption Parameters

When the subscriber logs Off, the CCU updates the DTMX5000 and collects the accounting information accumulated by the DTMX5000 for the subscriber. The CCU connects to the Control and Management (C&M) LAN.

- If the C&M LAN is protected by a Firewall, the appropriate actions must be taken to ensure connection between the CCU and the server (RIP2 messages from the CCU should be able to reach the proxy server) and between the CCU and the clients.
- For additional information, refer to the CCU User's Manual.

1.2.3 Network Management System

The DTMX5000 is an SNMP V2 client and can be fully controlled by any ANMP-based NMS application. The MIB parameters include the unit's configuration, statistic and diagnostic information. By editing and viewing these parameters, the service provider can configure and control the DTMX5000.

The NMS also enables the service provider to view and monitor realtime performance statistics, for example: Client information, memory usage, and packet information. The statistics can then be evaluated to enhance the QoS offered to subscribers.

1.3 DTMX5000 Features

The units's many configuration options enable service providers to tailor the operation of the DTMX5000 to suit their specific circumstances, to improve operational performance and to offer subscribers a high quality, versatile level of service.

DTMX5000 feature include the following:

- IP Multicast, enabling the same message to be sent to many subscribers simultaneously.
- IGMP client, enabling easy interfacing with standard routers.
- Data mapping mode for IP datagrams, piping, streaming or multiprotocol encapsulation (SI-DAT 360).
- Compliance with the DVB MPE standard, according to EN 301.192.
- DVB mapping options, enabling the unit to operate as a fully DVB compatible system, usable with SCPC and MCPC applications.
- Datagram flushing to maintain TCP/IP performance through DVB multiplexers with internal buffers.
- QoS prioritizing, to enable the service provider to optimize output bandwidth allocation according to subscribers profiles while guaranteeing minimum bit-rate requirements.
- Packet encryption for the privacy of DTMX5000 subscribers.
- Support for up to 8192 PID in the output Transport Stream.
- Dual input NICs, one for transportation and the other for control and management that ensures security and supports high availability.
- Passwords to enable remote NMS access.
- Remote downloads of new versions of the unit's software and firmware.
- Auxiliary transport Stream (TS) input to combine with the TS generated by the DTMX5000.
- On-the-Fly configuration, most DTMX5000 parameters can be configured without stopping the service.
- Support for both static and dynamic users, using the CCU.
- Support for user groups.

The values for these and other options can be set from the local terminal connected to the DTMX5000 and, with some restrictions, also from a remote NMS.

1.3.1 IP Multicast

The DTMX5000 receives TCP/IP datagram addressed to subscribers and maps them onto a DVB compatible MPEG2 transport stream. The DTMX5000 is capable of mapping two types of datagrams.

Unicast Packets	Each unicast packet is addresses to one individual user.
Multicasts Packets	Multicast packet are addressed are addressed to a group of users, and are simultaneously sent to all members of the group. These packets are usually for the distribution of files, or for streaming audio or video. It is possible to disable Multicast broadcasting if, example: this type of transmission is being handled by a separate DTMX5000. It is also possible to enable multicasting for predefined channels only.

1.3.2 IGMP Client

The DTMX5000 acts as an IGMP client (RFP 1122). For each registered multicast channel that it forwards, the unit generates an IGMP request and replies to IGMP queries. The IGMP protocol is managed on the Transportation NIC only.

1.3.3 Data Mapping and DVB Mapping

Data mapping specifies how IP datagrams are mapped onto the output transport stream. There are three mapping modes.

- Piping
- Streaming
- Multiprotocol Encapsulation

Data piping and data streaming are proprietary mapping, data piping without encryption and data streaming with encryption. Multiprotocol encapsulation is used for compatibility with other DVB based systems.

1.3.4 Quality of Service

Quality of Service (QoS) Management is a feature that determines the amount of bandwidth each subscriber is allocated. This feature can either be enabled or disabled.

- When QoS is enabled, subscribers receive their bandwidth share according to the level of service specified in their individual subscription fees.

- When QoS is disabled, the DTMX5000 will provide best effort service, resulting in the available bandwidth being equally divided among the various subscribers.

The DTMX5000 contains two QoS parameters for each user:

- Committed Information Rate
- Maximum Rate

The committed information rate is the maximum the DTMX5000 will allocate to that individual subscriber. The maximum rate specifics how the overall rate divides among all subscribers. If at a certain time free bandwidth is available; the subscribers may or may not receive more than their maximum rate, depending on the specified QoS mode.

1.3.5 On-the-Fly Configuration

Most of the configuration and maintenance parameters of the DTMX5000 can be configured without disturbing the flow of data. For example: using the NMS, the user can set a new CIR for a subscriber, without stopping the flow of data to the subscriber.

1.3.6 Packet Encryption

To provide privacy, the data addressed to individual subscribers is encrypted with the DES algorithm, implementing the CBC mode.

For additional encryption information, *refer to FIPS-46-2 and FIPS-81.*

1.3.7 Dual Input NIC

To ensure security and support high availability, the DTMX5000 has two input 10/100 BaseT NICs:

Transportation NIC	This NIC does not enable access to the C&M of the DTMX5000. This NIC can be connected to the unsecured network, such as the Internet. The DTMX5000 design prevents hackers from gaining access to the unit from the transportation NIC.
Control and Management	The Control and Management NIC of the DTMX5000 is via the Telnet, SNMP, and FTP. This NIC is connected to a secured C&M network. The C&M NIC can also act as an additional transportation NIC, enabling the sending of the IP datagrams from the C&M network to the DVB channel.

Note: The DTMX5000 supports full functionality even with only one input NIC. In this case, the C&M input NIC acts as C&M and Transportation.

Along with security, the two input NICs enable the support the high availability topologies. High availability will be supported in the next DTMX5000 version.

1.3.8 Accounting

The CCU informs the DTMX5000 each time a subscriber logs On or Off the system. The unit creates an account of the packets that each individual subscribers downloads, and the Billing Server later transfers this information for use.

The DTMX5000 also enables full access to the accounting information via the NMS. This enables an external system to retrieve the information.

1.3.9 Auxiliary Transport Stream Input

If enabled, the Auxiliary Transport Stream (Aux TS) input is compiled with the internal TS generated by the DTMX5000. The Aux IS input has precedence over the TS generated by the DTMX5000.

The TS generated by the DTMX5000 can be compiled with the Aux TS input in two ways:

1. The TS packets generated by the DTMX5000 will be transmitted only when there is free bandwidth in the output TS of the unit. It is up to the system architecture to ensure that such free bandwidth is available.

2. The TS packets generated by the DTMX5000 will be transmitted on free bandwidth, instead of DVB null packets in the Aux TS input.

1.3.10 Downloading Software

To enable new software versions of the DTMX5000 application and firmware to be downloaded, the NMS system can initiate a TFTP download process from any TFTP server. The DTMX5000 also supports FTP services.

1.3.10.1 Default Application Fallback

TFTP or FTP may be used to remotely download new software/firmware versions to the DTMX5000.

In the event that an invalid file is downloaded, the DTMX5000 will lock-up trying to run the invalid code. To correct this problem, a fixed default software application is provided on the DTMX5000's local hard drive. This default application enables the user to perform the download again.

Note: The Default application is set by the manufacturer and can not be altered.

Attaching a VGA display, rebooting the DTMX5000, and pressing <D> when prompted can access this file.

1.4 DTMX5000 Configuration

The DTMX5000 must be connected to a local serial terminal in order to enable definition of the unit's essential configuration parameters.

The DTMX5000 also can be accessed and configured remotely using the unit's NMS. In addition, the unit supports remote configuration via a Telnet terminal.

1.4.1 DTMX5000 Application

The operation of the DTMX5000 is determined by a software application, which is loaded automatically on Startup. A new release of this application can be downloaded to the DTMX5000 from a remote station. A new software release also can be downloaded using FTP.

1.4.2 Local Configuration

The unit's default operational behavior is determined by a configuration file (**CFG.INI**), which resides on the unit's internal hard drive. This file is persistent and is loaded by default into memory when the DTMX5000 is started up.

The **CFG.INI** file can be accessed and edited directly from a locally connected terminal, in the form of a <DUMB> terminal or PC.

1.4.3 VGA Display

An optional VGA display can be connected to the DTMX5000, for viewing startup and operational messages.

1.4.4 Remote Configuration

The DTMX5000 also can be controlled and configured remotely from a Telnet terminal. Setting the relevant parameters via the local terminal can enable Telnet services.

1.4.5 Firmware

The DTMX5000 contains a Field Programmable Gate Array (FPGA) which performs most of the mapping of IP datagrams onto the MPEG2 transport stream. The configuration of this FPGA is downloaded by the DTMX5000 application each time the DTMX5000 restarts.

This page is intentionally left blank.

2 Chapter 2. INSTALLATION

This section provides important information concerning the installation of the DTMX5000.

2.1 Overview

Note: For security reasons, the unit's vital parameters can only be configured through a direct serial connection to a local terminal. The remaining parameters can be configured either via the local terminal or remotely via a Telnet terminal.

An optional VGA display also can be connected to the DTMX5000 using a 15-pin cable for viewing, boot, and operational messages.

Never install the unit where it may be exposed to rain or moisture. Water in the unit may damage components and create a shock hazard.

Never remove the cover. This multiplexer has very sophisticated circuitry that should only be serviced by a fully trained technician.
Removal of the cover might:

- ***Void the warranty***
- ***Allow ESD damage to components***
- ***Create a shock hazard***

2.2 Connect and Configure

Perform the following procedures to connect the local terminal to the DTMX5000 and establish a communications link.

Note: Either a PC or a <DUMB> terminal, (a terminal processing no programming capabilities) can be used as a monitor. A PC may run a terminal emulation application, such as HyperTerminal™, which is supplied as an accessory with Win95™. The PC must have the following minimum requirements:

- Windows OS, with 16 Mbit/s of RAM
- EIA-232 Serial cable
- HyperTerminal application

To connect the local terminal to the DTMX5000, proceed as follows:

1. Attach one end of a EIA-232 serial cable to the back of the DTMX5000's COM1 connector.

2. Connect the other end of the EIA-232 serial cable to the COM1 or COM2 connector of the PC.

Configure the local terminal as follows:

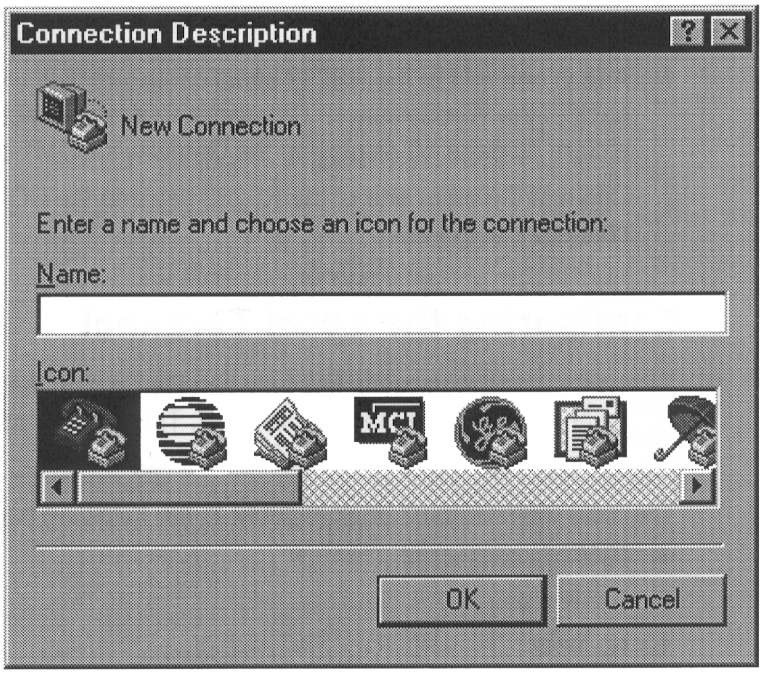
Note: To enable a communication link between the terminal and the DTMX5000, it is necessary to configure the local terminal. This configuration can be performed with the standard Windows HyperTerminal application.

The local terminal must be configured to the following parameters:

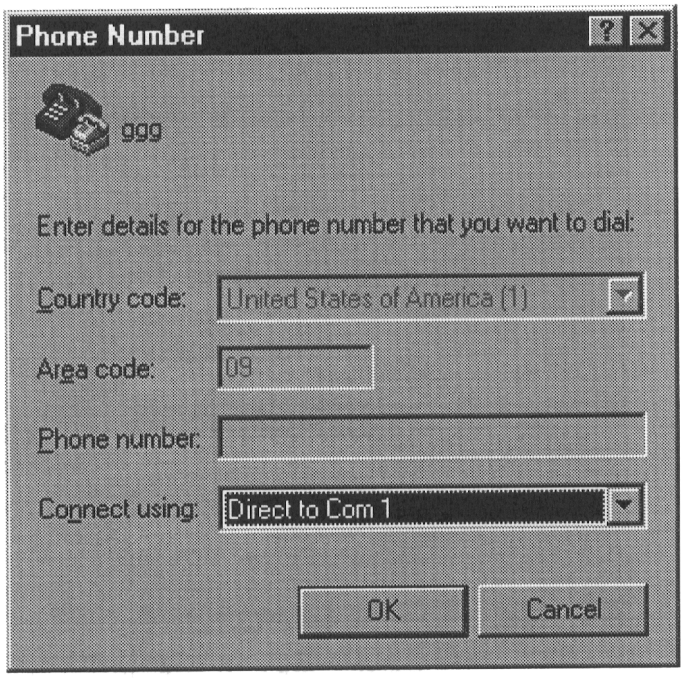
- Baud rate: 9600 bit/s
- Data bits: 8
- Parity: None
- Stop bit: 1
- Flow Control: Xon/Xoff

To configure the local terminal to the required parameters, proceed to the *Start* Menu bar and as follows:

1. Select the Program option to display the Programs menu.
2. Select the Accessories option to display the Accessories menu.
3. Select the HyperTerminal program group. The HyperTerminal program group window opens.
4. Double-click the Hypertrm.exe  . The Connection Description Windows opens.
5. Enter a name and choose an icon for the connection.

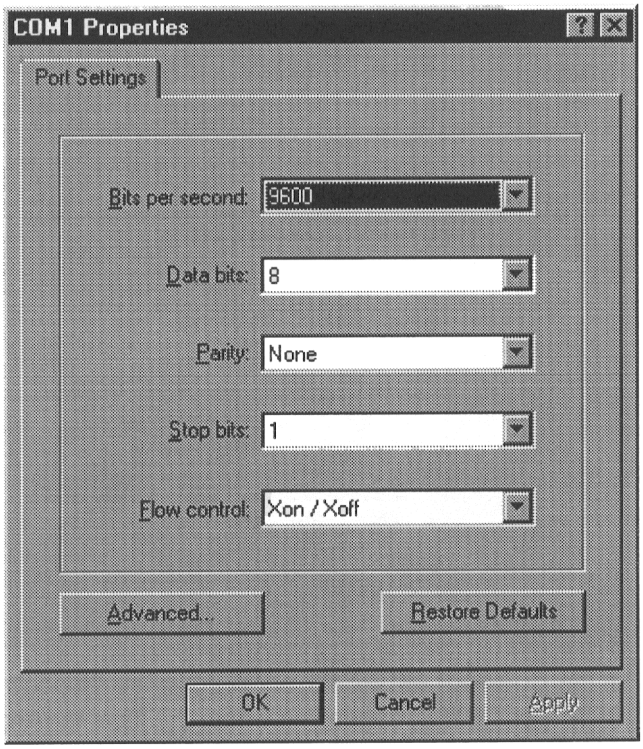


6. Click OK. The window closes and the Phone Number window opens.



7. In the Connect using field, scroll down the dropdown list and select either COM 1 or COM 2, depending where the local terminal is connected. Click OK. The Phone Number window closes and the COM Properties window opens.

8. In the Port Setting tab, enter the setting exactly as shown.



9. Click OK. The COM Properties window closes and is replaced with the HyperTerminal window.

2.3 Starting the DTMX5000

Note: The DTMX5000 can be started once the local terminal has been connected and configured. The optional VGA display can be connected at this time.

To start up the DTMX5000 and local terminal, proceed as follows:

Note: Ensure the local terminal is connected and configured.

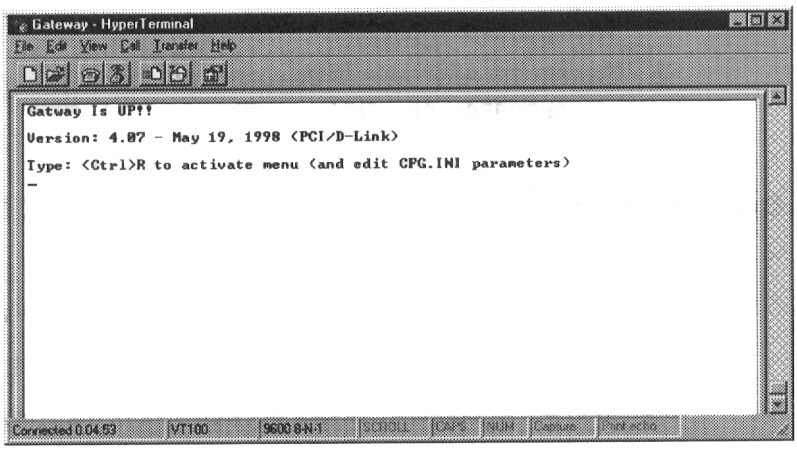
1. Double-click the icon defined for the local terminal's DTMX5000 connection. The HyperTerminal window opens.

2. Power-up the DTMX5000 and the local terminal. Observe the following:

DTMX5000	The booter, which is a software program, loads the application program, and the DTMX5000's parameters file (CFG.INI), from disk to memory. The application program controls all the DTMX5000's functionality. Then an FPGA programmable chip is loaded. This chip is responsible for the low level bit manipulation which creates the output transport stream.
VGA Display (Optional)	A confirmation message is displayed, stating that the booter has loaded the application program.

3. Observe the following screen, when the connection between the DTMX5000 and the local terminal is established. The local terminal and the DTMX5000 are now connected

4. Press <Ctrl>R to refresh the terminal display.



2.3.1 Connecting Network Interface Cards

Connect the Transportation Input NIC and Control and Management Input NIC.

2.3.1.1 Connect the Transportation NIC

The Transportation Input NIC connects to the Transportation LAN. The NIC is marked "TX NIC" to avoid confusion with the Control and Management Input NIC. After installation, verify the connection. The Transportation Input NIC does not reply to Ping (to ensure security), however, it will reply to ARP.

To verify connection, proceed as follows:

1. Ping from a computer on the Transportation LAN to the IP address of the Transportation Input NIC.

2. Browse the ARP table of that computer to verify that the IP address of the Transportation Input NIC appears.

2.3.1.2 Connect the Control and Management Input NIC

The Control and Management NIC connects to the Control and Management LAN. The NIC is marked "C&M NIC" to avoid confusion with the Control and Management Input NIC. Set the Control and Management NIC IP address and ping to verify the connection.

2.3.2 Connect the Output Transport Stream

The DTMX5000 has two optional output transport Stream Interfaces, LVDS and ASI. The Transport Stream is output on both interfaces. According to the target of the Transport Stream, select the appropriate output.

To verify the connection, proceed as follows.

1. Enable the Flushing mode in the DTMX5000.

2. In Flushing mode, the DTMX5000 generates a non-Null DVB compliant Transport Stream in its input.

2.3.3 Telnet Terminal

2.3.3.1 Connect the Telnet Terminal

The DTMX5000 as parameters can be configured and edited through a remote telnet terminal, connected via the Control and Management LAN connection of the DTMX5000. The Telnet terminal can run on any machine that has a TCP/IP connection with the DTMX5000. This connection can be local or remote, via the Internet.

Note: For security reasons, the unit's vital parameters can only be configured and edited through a local connection.

To connect the Telnet terminal to the DTMX5000 and establish a communications link between them, proceed as follows:

Notes:

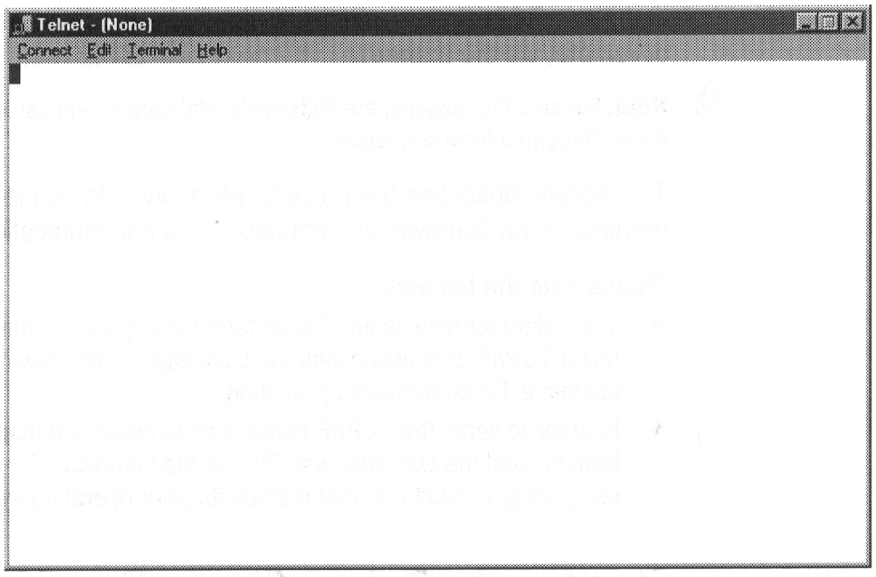
1. The Telnet terminal is any Telnet terminal application running on a machine that has a TCP/IP connection with the DTMX5000. All Windows™ operating systems contain a Telnet application.
2. Verify the TCP/IP connection between the machine running the Telnet terminal and the unit, use Ping to the unit.

2.3.3.2 Starting the Telnet Connection

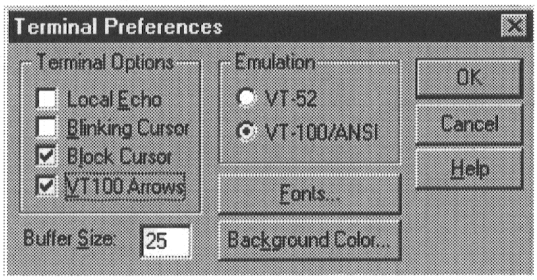
Note: Windows 95/98 or NT is required for the starting operation.

To start the Telnet connection, proceed as follows:

1. From the Windows Start menu, select the Run option.
2. In the command line, type Telnet. Press <Enter> . The Telnet application opens.

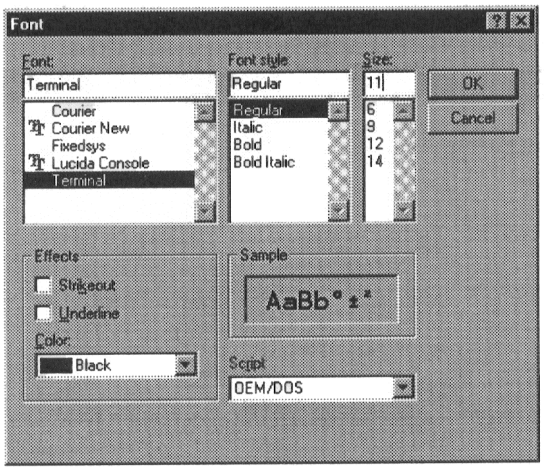


3. Select the Preferences option from the Terminal menu. The Terminal Preferences dialog box opens:



4. Select the VT100 Arrows check box.

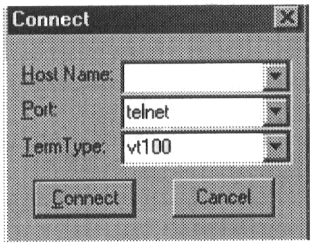
5. Click on the Fonts button. The Font dialog box opens.



6. Select Terminal in the Font list. Click OK.

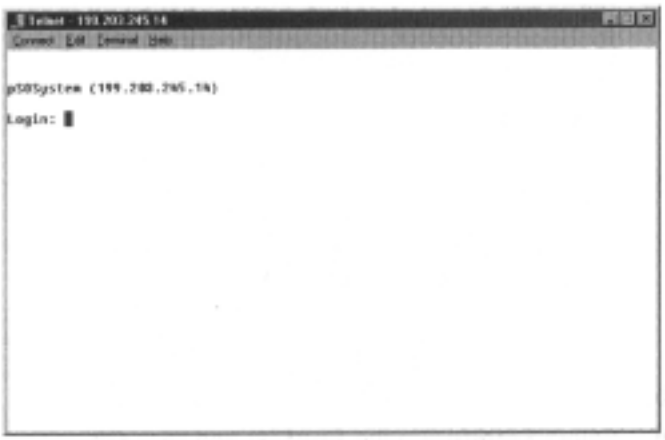
7. Click OK in the Terminal Preferences dialog box.

8. From the Connect menu, select the Remote System option. The Connect dialog box appears.

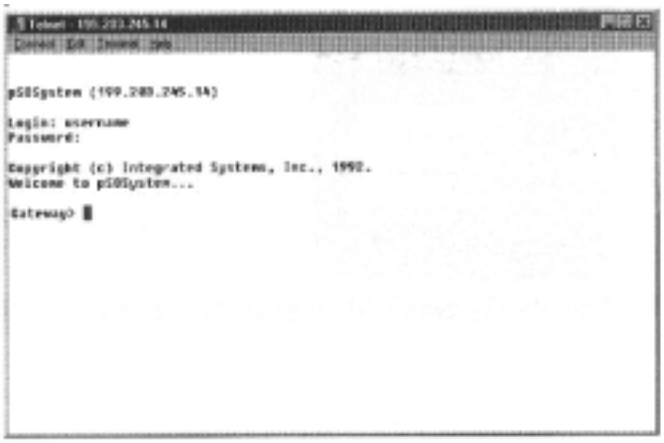


9. Enter the DTMX5000's IP address in the Host Name field.

10. Click Connect. The Telnet connection to the DTMX5000 is initialized and the following window is displayed.



11. Enter user Name and Password. (The user name and password are defined using a local terminal.) The following window should appear if user is authorized.



12. Type Terminal. DTMX5000 is operational.

This page is intentionally left blank.

Chapter 3. CONFIGURING THE GATEWAY USING A TERMINAL

DTMX5000 parameters can be configured through a menu driven interface through a local terminal or remotely using using a Telnet terminal.

3.1 Overview

There are two-types of parameters that can be configured:

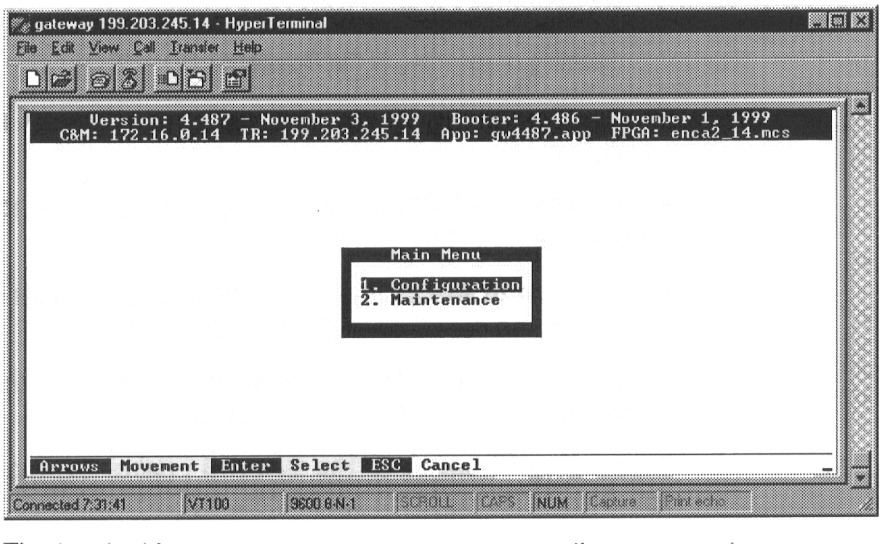
- Configuration Parameters. These parameters determine the default behavior of the Gateway. They are contained in the CFG.INI file, which is located in the root directory of the unit's internal hard drive.
- Maintenance Parameters. These parameters enable the definition of groups, static users, multicast users, and Telnet/FTP users. They also allow the enabling, disabling, or resetting of the unit.

3.2 Editing the CFG.INI Parameters

Note: Upon startup, the CFG.INI file or parameters file is loaded into memory. The file then can be edited through the unit's menu drive interface on the local terminal.

To edit the CFG.INI parameters, proceed as follows:

1. Establish a connection between the local terminal and the Gateway.
2. Press <Ctrl>R to refresh the screen.



The text lines at the top of the window describe the following:

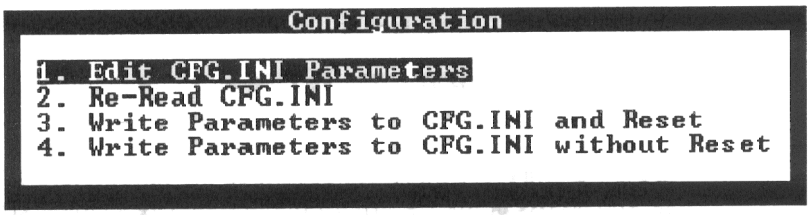
Version	The version number and date of the unit.
Booter	The version number and date of the unit pSoS.
C&M	The IP address of the Control and Management (C&M) interface.
TR	The IP address of the Transportation (Data) Interface.
App	The file name of the unit application.
FPGA	The file name of the unit firmware.

3. Select the Configuration option from the Main menu.

   Note: Options can be selected by doing one the following:

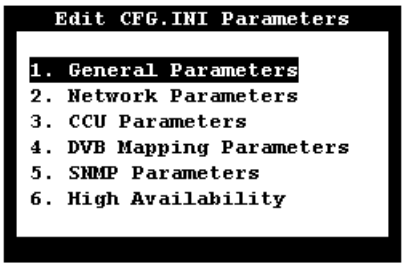
   - Type the associated option number
   - Navigate to the option using the [←] [↑] [→] [↓] on the cursor control keys.

4. Press <Enter> to activate the Configuration option. The Configuration menu opens.



Note: Pressing <Enter> always activates a selected option.

5. Select Option 1, Edit CFG.INI Parameters and press <Enter>. The Edit CFG.INI Parameters window opens.

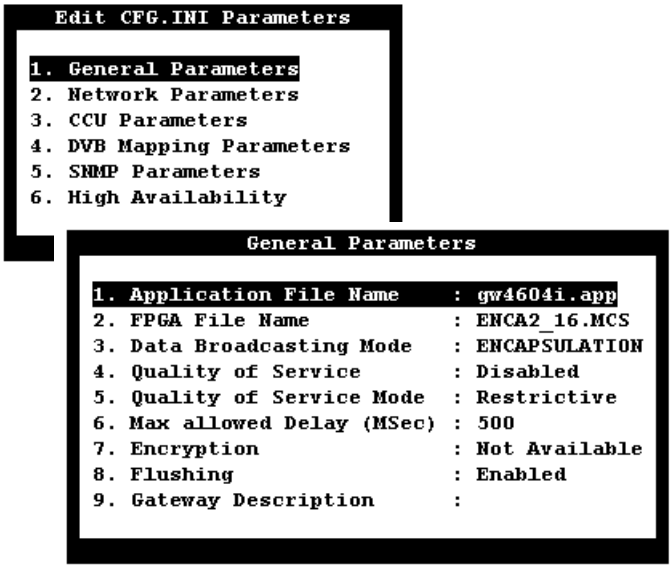


Note: The following CFG.INI parameters can be edited and configured from this window.

General Parameters	Describes the parameters which define the overall operation of the Gateway, including QoS, encryption options, stuffing options, and the name of the application to be loaded.
Network Parameters	Describes the parameters, which define the IP address and TCP/IP configurations for the unit's input NIC(s).
CCU Parameters	Describes the parameters, which define the list of IP addresses of the CCUs, which are allowed to control the unit.
DVB Mapping Parameters	Describes the parameters, which define the manner in which the DTMX5000 maps IP packets onto an MPEG2 transport stream. For addition data, refer to DVB SIDAT 360.
SNMP Parameters	Describes the parameters, which define the passwords required to access the DTMX5000 configuration parameters.
High Availability	Provisional for later upgrade.

3.2.1 General Parameters

The General Parameters define the overall operation of the Gateway.



Application File Name	Specifies the name of the application file to be loaded the next time the DTMX5000 will boot.
FPGA File Name	Specifies which of the previously downloaded FPGA configuration files will be loaded into the FPGA.
Data Broadcasting Mode	Specifies the data-mapping mode of IP datagrams onto the output Transport Stream.
Quality of Service	Specifies whether the unit should implement best effort service or offer QoS prioritizing.
Quality of Service Mode	Specifies the mode of operation of the QoS algorithm.
Maximum Allowed Delay	Specifies the maximum delay before a datagram is discarded.
Encryption	Enables or disables encryption on the DTMX5000 Link.
Flushing	Specifies whether to use the flushing option.
Gateway Description	Allows user to provide description of Gateway.

3.2.1.1 Application File Name

Path:	Edit CFG.INI Parameters/General Parameters/Application File Name
Description:	Specifies the name of the application file to be loaded on the next boot. Enter the name of the application file to be loaded.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.2 FPGA File Name

Path:	Edit CFG.INI Parameters/General Parameters/ FPGA File Name
Description:	Specifies which of the previously downloaded FPGA configuration files will be loaded into the FPGA on the next boot. Enter the name of the file to be loaded into the FPGA.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.3 Data Broadcasting Mode

Path:	Edit CFG.INI Parameters/General Parameters/Data Broadcasting Mode
Description:	Specifies the mapping mode of IP datagrams onto the output Transport Stream. Select one of the following mode options for mapping the data: • Piping • Streaming • Encapsulation The three modes have been define by the DVB organization for transmitting data onto a Transport Stream. Only Multiprotocol Encapsulation was specifically designed for TCP/IP mapping onto a Transport Stream, and is supported for compatibility with other DVB data streams. The first two modes are used for proprietary mapping modes, one without encryption (piping) and one, which supports encryption (streaming).

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.4 Quality of Service

Path:	Edit CFG.INI Parameters/General Parameters/Quality of Service
Description:	Specifies whether the Gateway should implement best effort service or offer QoS prioritizing. Select Enabled to enable QoS prioritizing, or Disable to disable the QoS feature and offer best service effort.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.5 Quality of Service Mode

Path:	Edit CFG.INI Parameters/General Parameters/Quality of Service Mode
Description:	Specifies the behavior of the unit in the event that a subscriber tries to exceed their maximum rate and there is free available bandwidth. This parameter is applicable only if the *QoS* parameter is set to Enabled. • Select Permissive to enable a subscriber to exceed the maximum rate if free bandwidth is available. • Select Restrictive to prevent the subscriber from exceeding the maximum rate under any circumstances.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.6 Maximum Allowable Delay

Path:	Edit CFG.INI Parameters/General Parameters/Maximum Allowable Delay
Description:	Specifies the maximum amount of time, in milliseconds, that a datagram can be delayed in the unit. If the delay is more than the specified number of milliseconds, the datagram is discarded. Enter the name specifying the maximum delay.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.7 Encryption

Path:	Edit CFG.INI Parameters/General Parameters/Encryption.
Description:	Specifies if subscriber's packets can be encrypted on the DTMX5000 Link. Select Enabled to enable subscribers to request encryption. Select Disable to specify that encryption will not be activated, regardless of a subscriber's request.

Note: The unit must be rebooted in order for settings to take effect.

3.2.1.8 Flushing

Path:	Edit CFG.INI Parameters/General Parameters/Flushing.
Description:	Enables/disables flushing. When flushing is enabled, flushing datagrams (not null DVB packets) are transmitted on the transport stream output whenever there is no valid data to send. Otherwise, null packets are generated. The flushing mechanism may be used for flushing the last datagrams from buffers in DVB multiplexers. If these datagrams are not flushed, they tend to cause TCP/IP performance degradation. Select Enabled to enable flushing. Select Disable to disable flushing.

Note: The unit must be rebooted in order for settings to take effect.

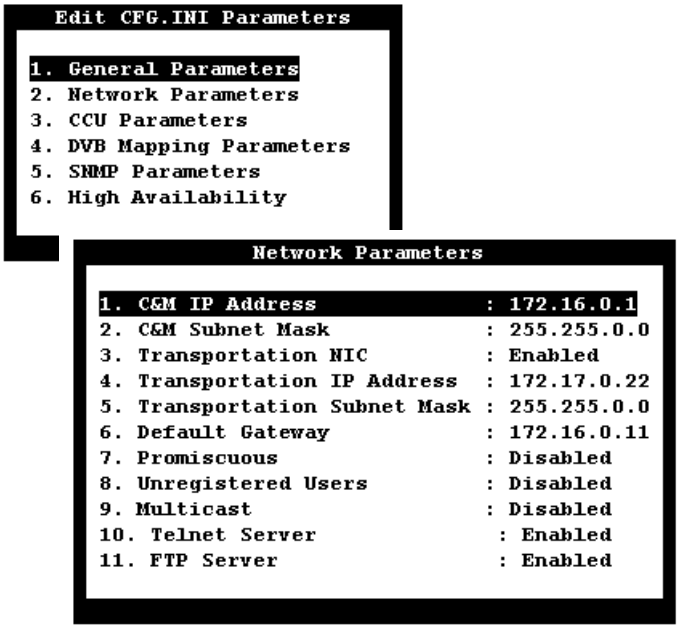
3.2.1.9 Gateway Description

Note: Provisional for later upgrade.

Path:	Edit CFG.INI Parameters/General Parameteres/General Parameters/Gateway Description
Description:	Allows user to manually assign a name or description to the Gateway.

3.2.2 Network Parameters

The Network Parameters define the overall operation of the DTMX5000.



C&M IP Address	Specifies the IP address for the unit's Control and Management NIC.
C&M Subnet Mask	Specifies the size of the subnetwork of the LAN segment to which the unit's Control and Management NIC is connected.
Transportation NIC	Specifies whether the DTMX5000 uses a separate data input NIC.
Transportation IP Address	Specifies the IP Address for the unit's Transportation NIC.
Transportation Subnet Mask	Specifies the size of the subnetwork of the LAN segment to which the transportation NIC is connected.
Default Gateway	Specifies the default unit IP address.
Promiscuous	Enables/disables Promiscuous mode.
Unregistered Users	Specifies the way in which the unit handles packets received for unregistered users.
Multicast	Specifies whether the unit will forward all Multicast datagrams to clients.
Telnet Server	Enables/disables remote unit configuration via a Telnet terminal.
FTP Server	Enables/disables FTP transmission of files to and from the unit.

3.2.2.1 C&M IP Address

Path:	Edit CFG.INI Parameters/Network Parameters/C&M IP Address.
Description:	Specifies the IP Address for the unit's Control and Management NIC. This must be a valid IP address. Enter the unit Control and Management IP address in place of the factory default setting.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.2 C&M Subnet Mask

Path:	Edit CFG.INI Parameters/Network Parameters/C&M Subnet Mask.
Description:	Specifies the size of the subnetwork of the LAN segment to which the unit's Control and Management NIC is connected. For example: 255.255.255.0 would indicate a 254-host subnetwork. Enter the Management Subnet IP mask in place of the factory default setting.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.3 Transportation NIC

Path:	Edit CFG.INI Parameters/Network Parameters/Transportation NIC.
Description:	Specifies whether the Transportation NIC is used. If Enabled, the Gateway will forward data coming from this NIC. If Disabled it will ignore the NIC. If the Transportation NIC is disabled, the unit will forward data from the Control and Management NIC.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.4 Transportation IP Address

Path:	Edit CFG.INI Parameters/Network Parameters/Transportation IP Address.
Description:	Specifies the IP Address for the unit's Transportation NIC. This must be a valid IP address. Enter the unit transportation IP address in place of the factory default setting.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.5 Transportation Subnet Mask

Path:	Edit CFG.INI Parameters/Network Parameters/Transportation Subnet Mask.
Description:	Specifies the size of the subnetwork of the LAN segment to which the unit's Transportation NIC is connected. For example: 255.255.255.0 would indicate a 254-host subnetwork. Enter the Subnet IP mask in place of the factory default setting.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.6 Default Gateway

Path:	Edit CFG.INI Parameters/Network Parameters/Default Gateway.
Description:	Responses, which are addressed to the DTMX5000, but originate from a different LAN from the one to which the unit is connected, will be routed to the default Gateway address. Enter a valid IP address for the default Gateway in place of the factory default IP address.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.7 Promiscuous

Path:	Edit CFG.INI Parameters/Network Parameters/Promiscuous.
Description:	Enables/disables Promiscuous mode.

Enabled	When Promiscuous mode is Enabled, the Gateway operates as a bridge (as opposed to a router), transparently interconnecting two remote LANs into one logical LAN. For example: The company has headquarters and a subsidiary. Majority of the traffic is on the local LAN. A event warrants the need to access the remote LAN. Promiscuous mode enables the contact of any host on the remote LAN. Each datagram has a manually entered MAC address (as opposed to the MAC address of the unit) that defines the destination host. In Promiscuous mode, the unit's NIC card allows this MAC address to be transmitted. The Gateway then uses it to identify the destination MAC address and the LAN to which it belongs.
Disabled	When Promiscuous mode is Disabled**,** the Gateway operates as a router, connecting two or mode LANs that have different IP addresses. In router mode, datagrams are sent with the unit's MAC address as the destination. The unit receives the datagrams and then maps the source IP address from one LAN to a destination IP address on a second LAN, according to a routing table. When this mode is selected, Unregistered Users is automatically Disabled.

Note: The unit must be rebooted in order for settings to take effect.

3.2.2.8 Unregistered Users

Path:	Edit CFG.INI Parameters/Network Parameters/Unregistered Users.
Description:	Specifies the way in which the Gateway handles packets received for users that have not been registered (in the CCU or via the NMS or terminal) and it does not recognize.

Enabled	When this parameter is Enabled, packets for unregistered users are sent using the MAC address of the destination LAN. This is only valid if Promiscuous mode is Enabled. The unit knows which MAC address to append because it already accessed the LAN via the bridge. Packets are sent to unregistered users using the default QoS parameters, with no encryption.
Disabled	When this parameter is Disabled, packets sent to unregistered users are discarded since the destination MAC address is unknown.

Note 1: Unregistered users will automatically be added to the default group, Group 1.
Note 2: Unregisterd users is automatically disabled when Promiscuous Mode is Disabled.

3.2.2.9 Multicast

Path:	Edit CFG.INI Parameters/Network Parameters/Multicast.
Description:	Enables/disables unregistered Multicast users. Multicast broadcasting is an extension of the unicast mode of transmission, which is the usual mode of transmission with TCP/IP, from one point to one destination. With Multicast, a datagram packet is sent to any users at once, for example: to all members of the group. It enables the same message to be sent to multiple users, for example: for video and audio streaming.

Enabled	When this parameter is Enabled, the unit forwards Multicast datagrams. Packets for unregistered multicast users also will be forward using default QoS parameters and no encryption.
Disabled	When this parameter is Disabled, only datagrams for registered multicast users are forwarded, while those for unregistered multicast users are discarded.

Note: The unit must be rebooted in order for settings to take

3.2.2.10 Telnet Server

Path:	Edit CFG.INI Parameters/Network Parameters/Telnet Server.
Description:	Enables/disables the user of a Telnet terminal for remote control and configuration of unit parameters.

Note: The unit must be rebooted in order for settings to take effect.

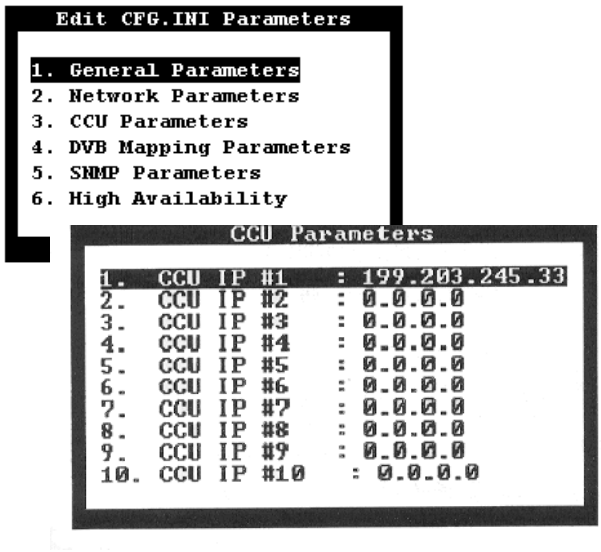
3.2.2.11 FTP Server

Path:	Edit CFG.INI Parameters/Network Parameters/FTP Server.
Description:	Enables/disables the user of FTP for transmission of files to and from the unit.

Note: The unit must be rebooted in order for settings to take effect.

3.2.3 CCU Parameters

The CCU parameters option specifies which CCU has permission to contact the Gateway and their IP addresses. If no CCU is specified, any CCU can contact the Gateway.

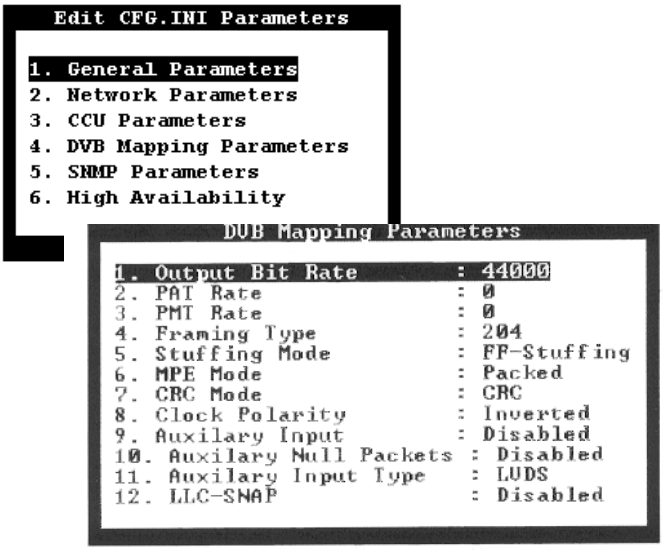


Path:	Edit CFG.INI Parameters/CCU Parameters/CCU Parameters.
Description:	Displays the CCU Parameter window. A CCU with a specified IP address can communicate with and control the Gateway. Select a CCU and press <Enter>. Specify the IP address for the CCU. Repeat for additional CCUs, as required.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4 DVB Mapping Parameters

Digital Video Broadcasting (DVB) Mapping is a method of mapping IP packets onto an MPEG2 transport stream. The DVB Mapping Parameters menu contains editable parameters. These enable the DTMX5000 to operate as a fully DVB compatible system, allowing it to be used for both SCPC and MCPC applications.



Output Bit Rate	Specifies the total output bit rate of the unit.
PAT Rate	Specifies the rate, in tables per second, at which the Program Association Table (PAT) packets will be sent.
PMT Rate	Specifies the rate, in tables per second, at which each Program Map Table (PMT) will be sent. The PMT defines the various PIDs of which a program is made.
Framing Type	Specifies what kind of framing (188, 204) to be used for the MPEG2 Transport Stream.
Stuffing Mode	Specifies the type of stuffing to be used to fill the remaining unused parts of an incomplete 188-byte MPEG packet.
MPE Mode	Defines the mode in which MPE operates, either packed or nonpacked.
CRC Mode	Specifies the way in which data integrity is checked.
Clock Polarity	Specifies the output polarity of the clock signal on the parallel LVDS interface, which may be inverted.
Auxiliary Input	Specifies whether the AUX Transport Stream input is enabled.
Auxiliary Null Packets	Specifies how the transport Stream from the AUX input will be combined with the output Transport Stream.
Auxiliary Input Type	Specifies which unit input would be used by the AUX input.
LLC-SNAP	Enables or disables the LLC-SNAP header.

3.2.4.1 Output Bit Rate

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/Output Bit Rate.
Description:	Specifies the output bit rate of the Gateway. This is the gross output bit rate, so that if the framing used is 204, the payload data rate will be somewhat lower (188/204) than the gross rate. Enter the output bit rate in the space provided.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.2 PAT Rate

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/PAT Rate.
Description:	Specifies the rate, in tables per seconds, at which the Program Association Table (PAT) packets will be sent. The PAT defines a structure from which the PMTs may be found. Enter the number for the rate at which the PAT packets will be sent.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.3 PMT Rate

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/PMT Rate.
Description:	Specifies the rate, in tables per seconds, at which the Program Map Table (PMT) packets will be sent. The PMT defines the various PIDs of which a program is made. Enter the number for the rate at which the PAT packets will be sent.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.4 Framing Type

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/Framing Type.
Description:	Specifies whether a placeholder for 16 Forward Error Correction (FEC) bytes is to be added to the packet.

188	Set the Framing Type to 188 to disable the framing option. This results in a higher payload.
204	Set the Framing Type to 204 to disable the framing option. This results in a higher payload.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.5 Stuffing Mode

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/Stuffing Mode.
Description:	This parameter is valid only when using MPE (multiprotocol encapsulation) in nonpacked mode. It specifies the type of stuffing to be used to fill the remaining unused parts of an incomplete 188-byte MPEG packet, so that transmission can occur.

FF Stuffing	FF (a reserved code) is filled in after the last byte of the packet, to make up a complete 188 byte packet.
Adaptation Field	The optional adaptation field in the MPEG header is enlarged to make up a complete 188-byte packet.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.6 MPE Mode

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/MPE Mode.
Description:	Defines the mode in which MPE operates either Packed or Nonpacked. This determines how incomplete 188-byte packet will be handled prior to transmission. Select either Packed or Nonpacked as follows:

Packed	If an MPE transport stream packet is incomplete, the next new MPE packet will begin from a point at which the last MPE packet ended. In Packed mode, stuffing is not required.
Nonpacked	Incomplete packets require stuffing prior to transmission.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.7 CRC Mode

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/CRC Mode.
Description:	Specifies the way in which data integrity is checked. Select one of the following:

Zero	CRC is not used.
Checksum	The sum of a group of data is used for error checking.
CRC	The integrity of a block of data is checked using CRC (Cyclic Redundancy Check). CRC is a common method of checking whether a datagram was correctly received. This method is similar to Checksum, but more powerful and effective.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.8 Clock Polarity

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/Clock Polarity
Description:	Specifies the output polarity of the clock signal on the parallel LVDS interface.

Inverted	Select Inverted to specify that the data is stable on the falling edge of the clock.
Not Inverted	Select Not Inverted to specify that the data is stable on the rising edge of the clock.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.9 Auxiliary Input

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/ Auxiliary Input.
Description:	Specifies whether the AUX Transport Stream input is Enabled or Disabled.

Enabled	If Enabled, the output transport stream of the unit combines the transport stream coming from the AUX input and the transport stream generated by the unit.
Responsibility	It is the Responsibility of the system architure to make sure that the output bit rate of the unit is not lower than sum of both transport streams rates (the transport stream from the AUX input and the transport generated by the unit). The transport stream from the AUX input has precedence over the transport stream generated by the unit. The transport stream generated by the unit will be transmitted only in the case of free bandwidth, meaning that the output bit rate is higher than the bit rate of the AUX input transport stream.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.10 Auxiliary Null Packets

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/ Auxiliary Null Packets.
Description:	Specifies how the Transport Stream from AUX input will be combined with the output transport stream.

Enabled	If Enabled, the unit will replace null packets in the incoming transport stream, with transport stream packets containing data that were generated by Gateway. This mode is effective only when Auxiliary input is enabled. The replacing of the null packets is performed together with the use of free bandwidth. Replacing the null packets with packets containing data enables increased utilization of the bandwidth.

Note: The unit must be rebooted in order for settings to take effect.

3.2.4.11 Auxiliary Input Type

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/ Auxiliary Input Type.
Description:	Specifies which physical input of the unit will be used as the AUX input, either LVDS or ASI.

Note: The unit is shipped with the ASI physical interface only. If you want to use the LVDS physical interface instead, a separate order must be made.

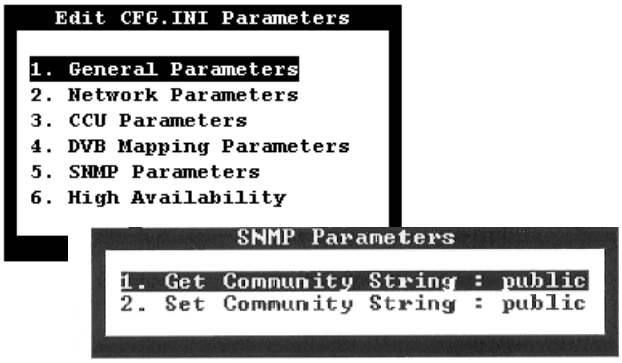
3.2.4.12 LLC-SNAP

Path:	Edit CFG.INI Parameters/DVB Mapping Parameters/ LLC-SNAP.
Description:	Enables or disables the LLC-SNAP header.

Note: If Enabled, the unit will add the LLC-SNAP header to the Transmitted datagrams.

3.3 SNMP Parameters

For security reasons, controlling the unit from a Network Management System (NMS) is restricted to those with password access. The following parameters enable these passwords to be set.



Get Community String	Specifies the password for executing read operations from an NMS.
Set Community String	Specifies the password for executing write operations from an NMS.

3.3.1 Get Community String

Path:	Edit CFG.INI Parameters/SNMP Parameters/Get Community String.
Description:	Specifies the password for executing read operations from an NMS system. Enter the string in the space provided.

3.3.2 Set Community String

Path:	Edit CFG.INI Parameters/SNMP Parameters/Set Community String.
Description:	Specifies the password for executing write operations from an NMS system. Enter the string in the space provided.

3.4 Writing the CFG.INI Parameters

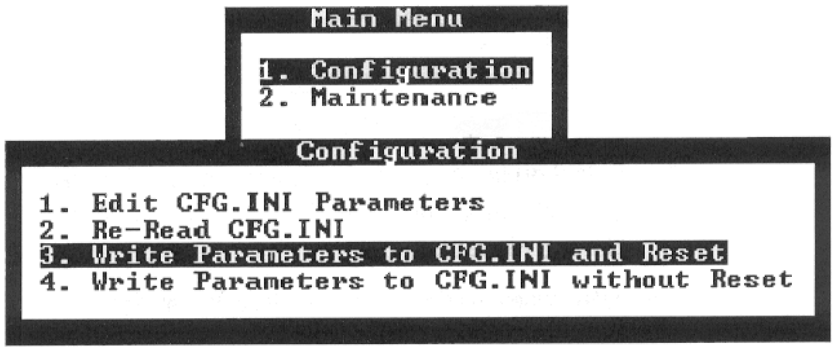
DTMX5000 parameters must be saved to the CFG.INI file after editing. These parameters will take effect when the unit is rebooted.

3.4.1 Write Parameters to CFG.INI and Reset

Note: Select this option to save the edited parameters as the unit's default. The unit automatically restarts, and the changes take effect.

To write the parameters to CFG.INI and reset the unit immediately, proceed as follows:

1. In the Main menu, select Configuration. The Configuration menu opens.
2. Select Option 3, Write Parameters to CFG.INI and Reset. The unit restarts and the edited CFG.INI files take effect.

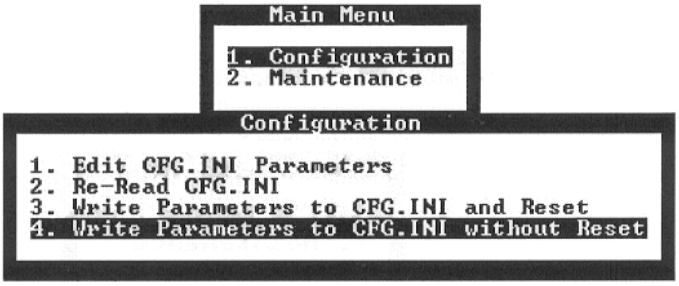


3.4.2 Write Parameters to CFG.INI without Reset

Select this option to save the changes without resetting the Gateway. The changes do not take effect until the unit is restarted. Manually restart the Gateway for the changes to affect the unit's operation.

To write the parameters to CFG.INI without resetting the Gateway, proceed as follows:

1. In the Main menu, select Configuration. The Configuration menu opens.
2. Select Option 4. Write Parameters to CFG.INI without Reset. The edited CFG.INI file will not affect the unit's operational functions until the unit is restarted.

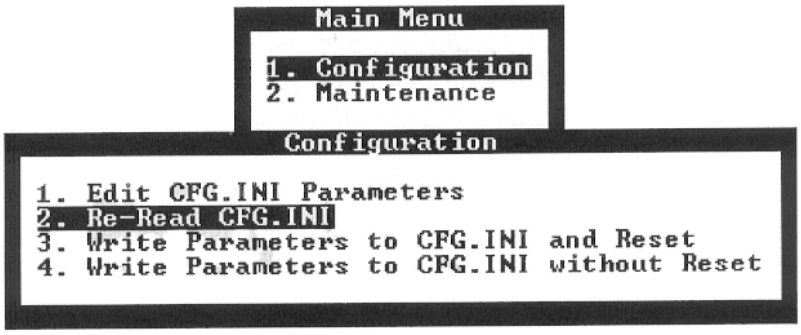


Note: When the CFG.INI file is edited, it is also possible to discard the changes and preserve the original configurations.

3.4.3 Discarding Changes to the CFG.INI File

To restore the saved version of the CFG.INI, proceed as follows:

1. In the Main menu, select Configuration. The Configuration menu opens.
2. Select Option 2, Re-Read CFG.INI. The edited parameters are not written to the CFG.INI file and the previously saved file remains the default operational file for the Gateway.



3.5 Configuring Maintenance Parameters

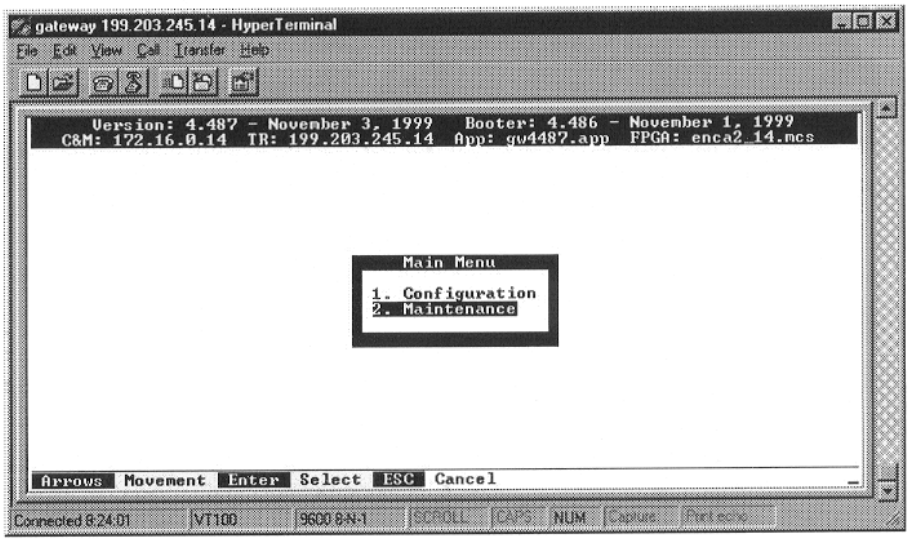
The DTMX5000 has several maintenance parameters, which can be configured through the unit's menu driven interface on the local terminal or remote Telnet terminal. These maintenance parameters enable the definition of groups, static users, and multicast users in the unit. The unit can also be enabled, disabled, or reset via these parameters.

To edit the maintenance parameter, proceed as follows:

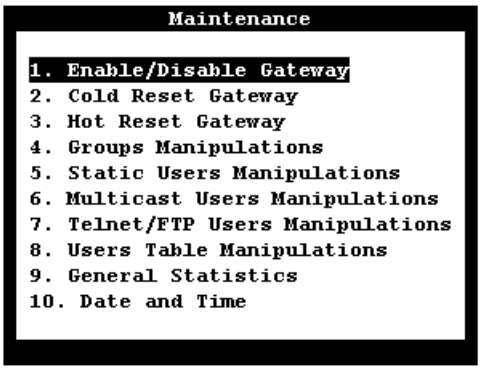
1. Establish a connection between the local terminal and the unit.
2. Press <Ctrl>R to refresh the screen. The following screen opens.
3. Select the Maintenance option from the Main menu.

   Note: Options can be selected by performing one of the following:

   - Type the associate option number.
   - Navigate to the option using the [←] [↑] [→] [↓] arrows on the cursor control keys.

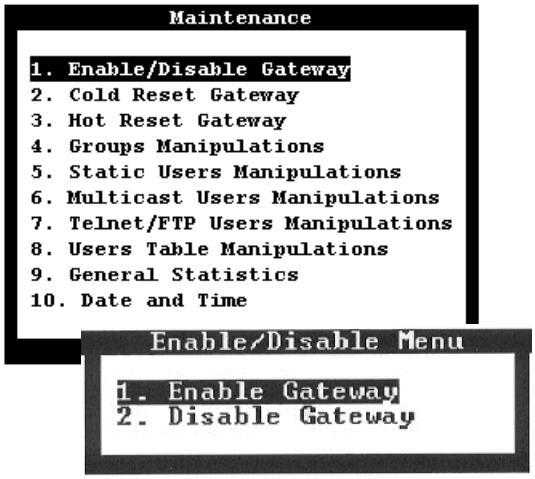


4. Press <Enter> to activate the Maintenance option. The Maintenance menu opens.



Note: Pressing <Enter> always activates a selected option.

3.5.1 Description of the Maintenance Parameters



Enable/Disable Gateway	Allows the user to enable or disable the unit.
Cold Reset Gateway	Allows the user to reboot the unit.
Hot Reset Gateway	Allows the user to reboot the unit without losing current information.
Groups Manipulations	Includes options that enable the user to create groups and define their parameters.
Static Users Manipulations	Includes options that enable the user to create static users and define their parameters.
Multicast User Manipulations	Includes options that enable the user to create multicast users and define their parameters.
Telnet/FTP Users Manipulation	Includes options that enable the user to create Telnet/FTP users and define their parameters.
User Table Manipulations	Includes tables with the information about users connected to the unit and their flow statistics.
General Statistics	Displays summary of all users' statistics.
Date and Time	Allows user to adjust Gateway's date and time.

3.5.1.1 Enable/Disable Gateway

To enable or disable the Gateway, proceed as follows:

Select an option from the Enable/Disable menu, as follows.

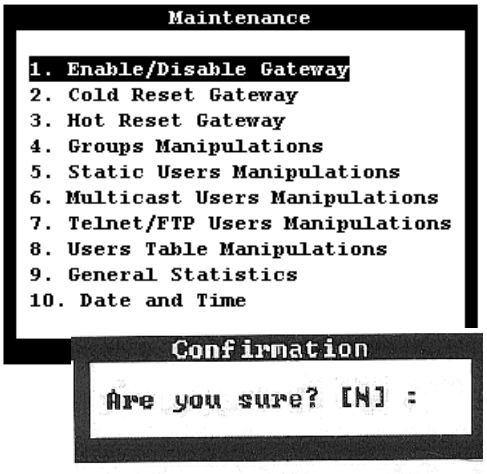
- Enable Gateway. This is the default option. The unit is fully functional.
- Disable Gateway. DTMX5000 function is halted and all transmitted packets are discarded.

3.5.1.2 Cold Reset Gateway

The Cold Reset Gateway parameter allows the user to reboot the Gateway. When the unit is rebooted, changes to parameter configurations take effect. After a Cold Reset, all the information held in the unit's memory will be lost. The unit will restart as if a hardware reboot has take place.

When this option is selected, the user is asked to confirm whether the Cold Reboot operation should be accomplished.

Type Y to reset the Gateway.
Type N to cancel the operation.

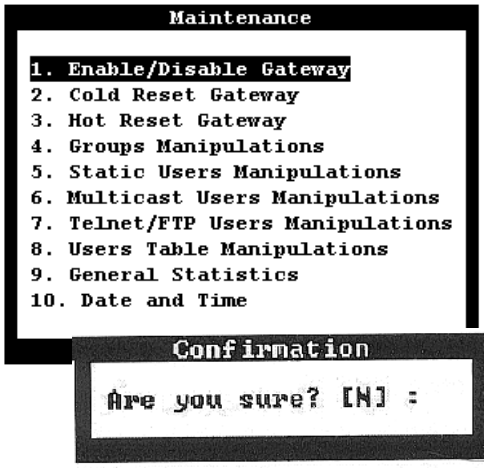


3.5.1.3 Hot Reset Gateway

This parameter allows the user to reboot the unit. After reboot, changes to the parameter configurations take effect. After a Hot Reset the DTMX5000 does not lose any information in memory (such as accounting information, number of discarded packets, and others) and will continue to work as before the reboot.

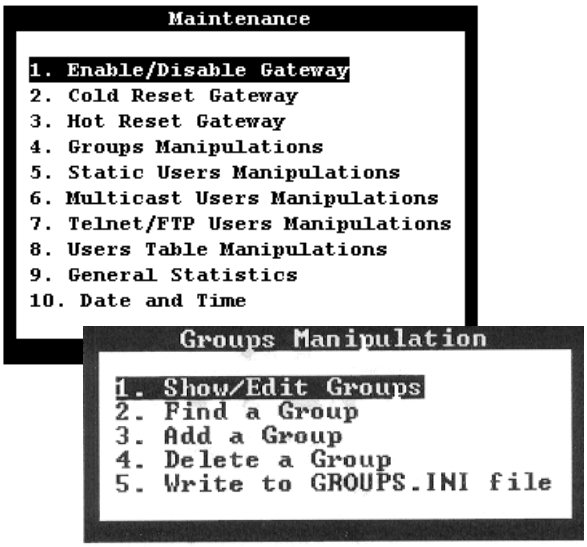
When this option is selected, the user is prompt to confirm whether the Hot reboot operation should be carried out.

Type Y to reset the DTMX5000.
Type N to cancel the request.



3.5.1.4 Groups Manipulations

The Gateway supports the concept of grouping. A group consists of several IP addresses for different users, including multicast users, which are all mapped under the same PID on the DVB. Groups enable logical aggregation of the data of groups of users or multicast users under separate PIDs. Groups are managed using the Groups Manipulations option of the Maintenance parameters.



For each group, various parameters can be defined, for example: the minimum and maximum bandwidth assigned for the group. When creating or modifying a group. The user can specify whether the group's QoS parameters are global or whether each individual's parameters take precedence over the group parameters.

Group 1 is the default group and cannot be deleted. Unregistered users, unregistered Multicast Channels and users that are not assigned to a group by the CCU, are added to Group 1.

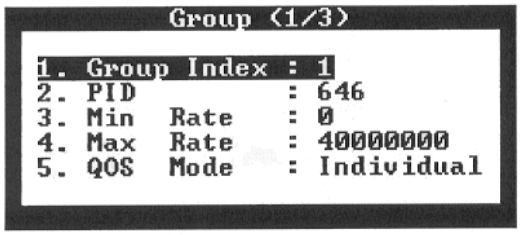
The Groups Manipulations Options consists of the following:

- Show/Edit Groups
- Find a Group
- Add a GroupDelete Group
- Write to GROUPS.INI File

3.5.1.4.1 Show/Edit Groups

This option enables the user to display and modify the definitions for existing groups. After selecting this option from the Groups Manipulations menu, use the [←] [→] on the keyboard to scroll through the existing groups.

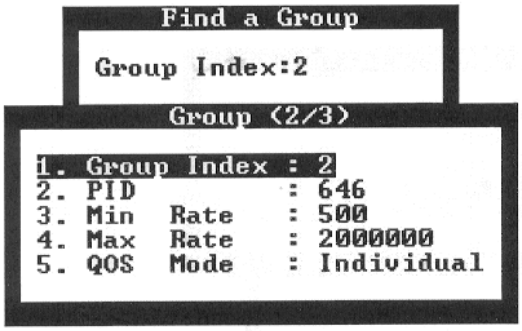
The following information is displayed for each group:



Heading (in this case Group 1/3)	Indicates the index number of the current group (1) and the total number of existing groups' (3).
Group Index	The group's identifying number.
PID	Specifies the PID under which data for this group will mapped.
Min Rate	Specifies the minimum bandwidth allocated by the unit's for this group.
Max Rate	Specifies the maximum bandwidth allocated by the unit for this group.
QoS Mode:	
Global	The unit calculates the total throughput of all the group members and then, for QoS purposes, the unit regards them as a single unit.
Individual	The group's QoS parameters are not relevant and each group member's individual parameters will be used.

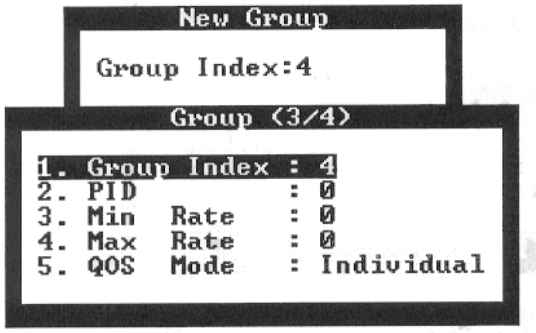
3.5.1.4.2 Find a Group

This option enables the user to search for and display the parameters for a specific group. After selecting this option from the Groups Manipulations menu, type the index number of the group that will be displayed.



3.5.1.4.3 Add a Group

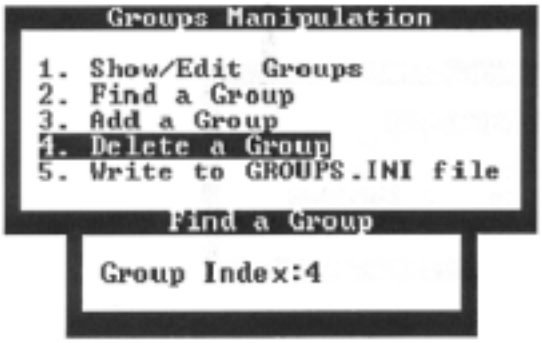
This option enables the user to create a new group and define the parameters. After selecting this option from the Groups Manipulations menu, enter an index number (not necessary a sequential number) for the new group and press <Enter>. The user can define the new group's parameters in the displayed window.



Note: If QoS mode Individual is selected, the group's Min Rate and Max Rate parameters will be irrelevant since each individual's QoS parameters will apply.

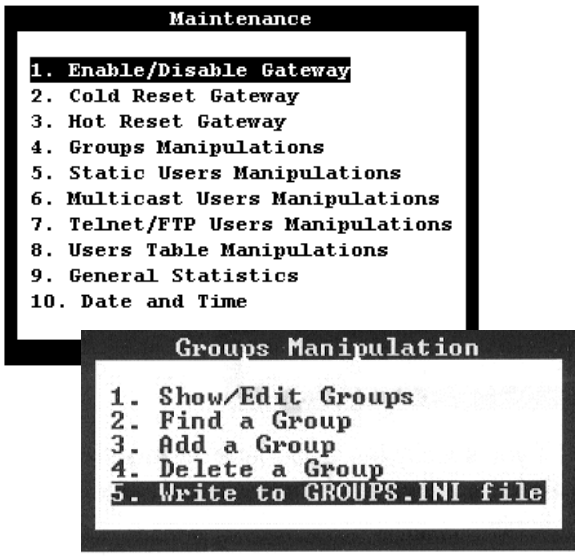
3.5.1.4.4 Delete Group

This Option enables the user to delete an existing group. After selecting this option, from the Group Manipulations menu, type in the index number of the group that is to be deleted and press <Enter>**.** After confirmation, the Group is deleted. The group members are not deleted; they no longer belong to that group.



3.5.1.4.5 Write to GROUP.INI File

This option enables the user to save all the group's parameters in a local GROUPS.INI file.

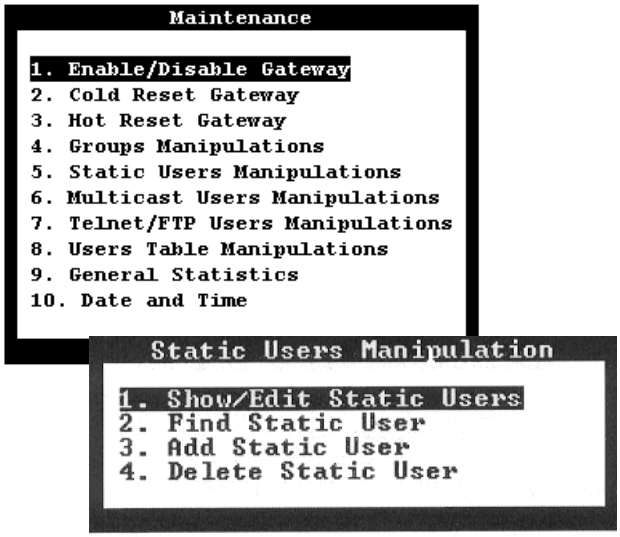


3.5.1.5 Static Users Manipulations

Static users are users with fixed IP addresses, as opposed to dynamic users who are allocated an IP address per session by the ISP.

Static Users	Parameters for specific static users can be defined in the Gateway via the terminal or the NMS. Static user parameters are stored in a user table in the unit.
Dynamic Users	The CCU identifies new users and their IP addresses and passes this information on to the unit. If users have a fixed IP address, this process can be bypassed.

Static users are managed using the Static Users Manipulations option of the Maintenance parameters. For each static user, the IP address, mask and MAC address are specified and the static user is included in a group. In addition, QoS parameters are defined for each static user.

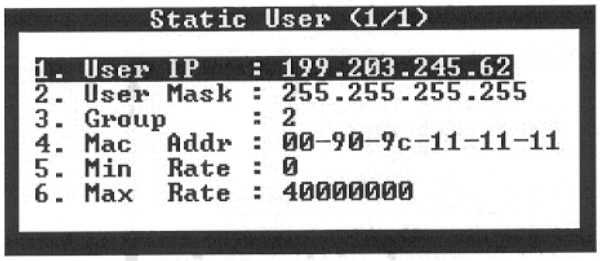


The Static User Manipulation Options consist of the following:

- Show/Edit Static User
- Find Static User
- Add Static User
- Delete Static User

3.5.1.5.1 Show/Edit Static User

This option enables the user to display and modify the definition for existing static users. After selecting this option form the Static Users Manipulation menu, use the [←] [→] on the keyboard to scroll through the existing static users.

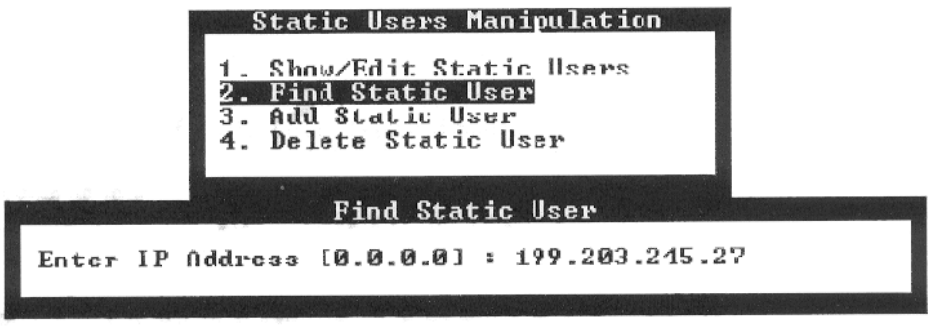


User IP	Specifies the user's fixed IP address.
User Mask	If the user is a network, this parameter defines, together with the IP address, the network's address. If the user is not a network, the subnet mask should be 255.255.255.255
Group	Specifies the group to which the user belongs.
Mac Addr	Specifies the physical address of the user's machine.
Min Rate	A QoS parameter that specifies the minimum bandwidth allocated for the static user.
Max Rate	A QoS parameter that specifies the maximum bandwidth allocated for the static user.

Note: These QoS parameters are not relevant if the group's QoS Mode parameter is set to Global.

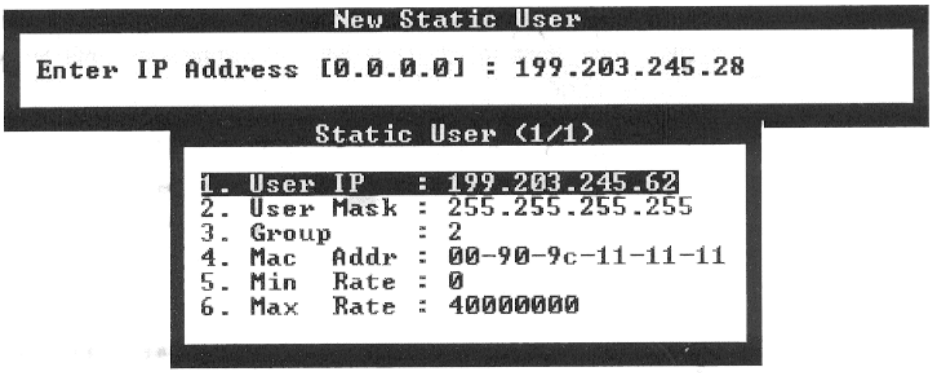
3.5.1.5.2 Find Static User

This option enables the user to search for and display the parameters for a specific group. After selecting this option from the Static Users Manipulations menu, type the index address of the static user that will be displayed.



3.5.1.5.3 Add Static User

This option enables the user to create a new group and define the parameters. After selecting this option from the Static User Manipulations menu, enter the new static user IP address and press <Enter>. The user can define the new static user parameters in the displayed window.



3.5.1.5.4 Delete Static User

This option enables the user to delete an existing static user. After selecting this option from the Static Users Manipulations menu, type in the IP address of the static user that will be deleted, press <Enter>. After confirmation, the static user is deleted.

Note: Changes to the static users database are kept automatically.

3.5.1.6 Multicast Users Manipulations

Multicast	One-to-many transmissions method that enables a single packet transmission to be routed to multiple users. For example: video can be transmitted simultaneously to three different hosts on a LAN.

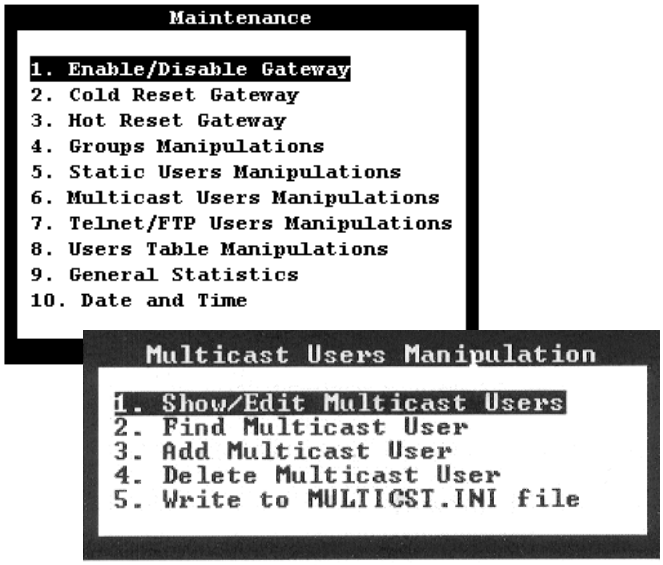
A packet transmitted to a multicast IP address is forwarded in single transmission and is only split when necessary. Over the DTMX5000 link, a packet only needs to be sent once and can reach all designated destinations.

Multicast users can be identified by special IP addresses which begin with 1110 (HEX E). The unit uses a formula to deduce the multicast MAC addresses from the IP addresses, thus identifying the packet destinations.

Multicast user addresses can be registered with the unit via the terminal or the NMS. Then, when a packet is sent to a registered multicast user address, it is forwarded using the QoS parameters defined specifically for that multicast user.

Each multicast user is assigned to one of the 15 SIDs (Service Ids) which are reserved for multicast transmissions. A SID is indexed to a set of odd and even keys used for data decryption, thus providing access to different kinds of information. The Gateway uses a double-buffering system in which these keys are continuously changed.

Multicast users are managed using the Multicast Users Manipulation option of the Maintenance parameters. For each multicast user, the IP address is specified and the multicast user is included in a group. In addition, QoS parameters are defined and the SID key to be used for decryption information is specified.



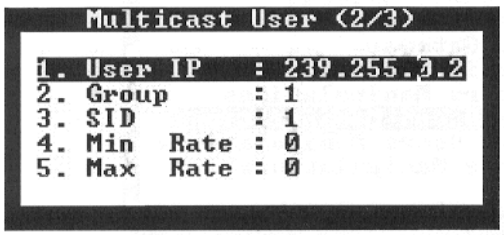
The Multicast Users Manipulations Options consists of the following:

- Show/Edit Multicast Users
- Find Multicast User
- Add Multicast User
- Delete Multicast User
- Write to MULTICAST.INI File

3.5.1.6.1 Show/Edit Multicast Users

This option enables the user to display and modify the definitions for existing multicast users. After selecting this option from the Multicast Users Manipulations menu, use the [←] [→] on the keyboard to scroll through the existing groups.

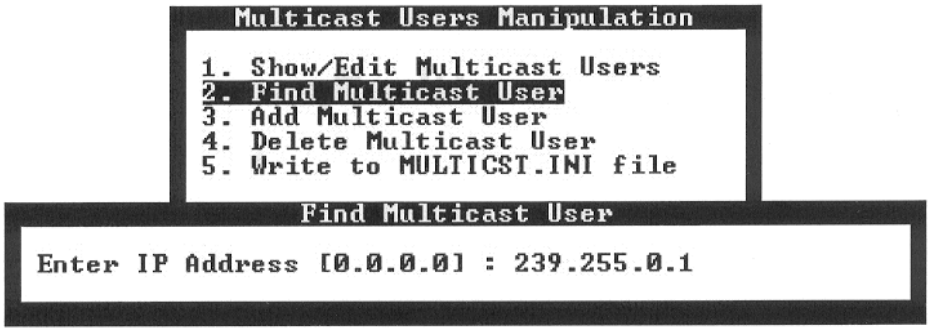
The following information is displayed for each group:



User IP	Specifies the multicast user's fixed IP address.
Group	Specifies the group to which the multicast user belongs.
SID	Specifies the SID that defines which set of keys is used for data decryption. This should be a number between 1 and 15.
Min Rate	A QoS parameter that specifies the minimum bandwidth allocated for the multicast user.
Max Rate	A QoS parameter that specifies the maximum bandwidth allocated for the multicast user. **Note:** These QoS parameters are relevant if the QoS Mode parameter of the group to which the multicast user belongs is set to Global.

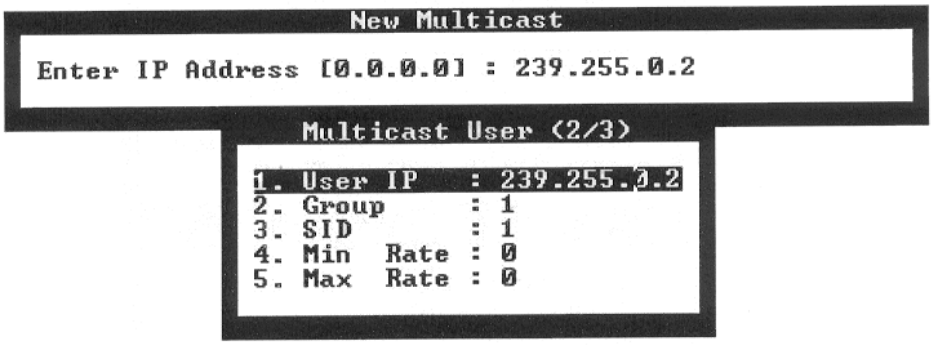
3.5.1.6.2 Find a Multicast User

This option enables the user to search for and display the parameters for a specific group. After selecting this option from the Multicast Users Manipulations menu, type IP address of the multicast user that will be displayed.



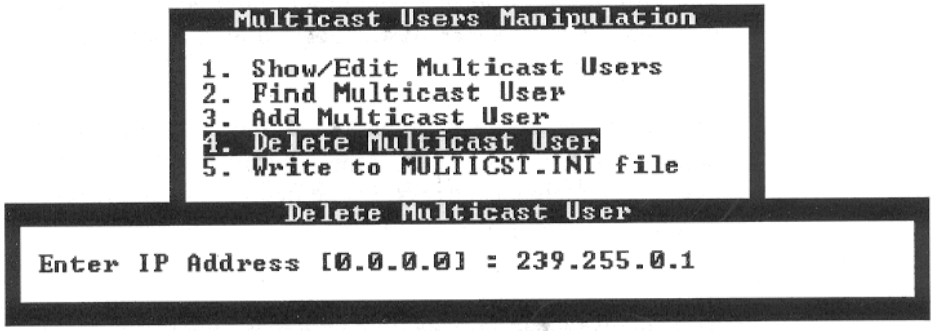
3.5.1.6.3 Add a Multicast User

This option enables the user to create a new multicast user's parameters. After selecting this option from the Multicast User's Manipulations menu, enter the new multicast user's IP address and press <Enter>. The user can define the new multicast user's parameters in the displayed window.



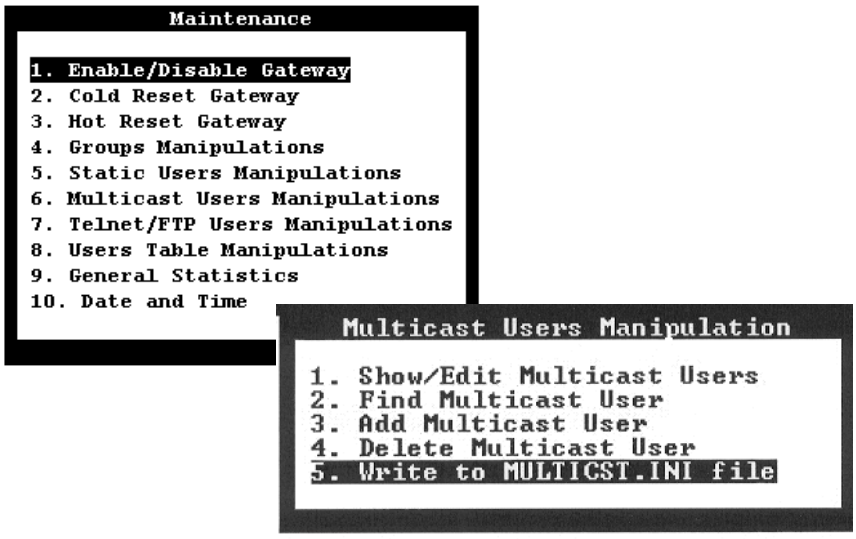
3.5.1.6.4 Delete Multicast User

This Option enables the user to delete an existing group. After selecting this option, from the Multicast User's Manipulations menu, type in the IP address of the multicast user that is to be deleted and press <Enter>. After confirmation, the Group is deleted.



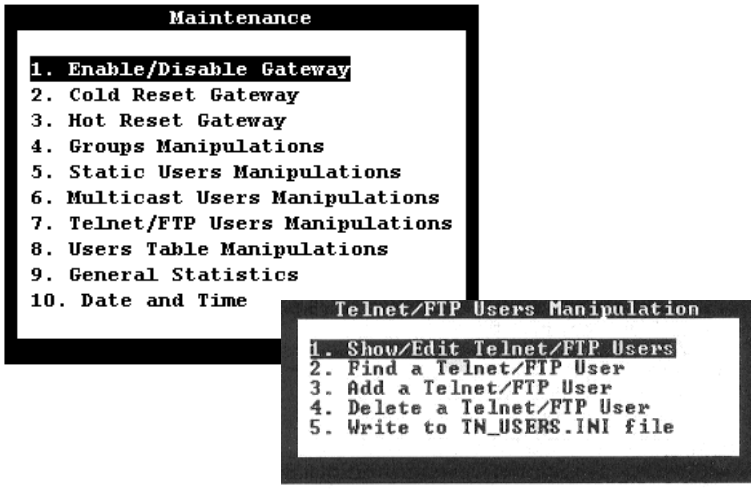
3.5.1.6.5 Write to MULTICAST.INI File

This option enables the user to save all the multicast user's parameters in MULTICST.INI file.



3.5.1.7 Telnet/FTP Users Manipulation

The DTMX5000 support remote control of the unit via a Telnet terminal, as well as FTP downloading and uploading of files to/from the unit's local disk. The unit acts as a Telnet server, thus enabling remote control and configuration of unit parameters from a Telnet terminal by authorized users. The unit checks Telnet users against a table of authorized users and their passwords. Once a Telnet user logs into the unit, configuration is the same as with the local terminal.



The DTMX5000 also acts as an FTP server, enabling files on the unit to be downloaded and new files to be uploaded. The FTP server uses the same user table as the Telnet server. The combination of these two features allows remote uploading of new software and firmware versions to the unit and easy reconfiguration of the unit to enable their use.

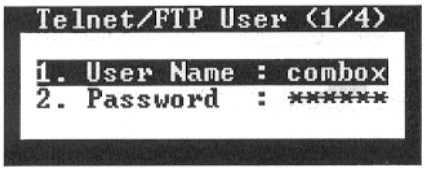
To enable Telnet or FTP services, the appropriate unit parameters must be configured. For security reasons, access to these parameters is via the local terminal only. The Telnet/FTP Manipulation options include:

- Show/Edit Telnet/FTP Users
- Find a Telnet/FTP User
- Add a telnet/FTP User
- Delete a Telnet/FTP User
- Write to TN_USERS.INI File

3.5.1.7.1 Show/Edit Telnet/FTP Users

This option enables the user to display and modify the definitions for existing Telnet/FTP users. After selecting this option from the Telnet/FTP Users Manipulations menu, use the [←] [→] on the keyboard to scroll through the existing groups.

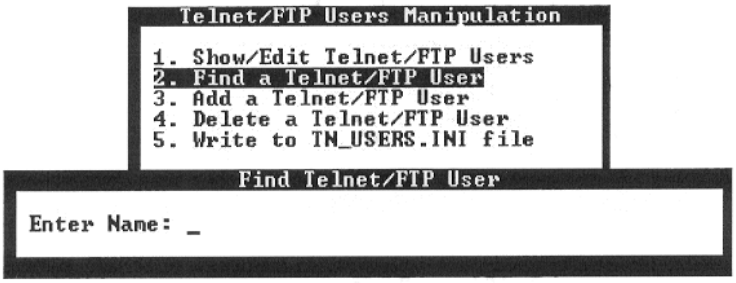
The following information is displayed for each group:



User Name	Specifies the Telnet/FTP user's name. This can be any string up to 29 characters.
Password	Specifies the user's password. Selecting this option opens the following window. **Note:** The password can be any string up to 19 characters.

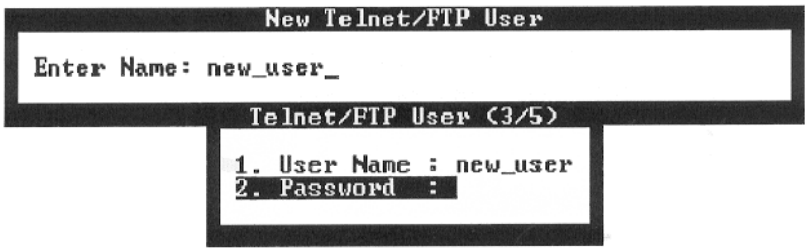
3.5.1.7.2 Find a Telnet/FTP User

This option enables the user to search for and display the parameters for a specific Telnet/FTP user. After selecting this option from the Telnet/FTP Users Manipulations menu, type the name of the Telnet/FTP user that will be displayed.



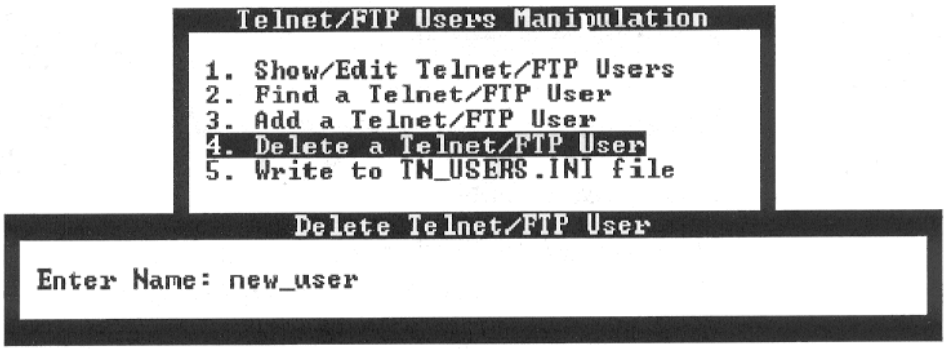
3.5.1.7.3 Add a Telnet/FTP

This option enables the user to add a new Telnet/FTP user and define the parameters. After selecting this option from the Telnet/FTP User's Manipulations menu, enter the new Telnet/FTP user's name and press <Enter>. The user can define the new Telnet/FTP user's parameters in the displayed window.



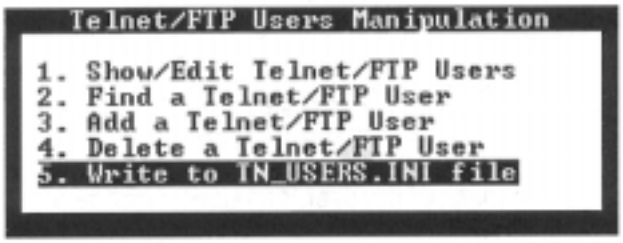
3.5.1.7.4 Delete Telnet/FTP User

This Option enables the user to delete an existing Telnet/FTP user. After selecting this option, from the Telnet/FTP User's Manipulations menu, type in the name of the Telnet/FTP user that is to be deleted and press <Enter>. After confirmation, the Telnet/FTP user is deleted.



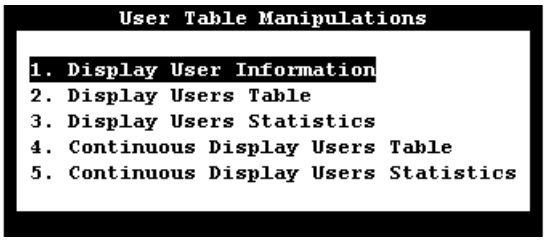
3.5.1.7.5 Write to TN_USERS.INI File

This option enables the user to save all the Telnet/FTP user's parameters in TN_USERS.INI file.



3.5.1.8 User Table Manipulation

The User Table Manipulations option consists of the following:



3.5.1.8.1 Display Users Table

This option enables the user to receive information about the users currently registered in the Gateway routing table.

```
IP Address       Mask             MAC Address   Grp/PID  By   Min Rate  Max Rate
-------------------------------------------------------------------------------
239.255.0.1      255.255.255.255  01005e7f0001    3/0300 MCT          0   4000000
239.255.0.2      255.255.255.255  01005e7f0002    2/0200 MCT          0   5000000
239.255.0.5      255.255.255.255  01005e7f0005    2/0200 MCT          0  10000000
239.255.0.6      255.255.255.255  01005e7f0006    3/0300 MCT          0   4000000
239.255.0.7      255.255.255.255  01005e7f0007    3/0300 MCT          0  50000000
-------------------------------------------------------------------------------
5 Users. Press any key to Continue...
```

IP Address — The IP address of the user. The IP address is used as an index for the table.

Mask — The subnet mask of the user. The user might be a host or a subnet.

MAC Address — The MAC address of the user's receive card.

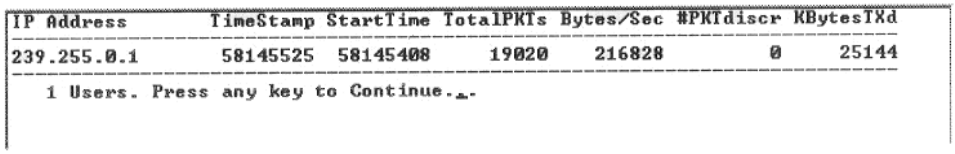
Group / PID — The index of the Group PID to which the user belongs.

By — Define the way the user was added to the table.

- USER: The user is a multicast channel that was automatically added by the Gateway.
- STU: The user is a registered static user.
- MCT: The user is a registered multicast channel.
- CCU: The user is a dynamic user that was added by the CCU.
- Min Rate: The QoS parameter defining the minimum rate for the user, if QoS is enabled.
- Max Rate: The QoS parameter defining the maximum rate for the user, if QoS is enabled.

3.5.1.8.2 Display Users Statistics

This option enables the user to receive information about the users currently registered in the unit's routing table.



IP Address	The IP address of the user. The IP address is used as an index for the table.
Time Stamp	The time stamp for the time when the last packet was sent to the user.
Start Time	The time stamp for the time the user was added to the table.
Total PKTs	The total number of packets that were sent to the user.
Bytes/Sec	The current throughput rate to the user.
#PKTdiscr	The number of packets sent to the user that were discarded by the unit. Packet discards occur when the total throughput to the users exceeds the output bit rate of the Gateway, or due to QoS definitions.
Kbytes Txed	The total number of data (in kbytes) sent to the client.

3.5.1.8.3 Continuous Display Users Table

This option displays the users table. This table is continually updated.

3.5.1.8.4 Continuous Display Users Statistics

This option displays the users statistics table. This table is continually updated.

Chapter 4. DTMX5000 MIB FILE

All DTMX5000 parameters can be configured and controlled remotely using any SNMP Network Management System (NMS). The Gateway's Management Information Base (MIB) file contains all the relevant parameters.

4.1 Overview

All Gateway parameters, with the exception of the Gateway's vital parameters, which are protected for security reasons, can be configured using the NMS. The Gateway's vital parameters can only be changes from a local terminal directly connected to the Gateway.

In general, all parameter configurations performed via the SNMP interface take effect immediately, without the need to reboot the Gateway. This enables On-the-Fly Gateway maintenance.

The parameters contained in the MIB are grouped as follows:

- Operation Mode Parameters
- Network Interface Configuration Parameters
- DVB Interface Parameters
- Multicast Channels Parameters
- Group Parameters
- Static Users Parameters
- CCU Parameters
- Software Download Parameters
- Diagnostics Parameters
- General Statistics Parameters
- Client Data Flow Statistics Table
- Client Configuration Parameters Table

4.2 Maintenance Information Base

4.2.1 Operation Mode Parameters

Operation Mode Parameters consists of the following:

- Gateway Enabled
- Gateway Software Reset
- Enable/Disable Encryption
- Maximum Allowable Delay
- QoS Mode
- QoS Enable/Disable
- Multicast Key Period
- Enable/Disable Promiscuous Mode
- Enable/Disable Unregistered Users
- Enable/Disable Multicast
- Client Information Reset
- Trace Mask
- Trace Level
- Trace Output Channel
- Gateway Description
- Software Version
- Application File Name
- FPGA File Name
- Time
- Date

4.2.1.1 Gateway Enable

MIB Object:	cbGatewayEnable
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbGatewayEnabled(1)
Description:	Enables/disables all Gateway operations
Data Types:	INTEGER cbEnabled (1) cbDisabled (0)
Access:	Read-write

4.2.1.2 Gateway Software Reset

MIB Object:	cbGatewaySWReset
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectrcast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbGatewaySWReset(2)
Description:	Enables the user to reset the Gateway software (by setting this parameter to cbTrue).
Data Types:	INTEGER cbTrue (1) cbFalse(0)
Access:	Write-only

4.2.1.3 Enable/Disable Encryption

MIB Object:	cbPktEncrypt
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247). spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbPktEncrypt(4)
Description:	Enables/disables encryption of the transmitted packets. If **cbPktEncrypt** is set to **cbTrue**, packets will only be encrypted if, for that client, the **cbCIEncrEnable** parameter is set to **cbTrue**.
Data Types:	INTEGER cbTrue (1) cbFalse(0)
Access:	Read-write

4.2.1.4 Maximum Allowable Delay

MIB Object:	cbMaxAllowableDelay
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2).cbGeneralParam(3). cbMaxAllowableDelay(9)
Description:	The maximum allowable time (in mSec) during which a packet can be delayed in the Gateway. Packets remaining in the Gateway after this time will be discarded.
Data Types:	INTEGER
Access:	Read-write

4.2.1.5 QoS Mode

MIB Object:	cbQoSMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2).cbGeneralParam(3). cbQualityofService(10).cbQOSMODE(1)
Description:	The parameter can be set to either Permissive or Restrictive mode. Permissive mode enables transmitting to users using data rates higher than their maximum rate, when bandwidth is available. In Restrictive mode, no data can be transmitted to users at data rates above their maximum rate, even if bandwidth is available.
Data Types:	INTEGER cbPermissive (1) cbRestrictive (2)
Access:	Read-write

4.2.1.6 QoS Enable/Disable

MIB Object:	cbQoSActive
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2).cbGeneralParam(3). cbQualityofService(10).cbQOSActive(2)
Description:	Specifies whether the Gateway should implement best effort service (cbFalse) or offer Quality of Service prioritizing (cbTrue). When Quality of Service is not implemented (cbFalse), the minimum CIR promised to users is ignored and data is transferred to users in the order it is received from the Ethernet by the Gateway.
Data Types:	INTEGER cbTrue (1) cbFalse (0)
Access:	Read-write

4.2.1.7 Multicast Key Period

MIB Object:	cbMulticastKeyPeriod
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbMulticastKeyPeriod(12)
Description:	Specifies the time interval (in seconds) at which multicast channel encryption keys are changes, for encrypted multicast transmissions.
Data Types:	INTEGER
Access:	Read-write

4.2.1.8 Enable/Disable Promiscuous Mode

MIB Object:	cbNetPromiscuous
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetPromiscuous(4)
Description:	Enables/disables Promicusous mode. Changes to this parameter will only take effect after system reset.
Data Types:	INTEGER cbEnabled (1) cbDisabled (0)
Access:	Read-write

4.2.1.9 Enable/Disable Unregistered Users

MIB Object:	cbNetUnregisteredUsers
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetUnregisteredUsers(5)
Description:	Enables/disables unregistered users.
Data Types:	INTEGER cbEnabled (1) cbDisabled (0)
Access:	Read-write

4.2.1.10 Enable/Disable Multicast

MIB Object:	cbNetMulticast
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetMulticast(6)
Description:	Enables/disables receives Multicast Packets.
Data Types:	INTEGER cbEnabled (1) cbDisabled (0)
Access:	Read-write

4.2.1.11 Client Information Reset

MIB Object:	cbClientInfoReset
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbClientsInfoReset(9)
Description:	This parameter is applicable only for users that were NOT added by the CCU. It specifies the maximum number of seconds that these users' information (statistics and encryption parameters) will be retained in the Gateway before being discarded. The value for this parameter must be greater than 0.
Data Types:	INTEGER
Access:	Read-write

4.2.1.12 Gateway Description

MIB Object:	cbGatewayDescription
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbGatewayDescription(5)
Description:	A general description of the Gateway. The description may be changes as required.
Data Types:	Display String
Access:	Read-write

4.2.1.13 Software Version

MIB Object:	cbSWVersion
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbSwVersion(6)
Description:	The Gateway application software version.
Data Types:	Display String
Access:	Read-write

4.2.1.14 Application File Name

MIB Object:	cbApplicationFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). CbApplicationFileNumber(7)
Description:	The name of the application file. **Note:** The application file will always reside in the ./psosapp sub-directory. This parameter only refers to the file name.
Data Types:	Display String
Access:	Read-write

4.2.1.15 FPGA File Name

MIB Object:	cbFPGAFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). CbFPGAFileNumber(13)
Description:	A string that specifies the MCS file name loaded on the Gateway's Encoder.

	Changes to parameter will only take effect after system reset.
Data Types:	Display String
Access:	Read-write

4.2.1.16 Time

MIB Object:	cbTime
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2).cbTimeDate(8) cbTime(1)
Description:	A string in the format HH:MM:SS that represents the Gateway's reflection of the current time. Single digits should be preceded by 0; example: 12:35:27; 01:50:00; 09:01:59
Data Types:	Display String
Access:	Read-write

4.2.1.17 Date

MIB Object:	cbDate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2).cbTimeDate(8) cbDate(2)
Description:	A string representing the Gateway's reflection of the current date. In order to set a different date, use the following format: <Full month name><1 or 2 digits of the day of the month>, <4 digits of year> Example: March 31, 2000; April 1, 2000
Data Types:	Display String
Access:	Read-write

4.2.2 Network Interface Configuration Parameters

Network Interface Configuration Parameters consists of the following:

- C&M NIC IP Address

- C&M NIC Subnet Mask
- C&M NIC Default Gateway
- Dual NIC Enable/Disable
- Transportation NIC IP Address
- Transportation NIC Subnet
- Telnet Server Enable/Disable
- FTP Server Enable/Disable

4.2.2.1 C&M NIC IP Address

MIB Object:	cbNetGatewayMngIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). CbNetGatewayMngIP(1)
Description:	The IP address of the Control and Management (C&M) NIC. Changes to this parameter will only effect after system reset.
Data Types:	IP Address
Access:	Read-write

4.2.2.2 C&M NIC Subnet Mask

MIB Object:	cbNetGatewayMngSubnetMask
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetGatewayMngSubnetMast(2)
Description:	The subnet mask of the C&M NIC. Changes to this parameter will only take effect after system reset.
Data Types:	IP Address
Access:	Read-write

4.2.2.3 C&M NIC Default Gateway

MIB Object:	cbNetDefaultGateway
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetDefaultGateway(3)
Description:	The IP address of the default Gateway.
Data Types:	IP Address
Access:	Read-write

4.2.2.4 Dual NIC Enable/Disable

MIB Object:	cbNetDualNIC
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetDualNIC(7)
Description:	Enables/disables the Transportation NIC. Changes to this parameter will only take effect after system reset.
Data Types:	INTEGER cbEnable (1) cbDisable (0)
Access:	Read-write

4.2.2.5 Transportation NIC IP Address

MIB Object:	cbNetGatewayDualIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetGatewayDataIP(8)
Description:	The IP Address of the Transportation NIC.
Data Types:	IP Address
Access:	Read-write

4.2.2.6 Transportation NIC Subnet

MIB Object:	cbNetGatewayData SubnetMask
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetGatewayDataSubnetMask(9)
Description:	The subnet mask of the transportation NIC. Changes to this parameter will only take effect after system reset.
Data Types:	IP Address
Access:	Read-write

4.2.2.7 Telnet Server Enable/Disable

MIB Object:	cbNetTelnet
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetTelnet(10)
Description:	Enables/disables the Telnet server in the Gateway.
Data Types:	INTEGER cbEnable (1) cbDisable (0)
Access:	Read-write

4.2.2.8 FTP Server Enable/Disable

MIB Object:	cbNetFTP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbNetworkParam(1). cbNetFTP(11)
Description:	Enables/disables the FTP server in the Gateway.
Data Types:	INTEGER cbEnable (1) cbDisable (0)
Access:	Read-write

4.2.3 DVB Interface Parameters

DVB Interface Parameters consists of the following:

- Output Bitrate
- PAT Rate
- PMT Rate
- Framing Type
- MPEG Stuffing Mode
- MPE Mode
- CRC Type
- Output Clock Polarity
- Auxiliary Input Control
- Auxiliary Null Packets Control
- Auxiliary Input Type
- LLC SNAP Control
- Data Mapping Mode
- Enable/Disable Flushing

4.2.3.1 Output Bitrate

MIB Object:	cbDVBOutputBitRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBOutputBitRate(1)
Description:	PLL frequency in kbps.
Data Types:	INTEGER
Access:	Read-write

4.2.3.2 PAT Rate

MIB Object:	cbDVBPAT
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBPAT(2)
Description:	PAT rate in tables per seconds
Data Types:	INTEGER
Access:	Read-write

4.2.3.3 PMT Rate

MIB Object:	cbDVBPMT
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBPMT(3)
Description:	PMT rate in tables per seconds
Data Types:	INTEGER
Access:	Read-write

4.2.3.4 Framing Type

MIB Object:	cbDVBFraming
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBFraming(4)
Description:	188/204 framing.
Data Types:	INTEGER
Access:	Read-write

4.2.3.5 MPEG Stuffing Mode

MIB Object:	cbStuffingMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbStuffingMode(5)
Description:	Stuffing mode, either FF stuffing or Adaptation Field stuffing.
Data Types:	INTEGER
Access:	Read-write

4.2.3.6 MPE Mode

MIB Object:	cbMpeMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbMpeMode(6)
Description:	MPE mode, either Packed MPE mode or Not packed MPE mode.
Data Types:	INTEGER
Access:	Read-write

4.2.3.7 CRC Type

MIB Object:	cbCRCMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbCRCMode(7)
Description:	CRC type: Check Sum, CRC or Zero
Data Types:	INTEGER
Access:	Read-write

4.2.3.8 Output Clock Polarity

MIB Object:	cbDVBClockPolarity
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBClockPolarity(8)
Description:	DVB clock polarity
Data Types:	INTEGER
Access:	Read-only

4.2.3.9 Auxiliary Input Control

MIB Object:	cbDVBAuxinput
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBAuxInput(9)
Description:	Specifies whether the auxiliary transport Stream (TS) input is enabled or disabled. If **Enabled**, the output Transport Stream of the Gateway combines the Transport Stream coming from the auxiliary input and the Transport Stream generated by the Gateway. It is the responsibility of the stream architure to ensure that the output bit rate of the Gateway is greater than the sum of the combined Transport Stream rates, example: Transport Stream from the Auxiliary Input + Transport Stream generated by the Gateway > Output Bit Rate The Transport Stream from the auxiliary input has precedence over the transport Stream generated by the Gateway. The Transport Stream generated by the Gateway will be transmitted only in case of free bandwidth, meaning that the output bit rate is higher that the bit rate of the auxiliary input Transport Stream.
Data Types:	INTEGER cbENable (1) cbDisable (0)
Access:	Read-write

4.2.3.10 Auxiliary Null Packets Control

MIB Object:	cbDVBAuxNullPackets
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBAuxNullPackets(10)
Description:	Specifies how the Transport Stream from the Auxiliary Input will be combined with the output Transport Stream. If **Enabled**, the Gateway will replace null packets in the incoming Transport Streams, with Transport Stream packets containing data that were generated by the Gateway. This mode is effective only when Auxiliary Input is enabled. The replacing of the null packets is performed together with the use of free bandwidth. Replacing the null packets with packets containing data enables increased utilization of the bandwidth.
Data Types:	INTEGER cbENable (1) cbDisable (0)
Access:	Read-write

4.2.3.11 Auxiliary Input Type

MIB Object:	cbDVBAuxAuxinputType
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBAuxInputType(11)
Description:	Specifies which physical input of the Gateway will be used as the auxiliary input, either **LVDS** or **ASI**. **Note:** The Gateway is shipped with the ASI physical interface only. If LVDS is desired, a separate order must be made. The Gateway can only use one input at a time.
Data Types:	INTEGER cbASI (1) cbLVDS (0)
Access:	Read-write

4.2.3.12 LLC SNAP Control

MIB Object:	cbDVBAuxLlcSnap
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbDVBOutputParam(2). cbDVBLlcSnap(12)
Description:	Enables/disables the addition of an LLC/SNAP header in MPE mode.
Data Types:	INTEGER cbEnable (1) cbDisable (0)
Access:	Read-write

4.2.3.13 Data Mapping Mode

MIB Object:	cbDataMappingMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). cbDataMappingMode(8)
Description:	Data Broadcast Mode – the mode of encoding data from the network, either Piping, Streaming, or MPE.
Data Types:	INTEGER cbDataPiping(1) cbDataStreaming (2) cbProtocolEncapsulation (3)
Access:	Read-write

4.2.3.14 Enable/Disable Flushing

MIB Object:	cbFlushing
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGeneralParam(3). CbFlushing(11)
Description:	Flushing packets on IDLE.
Data Types:	INTEGER
Access:	Read-write

4.2.4 Multicast Channel Parameters

Multicast parameters consist of the following:

- IP Address of the Multicast Channel
- Group
- SID
- Min Rate
- Max Rate

4.2.4.1 IP Address of the Multicast Channel

MIB Object:	cbMulticastIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigMulticastTable(6). cbMulticastTable(1).cbMulticastEntry(1).cbMulticastIP(1)
Description:	IP address of the multicast channel.
Data Types:	INTEGER
Access:	Read-write

4.2.4.2 Group

MIB Object:	cbMulticastGroup
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigMulticastTable(6). cbMulticastTable(1).cbMulticastEntry(1).cbMulticastGroup(2)
Description:	The group to which the multicast user belongs.
Data Types:	INTEGER
Access:	Read-write

4.2.4.3 SID

MIB Object:	cbMulticastSID
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigMulticastTable(6). cbMulticastTable(1).cbMulticastEntry(1).cbMulticastSID(3)
Description:	The group to which the multicast channel resides.
Data Types:	INTEGER
Access:	Read-write

4.2.4.4 Min Rate

MIB Object:	cbMulticastMinRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigMulticastTable(6). cbMulticastTable(1).cbMulticastEntry(1).cbMulticastMinRate(4)
Description:	The multicast minimum rate (CIR).
Data Types:	INTEGER
Access:	Read-write

4.2.4.5 Max Rate

MIB Object:	cbMulticastMaxRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigMulticastTable(6). cbMulticastTable(1).cbMulticastEntry(1).cbMulticastMaxRate(4)
Description:	The multicast maximum rate.
Data Types:	INTEGER
Access:	Read-write

4.2.5 Group Parameters

A Group is a collection of one or more users (Dynamic, Static, or Multicast). Three parameters can be defined for a group; PID, QoS values, and QoS mode. Group parameters are stored in a Group table in the Gateway (cbGroupsTable).

Group Parameters consists of the following:

- Group Index
- Group PID
- Group QoS Mode (Global or Individual)
- Group Minimum Rate
- Group Maximum Rate

4.2.5.1 Group Index

MIB Object:	cbGRTableIndex
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGroupsTable(4). cbGrTable(1).cbGroupsTableNode(1).cbGrtableIndex(1)
Description:	The group index
Data Types:	INTEGER
Access:	Read-write

4.2.5.2 Group PID

MIB Object:	CbGRTablePID
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGroupsTable(4). cbGrTable(1).cbGroupsTableNode(1).cbGrtablePID(2)
Description:	The PID of this group.
Data Types:	INTEGER
Access:	Read-write

4.2.5.3 Group QoS Mode (Global or Individual)

MIB Object:	CbGRTableQoSMode
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGroupsTable(4). cbGrTable(1).cbGroupsTableNode(1).cbGrtableQoSMode(3)
Description:	The group QoS mode (Global or Individual).
Data Types:	INTEGER
Access:	Read-write

4.2.5.4 Group Minimum Rate

MIB Object:	CbGRTableMinRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGroupsTable(4). cbGrTable(1).cbGroupsTableNode(1).cbGrtableMinRate(4)
Description:	The multicast minimum rate (CIR). This parameter is only relevant if QoSMode ≈ Global
Data Types:	INTEGER
Access:	Read-write

4.2.5.5 Group Maximum Rate

MIB Object:	CbGRTableMaxRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbGroupsTable(4). cbGrTable(1).cbGroupsTableNode(1).cbGrtableMaxRate(5)
Description:	The multicast maximum rate. This parameter is only relevant if QoSMode ≈ Global
Data Types:	INTEGER
Access:	Read-write

4.2.5.6 Procedure for Adding a New Group

Note: This procedure provides the basics for adding a new group.

Set:	1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbGroupsTable(1).cbGrTable(1).cbGroupsTableNode(1).cbGrTableIndex
to:	cbGrTableIndex Where: cbGRTableIndex is the index number of the new group. Set: cbGrTablePID, cbGrTableQoSMode, cbGrTableMinRate, and cbGrTableMaxRate to the desired values, as follows: cbGrTablePID = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbGroupsTable(1).cbGrTable(1).cbGroupsTableNode(2).cbGrTableIndex
	cbGrTableQoSMode = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbGroupsTable(1).cbGrTable(1).cbGroupsTableNode(3).cbGrTableIndex
	cbGrTableMinRate = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbgroupsTable(1).cbGrTable(1).cbGroupsTableNode(4).cbGrTableIndex
	CbGrTableMaxRate = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbgroupsTable(1).cbGrTable(1).cbGroupsTableNode(5).cbGrTableIndex

To delete a group, proceed as follows:

Set:	1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(4). cbgroupsTable(1).cbGrTable(1).cbGroupsTableNode(5).cbGrTableIndex
to:	0

4.2.6 Static Users Parameters

A static user is a definition of a valid host in the system. When a static user is created, the Gateway permits traffic to a specific static host. Parameters for specific static users can be defined in the Gateway via SNMP. When defining parameters for static users, the user defines the host IP address, MAC address, and Group number (PID).

Static users parameters are stored in a static user table in the Gateway (cbConfigSTU-Table). The index of the table is the static user's IP Address. Static users can be enabled or disabled by SNMP commands. Each static user may be defined to work with a specified group, and with a specified PIB.

Static Users Parameters consists of the following:

- Static User IP Address
- Subnet Mask
- Group
- MAC
- Minimum Rate
- Maximum Rate

4.2.6.1 Static User IP Address

MIB Object:	cbStaticUserIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry (1).cbStaticUserIP(1)
Description:	IP address of the static user.
Data Types:	IP address
Access:	Read-write

4.2.6.2 Subnet Mask

MIB Object:	cbStaticUserMask
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry (1).cbStaticUserMask(2)
Description:	If the user is a network, this parameter defines, together with the IP address, the network's address. If the user is not a network, the subnet mask should be: 255.255.255.255
Data Types:	INTEGER
Access:	Read-write

4.2.6.3 Group

MIB Object:	cbStaticUserGroup
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry (1).cbStaticUserGroup(3)
Description:	Specifies the group to which the static user belongs.
Data Types:	INTEGER
Access:	Read-write

4.2.6.4 MAC

MIB Object:	cbStaticUserMAC
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry (1).cbStaticUserMAC(4)
Description:	Specifies the physical address of the user's machine.
Data Types:	PhysAddress
Access:	Read-write

4.2.6.5 Minimum Rate

MIB Object:	cbStaticUserMinRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry (1).cbStaticUserMinRate(5)
Description:	A QoS parameter that specifies the minimum bandwidth allocated for the static user.
Data Types:	INTEGER
Access:	Read-write

4.2.6.6 Maximum Rate

MIB Object:	cbStaticUserMaxRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigSTUTable(5). cbStaticUserTable(1).cbStaticUserEntry(1).cbStaticUserMaxRate(6)
Description:	A QoS parameter that specifies the maximum bandwidth allocated for the static user.
Data Types:	INTEGER
Access:	Read-write

4.2.6.7 Procedure for Adding a New Static User

Note: This procedure provides the basics for adding a new static user.

Set:	1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(1).cbStaticUserIP
to:	cbStaticUserIP Where: cbStaticUserIP is the IP address of the new static user. Set: cbStaticUserMask, cbStaticUserGroup, cbStaticUserMAC, and cbStaticUserMinRateRate and cbStaticUserMaxRate to the desired values, as follows: cbStaticUserMask = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(2).cbStaticUserIP **Note:** For this parameter, use 255.255.255.255 if static user is not a network.
	cbStaticUserGroup = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(3).cbStaticUserIP **Note:** Be careful to first create the desired group, if using more than one group (and more than 12 PIDs).
	cbStaticUserMAC = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(4).cbStaticUserIP
	cbStaticUserMinRate = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(5).cbStaticUserIP
	cbStaticUserMaxRate = 1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(6).cbStaticUserIP

To delete a group, proceed as follows:

Set:	1.3.6.1.4.1.enterprises(2540).efdata(6247).spectracast(3).DTMX5000(1).cbConfig(5). cbConfigSTUTable(1).cbStaticUserTable(1).cbStaticUserEntry(1).cbStaticUserIP
to:	0.0.0.0

4.2.7 CCU Parameters

Note: CCU parameters communicate with the Gateway.

CCU Parameters consists of the following:

- CCU 1 Address
- CCU 2 Address
- CCU 3 Address
- CCU 4 Address
- CCU 5 Address
- CCU 6 Address
- CCU 7 Address
- CCU 8 Address
- CCU 9 Address
- CCU 10 Address

4.2.7.1 CCU 1 Address

MIB Object:	cbCCU1
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). CbCCU1(1)
Description:	IP address of CCU #1
Data Types:	IP address
Access:	Read-write

4.2.7.2 CCU 2 Address

MIB Object:	cbCCU2
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU2(2)
Description:	IP address of CCU #2
Data Types:	IP address
Access:	Read-write

4.2.7.3 CCU 3 Address

MIB Object:	cbCCU3
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU3(3)
Description:	IP address of CCU #3
Data Types:	IP address
Access:	Read-write

4.2.7.4 CCU 4 Address

MIB Object:	cbCCU4
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU4(4)
Description:	IP address of CCU #4
Data Types:	IP address
Access:	Read-write

4.2.7.5 CCU 5 Address

MIB Object:	cbCCU5
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU5(5)
Description:	IP address of CCU #5
Data Types:	IP address
Access:	Read-write

4.2.7.6 CCU 6 Address

MIB Object:	cbCCU6
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU6(6)
Description:	IP address of CCU #6
Data Types:	IP address
Access:	Read-write

4.2.7.7 CCU 7 Address

MIB Object:	cbCCU7
OID:	Iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU7(7)
Description:	IP address of CCU #7
Data Types:	IP address
Access:	Read-write

4.2.7.8 CCU 8 Address

MIB Object:	CbCCU8
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU8(8)
Description:	IP address of CCU #8
Data Types:	IP address
Access:	Read-write

4.2.7.9 CCU 9 Address

MIB Object:	cbCCU9
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU9(9)
Description:	IP address of CCU #9
Data Types:	IP address
Access:	Read-write

4.2.7.10 CCU 10 Address

MIB Object:	cbCCU10
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbCCUParame(10). cbCCU10
Description:	IP address of CCU #10
Data Types:	IP address
Access:	Read-write

4.2.8 Software Download Parameters

Note: Software download parameters relate to the remote upgrades of the Gateway's software and firmware.

Software Download Parameters consists of the following:

- Server IP Address
- Application File Name on the Server
- Application File Name on the Gateway
- Software Download Start Command
- Software Download Status
- Firmware Filename on the Server
- Firmware Filename on the Gateway
- Firmware Download Start Command
- Firmware Download Status

4.2.8.1 Server IP Address

MIB Object:	cbSWServerIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbSWServerIP(1)
Description:	The IP address of the TFTP server from which the software file will be TFTPed. Use 0.0.0.0. to load a different local file (without TFTP).
Data Types:	IP address
Access:	Read-write

4.2.8.2 Application File Name on the Server

MIB Object:	cbSWSourceFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbAppDownload(2).cbSWSourceFileName(1)
Description:	The software file name and its optional path (relative to the TFTP server root definition) to be downloaded from the server. Example: catvgw.dat
Data Types:	String
Access:	Read-write

4.2.8.3 Application File Name on the Gateway

MIB Object:	cbSWTargetFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbAppDownload(2).cbSWTargetFileName(2)
Description:	The software file name (without path) on the Gateway. Example: ram.abs
Data Types:	String
Access:	Read-write

cbApplicationFileName (under cbGeneralParam) is the name of the running software file. If cbSWTargetFileName is different from cbApplicationFileName, it will only be downloaded to the Gateway but will not be used until cbApplicationFileName is changed (in CFG.INI) to be the same as cbSWTargetFileName.

Example: catvgw.dat

4.2.8.4 Software Download Start Command

MIB Object:	cbSWDownloadStart
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbAppDownload(2).cbSWDownloadStart(3)
Description:	Set cbSWDownloadStart to cbTrue in order to start the software download process. Set cbSWDownloadStart to cbFalse to interrupt (and stop) the software download in progress (when cbSWDownloadStatus = cbDownloadInProgress). Example: catvgw.dat
Data Types:	INTEGER
Access:	Write-only

4.2.8.5 Software Download Start Command

MIB Object:	cbSWDownloadStatus
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbAppDownload(2).cbSWDownloadStatus(4)
Description:	Status of the software download: **cbldle:** Download has not started yet or has finished and the Gateway has already restarted with the new version (not an error). **cbDownloadInProgress:** Download is currently in progress (not an error). **cbERRORTFTPServernotFound:** Cannot find a TFTP server at the specified IP Address – check and correct cbSWServerIP. **cbERRORFileNotFound:** Cannot find the specified file – check and correct cbSWFileName. **cbERRORNotaSWFile:** The specified file is not a software file – check and correct cbSWFileName. **cbERRORBadChecksum:** Bad checksum – Repeat download. **cbERRORCommunicationFailed:** Communication with the server failed – Repeat download. **cbDownloadAborted:** the SNMP manager aborted Download (cbSWDownloadStart was set to cbFalse during download). Example: catvgw.dat
Data Types:	INTEGER
Access:	Read-only

4.2.8.6 Firmware Filename on the Server

MIB Object:	cbFPGASourceFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbFPGADownload(3).cbFPGASourceFileName(1)
Description:	The FPGA file name and its optional path (relative to the TFTP server root definition) to be downloaded from the server. Example: FPGA.MCS
Data Types:	String
Access:	Read-write

4.2.8.7 Firmware Filename on the Gateway

MIB Object:	cbFPGATargetFileName
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbFPGADownload(3).cbFPGATargetFileName(1)
Description:	The FPGA file name (without path) on the Gateway. Example: FPGA.DAT
Data Types:	String
Access:	Read-write

4.2.8.8 Firmware Download Start Command

MIB Object:	cbFPGADownloadStart
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbFPGADownload(3).cbFPGADownloadStart(3)
Description:	Set cbFPGADownloadStart to cbTrue in order to start the FPGA download process. Set cbFPGADownloadStart to cbFalse to interrupt (and stop) FPGA download in progress (when cbFPGADownloadStatus = cbDownloadInProcess).
Data Types:	INTEGER
Access:	Read-only

4.2.8.9 Firmware Download Status

MIB Object:	cbFPGADownloadStatus
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbSWDownload(4). cbFPGADownload(3).cbFPGADownloadStatus(4)
Description:	Status of the FPGA download: **cbldle:** Download has not started yet or has finished and the Gateway has already restarted with the new version (not an error). **cbDownloadInProgress:** Download is currently in progress (not an error). **cbERRORTFTPServernotFound:** Cannot find a TFTP server at the specified IP Address – check and correct cbSWServerIP. **cbERRORFileNotFound:** Cannot find the specified file – check and correct cbFPGAFileName. **cbERRORNotaSWFile:** The specified file is not a software file – check and correct cbFPGAFileName. **cbERRORBadChecksum:** Bad checksum – Repeat download. **cbERRORCommunicationFailed:** Communication with the server failed – Repeat download. **cbDownloadAborted:** the SNMP manager aborted Download (cbFPGADownloadStart was set to cbFalse during download).
Data Types:	INTEGER
Access:	Read-only

4.2.9 General Statistics Parameters

Diagnostics Parameters consists of the following:

- Number of Transmitted Bytes
- Number of Transmitted Packets
- Average Packet Size
- Average Bytes per Second
- Number of Packets Discarded
- Number of Received NMS Packets
- CPU Load
- Memory Usage
- Reset General Statistics
- Number of Current Connected Clients

4.2.9.1 Number of Transmitted Bytes

MIB Object:	cbStatNumBytesTxed
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatNumBytesTxed(1)
Description:	Number of Bytes transmitted since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.2 Number of Transmitted Packets

MIB Object:	cbStatNumOfPackets
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatNumOfPackets(2)
Description:	Number of IP packets transmitted since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.3 Average Packet Size

MIB Object:	cbStatAvrPktSize
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatAvrPktSize(3)
Description:	Number of Average packet size since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.4 Average Bytes per Second

MIB Object:	cbStatBytesPerSec
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatAvrBytesPerSec(4)
Description:	Average speed in bytes per second since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.5 Number of Packets Discarded

MIB Object:	cbStatNumPacketDiscarded
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatNumPacketDiscarded(5)
Description:	Number of data packets that were discarded since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.6 Number of Received NMS Packets

MIB Object:	cbStatNumNMSFrames
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatNumNMSFrames(6)
Description:	Number of NMS packets received since the last statistics reset.
Data Types:	Counter
Access:	Read-only

4.2.9.7 CPU Load

MIB Object:	cbCPULoad
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbCPULoad(7)
Description:	Current CPU load as a percentage (0-100)
Data Types:	Counter
Access:	Read-only

4.2.9.8 Memory Usage

MIB Object:	cbMemoryUsage
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbMemoryUsage(8)ff
Description:	Current memory usage as a percentage (0-100)
Data Types:	Counter
Access:	Read-only

4.2.9.9 Reset General Statistics

MIB Object:	cbStatReset
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatReset(9)
Description:	Set to cbTrue in order to reset the general statistics values.
Data Types:	INTEGER
Access:	Write-only

4.2.9.10 Number of Current Connected Clients

MIB Object:	cbStatNumClients
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(1).cbStatNumClients(10)
Description:	Number of clients currently connected to the Gateway. This parameter is not affected by cbStatReset.
Data Types:	Counter
Access:	Read-only

4.2.10 Client Data Flow Statistics Table

The data flow statistics information is stored in the Gateway in a table containing the following columns:

- Client IP address.
- Time stamp of the packet sent to the client.
- Start time stamp.
- Total IP packets sent to the client.
- Average byte per second sent to the client in the last second.
- Number of packets for the client that were discarded.
- Total kbytes transmitted to the client.

Note: The index of the Table (its first column) is the client IP address.

Each information object can be accessed by means of two methods:

By row (single client method)	The information is retrieved for a client whose IP address is a set in the **cbClientIP** object. Each **NEXT** command will retrieve the next statistics object for the client.
By Column (table method)	The information is retrieved by information type. Each **NEXT** command will retrieve the information object of the next client. This identifies the first parameter as the client's IP address, then the stamp, and so on.

4.2.10.1 Data Flow Statistics Single Client Method

Data Flow Statistics Single Client Method consists of the following:

- Client IP Address
- Client Connection Time
- Kbytes Transmitted to the Client
- Number of Packets Transmitted to the Client
- Average Speed of Transmission to the Client
- Number of Packets Transmitted to the Client that were Discarded
- Reset Statistics Value for the Client
- Encryption Enable/Disable

4.2.10.1.1 Client IP Address

MIB Object:	cbClientIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatGeneral(2).cbClientIP(1)
Description:	IP address of the client. The rest of the parameters in this table refer to this IP address.
Data Types:	IP Address
Access:	Read-write

4.2.10.1.2 Client Connection Time

MIB Object:	cbCINumSeconds
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatClient(2).cbClientStatistics(2).cbCINumSeconds(1)
Description:	The number of seconds since the client statistics became active. The statistics values are reset automatically by the Gateway (as well as by setting cbCIReset), according to the value of cbFreqClientInfoReset.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.3 Kbytes Transmitted to the Client

MIB Object:	cbCINumKBytes
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCINumKBytes(2)
Description:	Number of bytes transmitted to IP == cbClientIP in the last cbCINumSeconds seconds.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.4 Number of Packet Transmitted to the Client

MIB Object:	cbCINumPackets
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCINumPackets(3)
Description:	Number of packets transmitted to IP == cbClientIP in the last cbCI-NumSeconds seconds.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.5 Average Speed of Transmission to the Client

MIB Object:	cbCIAvrBytesPerSecond
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCIAvrBytesPerSeonds(4)
Description:	Average transfer rate in bytes per seconds for this client.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.6 Number of Packets Transmitted to the Client that were Discarded

MIB Object:	cbCINumPacketsDiscarded
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCINumPacketsDiscarded(5)
Description:	Number of packets transmitted to IP == cbClientIP that were discarded in the last cbCINumSeconds seconds.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.7 Reset Statistics Value for the Client

MIB Object:	cbCIStatReset
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCIStatReset(6)
Description:	Set to non-zero in order to reset the statistics values for the client cbClientIP.
Data Types:	INTEGER
Access:	Read-only

4.2.10.1.8 Encryption Enable/Disable

MIB Object:	cbCIEncrEnbled
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatClient(2).cbClientStatistics(2).cbCIEncrEnbled(7)
Description:	If this variable is True, then encryption is enabled for this client. This value may not be changes and it is NOT changes by cbCIStatReset.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2 Data Flow Statistics – Table Method

The Data Flow Statistics – Table Method consists of the following:

-
- IP Address of the Client
- Client's Stamp Time
- Client's Start Time
- Total Packets Transmitted to the Client
- Transmission Rate to the Client
- Number of Discarded Packets
- Kbytes Transmitted to the Client
- Reset Statistics Values for the Client

4.2.10.2.1 IP Address of the Client

MIB Object:	cbCITableIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbSatCITable(3).cbCITable(1).cbCITableNode(1).cbCITableIP(1)
Description:	IP address to the client.
Data Types:	IP Address
Access:	Read-only

4.2.10.2.2 Client's Stamp Time

MIB Object:	cbCITableStampTime
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITableStampTime(2)
Description:	Length of time (in seconds) since a packet was last transmitted to the client.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2.3 Total Packets Transmitted to the Client

MIB Object:	cbCITableTotalPackets
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITableTotalPackets(4)
Description:	Total number of packets that have been transmitted to the client in this session.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2.4 Transmission Rate to the Client

MIB Object:	cbCITableBytesinSec
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITableBytesinSec(5)
Description:	Throughout (in bytes per second) transmitted to the client.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2.5 Number of Discarded Packets

MIB Object:	cbCITableKBytesTxed
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITablePacketsDiscr(6)
Description:	Total number of packets intended for the client that were discarded by the Gateway.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2.6 Kbytes Transmitted to the Client

MIB Object:	cbCITableKBytesTxed
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITableKBytesTxed(7)
Description:	Total kbytes transmitted to the client.
Data Types:	INTEGER
Access:	Read-only

4.2.10.2.7 Reset Statistics Values for the Client

MIB Object:	cbCITableReset
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbStatistics(1). cbStatCITable(3).cbCITable(1).cbCITableNode(1). cbCITableReset(8)
Description:	Resets the clients statistics.
Data Types:	INTEGER
Access:	Read-only

4.2.11 Client Configuration Parameters Table

The client configuration parameters table is read-only. Client configuration information is kept in the Gateway in a table containing the following columns:

- Client IP address.
- Client subnet mask.
- Client MAC address.
- Group
- How the client as added to the Gateway (MCT, STU, or CCU).
- Minimum rate
- Maximum rate
- Encryption

Note: The index of the Table (its first column) is the client IP address.

The client configuration information can only be accessed by the table method (columns only).

4.2.11.1 Client IP Address

MIB Object:	cbCfgCITableIP
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableIP(1)
Description:	IP address of the client.
Data Types:	IP Address
Access:	Read-only

4.2.11.2 Subnet Mask

MIB Object:	cbCfgCITableMask
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableMask(2)
Description:	If the user is a network, this parameter defines (together with the IP Address) the network's address. If the user is not a network, the subnet mask should be: 255.255.255.255
Data Types:	INTEGER
Access:	Read-only

4.2.11.3 Group

MIB Object:	cbCfgCITableGroup
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableGroup(4)
Description:	Specifies the group to which the client belongs.
Data Types:	INTEGER
Access:	Read-only

4.2.11.4 How the Client was Added to the Gateway

MIB Object:	cbCfgCITableBy
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableBy(5)
Description:	CCU user (in promiscuous mode), STU (static user), MCT (multicast user)
Data Types:	String
Access:	Read-only

4.2.11.5 Minimum Rate

MIB Object:	cbCfgCITableMinRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableMinRate(6)
Description:	A QoS parameter that specifies the minimum bandwidth allocated for the client.
Data Types:	INTEGER
Access:	Read-only

4.2.11.6 Maximum Rate

MIB Object:	cbCfgCITableMaxRate
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableMaxRate(7)
Description:	A QoS parameter that specifies the maximum bandwidth allocated for the client.
Data Types:	INTEGER
Access:	Read-only

4.2.11.7 Encryption

MIB Object:	cbCfgCITableEncrypt
OID:	iso(1).org(3).dod(6).internet(1).private(4).enterprises(1). efdata(6247).spectracast(3).DTMX5000(1).cbConfig(2). cbConfigCITable(7).cbCfgCITable(1).cbCITableNode(1). cbCfgCITableEncrypt(8)
Description:	Specifies whether or not data transmitted to the client is encrypted.
Data Types:	INTEGER
Access:	Read-only

This page intentionally left blank

Chapter 5. TROUBLESHOOTING

This chapter is intended to assist the user in troubleshooting the installation phase or during ongoing maintenance of the Gateway.

5.1 Troubleshooting

The following is provided as a troubleshooting guide:

- The Gateway Does Not Power Up
- No Communication between the Gateway and the Local Terminal
- The Gateway Does Not Reply to Ping from the Control and Maintenance Interface
- The Gateway Does Not Reply to Ping from the Transportation Interface
- Gateway Statistics Tables Indicate that there is No Data Flow to Users
- The Gateway Does Not Reply to Telnet/FTP Users
- No Telnet/FTP/SNMP Communication from Outside the LAN
- The Gateway Does Not Reply to SNMP Set or Get Commands
- The Modulator Cannot Synchronize with the Transport Stream (TS) Generated by the Gateway
- The CCU Does Not Communicate with the Gateway
- The Gateway's Output is Connected to a DVB Multiplexer's Input but the DVB Multiplexer Indicates that there is No TS Input
- MPE Compatible Receivers Cannot Receive IP Data from the Gateway

5.1.1 The Gateway Does Not Power Up

Possible Cause	Solution
The power cord is loose, faulty or not connected to the Gateway.	Check that the power cord is properly connected to the Gateway and the power outlet.
Power outlet is faulty.	Check outlet or utilize another outlet.
If problem remains, the Gateway may be faulty	Contact EFData Customer Support department.

5.1.2 No Communication Between the Gateway and the Local Terminal

Possible Cause	Solution
Faulty terminal cable.	Use a continuity test to verify the terminal cable functioning. Pins 2 and 3 should be crossed and Pin 5 should be connected between both sides. If OK, utilize a different cable.
Incorrect terminal settings.	Check terminal settings and change if necessary.

5.1.3 The Gateway Does Not Reply to Ping from the Control and Management Interface

Possible Cause	Solution
Incorrect IP address setting for the Control and Management interface.	Check the IP address setting and change if necessary.
Incorrect Ethernet cable connection.	Ensure that the Control and Management NIC cable is connected to the correct Ethernet port.

5.1.4 The Gateway Does Not Reply to Ping from the Transportation Interface

Possible Cause	Solution
This is normal before connecting the Transportation NIC.	

5.1.5 Gateway Statistics Tables Indicate that there is No Data Flow to Users

Possible Cause	Solution
Incorrect Transportation NIC IP address setting.	Check that the transportation NIC IP address is correctly specified and change if necessary.
The Transportation NIC is disabled.	Enable the transportation NIC.
The Transportation NIC is not connected to the network.	Check the connection between the server and the Transportation NIC by using Ping and ARP.

5.1.6 The Gateway Does Not Reply to Telnet/FTP Users

Possible Cause	Solution
The Gateway is not connected to the network.	Ping the Control and Management interface. If no reply, refer to "The Gateway Does Not Reply to Ping from the Control and Management Interface."
Telnet/FTP service is disabled.	Enable Telnet/FTP servers.
No Telnet/FTP users are defined.	Check that there are users in the Telnet.FTP users list and define users if necessary.

5.1.7 No Telnet/FTP/SNMP Communication from Outside the LAN

Possible Cause	Solution
Incorrect default Gateway settings.	Check the default Gateway settings and change if necessary.

5.1.8 The Gateway Does Not Reply to SNMP Set or Get Commands

Possible Cause	Solution
Incorrect community string settings.	Check the community string setting and change if necessary.

5.1.9 The Modulator Cannot Synchronize with the Transport Stream (TS) Generated by the Gateway

Possible Cause	Solution
Incorrect framing settings.	Check the framing settings and change if necessary.
Faulty LVDS/ASI cable.	Check the cables connecting the Gateway to the modulator and replace if necessary.
The Gateway output bit rate is not set according to the modulator input bit rate.	Check the Gateway output bit rate and change if necessary.
Incorrect clock polarity (if using LVDS interface).	Check the clock polarity setting and change if necessary.
Faulty modulator.	Replace modulator.
The Gateway output (either ASI or LVDS) may not be functioning properly.	Replace modulators with the alternate input type (either ASI or LVDS).
Unsuccessful encoder card programming.	Connect a monitor to the Gateway's VGA output and verify that the FPGA was programmed.
Faulty Gateway.	Contact EFData Customer Support department.

5.1.10 The CCU Does Not Communicate with the Gateway

Possible Cause	Solution
The CCU is not defined.	Check that the CCU's IP address appears in the CCU list.
No network connection between the CCU and the Gateway.	Ping from the CCU to the Gateway. If no reply, refer to "The Gateway Does Not Reply to Ping from the Control and Management Interface."

5.1.11 The Gateway's Output is Connected to a DVB Multiplexer's Input but the DVB Multiplexer Indicates that there is NO TS Input.

Possible Cause	Solution
The Gateway is not generating PAT/PMT tables.	Ensure that the PAT/PMT rate parameters are not set to zero.
The Gateway is not generating TS.	Refer to "The Modulator Cannot Synchronize with the Transport Stream (TS) Generated by the Gateway."
The DVB multiplexer input is disabled.	Check the DVB multiplexer settings.

5.1.12 MPE Compatible Receivers Cannot Receive IP Data from the Gateway

Possible Cause	Solution
The Gateway is set to Streaming mode.	Ensure that the Gateway is set to MPE mode.
The receiver does not support MPE packed mode.	Check the MPE Mode and change if necessary.

5.2 Ongoing Maintenance

Issue that may be encountered during the daily functioning of the Gateway, such as:

- A User Indicates RF Lock but Cannot Receive Data
- The Gateway Statistics Indicate a Large Number of Discarded Packets
- The Gateway Does Not Reply to Telnet but Does Reply to SNMP and Terminal Communication
- A User Cannot Receive Multicast Channels or Loses Multicast Packets
- A PC Connected to a LAN Fed by a Satellite Receiver (Static User) Does Not Receiver Unicast Transmissions
- The CCU Cannot Register a User in the Gateway

5.2.1 A User Indicates RF Lock but Cannot Receive Data

Possible Cause	Solution
The user is not registered in the Gateway's routing table.	Check that the user appears in the Gateway's routing table.
Incorrect Group settings.	Check that the user's Group setting is correct and change if necessary.
Incorrect Group PID settings.	Check the Group's PID setting and change if necessary.
No data is being sent to the user.	Check the user statistics table to verify that the Gateway is transmitting data.
The receiver does not provide full MPE support.	Check the LLC-SNAP parameters and change if necessary.

5.2.2 The Gateway Statistics indicate a Large Number of Discarded Packets

Possible Cause	Solution
The Gateway's output bit rate is too low.	Check the output bit rate and change if necessary.
If QoS is activated, TCP protocol will increase the output bit rate until packets are discarded. This is normal for TCP connections.	

5.2.3 The Gateway Does Not Reply to Telnet but Does Reply to SNMP and Terminal Communication

Possible Cause	Solution
High CPU Load. This situation can occur when the Gateway is highly loaded – high bit rate with small IP packets.	Use SNMP to check the CPU load.

5.2.4 A User Cannot Receive Multicast Channels or Loses Multicast Packets

Possible Cause	Solution
Multicast is disabled or the Multicast channel is not registered.	Check that Multicast is enabled and that the specific Multicast Channel is registered.
QoS maximum bit rate is too low.	Check QoS parameters for Multicast channel. If Multicast is enabled, then the Gateway assigns the maximum bit rate of 2 Mbit/s for each. If the user consumes more, packets will be lost.

5.2.5 A PC Connected to a LAN Fed by a Satellite Receiver (Static User) Does Not Receive Unicast Transmissions

Possible Cause	Solution
The receiver is not functioning.	Check whether other PCs on the LAN can RX Unicast. Check the status reported of the receiver.
No network connection between the LAN and the satellite receiver machine.	Check the local LAN connections by pinging from the client to the receiver.
Incorrect static user settings.	Check that the static user settings are set to unicast rather than Multicast and change if necessary. In the Static user definition ensure that the PC is in the subnet.

5.2.6 The CCU Cannot Register a User in the Gateway

Possible Cause	Solution
The user is already registered as a Static User.	Check the users table to ensure that the user is not registered as a Static User.

Appendix A. SPECIFICATIONS

This appendix includes the Gateway specifications, external connections, and pin assignments.

A.1 Overview

This appendix includes the specification of the Gateway, external connections, and pin assignments.

A.2 Specifications

Refer to Table A-1 for Gateway specifications.

Table A-1. Gateway Specification

Parameters	Specifications
Accounting	Per IP, Bytes and packets reporting
CE	Safety – EN60950 Emissions – EN55022 Class A Susceptibility – EN50082-1 (1997)
Chassis	19-inch (48.26 cm) rack mountable, 4U height
CPU	Intel Pentium 3™ (450 MHz)
Craft Interface	Interface: Serial EIA-232 Baud Rate: 9600 Information Bit/s: 8 Parity: None Stop Bit/s: 1 Compatible: VT100 Terminal Application: Telnet
Encryption	DES based 56 bit keys
FCC	Standard 47, CFR Part 15, Subpart B
Format	DVB/MPEG2 Transport Stream
Input Interface	Transportation input –10/100 BaseT (auto-detect) Control and Management Input – 10/100 BaseT (auto-detect)
IP Table size	Up to 10,000 IPs for unicast or multicast streams
Mapping	EN 301 192 Data Streaming Multiprotocol Encapsulation (MPE)
Monitor and Control	SNMP based through LAN interface
Monitoring Features	Elaborate statistics, Memory, CPU and total bandwidth usage
Multicast Authorization	DES scrambling based – 56 bit
Number of PIDs	8192
Number of Users	10,000 maximum
Operating System	Real time operating system – PSOS
Output Interface	Parallel LVDS and Serial ASI (Simultaneously)
Power	65 to 250 VAC, 50 to 60 Hz, < 200W
Protocols	IP for Unicast and Multicast
QoS	Settings per IP address or groups, unlimited levels: Permissive or Restrictive modes
Software Upgrades	TFTP Based, to hard drive
Temperature: Operating Storage	 0 to +45°C (32 to 113°F) Humidity 10% to 80% –20 to –70°C (–4 to –94°F) Humidity 10% to 90%
Transfer Rate	See Figure A-1.
Weight	15 kg (7 lbs)

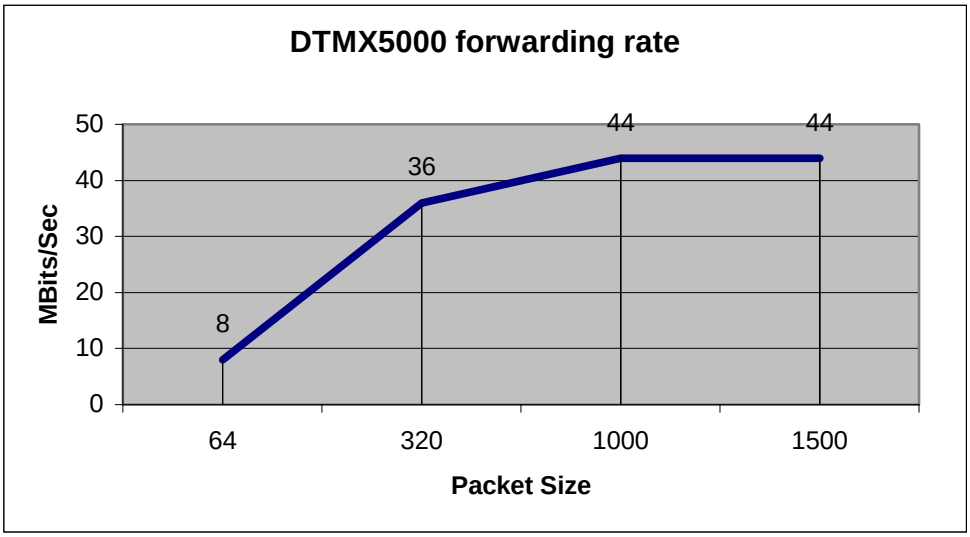


Figure A-1. Forwarding Rate as a Function of Packet Size

A.3 External Connections

Refer to Figure A-2 for a view of the back panel of the Gateway depicting the various connection sockets.

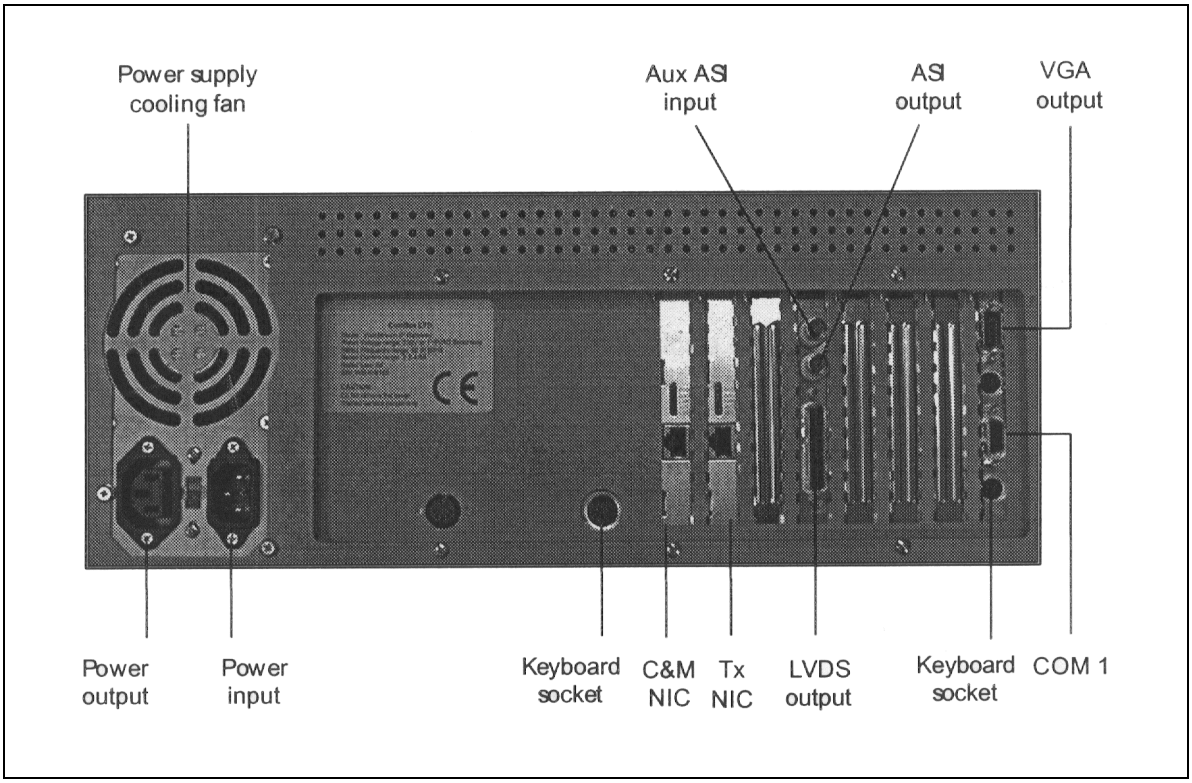


Figure A-2. External Connections

110/220V Power Socket	Connects the Gateway to a power outlet. Verify the 110/220V setting of the power supply.
Keyboard Socket	Connects the Gateway to an optional keyboard.
DVB LVDS	This D-type 25-pin female connector outputs the transport stream as an LVDS format.
AUX ASI Input	[Asynchronous Serial Interface (ASI)] This coaxial connector can be used for combining the external Transport Stream.
ASI Output	This outputs the Transport Stream on an asynchronous serial interface.
Control and Management (C&M) 10/100 BaseT Input NIC	J45 interface to the C&M LAN
Transportation (TX) 10/100BaseT Input NIC	J45 interface to the Transportation LAN.
VGA Output	Connects to the VGA display. To view the startup sequence, an optional VGA display also can be connected to the Gateway.
COM1	Connects directly to the local terminal through an RS232 serial cable. The DTMX5000 IP Gateway must be connected to a local terminal in order to perform various configuration procedures.

A.4 Parallel Output Pin Assignment

Table A-2 provides pin assignments for the Gateway's DB25 output connector.

Table A-2. Parallel Output Pin Assignment

PIN Number	Pin Name	Type	Description
1	Clock A	Output	Output clock signal
2	GND	Output	
3	Data 7A	Output	
4	Data 6A	Output	
5	Data 5A	Output	
6	Data 4A	Output	
7	Data 3A	Output	
8	Data 2A	Output	
9	Data 1A	Output	
10	Data 0A	Output	
11	DVALID A	Output	Data valid signal A
12	SYNC A	Output	SYNC signal A
13	Cable Shield	Output	
14	Clock B	Output	Output clock signal
15	Board GND	Output	
16	Data 7B	Output	
17	Data 6B	Output	
18	Data 5B	Output	
19	Data 4B	Output	
20	Data 3B	Output	
21	Data 2B	Output	
22	Data 1B	Output	
23	Data 0B	Output	
24	DVALID B	Output	Data valid signal B
25	SYNC B	Output	SYNC signal B

Note: All signals are outputs. The Gateway generates clock signals.

This page is intentionally left blank.

APPENDIX B. CENTRAL CONFIGURATION UNIT

This appendix describes the Central Configuration Unit (CCU) is the access and configuration controller for clients. This appendix provides an overview of the CCU's central role, starting when a subscriber logs on and starts a session, through the request and receipt of information, and ending with the termination of the session.

B.1 Overview

The CCU runs on a Windows NT workstation, which is located at the hub. The CCU is responsible for the following activities:

- Authentication of clients (with the help of an external authentication system – a RADIUS Authentication Server).
- Automatic parameter configuration of the modem at the client's PC.
- Dynamic routing of clients' packets towards the Gateway, at the hub.
- Transferal of clients' activity statistics from the Gateway to the RADIUS Billing Server.
- Load-balancing, to distribute clients evenly among Gateways.
- Quality of Service (QoS) allocation. Quality of Service determines how much bandwidth share each subscriber receives. The specific information about the Quality of Service that each subscriber is entitled to receive comes from the external authentication system (a RADIUS Authentication Server).

B.2 DTMX5000 Service

The DTMX5000 service is incremental, meaning that it enhances the downloading speed of a subscriber's existing standard Internet connection. This existing connection can be any standard connection, for example, a simple dial-up account, an ISDN connection, or a frame-relay service.

The DTMX5000 service makes use of the subscriber's existing Internet connection, and enhances the bandwidth of the downstream traffic (meaning traffic coming from the internet to the client). The upstream bandwidth is not changed, but due to the asymmetrical nature of typical Internet access (downstream traffic requires far more bandwidth than upstream traffic), overall web access becomes much faster.

Figure 1-2 illustrates the interaction between the elements of the DTMX5000 system.

The stages involved between starting and terminating a session are described in detail on the subsequent pages.

B.3 Starting a Session

The client's existing Internet connection should already be active, prior to activating the DTMX5000 client application. For example, if the subscriber's existing Internet connection is through a dial-up modem, the dial-up connection should be activated before the DTMX5000 client application is initiated.

After the client's standard internet connection has been activated, the client should run the DTMX5000 client application, which initiates a fast Internet session with the DTMX5000 service.

B.3.1 DTMX5000 Client Application Contacts CCU

When the DTMX5000 client application is activated, it contacts the CCU using the subscriber's existing Internet connection. A brief bi-directional exchange occurs, in which the DTMX5000 client application relays the following parameters to the CCU:

User Name	Informs the CCU of the subscriber's unique user name.
Encrypted Password	Enables the Authentication Server to confirm the identity of the subscriber.
IP Address	Informs the system of its dynamically allocated IP address. The DTMX5000 Gateway identifies the DTMX5000 subscriber's data by this address.
MAC (Media Access and Control) Address	Enables the DTMX5000 Gateway to encapsulate TCP/IP packets with this MAC address.
Encryption Key	Enables the DTMX5000 Gateway to encrypt data sent over the DVB link.

The CCU responds with its own set of parameters as soon as all of the elements in the system have been notified of this new subscriber's connection. These parameters are specified at the end of this section.

B.3.2 CCU Contacts Authentication Server

The CCU contacts a selected RADIUS Authentication Server to confirm whether or not the specific subscriber is allowed to enter the system. The RADIUS Authentication Server maintains a local database comprising all the subscribers who are allowed access to the system, as well as each subscriber's service profile, for example, Quality of Service Level.

B.3.3 Authentication Server Allows Access

Authentication is performed through the submission of the subscriber's unique user name and encrypted password. Only the subscriber and the RADIUS Authentication Server know this password. If the subscriber is allowed access, the CCU receives confirmation from the Authentication Server. The Authentication Server attaches to its confirmation message the QoS (Quality of Service) Level, the subsriber's Group ID and the multicast channels to which the subscriber is entitled.

Upon receiving confirmation from the Authentication Serve, The CCU contacts the DTMX5000 Gateway.

B.3.4 CCU Contacts DTMX5000 Gateway

The CCU relays the following subscriber's parameters to the DTMX5000Gateway:

IP Address	The DTMX5000 Gateway identifies the DTMX5000 subscriber's data by this address.
Media Access and Control (MAC) Address	Enables the DTMX5000 Gateway to encapsulate TCP/IP packets with this MAC address.
Encryption Ke	Enables the DTMX5000 Gateway to encrypt date sent over the DVB LAN.
Quality of Service (QoS) Level	The QoS parameter determines the bandwidth share the subscriber receives, according to the level of quality specified in the individual subscription fees. The CCU obtains the Quality of Service Level for each subscriber from the external authentication system (a RADIUS Authentication Server).
Accounting Information	The DTMX5000 Gateway counts the amount of data received by each subscriber. This accounting information is then used to submit billing, for processing by the RADIUS Billing Server.
Group ID	Enables the DTMX5000 Gateway to recognize the group to which the subscriber belongs. Groups enable logical aggregation of the date of groups of users or multicast users under separate PIDs.
Multicast Group Information	The CCU receives a list from the RADIUS Server of multicast channels to which a subscriber is entitled. Based on this list, the CCU sends the appropriate encryption keys to the client.

Refer to *Client Parameters Sent from the RADIUS Authentication Server*.

B.3.5 CCU Contacts Billing Server

The CCU contacts the RADIUS Billing Server and notifies it that a subscriber has started a session. The Billing system accumulates the data necessary for submitting invoices to a subscriber, based on either time or bandwidth usage. For more information about the Billing Serve, refer to the RADIUS Billing Server documentation.

B.3.6 CCU Contacts Proxy Server

The Proxy Server acts as an intermediary between the subscriber and the Internet. Information requests originating from the subscriber pass through the proxy Serve on their way to the Internet. In the reverse direction, the Proxy Server routes the information from the Internet, towards the subscriber, through the DTMX5000.

The CCU contacts the selected Proxy Server in order to update the Proxy Server's Routing Table with the new subscriber's IP address. This enables the Proxy Server to route information from the Internet towards the subscriber. To support the use of Proxy Servers, the subscriber's browser proxy settings should be set to the IP address of a Proxy Server.

Refer to the *DR5000 Satellite IP RouterUser's Guide* for further information.

B.3.7 CCU Responds to DTMX5000 Application

As soon as the CCU has successfully completed contacting the Authentication Server, the Billing Server, the DTMX5000, and the Proxy Server, it responds to the connecting DTMX5000 application.

The CCU includes the following parameters in its response to the connecting DTMX5000 application. These parameters are required by the DTMX5000 application in order to successfully receive and interpret the broadcast:

PID	The MPEG-2 program ID of Group 1 in the DTMX5000..
Frequency:	Broadcast frequency
Symbol Rate	Broadcast symbol rate
Polarity	Satellite broadcast polarity. Available for SatStream clients only.
Range	Satellite broadcast range which sets the subscriber's antennas' LNB for higher or lower bandwidth.
Modulation Type	The modulation type used.

Note: The above parameters are taken from the DTMX5000 properties in the System Parameters dialog box (see Configuring the CCU).

The CCU sends the DTMX5000 application a list of the CCUs in the system. The DTMX5000 application uses this list to implement CCU load-balancing. Each time the DTMX5000 application opens a new session, it randomly chooses a different CCU, thus distributing the load over all the CCUs in the system. The list sent is taken from the CCU Server branch in the System Parameters dialog box (see Configuring the CCU).

B.4 Processing Information Requests

The subscriber requests information by, for example, browsing the Internet with a web browser, or using an FTP client application. These applications generate Internet Protocol (IP) packets, which contain the information requests. These applications must be configured with the IP address of one of the Proxy Server(s) situated at the hub.

The subscriber's information requests are routed towards the Proxy Server at the hub. The requests reach the Proxy Server in the hub through the subscriber's existing Internet connection (such as dial-up modem).

B.4.1 Proxy Server Requests/Receives Information

The Proxy Server reads the subscriber's information request and creates a new request on behalf of the subscriber, which contains the same details as the original request. The only difference is that the source (originator) IP address of the request is changed to that of the Proxy Server, instead of the IP address of the subscriber.

The new request is routed from the Proxy Server through the Internet to the destination server (for example, the web server at the web site that is currently being browsed by the subscriber). The destination server sends a reply to the Proxy Server with the requested information, and the Proxy Server receives this reply.

B.4.2 Proxy Server Sends Information to DTMX5000 Gateway

Proxy Server replies to subscribers are forwarded via the DTMX5000 Gateway, *and not through the subscriber's existing Internet connection*. By sending downstream information to the subscriber through the DVB link, instead of through the subscriber'' existing Internet connection, the system makes use of the tremendous speed advantage of the DVB link.

The routing table enables the Proxy Server to identify that the packet is to be routed to the subscriber through the DTMX5000 Gateway, and not through the subscriber's existing Internet connection. The CCU maintains and updates the Proxy Server's routing table with every subscriber that connects/disconnects from the system.

B.4.3 DTMX5000 Gateway Routes Information to Subscriber

The packet exits the DTMX5000 Gateway, and is sent over the DVB link back to the subscriber. This completes the cycle in which the subscriber requests and receives information from the Internet.

B.5 Terminating a Session

The CCU maintains a local database of all subscribers connected to the system. The subscribers are periodically polled to detect if they are still connected.

When the subscriber terminates a session, either in a conventional manner (by closing the DTMX5000 application) or in an unconventional manner (for example, by turning the computer off while the application is running), the CCU determines from the lack of response to the polling that the subscriber has disconnected.

The CCU, upon detecting that the subscriber has disconnected, informs the proxy Server to remove the client from the routing table.

The CCU then proceeds to inform the DTMX5000 Gateway that the subscriber has logged off. The DTMX5000 Gateway, in return, supplies the CCU with the accounting information. This includes the number of bytes and packets that have been transmitted through the DTMX5000 Gateway for this particular subscriber.

The CCU forwards this accounting information to the Billing Server. The Billing Server compiles invoices according to the subscriber's accumulated usage.

B.6 Installing the CCU

B.6.1 System Requirements

Prior to CCU installation procedures, check that the necessary hardware and software requirements are met:

Requirements	Description
Computer	• Pentium II or equivalent • 32 Megabytes of Ram • 50 Megabytes of free disk space
Operating System	Microsoft Windows NT™ Ver: 4.0

In the CCU package, check for the following:

- Software installation CD-ROM.
- This manual.

After verifying that you have all the necessary hardware and software, you are ready to install the CCU.

B.6.2 Installing Data Access Objects (DAO)

To operate the CCU, it is necessary to install Microsoft's Data Access Objects (DAO). The Data Access Objects installation is included on the CCU installation CD-ROM.

To install the Data Access Objects, proceed as follows:

1. Insert the CCU installation CD-ROM into the computer's CD-ROM drive.

2. In the Windows file explorer, open the DAO folder, located under the root directory of the CD-ROM> Then open the Disk1 folder, located under the DAO folder.

3. Double-click the Setup.exe file. The DAO installation screen is displayed.

4. Follow the installation instructions displayed on the screen. Accept all default parameters provided by the DAO Setup program.

B.6.3 Installing the CCU Application

Note: Prior to installing the CCU application, Microsoft Data Access Objects must be installed, as described in the previous section Installing Data Access Objects.

To install the CCU application, proceed as follows:

1. Insert the CCU installation CD-ROM into the computer's CD-ROM drive.
2. Double-click the Setup.exe file under the root directory of the CD-ROM. The CCU installation window is displayed.
3. Click Next in the *Installation* window.
4. Follow the installation instructions displayed on the screen.
5. When installation is complete, a new directory called CCU is created. This directory contains the program files.

Note: Following installation, the CCU must be configured, as described in Configuring the CCU.

B.6.4 Getting Started

Note: After the CCU is successfully installed, the CCU application is located in the *Program Files* directory, with a shortcut accessible from the Windows NT™ Taskbar.

To start the CCU application, proceed as follows:

1. Click on the Start button (located at the left side on the Windows NT™ Taskbar). Select Programs and then select CCU from within the Programs popup menu.

2. Click on the CCU icon. The CCU starts up, and the main CCU window is displayed. The CCU starts automatically.

Note: If the CCU is stopped, it can be restarted either by clicking the Restart button or accessing the CCU menu.

B.6.5 Uninstalling the CCU Application

To uninstall the CCU application, proceed as follows:

1. From the Start Menu, select Control Panel from the Settings submenu. The Control Panel window opens.

2. Double-click the Add/Remove icon. The Add/Remove Program Properties window opens, as shown below:

3. Select CCU from the list and click the Add/Remove button. A warning dialog opens.

4. Click Yes to uninstall the CCU. The dialog closes and the CCU is uninstalled.

B.7 Configuring the CCU

The CCU must be configured upon initial installation and whenever a new element is added to the system

Parameter changes take effect only after the CCU is restarted by clicking the Restart button or accessing the CCU/menu and selecting Restart**.**

The CCU's central role dictates that it is the last element in the DTMX5000 system to be configured. After the CCU has been configured and restarted, it is ready to accept connection requests from clients.

This chapter explains how to configure the CCU to communicate with the following elements:

B.7.1 Specifying CCU Server Properties

The properties for the CCU Server consist of the CCU Server name and IP address. These properties must be defined for the CCU Server after installation, and for each new CCU Server added.

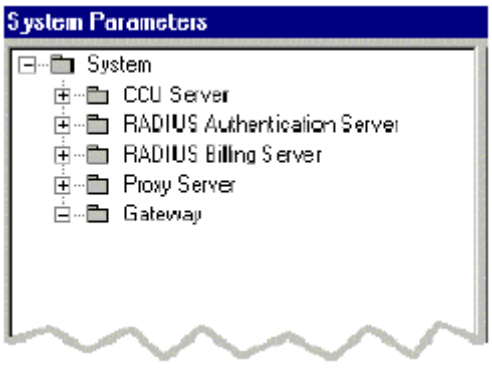
To specify the properties for a CCU Server, proceed as follows:

1. Either click the System Parameters button

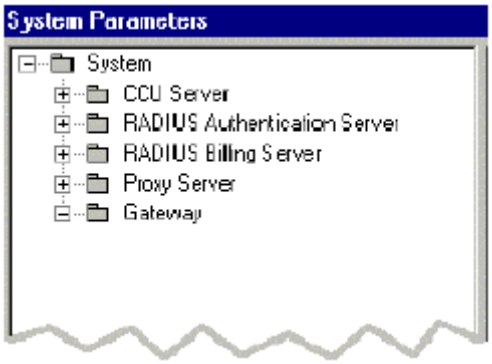
   Or

   Select System Parameters from the Configurtaion menu. The System Parameters window opens.

2. Click on the + beside the System folder to reveal the subtrees of the System tree, as shown below:



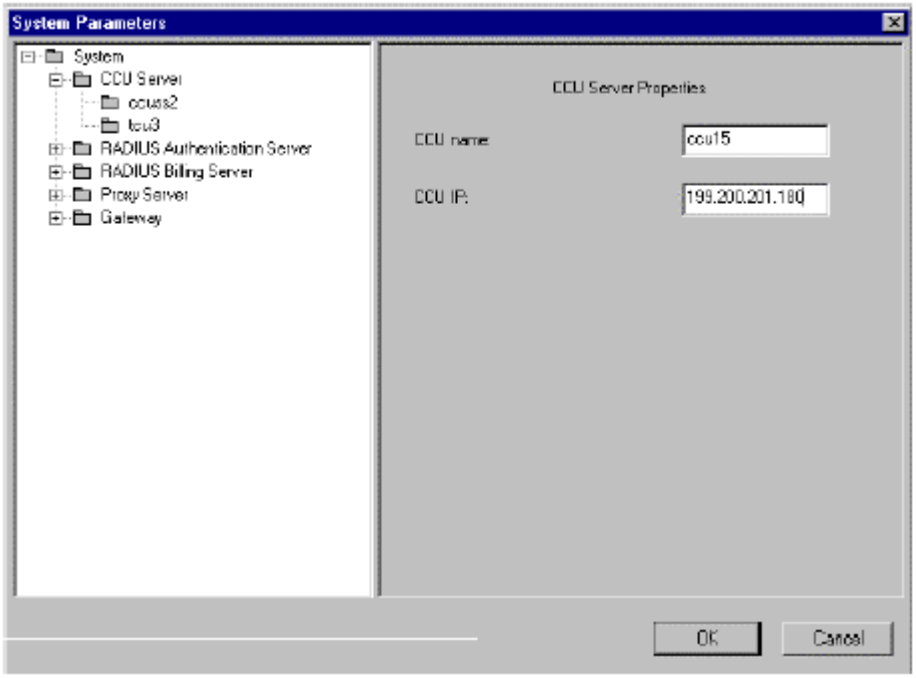
3. Click on the + beside the CCU Server folder. The CCU Server folder expands to reveal the CCU Servers on the system, as shown in the example below:



4. Select the required CCU.

CCU name	Enter a meaningful CCU name. The Server uses this name to identify this specific CCU from other CCUs. This name will also be used in log messages referring to this CCU.
CCU IP	Enter the CCU IP ad*dress.*

The CCU Server Properties dialog opens on the right, as shown below:



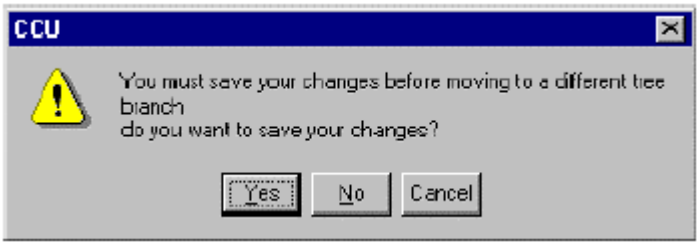
The new properties must be saved in order to configure the CCU to the CCU Server. This can be performed in either of the following two ways:

1. To save the CCU Server properties without performing further configurations, proceed as follows:

   - Click OK. The CCU Server Properties dialog closes and the properties are saved.

2. To save the CCU Server properties and continue with further configurations:

   a. In the tree branch, click the next element to be configured. The following window opens:



   Note: Clicking Yes to save the changes before moving to a different tree branch is an irreversible process, meaning the changes cannot be undone, even by clicking the Cancel button.

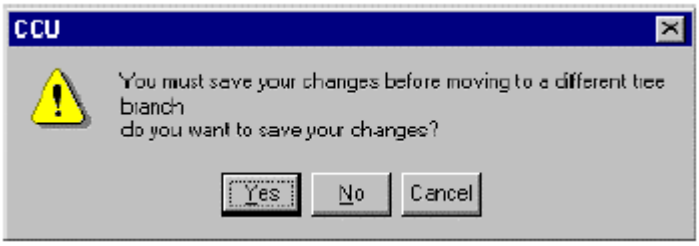
   b. Click Yes. The properties are saved, the CCU Server Properties dialog closes and the next element can be configured.

B.7.2 Adding a CCU Server

Add additional CCU Servers and define the properties for each new server, as follows:

To add another CCU Server, proceed as follows:

1. In the tree branch, right-click on the current CCU, and select New from the popup menu. The following window opens:



Note: Clicking Yes to save the changes before moving to a different tree branch is irreversible process, meaning the changes cannot be undone, even by clicking the Cancel button.

2. Click Yes**.** A new CCU Server Properties dialog is displayed. Add the appropriate parameters in the dialog, and save or cancel your changes as described in the previous section.

B.7.3 Deleting a CCU Server

Deleting a CCU Server removes it from the CCU Servers folder and makes it unavailable to client applications.

To delete a CCU Server, proceed as follows:

1. In the tree branch, right-click on the current CCU, and select Delete from the popup menu. A confirmation window opens.

2. Click Yes to delete the server.

B.8 Configuring the CCU to the RADIUS Authentication Server

The RADIUS Authentication Server is responsible for checking a client's access rights and informing the CCU if a client is to be allowed access to the system, as well as the client's service profile.

The CCU is configured to a specific Authentication Server. The Authentication Server properties can be obtained from the Authentication Server operator, and should be entered as described below.

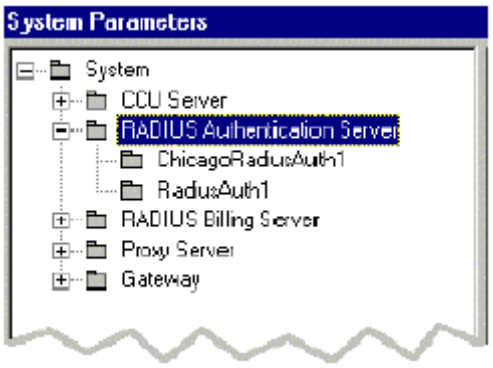
To access a specific Authentication Server, proceed as follows:

1. Either click the System Parameters button,

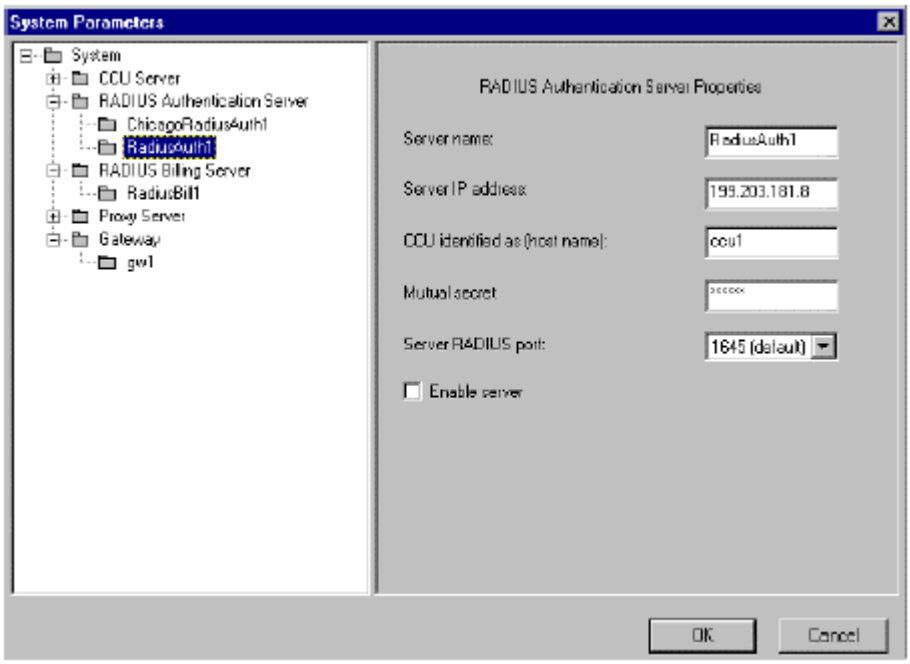
   Or

   Select System Parameters from the Configuration menu. The System parameters window opens.

2. Click the + beside the RADIUS Authentication Server folder. The RADIUS Authentication Server folder expands to reveal a sub-tree level containing the names of the Authentication Servers on the system, as shown in the example below:



3. Click the specific RADIUS Authentication Server folder to which the CCU is to be configured. The RADIUS Authentication Server Properties dialog opens on the right, as shown below:



The CCU can configured to the selected Authentication Server by entering properties in the following fields:

Note: The properties should be obtained from the server operator.

Server name:	Enter a meaningful Authentication Server name. This name will be used in log messages referring to this server. This name can be identical to the name specified in the CCU identified as (host name) field (see below).
Server IP address.	Enter the specific Server IP number.
CCU identified as (host name).	Enter the name of the CCU. The sever uses this name to identify this specific CCU from the cluster of other CCUs that may be using the same server. The name entered in this field should be the same as the name specified in the parallel field in the Authentication Server itself.
Mutual Secret.	Enter the password that is shared between the CCU and the Authentication Serve. The password is never sent to the server. It enables the CCU and the server to authenticate each other's messages. This is performed by means of a specially encrypted digital signature based upon the password.
Server RADIUS port.	From the dropdown list, select either the 1645 (Default**)** value or the 1822 (Official) value. Most RADIUS Servers use the 1645 (Default) value.
Enable server	Check the Enable server to checkbox to activate the RADIUS Authentication Server. IF the checkbox remains unchecked, the Authentication Server is disabled and the CCU will allow all users to connect, regardless of their user name and password.

Note: This disabled Authentication Server mode is useful only if you do not wish to place any access restrictions on connecting users. It should not be used otherwise.

1. Save the properties by either clicking the OK button.

   Or

   Click on another element to be configured. For more information, refer to the saving procedures described in Specifying CCU Server Properties.

To add another Authentication Server, proceed as follows:

- Refer to the similar procedure described in the Adding a CCU Server.

To delete an Authentication Server, proceed as follows:

- Refer to the similar procedure described in the Deleting a CCU Server.

B.9 Configuring the CCU to the RADIUS Billing Server

The RADIUS Billing Server compiles invoices for clients based upon their usage of the system. Due to the fact that a Billing Server can serve multiple CCUs, it is essential that the CCU uniquely identifies itself to the Billing Server.

The CCU is configured to a specific Billing Server. The Billing Server properties can be obtained from the Billing Server operator, and should be entered as described below.

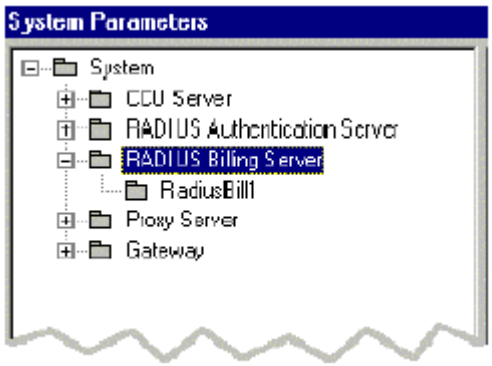
Specify the Billing Server's properties, as follows:

1. Either click the System Parameters button

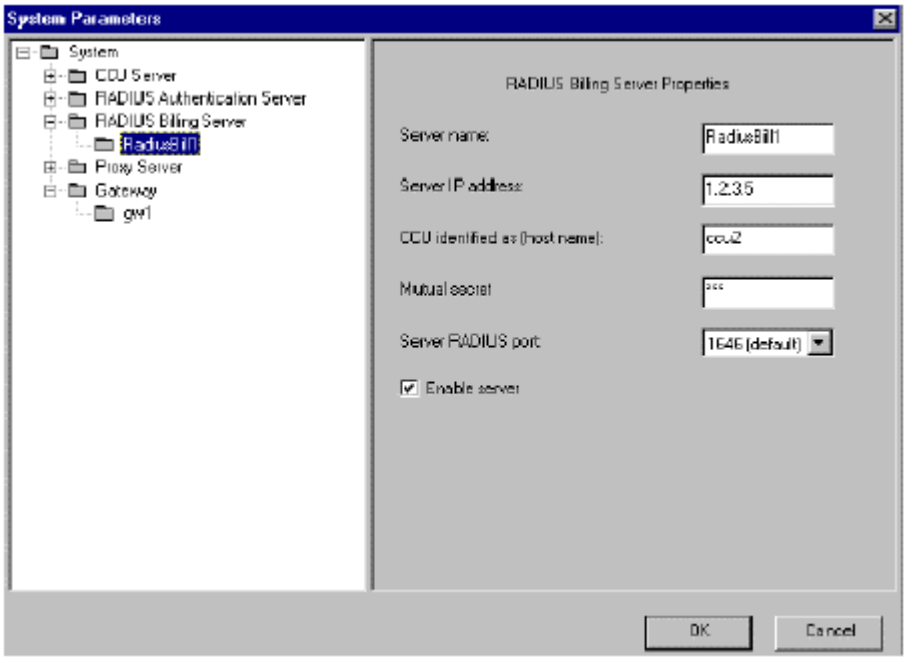
   Or

   Select System Parameters from the Configuration menu. The System Parameters window opens.

2. Click the + beside the RADIUS Billing Serverfolder. The RADIUS Billing Server folder expands to reveal a sub-tree level containing the names of the Servers on the system, as shown in the example below:



3. Click the specific Billing Server folder to which the CCU is to be configured. The RADIUS Billing Server Properties dialog opens on the right, as shown below:



The CCU can be configured to the selected RADIUS Server by entering properties in the following fields:

Note: The properties should be obtained beforehand from the server operator.

Servername:	Enter a meaningful Billing Server name. This name is used in log messages referring to this Server. This name can be identical to the name specified in the CCU identified as (host name) field (see below).
Server IP address.	Enter the specific Server IP number.
CCU identified as (host name).	Enter the name of the CCU. The Server uses this name to identify this specific CCU from the cluster of other CCUs that may be using the same server.
Mutual secret.	Enter the password that is shared between the CCU and the Billing Server. The password is never sent to the server. It enables the CCU and the server to authenticate each other's messages, by means of a specially encrypted digital signature based on the password.
Server RADIUS port.	From the dropdown list, select either the 1646 (Default) value or the 1813 (Official) value. Most RADIUS Servers use the 1646 (Default) value.
Enable server	Check the checkbox to activate the RADIUS Billing Server. If the checkbox remains unchecked, Billing is not activated for any clients accessing the system, meaning that all traffic is free of charge. This mode is useful if you do not want to work with a Billing Server.

3. Save the properties by either clicking the OK button,

   Or

   Click on another element to be configured. For more information, refer to the saving procedures described in the section Specifying CCU Server Properties.

To add another Billing Server, proceed as follows:

- Refer to the similar procedure described in the section Adding a CCU Server.

To delete a Billing Server, proceed as follows:

- Refer to the similar procedure described in the section Deleting a CCU Server.

B.10 Configuring the CCU to the Proxy Server

The Proxy Server relays requested information to a client from the Internet or from its own cache. Each CCU is configured to a specific Proxy Server.

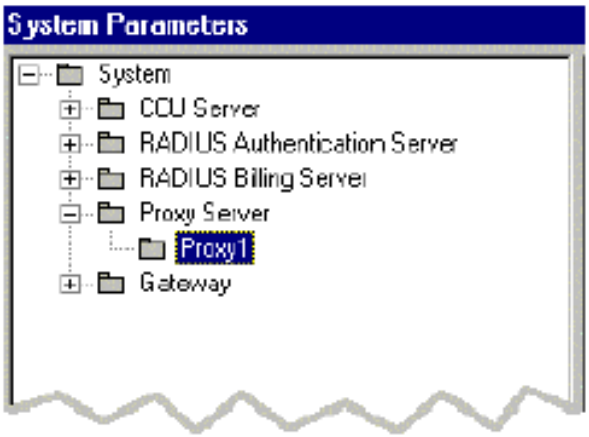
To specify the Proxy Server's properties, proceed as follows

1. Either click the System Parameters button,

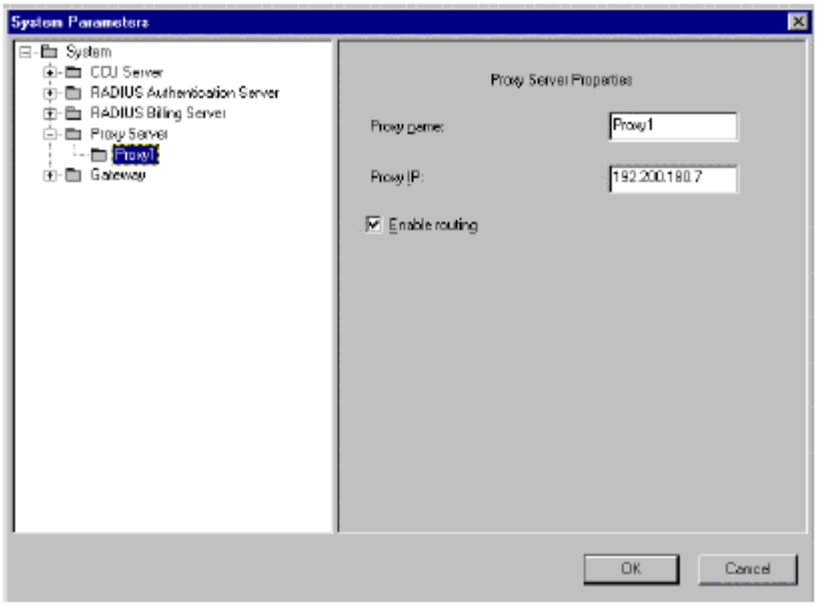
   Or

   Select System Parameters from the Configuration menu. The System Parameters window opens.

2. Click the + beside the Proxy Server folder. The Proxy Server folder expands to reveal a sub-tree level containing the names of the Proxy Servers on the system, as shown in the following example:



3. Click the folder for the specific Proxy Server, to which the CCU is to be configured. The Proxy Server Properties dialog opens on the right, as shown below:



The CCU can be configured to the selected Proxy Server by entering properties in the following fields:

Note: The properties should be obtained beforehand from the DVB channel operator, satellite or cable.

Proxy name:	Enter a meaningful Proxy name: This name will be used in log messages referring to this Proxy Server.
Proxy IP:	Enter the Proxy Server's IP address.
Enable routing	Check the Enable routing checkbox to specify that the CCU should perform routing at the Proxy Server. If unchecked, the CCU does not modify the routing table of the Proxy Server.

4. Save the properties either by clicking the OK button,

   Or

   Click on another element to be configured. For more information, refer to the saving procedures described in the section Specifying CCU Server Properties.

To add another Proxy Server, proceed as follows:

- Refer to the similar procedure described in the section Adding a CCU Server.

To delete a Proxy Server, proceed as follows:

- Refer to the similar procedure described in the Deleting a CCU Server.

B.11 Configuring the CCU to the DTMX5000Gateway

The DTMX5000 Gateway sends the client's requested information through the DVB link. The CCU is configured to a specific DTMX5000 Gateway. The DTMX5000 Gateway properties can be obtained from the DVB channel operator and should be entered as described below.

Note: Many of the DTMX5000 Gateway's properties are sent to each DTMX5000 application that connects to the CCU. These parameters are taken from the dialog described below. These parameters are subsequently used by the DTMX5000 application to receive and correctly interpret the broadcast. Therefore, it is crucial to verify that these parameters are accurate.

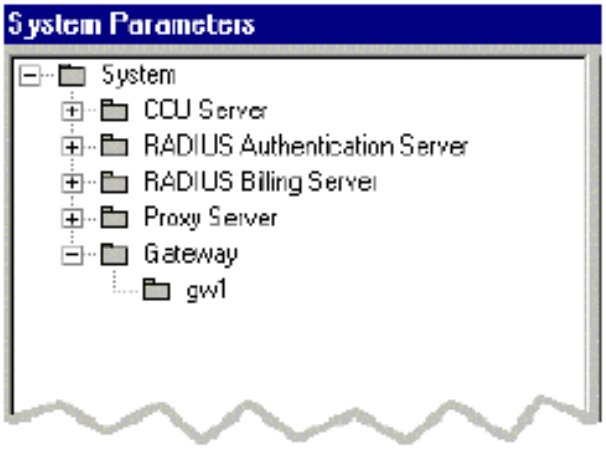
To specify the DTMX5000 Gateway's properties, proceed as follows:

1. Either click the System Parameters button,

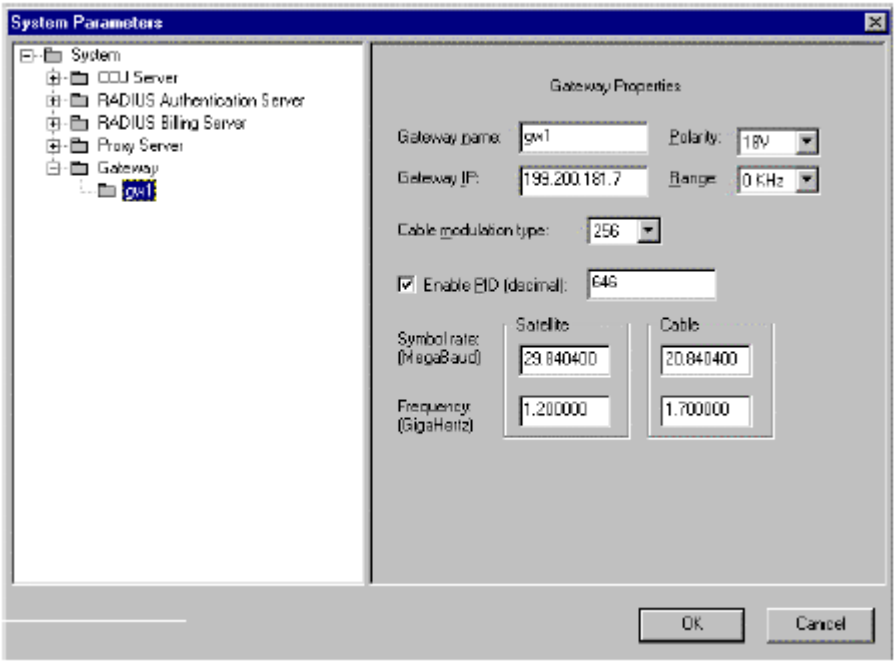
   Or

   Select System Parameters from the Configuration menu. The System Parameters window opens.

2. Click the + beside the Gateway folder. The Gateway folder expands to reveal a sub-tree level containing the names of the DTMX5000 Gateways on the system, as shown in the example below:



3. Click the folder for the specific Gateway to which the CCU is to be configured. The Gateway Properties dialog opens on the right, as shown below:



The CCU can be configured to the selected Gateway by entering the correct properties in the following fields:

Note: The properties should be obtained beforehand from the DVB channel operator.

Gateway name	Enter a meaningful DTMX5000 Gateway name. This name will be used in log messages referring to this DTMX5000 Gateway.
Polarity	Select a polarity value from the dropdown list.
Gateway IP	Enter the Gateway IP address.
Range	Select a range value from the dropdown list.
Cable modulation type	Select a cable modulation type from the dropdown list.
Enable PID (decimal)	Check the Enable PID (decimal) checkbox to activate the field. If there is a multiplexer presents in the system, enter the PID value obtained from the DVB channel operator. Otherwise, enter the PID value exactly as specified in the Gateway CFG.INI file. This is the PID of Group 1 in the Gateway. Refer to t he DTMX5000 Manual for further information.

If the checkbox is unchecked, the PID number is irrelevant.

Symbol rate	Enter the symbol rate (in MegaBaud) in the Satellite and Cable fields.
Frequency	Enter the frequency (in GigaHertz) in the Satellite and Cable fields.

4. Save the properties either by clicking the OK button,

   Or

   Click on another element to be configured. For more information, refer to the saving procedures described in the section Specifying CCU Server Properties.

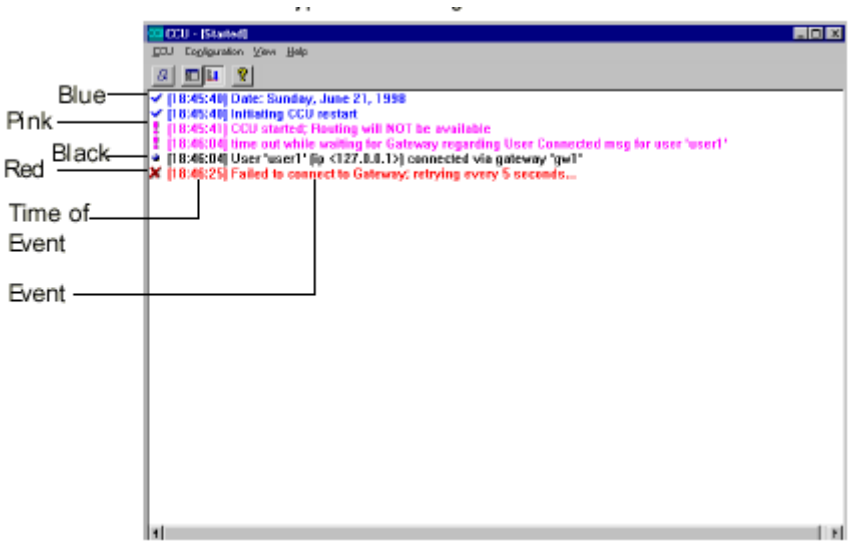
B.12 Operating the CCU

In addition to configuring CCU parameters, the following operations are available from the CCU.

B.12.1 Monitoring the Events Log

The operator can monitor the CCU via an events log which records routing events, infrequent events and error messages. Upon startup, the events log appears in the main CCU window. The CCU automatically updates the events log when an event occurs. Each event has a unique color code and icon, according to the event's frequency and message.

The window below shows a typical events log for the CCU.



The table below describes the color and icon for each event category:

Color Code	Icon	Category	Example
Black	•	Normal routine events.	User xxx is connected to the Gateway.
Blue	✔	Infrequent events	Restarting the Gateway
Red	✕	Warning, error messages	CCU failed to connect to the Gateway
Pink	!	Error messages	Routing is not available

Note: When an event is added to the log, the time of the event is also recorded

The events log can store up to 10,000 events, after which it overwrites the oldest entry, and then the second oldest entry, and so on. When a new event occurs, the automatic scrolling feature automatically scrolls to the new entry. The CCU operator can configure the events log to activate/deactivate the automatic scrolling feature.

To activate automatic scrolling, proceed as follows:

1. Either click the Auto Scroll button in the toolbar (the button appears selected),

   or

   Check the Auto Scroll feature in the Viewmenu.

2. The automatic scrolling feature is activated. The events log automatically scrolls down to a new event entry each time it occurs.

To deactivate automatic scrolling, proceed as follows:

1. Either click the Auto Scroll button in the menu bar (the button appears deselected),

   or

   Uncheck the Auto Scroll feature in the View menu.

   The automatic scrolling feature is deactivated. The feature is useful if the CCU operator is reviewing events and does not want the events log to move automatically to the latest event entry

B.12.2 The CCU Logfile Mechanism

The CCU Logfile Mechanism records to a disk file a copy of the events log that appears in the main CCU window. This file, called “logfile 000.txt”, is located in the default CCU directory (C:\Program Files\CCU).

Logfile size is limited to 10 megabytes of disk space. Up to 15 logfiles may be stored in the CCU directory.

Each time the CCU starts up, or if the current logfile exceeds 10 megabytes during program execution, the following sequence of events occurs:

The current logfile (logfile 000.txt) is closed and renamed as logfile 001.txt.

The numbers of the following logfiles are all incremented by one so that logfile 001.txt becomes logfile 002.txt, logfile 002.txt becomes logfile 003.txt, and so on. The oldest logfile (logfile 014.txt) is deleted.

A new logfile 000.txt is opened and becomes the current logfile for subsequent messages.

Since there may be up to 15 logfiles in the CCU directory (logfile 000.txt through logfile 014.txt) they may consume up to a total of 150 megabytes of disk space. However, since a new logfile is opened each time the CCU is run, each logfile may not reach its full capacity and therefore less disk space may be consumed by the logfiles.

All log messages are preceded by a single letter which indicates the color and type of message, as displayed in the CCU event log. This enables you to search for specific messages by color, as follows:

k = Black

b = Blue

p = Pink

r = Red

For example: Specify **r[** to search for all red messages.

B.13 Client Parameters Sent from the RADIUS

B.13.1 Authentication Server

The RADIUS Authentication Server is used by the CCU for two purposes:

- Client authentication
- Relay of client parameters

The CCU needs certain client parameters in order to customize the system for each client's requirements and level of service. These parameters are sent to the CCU by the RADIUS Authentication Server.

Note: These parameters are not part of the authentication process, and authentication can proceed without them.

The following client parameters are relayed to the CCU in a RADIUS Authentication Packet:

B.13.1.1 Quality of Service

Quality of Service (QoS) Level. The QoS parameter determines the bandwidth share the subscriber receives. IT is measured by two parameters:

- Committed Information Rate (CIR): The minimum information rate (in bits per second) that the client is guaranteed to receive.
- Maximum Bit Rate: The maximum bit rate that the client may receive at any time. This rate must be equal to or greater than the CIR>

This parameter must be encoded in a FilterID (Type 11) RADIUS attribute (see RFC2138 – RADIUS) in the following format:

A string which contains the CIR in bits per second, then a dash ("-") and then the maximum bit rate in bits per second. For example, 300000 – 1000000.

B.13.1.2 Group ID

Enables the DTMX5000 Gateway to recognize the group to which the client belongs. Groups enable aggregation of the date of groups of users or multicast users logically under separate PIDs. This parameter must be encoded in a Callback-ID (Type 20) RADIUS attribute, as a string containing the Group ID number.

B.13.1.3 Multicast Group Information.

The CCU receives a list from the RADIUS Server of multicast channels to which a subscriber is entitled. Based on this list, the CCU sends the appropriate encryption keys to the client. Multicast is a one-to-many transmission method that enables a single packet transmission to be routed to multiple users.

This parameter must be encoded in a Callback-Number (Type 19) RADIUS attribute, as a string containing the Multicast Group numbers the client is entitled to receive, separated by commas. The valid Multicast Group are group number 1 through group number 15. You can enter any or all of these group numbers, separated by commas. The string may also be empty if the user is not entitled to receive any Multicast Group.

For example: the string 1, 2, 15 specifies that the user is entitled to receive Multicast Groups 1, 2 and 15. A shortcut can be used for a group range.

For example, to specify that the user is entitled to receive Multicast Groups 1,2, 3, 7, 12, 13, 14, the following string is also valid 1-3, 7, 12-14.

Note: The above is a general description of the client parameters sent from the RADIUS Authentication Server to the CCU. It applies to any RADIUS-compliant Authentication Server. For instructions on how to configure a specific RADIUS Server (for example NTXacs RADIUS Authentication Server) to send client parameters to the CCU, please refer to the relevant Application Notes.

This page is intentionally left blank.

Appendix C. HIGH AVAILABILITY SERVER (HAS-2000)

The purpose of high availability server is to develop Broadband IP transmission using DVB technology over cable TV and satellite system that which will have high availability so that the operators can provide “Always ON” services.

C.1 Overview

The High Availability Server (HAS-2000) is located in a satellite hub or at a cable operator head-end site. It has two main physical interfaces and multiple logical connections. There is a physical interfaces of 100Base T connected to the control and management (C&M) LAN on which all of the Gateways/INAs at the head-end are connected.

Another physical connection is an EIA-232 port that is used to connect the HAS-2000 with an IF switch that enables to switch the IF inputs/outputs between the Gateways/INAs. The same connection to the IF switch can be done via the C&M LAN since the switch over command of the HAS-2000 also is send as IP packet. In this case there is a need for external device that converts the IP packet to a physical interface of the IF switch.

C.1.1 Standard References

1.System standards

- SNMPv2RFC1902-RFC1906
- IEEE 802.3 Ethernet 100BaseT
- RFC 791 IP

2. ETSI standards

- ETS 300 800
- ETS 300 429
- EN 300 192

C.2 General Description

C.2.1 Brief System Description

The HAS-2000 functionality is to monitor constantly the status of the Gateways/INAs connected to the C&M LAN and verify their availability. It is keeping date base mirror of all active Gateways/INAs and update it when there is a change in one of the Gateways/INA's parameters. When a faulty condition is detected in one of the Gateways/INAs, the HAS-2000 will switch the traffic of the faulty unit to a stand-by unit. The switch over will be done in following steps:

- Download the relevant mirror data base to the stand-by Gateway / INA
- In parallel, switch over the IF transmission
- Send deactivated command to the faulty unit
- Activate the stand-by unit

The HAS-2000 is based on a PC that has 100BaseT interface and RS-232 port for IF switch connection. The software system available on the PC is completing the product functionality.

C.3 Detailed Description

C.3.1 System Details

- The system serves multiple active and stand-by Gateways / INAs.
- Any one of the stand-by Gateways / INAs can replace an active Gateway / INA.
- Any combination between active and stand-by units is supported.
- Each Gateway / INA (active and stand-by) has fixed IP address on the C&M LAN.
- Only active Gateways / INAs have IP address on the date LAN. When a stand-by Gateway / INA replaces an active Gateway / INA, it gets the data LAN IP address of the active Gateway / INA it replaced.
- The HAS-2000 does health monitoring to the active and stand-by Gateways / INAs by sending a proprietary IP TEST packet in a fixed time period.
- The TEST packet commands the Gateway / INA to perform a sanity check. The result of the sanity check can get one of two values – "O.K." or "Not O.K.". The sanity check result is send by a trap back to the HAS-2000. The HAS-2000 decides to switch over in two cases:
    - ♦ No trap was recieved from the tested Gateway / INA within a fixed time window.
    - ♦ A "Not O.K." trap was received from a tested Gateway / INA.
- The HAS-2000 holds mirror database for of each active Gateway / INA. An active Gateway/INA updates the HAS-2000 each time its database is changed by sending an SNMP trap. The database is designed to be generic, in a way it would not be affected by new Gateway/INA parameters. The mirror database can be stored in the HAS-2000 or in another network element (for example – the SNMP management station).
- The HAS-2000 can be controlled via SNMP or GUI application since it includes a proprietary MIB.

- The switch over operation is done with the following steps (HAS-2000 side):
    - ♦ Sends TRAP (Start of Switching) to the NMS.
    - ♦ Sends disable command to the active Gateway/INA.
    - ♦ Sends disable command to the active Gateway/INA. The switch over information is an IP packet that includes the new data LAN IP address (of the active Gateway/INA), the host details and path of the mirror database.
    - ♦ Activate the stand-by Gateway/INA.
    - ♦ Sends TRAP (End of Switching) to the NMS.
    - ♦ Switch the IF switch.
- Switching operation (Stand-by Gateway/INA Side):
    - ♦ Receives switch over information from the HAS-2000 that includes the new data LAN IP address (of the active Gateway/INA), the host details and path of the mirror database.
    - ♦ Loads the active Gateway / INA database from the host.
    - ♦ Receives activation command.
    - ♦ Sends gratuitous ARP to announce the new IP-MAC address pair.
- The return to work of the active Gateway/INA is done by a manual command send from the management application.

C.3.2 System Diagram

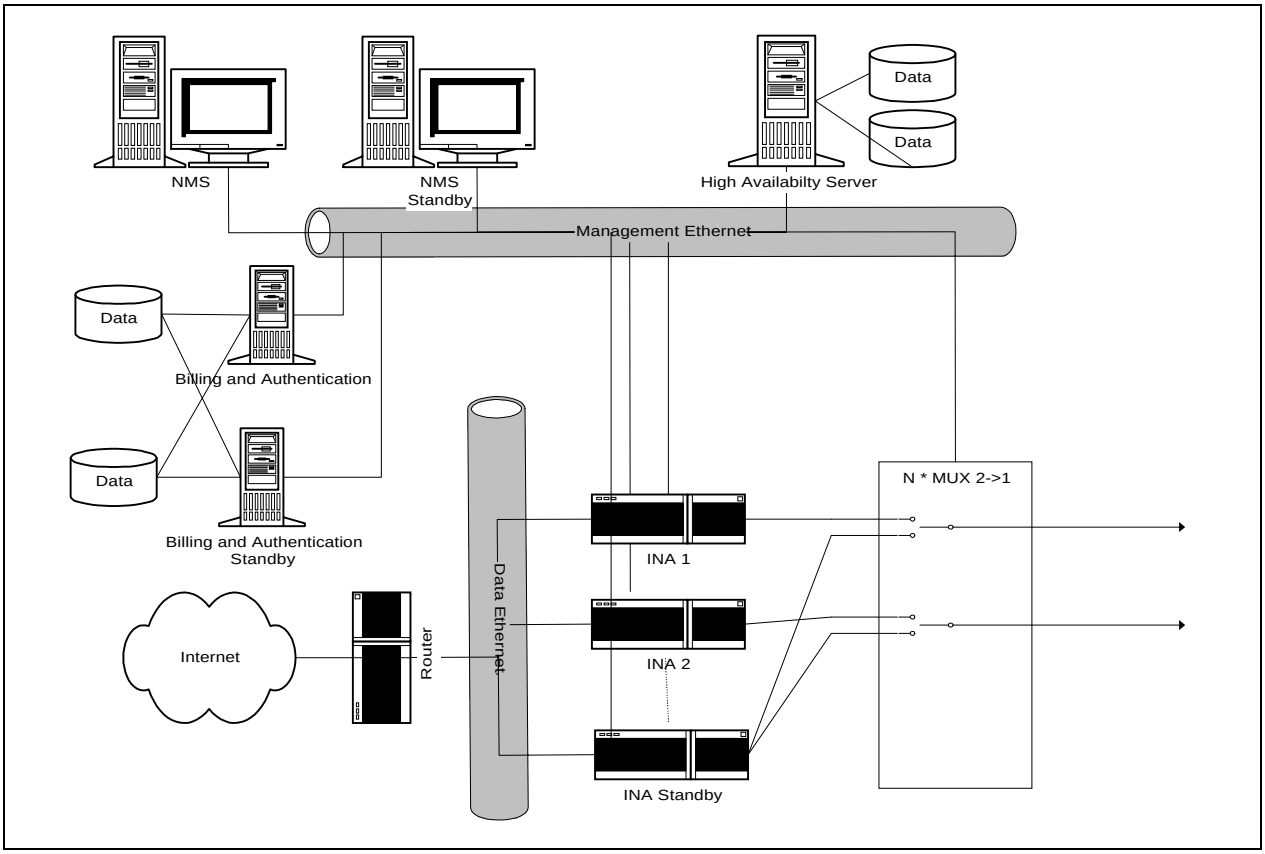


Figure C-1. System Diagram

C.3.3 Technical Specifications

Active Gateways	Up to 30.
Standby Gateways	Up to 30.
Combination of active and Standby Gateways	Any combination supported by the switching device. Up to 30 Gateways.
Detection time	Typical: 0 to 3 sec.
Switch over time	Up to 2 sec.
Switch over decision	Based on: • Gateway's failure to response to self-sanity check. • Gateway's report on self-sanity check failure: • High CPU load • Hardware status • Activity on the LANs
Switch over modes	Automatic\ Manual.
IF switch support	Currently support 2->1 ASI switch. Can support any other PC controlled switch
Redundancy	The system continues to work on any single failure
Management	GUI and SNMP
HAS – Gateway protocols	TLV over TCP/IP for backward and forward compatibility.
Database	LDAP server
Hardware	CPU: Pentium 3 450MHz or higher. Memory: 128 MB or higher.
Operating system	Windows 2000 server.

Glossary

The following is a list of acronyms and abbreviations that may be found in this manual.

Acronym/ Abbreviation	Definition
Ω	Ohms
8PSK	Eight Phase Shift Keying
16QAM	Sixteen Quadrature Amplitude Modulation
ARP	Address Resolution Protocol
ASI	Asyncchronous Serial Interface
Aux	Auxiliary
C&M	Control and Management
CCU	Central Configuration Unit
CIR	Committed Information Rate
COM	Common
CRC	Cyclic Redundancy Code
DVB	Digital Video Broadcasting
EIA	Electronic Industries Association
EN	European Norms
ESD	Electrostatic Discharge
ETS	European Telecommunications Standards
ETSI	European Telecommunications Standard Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
ID	Identification
IP	Internet Protocol
LAN	Local Area Network
LLC	Logical Link Control
LVDS	Low Voltage Differential Signal
Max	Maximum
MCPC	Multiple Channel per Carrier
MIB	Management Information Base
Min	Minimum
MPE	Multiprotocol Encapsulation

Acronym/ Abbreviation	Definition
MPEG	Moving Picture Expects Group
Mux	Multiplexer
NIC	Network Interface Cards
NMS	Network Management System
PAT	Program Association Table
PC	Personal Computer
PID	Packet Identifier
PMT	Program Map Table
QoS	Quality of Service
QPSK	Quaternary Phase Shift Keying
RMA	Return Material Aurthorization
RS	Recommneded Standard
SCPC	Single Channel per Carrier
SIDs	Service IDs
SNMP	Simple Network Management Protocol
TN	Telnet
TS	Transport Stream
TX	Transmit
VGA	Video Graphics Adapter

Index

T

U

V

W

This page is intentionally left blank.