Installation and Operation

TEAM 2B1Q for PC

Version 2.0.0

General DataComm

Warning

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to CISPR-22 of FCC and international rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. The user is cautioned that any changes or modifications not expressly approved by General DataComm void the user's authority to operate the equipment.

This digital apparatus does not exceed Class A limits for radio noise emissions from digital apparatus described in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Warranty

General DataComm warrants that its equipment is free from defects in materials and workmanship. The warranty period is one year from the date of shipment. GDC's sole obligation under its warranty is limited to the repair or replacement of the defective equipment provided it is returned to GDC, transportation prepaid, within a reasonable period. This warranty will not extend to equipment subjected to accident, misuse, or alterations or repair not made by GDC or authorized by GDC in writing. *The foregoing warranty is exclusive and in lieu of all other warranties, express or implied, including but not limited to, warranties of merchantability and fitness for purpose.*

Trademarks and Patents

General DataComm, the General DataComm logo and the following are trademarks of General DataComm, Inc in the United States and other countries: ACCULINE, ANALOOP, AUTOFRAME, BERT 901, DATACOMM SECURE-PAK, DATALOOP, DIGIDIAL, ENmacs, FASTPRO, FIRST RESPONSE, GDC, GDC APEX, GENERAL DATACOMM X-PRESS, GEN*NET, GEN*PAC, IMAGE*TMS, KILOMUX, LAN*TMS, MEGA*BRIDGE, MEGAMUX, MEGAMUX TMS, MEGANET, MEGASPLIT, MEGASWITCH, MEGAVIEW, NETCON, NETSWITCH, NMC, QUIKSHIPPERS, SERVI-CHECK, SERVI-SNAP, WINmacs.

ANALOOP and DATALOOP respectively are protected by U.S. patents 3,655,915 and 3,769,454. All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries concerning such trademarks should be made directly to those companies.

HP OpenView is a trademark of the Hewlett-Packard Company.

Copyright

Table of Contents

Antistatic Precautions

Electrostatic discharge (ESD) results from the buildup of static electricity and can cause computer components to fail. Electrostatic discharge occurs when a person whose body contains a static buildup touches a computer component.

The equipment may contain static-sensitive devices that are easily damaged and proper handling and grounding is essential. Use ESD precautionary measures when installing parts or cards and keep the parts and cards in antistatic packaging when not in use. If possible, use antistatic floorpads and workbench pads.

When handling components, or when setting switch options, always use an antistatic wrist strap connected to a grounded equipment frame or chassis. *If a wrist strap is not available, periodically touch an unpainted metal surface on the equipment.* Never use a conductive tool, like a screwdriver or a paper clip, to set switches.

Safety Guidelines

The following symbols are used when unsafe conditions exist or when potentially hazardous voltages are present: *Caution state-ments identify conditions or practices that can cause damage to the equipment or loss of data. Warning statements identify conditions or practices that can result in personal injury or loss of life.*

Always use caution and common sense. *To reduce the risk of electrical shock, do not operate equipment with the cover removed.* Repairs must be performed by qualified service personnel only.

- Never install telephone jacks in a wet location unless the jack is designed for that location.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.
- Use caution when installing telephone lines and never install telephone wiring during an electrical storm.

FCC Part 68 Compliance

Connection of data communications equipment to the public telephone network is regulated by FCC Rules and Regulations. This equipment complies with Part 68 of these regulations which require all of the following.

All connections to the telephone network must be made using standard plugs and telephone company provided jacks or equivalent. Connection of this equipment to party lines and coin telephones is prohibited. A label on the back of the front panel of data communications equipment and on the underside or rear panel of other equipment provides the FCC Registration number and the Ringer Equivalence Number (REN) for the unit. If requested, give this information to the telephone company.

If the unit causes harm to the telephone network, the telephone company may discontinue your service temporarily and if possible, you will be notified in advance. If advance notice is not practical, you will be notified as soon as possible and will be advised of your right to file a complaint with the FCC. The telephone company may change its communication facilities, equipment, operations and procedures where reasonably required for operation. If so, the telephone company will notify you in writing. You must notify the telephone company before disconnecting equipment from 1.544 Mbps digital service. All repairs or modifications to the equipment must be performed by General DataComm. Any other repair or modification by a user voids the FCC registration and the warranty.

Canada DOC Notification

The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. *Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.*

Deutschland

Installations Anweisungen: Installieren Sie die Telefonleitungen nicht während eines Gewitters. Installieren Sie die Telefonleitungen nicht in einem feuchten Raum, auβer die Dose entspricht den Vorschriften für Feuchträume. Berühren Sie unisolierte Telefonleitungen oder Einrichtungen nicht, auβer diese sind vom Telefonnetz getrennt. Vorsicht bei der Installierung oder Änderung von Telefonleitungen. *Achtung:* Es gibt keine durch den Benutzer zu wartende Teile im Gerät. Wartung darf nur durch qualifiziertes Personal erfolgen.

Registration Status	Port ID	SOC	FIC	USOC

1 System Description

Overview

This chapter provides an overview to GDC's Team 2B1Q Management System.

UAS 2B1Q System Components

The UAS 2B1Q consists of the following components:

- SpectraComm 616
- SpectraComm 613
- SpectraComm 611
- DataComm 610
- DataComm 612
- DataComm 621
- SpectraComm Manager (SCM)

SpectraComm 616 (SC616) - The SC616 is a six channel Line Termination Unit (LTU). The unit supports three 2B1Q U-interfaces that are compatible with requirements of ANSI T1.0601-1992 and six co-directional 64 kbps interfaces that are compatible with the requirements of ITU-T G.703. Each 2B1Q U-interface is permanently routed to a specific pair of G.703 interfaces. You may control the SC616 by a SCM via the SpectraComm management bus.

SpectraComm 611 (SC611) - The SC611 is a single channel 2B1Q data transmission device. The unit supports ANSI T1.601-1992 2B1Q U-interface and one ITU-T V.35 or EIA/TIA-232-E DTE interface (optionally, ITU-T X.21 and EIA-530). The SC611 has a sub-rate capability (X.50) provided by the SC621.

SpectraComm 613 (SC613) - The SC613 is a three channel 2B1Q data transmission device. The unit supports three ANSI T1.601-1992 2B1Q U-interfaces and three modified ITU-T X.21 DTE interfaces. Each 2B1Q U-interface is permanently assigned to a specific X.21 interface port operating at either 64 or 128 kbps.

The SpectraComm SC616, SC611 and SC613 pass software configuration and control commands over the EOC (Embedded Operations Channel) from the SCM to a DataComm (DC) 600 series tail circuit. As LTUs, the The SC616, SC611 and SC613 originate ANSI EOC B1 and B2 loopback commands. This allows the units to inter-operate with other (competitor) devices that comply with the ANSI specification. The SC611 and SC613 are capable of responding to V.54 loopback control from the U-loop as an enable/disable option.

DataComm 621 (DC621) - The DC621 is a low-cost Network Termination Unit (NTU). The unit complys with ANSI T1.601-1992 line coding requirements on the network side, and provides a DTE interface on the business equipment side.

The line coding scheme is a 2B1Q as defined in T1.601. The DTE interface may be used to X.50 compatible rate adaption is performed. The unit works with both synchronous and asynchronous DTEs. The basic DTE channel interface provided is ITU-T V.35 or EIA/TIA-232-E on card. Hardware hooks are provided for optional DTE interface types. Switches are provided for configuration but the unit will also respond to messages from the EOC.

DataComm 610 and 612 (DC610/612) - The DC610 and DC612 are single channel and dual channel Network Terminating Units (NTUs). They are compatible with ANSI T1.601-1992 line coding requirements and support an operating range of up to 18 kilo feet over a two-wire 26 gauge line.

V.35 and ITU-T V.24/V.28 interfaces are selectable by jumpers. Optional 530 or X.21 interface cards are available.

SpectraComm Manager (SCM) - SpectraComm Manager (SCM) acts as the SNMP agent through which TEAM management applications communicate with UAS 2B1Q components. All management communications are directed to the SCM card Internet Protocol (IP) address. The SCM card relays commands and responses between management applications and hardware components, using a slot addressing scheme to communicate over the SpectraComm shelf backplane with the other UAS 2B1Q components. The SCM is transparent to the applications, which operate as though they were communicating directly with the hardware units.

2 Installation

System Requirements

Table 2-1 lists minimum and recommended requirements for the TEAM Manager. Systems purchased from GDC have the required software installed. This includes the hardware and software components in the Recommended System column of *Table 2-1*. If you want system options, e.g., a printer, you must provide and install the software for these options as per the manufactures procedures. The instructions that follow describe how to install the GDC Team 2B1Q Management System software in the event you must configure a system yourself.

Table 2-1   System Requirements

Minimum System	Recommended System
486 DX2-66Mhz IBM PC-compatible with minimum of 16 Megabytes of RAM	Pentium or Pentium Pro series IBM™ PC-Compatible with 32 Megabytes of RAM
VGA Color monitor	VGA Color monitor
540 Kilobytes free conventional memory	540 Kilobytes free conventional memory
20 Megabytes of free hard disk space	20 Megabytes of free hard disk space
MS-DOS 6.0, MS Windows For Workgroups 3.11 and FTP Software Onnet 2.01 or MS Windows 95 and MS TCP/IP Network Protocol	MS Windows 95 and MS TCP/IP Network Protocol
8 bit Ethernet Card 10baseT or 10base2	16 bit Ethernet Card 10baseT or 10base2
Mouse	Mouse
HP OpenView™ for Windows Version 7.2C	HP OpenView for Windows Version 7.2C

Operating System Software

HP OpenView for Windows and GDC Team 2B1Q Management System runs on either MS™ Windows For Workgroups 3.11 or MS Windows 95. GDC recommends the use of Windows 95™ for best overall performance.

Regardless of which Operating system you choose to install, you should follow the installation instructions provided by Microsoft.

Comments on MS Windows 95

To use the TEAM Manager on Windows 95, Microsoft's TCP/IP Network protocol must be installed and properly configured.

Installing Windows 95 TCP/IP

Follow these steps to install Microsoft's TCP/IP:

1.   Press the START button, select `Settings...`, then `Control Panel`.

2.   Double-click the Network icon. You'll see a dialog box. Make sure the Configuration tab is selected. Both your Network Adapter and TCP/IP should be present in the list of network components installed. If they are, you're ready to proceed to Configuring Windows 95 TCP/IP.

3.   To install TCP/IP, Press the `Add` button, double-click Protocol, then select Microsoft, then TCP/IP, and select OK.

4.   To add your adapter, press the `Add` button, double-click Adapter, then scroll down the list until you see your card's vendor on the list. Choose the correct adapter and press `OK`. Now your Network dialog box should contain both your Adapter and TCP/IP.

5.   Select the adapter, click `Properties, Bindings`, and make sure the TCP/IP box is checked

6.   You're now ready to proceed to Configuring Windows 95 TCP/IP.

Configuring Windows 95 TCP/IP

Follow these steps to configure Microsoft's TCP/IP:

1.   Press the `START` button, select `Settings`, then `Control Panel`.

2.   Double-click the Network icon. You should get a dialog box.

3.   Click on the TCP/IP protocol and press the `Properties` button. This will display the TCP/IP Properties box. There are six tabs in this dialog box.

4.   *IP Address*: Select the Specify an IP address option. Then type in the IP address for your computer. Next, fill in the Subnet Mask. This number will probably be 255.255.255.0 for a class "C" TCP/IP Network.

5.   *WINS Configuration*: Select the Disable WINS Resolution option unless you know your network has a Windows Name Server.

6.   *Gateway*: Type in the IP address for the gateway(router) that you are using on your LAN. Once you've entered this number, press the `Add` button. If your network is a simple and you do not have a router to another network segment, leave this tab blank.

7.   *Bindings*: By default, the Client for Microsoft Networks option is checked. Leave it alone. If you have another client (such as Novell) loaded for your network, make sure it is checked as well.

8.   *Advanced*: Make sure the Set this protocol to be the default protocol option is checked.

9.   *DNS Configuration*: If your organization has a Domain Name Server to map IP addresses to names, select the `Enable DNS` option. Enter your computer name in the Host box. In the Domain textbox, enter the domain name of your organization, i.e. abc.com. In the DNS Server Search Order section, put in the IP address of your provider's name server and press the `Add` button. In the Domain Suffix Search Order section, type in the domain suffix (usually the same as the domain) and press the `Add` button. If your network is simple and you do not have a Domain Name Server, select `Disable DNS`.

10.   When you're done setting these options, press the OK button. Then press the OK button in the Network dialog box. Windows 95 will ask you to reboot to complete the changes.

Comments on MS Windows for Workgroups

Comments on Installing DOS

HP OpenView for Windows and the GDC Team 2B1Q Management System require DOS 6.0 or higher. *Be sure to install DOS before installing system software.*

Do not install the DOS Share utility.

It is suggested that CONFIG.SYS contain the following commands:

FILES=40

BUFFERS=40

For information concerning CONFIG.SYS, consult your DOS manual.

Comments on Installing MS Windows for Workgroups 3.11

We recommend that you use a disk optimizer on your hard drive before installing: MS Windows For Workgroups.

MS Windows For Workgroups offers a disk-caching program called *SMARTDrive.* It is recommended that you use it. For further information consult your MS Windows For Workgroups documentation.

You must install networking software for MS Windows For Workgroups.

MS Windows For Workgroups installation asks if you want the AUTOEXEC.BAT and CONFIG.SYS files modified. Let the installation modify them. If you choose otherwise, you may have to modify these files later. For information concerning AUTOEXEC.BAT and PATH, consult your DOS manual.

HP OpenView for Windows

The following paragraphs contain information needed to install OpenView, create a network map, and monitor your network. It describes:

- OpenView requirements

- Installing and running OpenView

- Setting passwords

- Quick start instructions to create a map and monitor your network

For more information about OpenView features, refer to your HP OpenView User's Manual.

Installing OpenView

Before installing OpenView, install and test your network software. If you are going to install FTP communications software on Windows 3.11 For Workgroups, do so before installing OpenView. Refer to the HP OpenView manual for FTP software installation instructions. Install OpenView using the MS Windows For Workgroups Setup process. The following procedure assumes that you are using the A: drive.

Perform the following steps:

1. Insert OpenView diskette #1 in the disk drive.

2. For Windows 95, Click on the START Menu and select Run. For Windows For Workgroups select File: Run from Program Manager.

3.   Type in **A:\SETUP**.

4.   Follow the instructions that appear on the screen. You are alerted when installation is complete.

5.   Ensure that the OpenView directory is in the DOS path statement in the AUTOEXEC.BAT file.

At the end of the installation process, an OpenView program group is created containing HP OpenView, Installation Tips, HP OpenView Help, What's New, and Troubleshooting Guide.

GDC TEAM 2B1Q Management System

Before installing system software, be sure that Windows 95 or Windows For Workgroups and HP OpenView For Windows are already installed. Be sure that OpenView is currently not running.

Installing the GDC TEAM 2B1Q Management System

To install GDC Team 2B1Q Management System software is distributed on diskettes. The installation is run from the Windows environment.

To install the GDC TEAM Software:

1.   Insert TEAM software diskette #1 in the disk drive.

2.   Start MS Windows 95 or Windows For Workgroups.

3.   For Windows 95, Click on the START Menu and select Run. For Windows For Workgroups, select File: Run from Program Manager.

4.   Type in **A:\SETUP**.

Follow the instructions that appear on the screen. You are alerted when installation is complete.

5.   Start HP OpenView and proceed to the next section, *Getting Started.*

Getting Started

Setting Up OpenView Passwords

The Set Password command lets you grant access to parts of OpenView through the assignment of security levels. There are three security levels:

Supervisors have access to all OpenView features including the editing of maps and setting of passwords.

Operators have access to all OpenView features except the setting of passwords.

Observers are able to view information only.

To set a password for each security level:

1.   From the Options menu select the Set Password option.

The Set Password dialog box appears.

2.   Select a security level, i.e., Supervisor, Operator, or Observer.

3.   Type in a password.

        You must confirm your entry.

4.   Click on the OK button.

After you start OpenView, the Log In dialog box appears prompting you to select a security level and enter a password if one was assigned for that level. You can select the Log In menu option at any time to log in at a different security level.

To disable all menu items, except Autodiscovery, and lock the map:

1.   From the Options menu, select the Log Out option.

        The only menu option that is functional (not grayed) is Log In in the Options menu and the Help menu.

Configuring GDC SpectraComm Manager Card (SCM)

Initial Setup

To communicate with the GDC SCM some initial configuration may be required using an ASCII terminal.

1.   Connect ASCII terminal to SCM front panel jack. The terminal must be set to 9600 bps, no parity, 8 data bits and 1 stop bit (9600 N-8-1).

2.   Select Option (1) IP address <ENTER>

3.   Select Option (2) Ethernet Interface <ENTER>

4.   Type SCM IP Address (ie.192.9.200.10) <ENTER>

5.   Type Subnet Mask (i.e... 255.255.255.0)<ENTER>

Creating A Map and Monitoring Your Network

You can create a map and monitor your network using HP OpenView's Autodiscovery, Polling, and the Trap Manager.

To create a network map and then monitor your network:

1.   Configure Autodiscovery:

        a.   Select *Discovery Networks* from *Configure* in the Autodiscovery menu.

        b.   Ensure that there is at least one network listed in the Networks box for IP discovery and that the Discover All IPX Networks check box is checked for *IPX discovery*.

        c.   Ensure that the correct Subnet Mask is entered.

        d.   Ensure that there is a valid address for the IP Default Gateway.

        e.   This must be a device that has an ARP cache table, e.g., a router, some types of bridges, etc. If the device's Community Name is not *public*, select *Customize Device Access* in the OpenView Options menu and change it to *public.*

Note	*If you specified a DNS (Domain Name Server) during TCP/IP setup, OpenView discovery will use names for network nodes otherwise the name will be the IP address of the device.*

2.   Start Autodiscovery:

   a.   Select *Discovery Manager* from *Discover* in the Autodiscovery menu.

   After a few seconds, 'Idle: Start in 10 minutes,' appears in the Status Bar.

   b.   Click on *Start Discovery.*

Note	*Messages in the Status Bar indicate the progress of Autodiscovery and the devices that are being added to the database.*

3.   Perform a Layout:

   a.   Wait until the Status Bar displays the message *Idle* then select *Do Basic Layout* from *Layout* in the Autodiscovery menu.

   b.   When the layout is completed, select *Save As* from the *File* menu to save the map.

4.   Start Polling your network:

   a.   Select one or more devices in the map, or select a submap.

   b.   Select *Add Device(s)* from *Polling* in the Monitor menu to start the polling process.

   c.   Select *Start Polling* from *Polling* in the Monitor menu. After a few seconds you see the selected nodes turning green or red, indicating their status.

5.   Monitor Trap alarms (optional) as follows:

   a.   Follow the manufacturer's instructions for providing the device with OpenView's network address.

   b.   When OpenView receives Traps entries are made automatically in the alarm log.

Note	*You may wish to increase the time interval in which autodiscovery is performed. The default time is every 10 minutes. If your Network is not changing often, unnecessary network traffic is generated.*

Configure ALARM Subsystem

Alarms (SNMP) Traps from the UAS system components are generated from the SCM (Proxy device). Traps from the SCM are logged in the HP Alarm Log in a raw format with no description as to which unit and what type of trap occurred. In order to determine which slot unit actually sent the alarm and the specific trap type, the UAS software runs an invisible background program to intercept SCM traps, decode them and place them in the HP Alarm Log.

Since the raw trap entries in the OpenView alarm log provide little meaning, they should be filtered out of the display. Use the following steps to filter these raw traps from the OpenView Alarm Log.

1.   Click on OpenView Monitor menu

2.   Select Customize Traps

3.   Select Option button Add Device Class

4. In the list box, select GDC SCM (Alarm) and then choose OK. This entry will now appear in the Device Class list box.

5. Select this entry from the Device Class list box, and then select Option button Ignore Device Class

6. Select the OK button to close the window

In order for traps to be recorded, the SCM must be configured to forward traps to your PC. This configuration is discussed in the section *SCM Configuration.*

Support

For information concerning software maintenance service, contact your local sales representative or Service Marketing at (203) 574–1118.

General Help

If the system does not work:

1. Review the setup and configuration of the PC hardware. If this addressing conflicts with existing options installed on your PC, either remove the existing options or readdress them.

2. Ensure that DOS boots. If not, consult your DOS documentation.

3. Ensure that MS Windows For Workgroups starts. If not, consult your MS Windows For Workgroups documentation.

4. Ensure that you have correct versions of DOS and MS Windows For Workgroups: MS/PC DOS version 6.0 or higher, and MS Windows For Workgroups 3.11 or higher.

5. Check the size of the DOS partition on the C drive. It must be a minimum of 16 Megabytes.

6. View AUTOEXEC.BAT and CONFIG.SYS files. Ensure that they contain the proper commands.

7. If the HP OpenView for Windows rel 7.2B fails to operate after performing steps 1 – 5, check for proper PC operation by running diagnostic routines if provided with your PC.

   For further information consult your HP OpenView User's manual.

Online Help

The TEAM Manager contains online help. Press F1 at any time if you need further information on a particular window. There is also a Help menu on all application windows.

TEAM 2B1Q System Overview

The SCM acts as an SNMP agent for the devices in the SpectraComm shelf. As such it provides the necessary translation of the SNMP packets to the proprietary backplane communication protocol and vice versa. User application components use MIB variables to retrieve and set values on the devices. The alarms from these devices are first sent to the SCM which then sends them to the Manager via SNMP Traps.

Figure 2-1 illustrates a sample flow of system operation. Here the HP OpenView for Windows main window is illustrated. From this window you can access the HP OpenView alarm utility. To get to an SCM you may need to traverse several levels. This can be done by double clicking on the icons in each screen.

When the SCM icon is located, to start the system:

1. Click on the SCM icon to highlight it.

    If you skip this step and perform step number 2, an error results with the message, No map object selected. *Should this occur, begin at step 1.*

2. Double click on the icon to start the application.

<div align="center">or</div>

Select the GDC Shelf option on the Control menu off the HP OpenView menu.

Note   *Either of these actions opens the GDC Shelf window that contains the SCM in that shelf. From this window you can select options indicated in Figure 2-1.*
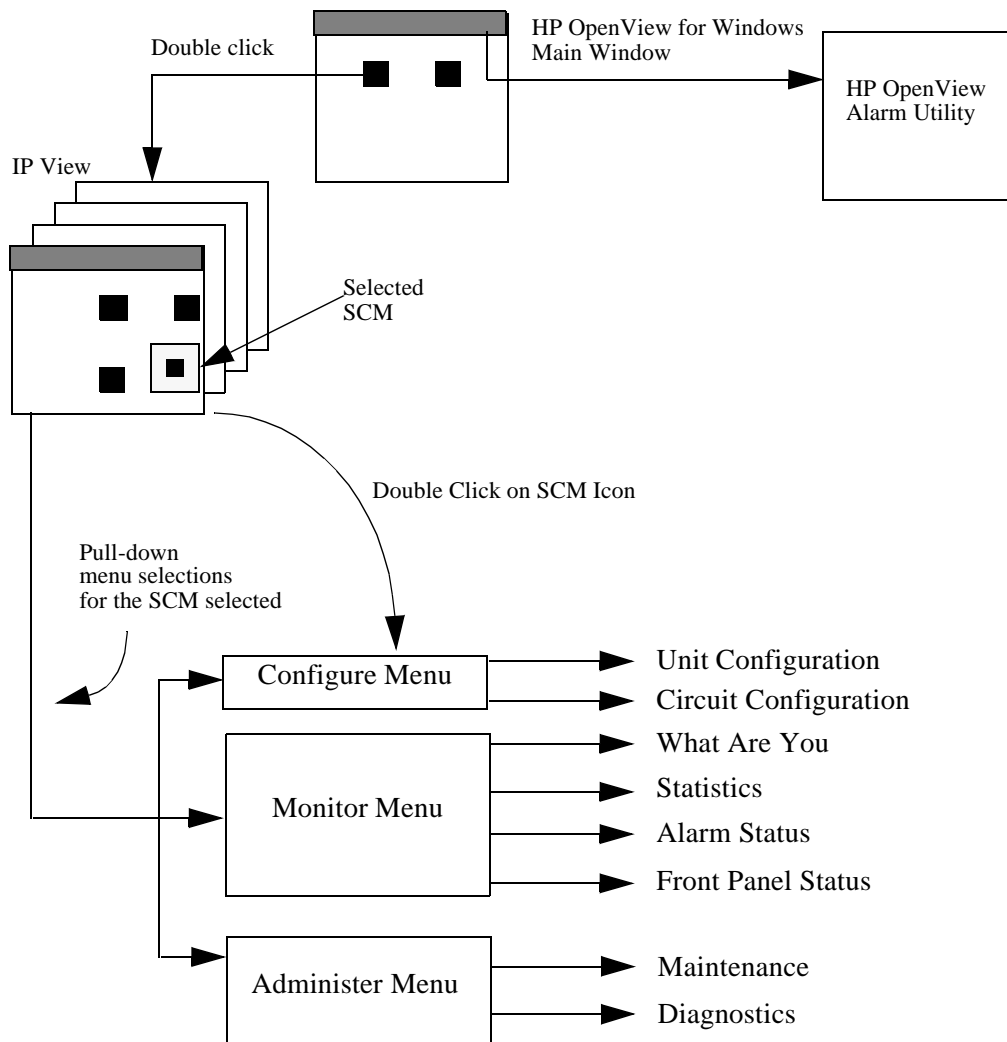
Figure 2-1   System Flow

GDC Shelf Application

The GDC Shelf application is a graphical representation of an actual equipment shelf. It is used as the main launching point for other applications such as configuration, monitoring, and administrative functions. To start the GDC Shelf Application, select a SCM icon in the HP OpenView map, and double-click on the icon.

The images of the card slots are selectable by clicking on them with the mouse. Once a card image is selected, the functions located on the top level menu are enabled depending on the particular unit selected. Not all menu options apply to all units. If there are any remote units associated with a particular unit, they appear in the Remotes listbox. These images which represent the remote units are also selectable, and the top level menu functions that apply to that unit type are enabled.

The GDC Shelf application contains the following menu items:

`File`

> **Load Shelf** - refreshes the contents of the shelf display. The SCM is queried for the current shelf contents as well as the alarm states of the individual units.
>
> Exit - dismisses the window and closes the application.

`Edit`

> **Delete** - Deletes the selected unit from the graphical display, and informs the SCM that the unit is no longer in service.
>
> **Delete All Inactive** - Deletes all inactive units from the graphical display, and informs the SCM that they are no longer in service.

`Configure`

> **Circuit Configuration** - Opens the Circuit Configuration application whereby remote units can be added to a unit.
>
> **Unit Configuration** - Opens the Unit Configuration window whereby the current operating characteristics of a unit can be selected.
>
> **Local Alarms** - Opens the Local Alarm application for the unit. This is used to mask or set the severity of the alarms that can trigger the Local Alarm Card for alarm display on a light panel.
>
> **System Configuration** - Opens the System Configuration application. This is used to setup highway assignments and system timing for the cards in the shelf on a system basis.

`Monitor`

> **What Are You** - Opens the What Are You application. This applications displays identification and version information for the unit.
>
> **Statistics** - Opens the Statistics application. The application displays time-stamped tabular statistics that have been accumulated by the unit.
>
> **Call Statistics** - Opens the Call Statistics application. This application displays switched network call statistics.
>
> **Status** - Opens the Status application. This application displays the status of certain operating functions and the state of certain DTE signals.
>
> **Alarm Summary** - Opens the Alarm Summary application. The current state of the units alarms are displayed and the ability to disable reporting and selecting thresholds of alarms can be selected.
>
> **Front Panel Status** - Opens the Front Panel Status application. This application is an enlarged graphical representation of the units front panel. The state of the LED's are displayed. This is also an alternate launch point for applications regarding this unit.

```
Administer
```

Diagnostics - Opens the Diagnostic application for the unit and any associated remotes. Various diagnostics tests can be performed depending on the unit type.

Upgrade Firmware - Opens the Upgrade Firmware window. This application allows firmware to be downloaded to units which support flash upgradeable PROMs.

Maintenance - Opens the Maintenance application. Various administrative functions such as resetting the unit can be performed.

Dial/Terminate - Opens the Dial/Terminate window. For units that support dialing, switched network calls can be initiated and terminated.

Service States - Opens the Service State window. This allows certain unit types to be put into or taken out of service.

NOTE: For units that contain multiple products on one card i.e. dual V.34 modem, the menu items will be modified to include an entry for each separate product. For example there would be two entries for Unit Configuration: Unit Configuration A and Unit Configuration B.
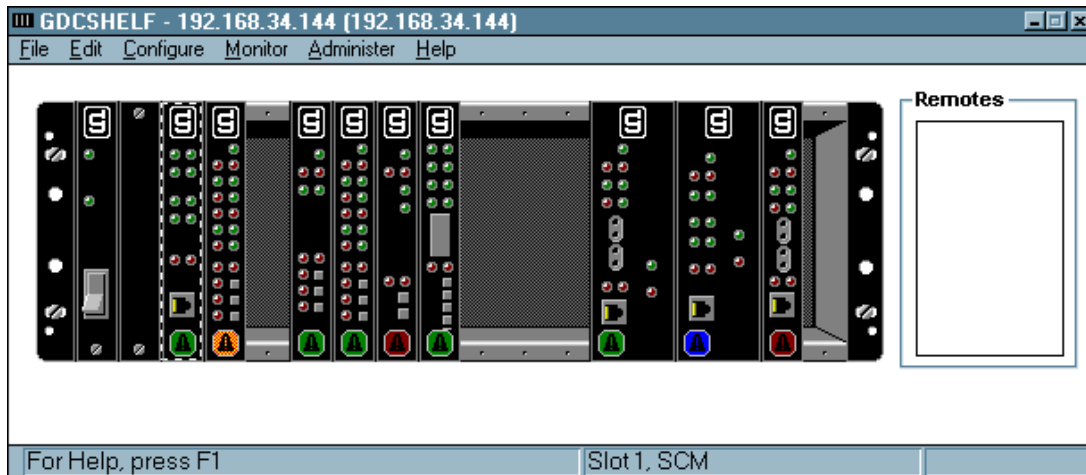
Figure 2-2   GDC Shelf Window

The GDC Shelf application displays the highest severity alarm for every unit. This is displayed by the colored alarm image at the bottom of the slot images. If traps have been forwarded to the Network Manager, then these images update in real-time, otherwise they are updated approximately every 10 minutes.

3 SCM Configuration

Introduction

The SCM Configuration application lets you configure the SCM Community Name and Trap Destination Table options. You can access the other MIB2 system group, the Ethernet group, and GDC common MIB via the HP OpenView MIB browser. Later in this section the topic *Communications* presents some sample configurations which use an SCM.

Setting Up the SCM

Before you can access the SCM, you must do the following.

1.   Double click on the SCM icon in the HP OpenView map.

      This opens the GDC Shelf window.

2.   Select the SCM card image.

3.   From the Configure menu select the `Unit Configuration` option.

      This opens the Administration Password window (*Figure 3-1*).

4.   Type in the password, then click on the `OK` button. (The default provided by GDC is sc-madmin.)

      Note that if you want to use the Community Name set using the Customize Device Access option in OpenView for this SCM, just click on the `OK` button.

      If you do not type in a password, you can only set the Trap Address options. You are unable to change the Community Names. In this case, to set the Community Names you must use the Administration Password. The password field is case sensitive. You may enter up to 36 characters.

      The community name option tab appears.

5.   You may set up the IP Trap Address if desired.

      For further information, *refer to the topic entitled Trap Address Options in this chapter.*

6.   From the View menu select `Community Names Options`.

      This opens the Community Name Options window.

7.   In this window set the Community Name.

      For further information, *refer to the topic entitled Community Names Options in this chapter.*

8.   From the File menu select the `Exit` option.

9.   Proceed to the HP OpenView map and click once on the SCM icon to select it.

10.   From the Options menu select the `Customize Device Access` option.

      This opens the Customize Device Access window.

11.   Click on the `Add` button.

12. A window opens, displaying the following fields:

    IP Address of the SCM

    Community Name

    Set Community Name (Be sure the name has both read/write privileges.)

    Enter the appropriate information.

13. Enter the appropriate information in the Retries and Timeout fields. In the Proxy Agent field enter No.

14. Click on the OK button.

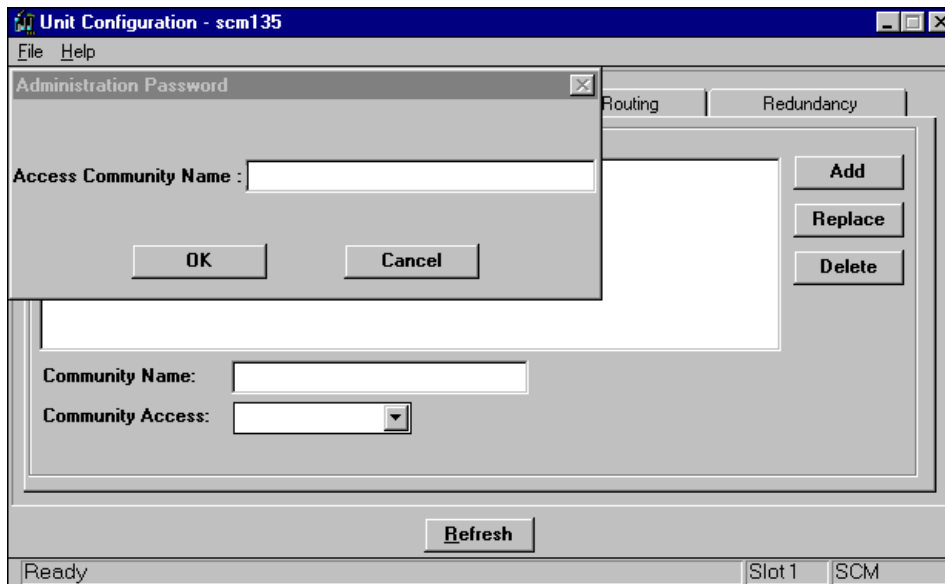   This adds the SCM to the Customize Device Access Table. You may view it using the Customize Device Access window.

Figure 3-1 Administration Password Window

Community Names Options

Community Names are used in SNMP to restrict access to an agent. You can define a Community Name to permit both read and write or just read access to MIB variables using the Community Name Options window (*Figure 3-2*).

The SCM lets you add, delete, and view Community Names in a table. The SCM can store up to five Community Names, each with its associated access. Access in the SCM can be defined as read-only, read-write, or No Access. Status is used to delete a Community Name from the table. A special Community Name, scmadmin, is required to add and delete entries from the table. It acts as a super user Community Name. This Community Name is hidden and can only be changed from the front panel port on the SCM. For further information, *refer to your SCM documentation.*

When the SCM is initially powered up it contains one default Community Name with read-only access, public. This default can be removed or changed.

Note	*You must have at least one Community Name with read-write access set in the Community Name Table before you can set any other MIB objects using the SCM. Use the Administration Community Name to set the first privileged Community Name, then use that Community Name to set all other MIB objects.*

To add a Community Name:

1. Double click on the SCM icon in the HP OpenView map.

    This opens the GDC Shelf window.

2. Select the SCM card image from the shelf.

3. From the Configure menu select the Unit Configuration option.

    This opens the Administration Password window.

4. Type in the password then click on the OK button.

    The Trap Address Options window opens.

5. From the View menu of the Trap Address Options window, select Community Names Options.

    This opens the Community Names Option TAB.

6. Click the pointer in the Community Name field. When the cursor appears, enter the Community Name.

7. In the Community Access field choose an access level.

    This field determines the access that users have with regard to the Community. For example, if you select Read Write, users are able to both read and write the MIB variables of an agent.

8. Click on the Add button.

To edit a Community Name:

1.   Select the Community Name that you want to edit.

        Community Name information appears in the appropriate fields.

2.   Perform the desired changes.

3.   Click on the `Replace` button.

To delete a Community Name:

1.   Select the Community Name that you want to delete.

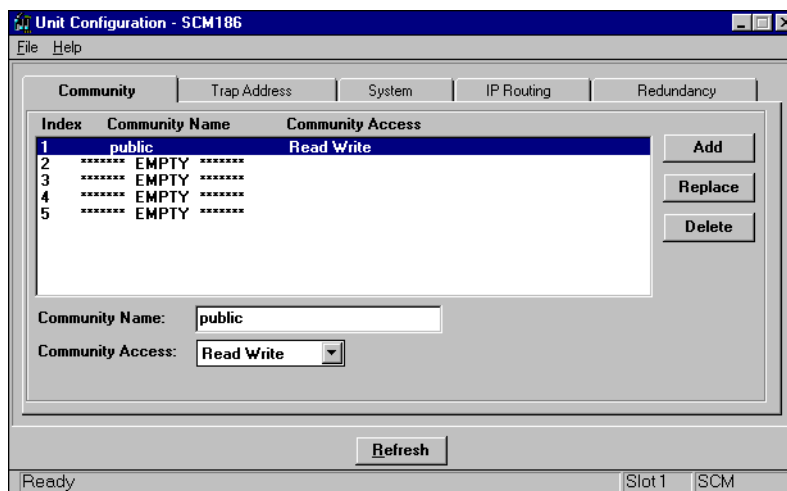2.   Click on the `Delete` button.

Figure 3-2   Community Name Options Window

Trap Address Options

Traps are used in SNMP to send unsolicited information to a network manager. The information usually consists of events or alarms sent to the network manager for reports or special processing.

The Trap Destination Table in the SCM, defined in a MIB, must be filled out if a network manager is to receive Traps. The SCM can store up to five Trap Destinations, which includes the IP Address and UDP port of the network manager.

The SCM Trap group is located in non-volatile RAM and therefore need not be recreated each time the SCM is powered up. The following information is defined in the Trap Address Options window (*Figure 3-3*):

    `Destination IP Address` – IP Address where the Trap is sent.

    `UDP Destination` – UDP port where the Trap is sent.

	The UDP field should normally be 162, the port number defined for SNMP. You
Note	*should change this only under special operating conditions such as a proxy*
	agent that listens for Traps on a different port number. Changes should only be
	performed by experienced administrative personnel.

`Community Name` – Community Name used when sending the Trap.
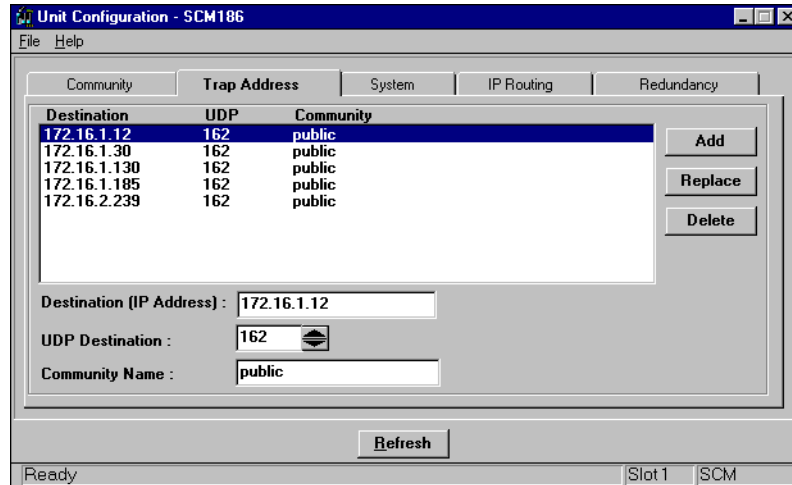
Figure 3-3   Trap Address Options Window

To add a Trap destination:

1. Double click on the SCM icon in the HP OpenView map.

   This opens the GDC Shelf window.

2. Select the SCM card image from the shelf.

3. From the Configure menu select the `Unit Configuration` option.

   This opens the Administration Password window.

4. Type in the password, then click on the `OK` button.

   The community name option tab appears. Click on the `TRAP` address tab.

5. In the Destination IP Address field enter the IP Address of the destination where traps are to be sent.

6. In the UDP Destination field, select the port used by the SNMP manager. The default of 162 should in most cases be used.

7. In the Community Name field enter the Community Name associated with the Trap destination.

8. In the Trap Global field enter `Enable` to allow all Traps in the display to be sent to their respective destinations. Enter `Disable` if you want to disable all Traps in the display from being sent to their respective destinations.

9. Click on the `Add` button.

To edit a Trap destination:

1. Select the Trap destination that you want to edit.

   Trap information appears in the appropriate fields.

2. Perform the desired changes.

3. Click on the `Replace` button.

To delete a Trap destination:

1. Select the Trap destination that you want to delete.

2. Click on the `Delete` button.

System Options

This option lets you designate information that is general to the system. The following information is defined in the System Options window (*Figure 3-4*):

`Contact` – is a text field that indicates the person, place or thing that you should contact in case of a problem.

`Name` – is a text field that indicates the person, place or thing that you would contact if there is a problem.

`Location` – is a text field that indicates the site of the Contact or Name field information.

`Description` – identifies the device with which you are in communication.

`Download Mode` – enables the SCM's firmware to be upgraded.

`Telnet Mode` – enables the SCM to accept Telnet sessions.
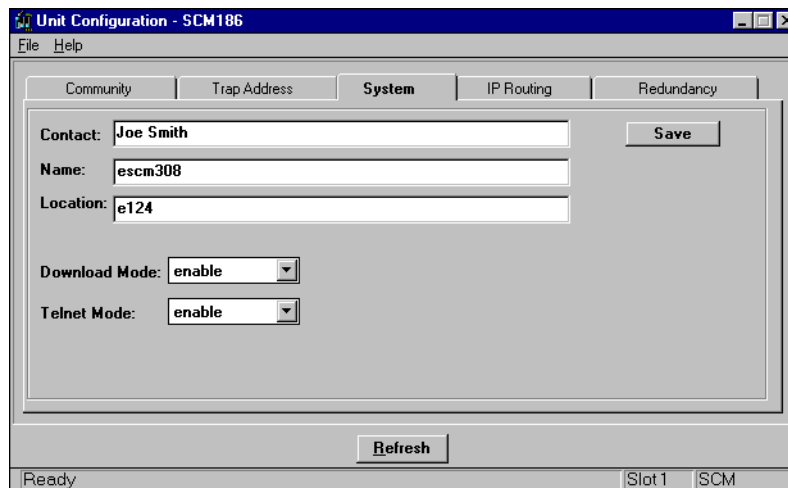
Figure 3-4 System Options Window

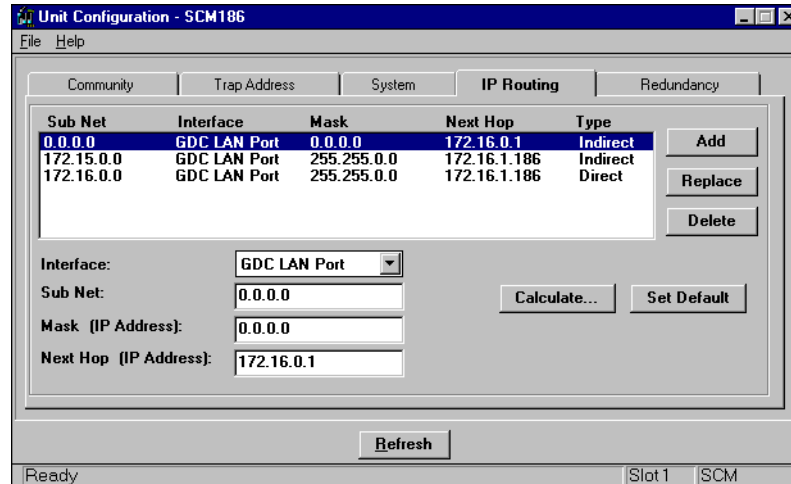To configure the System Options window:

1.   Double click on the SCM icon in the HP OpenView map.

      This opens the GDC Shelf window.

2.   Select the SCM card image from the shelf.

3.   From the Configure menu select the `Unit Configuration` option.

      This opens the Administration Password window.

4.   Type in the password, then click on the `OK` button.

      The community name options tab appears.

5.   Click on the `System Tab`.

6.   Click the pointer in the `Contact` field and when the cursor appears, enter the person, place or thing that you would contact in case of a problem.

7.   Click the pointer in the `Name` field and when the cursor appears enter the name of the person, place or thing that you would contact in case of a problem.

8.   Click the pointer in the `Location` field and when the cursor appears enter the site of the person place or thing.

9.   Click the pointer in the Download mode field. Change the selection to `disable` to disable downloading of new SCM code or leave it as `enable`.

10.   Click the pointer in the Telnet mode field. `Enable` permits Telnet functionality. `Disable` does not allow Telnet functionality.

11.   When finished, click on the `Save` button to save your input

IP Routing Options

This option lets you designate information that is general to the system. The following information is defined in the IP Routing window (*Figure 3-5)*:

`Interface` – indicates the routing interface type, i.e., LAN or WAN port.

`Sub Net` – identifies the network segment on which the target is resident. This field contains the following buttons:

- Calculate if the selected route is indirect, you may use the system to calculate Sub Net. A pop-up opens requesting the target/destination IP Address of the device. The system then ANDs this address with the mask to provide the proper Sub Net value. Alternatively, you may enter the valid Sub Net value directly. Note that if you are uncertain of the Sub Net value, use the system to calculate it.

- Set `Default` if the route type is direct, then use this to set the Sub Net value. The system ANDs the next hop address and the mask to determine the Sub Net.

`Mask` – used to divide IP Addresses into network identifier and host identifier. The bits set to `1` in the mask correspond to the network identifier. The entire network identifier portion must be contiguous and to the left of the host identifier portion.

For example:

```
        Some valid subnet masks are:

        255.0.0.0        Standard Class A network mask
        255.128.0.0      Class A network, 2 subnetworks
        255.192.0.0      Class A network, 4 subnetworks
        255.224.0.0      Class A network, 8 subnetworks

        255.255.0.0      Standard Class B network mask
        255.255.128.0    Class B network, 2 subnetworks
        255.255.192.0    Class B network, 4 subnetworks
        255.255.224.0    Class B network, 8 subnetworks

        255.255.255.0    Standard Class C network mask
        255.255.255.128  Class C network, 2 subnetworks
        255.255.255.192  Class C network, 4 subnetworks
        255.255.255.224  Class C network, 8 subnetworks

        Subnet mask      IP Address      Network Ident    Host
        Ident

        255.255.255.0    192.9.200.100   192.9.200.0       100
                         192.9.200.200   192.9.200.0       200

        255.255.255.128  192.9.200.200   192.9.200.0       200

        255.255.255.128  192.9.200.100   192.9.200.0       100
                         192.9.200.200   192.9.200.128      72

        255.255.255.192  192.9.200.100   192.9.200.64       36
                         192.9.200.200   192.9.200.192       8
```

Note	*This mask is the filter used to establish the Routing Table. It must be set by experienced system administrative personnel.*

`Next Hop` – specifies the IP Address of the next SCM.

`Route Type` – selects one of the following routing types:

- `Direct` – signifies that the target device is on the same segment.
- `Indirect` – signifies that the target device is not on the same segment.

Figure 3-5 IP Routing Window

To add an IP Route:

1.   Double click on the SCM icon in the HP OpenView map.

        This opens the GDC Shelf window.

2.   Select the SCM card image from the shelf.

3.   From the Configure menu select the `Unit Configuration` option.

        This opens the Administration Password window.

4.   Type in the password, then click on the `OK` button.

        The community name options tab appears.

5.   Click the `IP Routing` tab.

        This opens the IP Routing Options tab.

6.   In the IP Routing Options tab, select an interface type from the Interface field.

        In the Sub Net field enter the appropriate address.

        To calculate a Sub Net value you may use the `Calculate` button. To set the default, you may use the `Set Default` button.

7.   Click the pointer in the `Mask (IP Address)` and when the cursor appears, enter an IP Address.

8.   Click the pointer in the `Next Hop` field and when the cursor appears enter the address of the next hop.

9.   Select the appropriate route type from the `Route Type` field.

10.   Click on the `Add` button.

To edit an IP Route:

1.   In the IP Routing Options tab, select the item that you want to edit.

        IP Routing information appears in the appropriate fields.

2.   Perform the desired changes.

3.   Click on the `Replace` button.

To delete an IP Route:

1.   In the IP Routing Options tab, select the item that you want to delete.

2.   Click on the `Delete` button.

Redundancy Options

This option allows you to designate information that pertains to redundancy. The redundancy option is present with SCM application version 3.00 or higher. The options are described as follows:

`SCM Type` - this is read only information. Display values are Primary or Redundant.

`IP Address` - this is read only information. The IP address of the primary or redundant SCM is displayed.

`Alive Trap Interval` - this allows a value, represented in minutes, to be set for the SCM Alive Trap interval. A trap is sent from the SCM to a network manager every"n" minutes, based on this option. No trap is sent when the option is set to `disable`. The default is `disable`. This option applies to a primary and a redundant SCM.

`Redundant Timeout` - this option sets the redundant timeout value in seconds. It applies only to a redundant SCM. A redundant SCM will take control of the management bus when it stops receiving messages from the primary SCM based on the value of this option.

`Operating Mode` - this option is read only for a primary SCM. A redundant SCM can take immediate control of the management bus when this option is set to `active`. It can also give up control of the management bus by setting this option to `standby.`
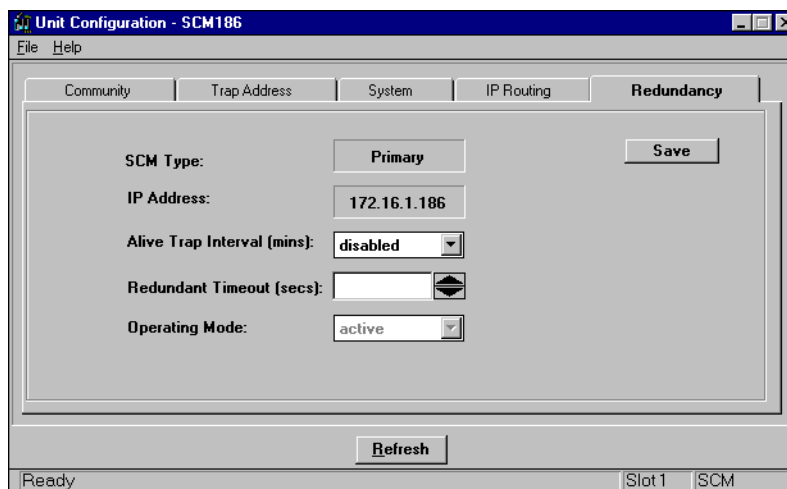
Figure 3-6   Redundancy Options Window

To configure the Redundancy Options windows:

1.   Double click on the SCM icon in the HP Open View map. This opens the GDC Shelf window.

2.   Select SCM card image from the shelf.

3.   Unit Configuration option. This opens the Administration Password window.

4.   Type in the password, then click on the OK button. The community name option tab appears.

5.   Click on the Redundancy Tab.

If the SCM Type is Primary, set the desired amount of time in minutes of the Alive Trap Interval field. If the SCM Type is Redundant, set the desired values of the Alive Trap Interval, Redundant Timeout and Operating Mode fields

Communications

The following is a discussion of some sample communication configurations.

SCM Communications via LAN

Figure 3-7 illustrates an installation where the 2B1Q manager and one or more SCMs are connected to the same LAN segment. Communication between network manager and SCM(s) occurs over Ethernet. Each SCM can communicate independently using its own set of MAC and IP Addresses. No routing of packets is required within the SCM. You should set IP Addresses of the manager and LAN ports of the SCM for the same subnetwork so that no SCM Gateway Address is required.
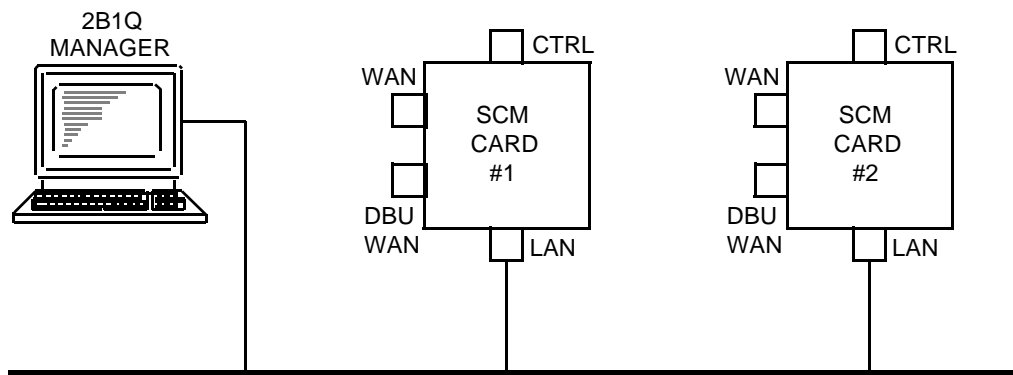

Figure 3-7 LAN-Based Manager Configuration

The following is an example of addressing for a DMS network manager and two SCMs:

```
2B1Q Manager

IP Address: 192.9.200.1

SCM #1

LAN IP Address: 192.9.200.2

Subnet Mask: 255.255.255.0


SCM #2

LAN IP Address: 192.9.200.3

Subnet Mask: 255.255.255.0
```

Manager Communications via LAN

Figure 3-8 illustrates an installation where the 2B1Q manager and an SCM are connected to different LAN segments. Communication on the Ethernet between network manager and SCM must pass through the router, which acts as the gateway between the two LAN segments. You should set the IP Address of the DMS network manager to its own subnetwork and the LAN port of the SCM to its own subnetwork. The SCM requires a Gateway IP Address which is the IP Address of the router.
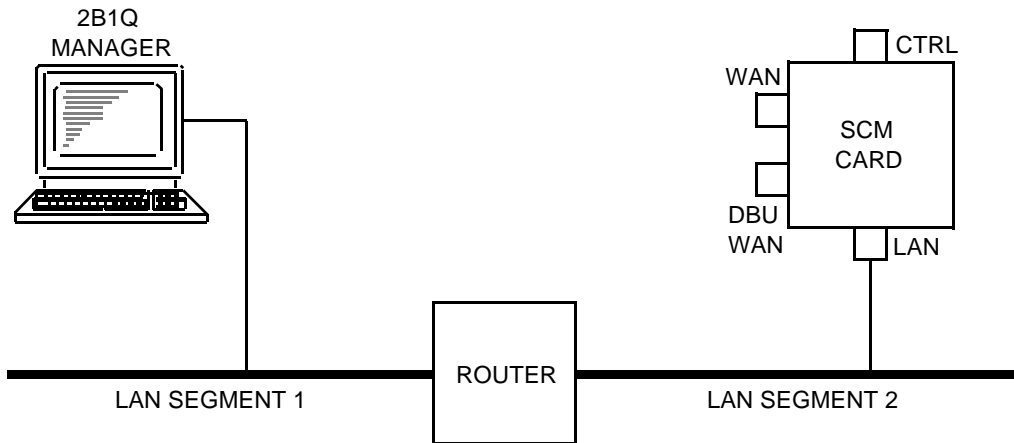
Figure 3-8   Segmented LAN-Based Manager Configuration

The following is an example of addressing in this type of installation:

```
Router

LAN Segment 1 IP Address: 192.9.200.40

LAN Segment 2 IP Address: 192.9.100.40


SCM

LAN IP Address: 192.9.100.3

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.9.100.40

Gateway Subnet Mask: 0.0.0.0
```

2B1Q Manager to SCM Communications via WAN

Figure 3-9 illustrates an installation where the 2B1Q manager communicates with one or more SCMs by WAN connections. Each SCM communicates with the manager independently, using its own IP Address and employing Point-to-Point Protocol (PPP). No packet routing is required within the SCM. You should set the IP Addresses of the 2B1Q manager and the WAN port of the SCM to the same subnetwork. This foregoes the need for a SCM Gateway Address.
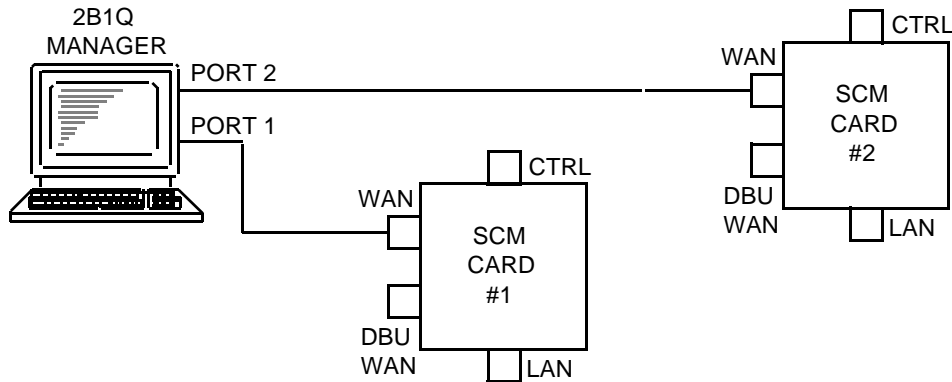
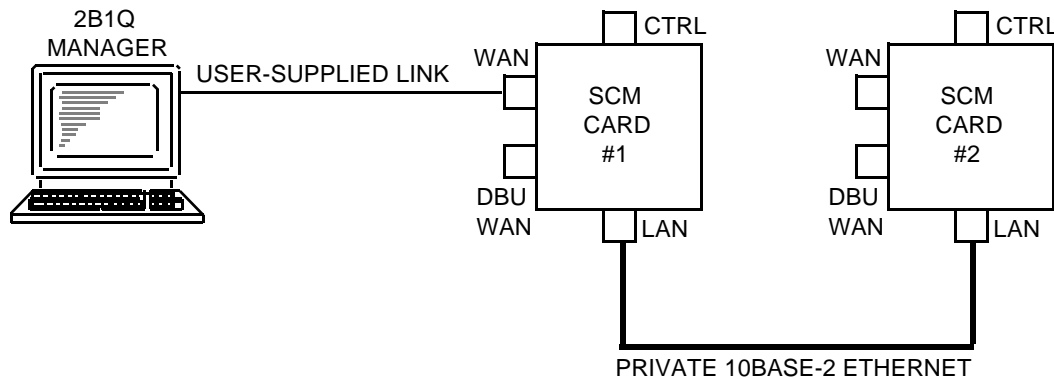**Figure 3-9**   Local WAN Configuration

The following is an example of addressing for a 2B1Q manager and two SCMs in this type of installation:

```
2B1Q Manager

Port 1 IP Address: 192.9.10.1

Port 2 IP Address: 192.9.20.1


SCM #1

WAN IP Address: 192.9.10.2

Subnet Mask: 255.255.255.0


SCM #2

WAN IP Address: 192.9.20.3

Subnet Mask: 255.255.255.0
```

Manager Communications via WAN with DBU

Figure 3-10 illustrates an installation where the SNMP network manager communicates with an SCM via a WAN connection with provision for use of a Dial Backup (DBU) WAN connection. WAN and DBU WAN ports share common resources on the SCM. Only one can be active at a time. If a PPP session is in progress through the WAN port, when the DCD signal of the DBU WAN port goes active, the existing session is interrupted. A new PPP session must be established each time the state of DCD changes at the DBU WAN port. You should set the IP Addresses of the manager and the WAN ports of the SCM WAN for the same subnetwork. This foregoes the need for an SCM Gateway Address.
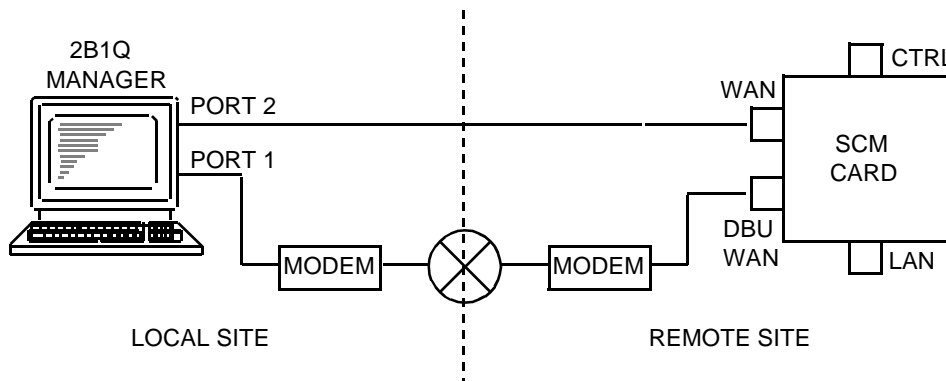
Figure 3-10 WAN Configuration with Dial Backup

The following is an example of addressing for a 2B1Q manager and an SCM in this type of installation:

```
2B1Q Manager

Port 1 IP Address: 192.9.10.1

Port 2 IP Address: 192.9.10.2


SCM

WAN IP Address: 192.9.10.3

Subnet Mask: 255.255.255.0
```

Note   *SCM uses the WAN IP Address for both the WAN and DBU WAN ports.*

Single WAN Link to Multiple SCM Cards

Figure 3-11 depicts an installation where the 2B1Q manager communicates with one SCM via a WAN connection and, through a private 10Base-2 Ethernet link, with one or more SCMs connected to the first. This illustration demonstrates the ability of the SCM to route packets to destinations other than to itself.

Since SCMs downstream on the Ethernet do not receive their IP Addresses through Autodiscovery, you must enter them. The routing SCM, the one with WAN connection, serves as the gateway for downstream SCMs. As a result, the IP Address of the routing SCM must be entered as the Gateway IP Addresses of downstream SCMs.

Figure 3-11 WAN Configuration With Multiple SCMs

The following is an example of addressing for a 2B1Q manager and two SCM cards in this type of installation:

```
2B1Q Manager
IP Address: 192.9.10.1


SCM #1
LAN IP Address: 192.9.200.2
Subnet Mask: 255.255.255.0
WAN IP Address: 192.9.10.2
Subnet Mask: 255.255.255.0


SCM #2
LAN IP Address: 192.9.200.3
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.9.200.2
```

4 Unit Configuration

Introduction

The devices that the UAS supports must be configured. You can access the various applications for configuring these devices using the GDC Shelf display. You will use the following options from the Configure menu when configuring a device:

- Unit Configuration - opens a window that lends access to unit configuration. This window lets you display and modify 2B1Q parameters.
- Circuit Configuration - opens a window that lets you add or delete a remote unit.

Circuit Configuration

To add a remote unit:

1. Select a unit from the GDC Shelf display.

2. From the Configure menu select the `Circuit Configuration` option.

   This opens the Circuit Configuration window for the unit. The unit is queried for information which is displayed in the window. *See Figure 4-1, below.*
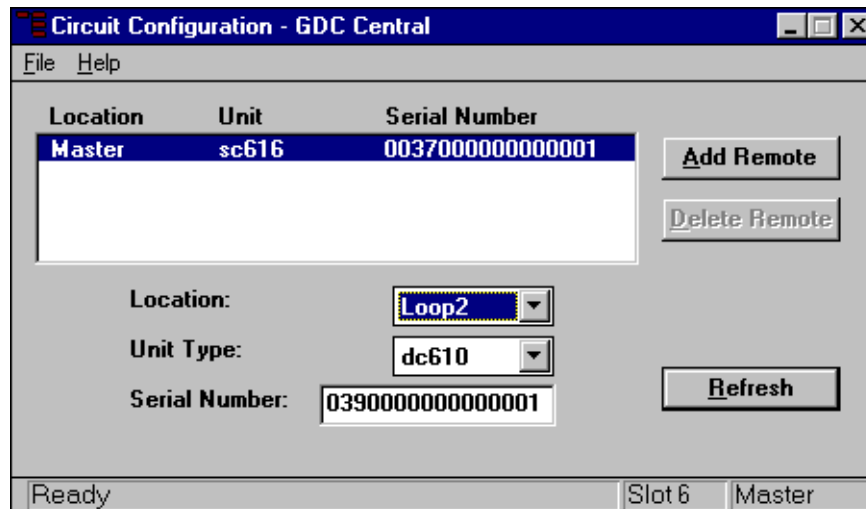
Figure 4-1 Circuit Configuration Window

3.   Enter the appropriate information in the fields as follows:
   •   Location - indicates the circuit location.
   •   Unit - indicates the unit type.
   •   Serial Number - enter the serial number of the unit.

4.   Click on the Add Remote button.

      The addition appears in the display.

To delete a remote unit from a circuit:

1.   Select a unit from the GDC Shelf display.

2.   From the Configure menu select the Remote Configuration option.

      This opens the Circuit Configuration window for the unit. The unit is queried for information which is displayed in the window.

3.   Select the unit in the display that you want to delete.

4.   Click on the Delete Remote button.

      The deletion is removed from the display.

Unit Configuration

To configure a unit:

1.   Select a unit from the GDC Shelf display.

2.   From the Configure menu select the Unit Configuration option.

      You can also select the this option from the Front Panel Status application using the Configure menu item.

      This opens the Unit Configuration window for the unit. The unit is queried for information which is displayed in the window. If at any time you want to update the window, click on the Load button. *See Figure 4-2, below.*
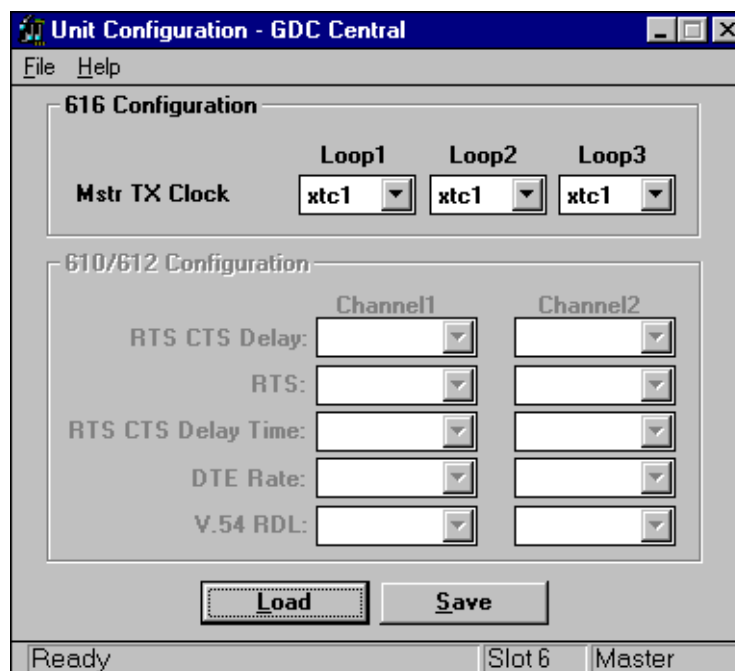
Figure 4-2   Unit Configuration Window

3.   Enter the appropriate information in the fields as follows:

616 Configuration

•   `Mas TX Clock Mode` - indicates the source (xtc1, xtc2) of the loop master trans-
     mit clock.

610/612 Configuration

•   `RTS CTS Delay` - selects whether there is or is not an RTS/CTS delay for a given
     channel. Selections are:

         1.   No Delay = no delay between RTS/CTS.

         2.   Delay = allows channel to have delay for RTS/CTS (see delay times).

•   `RTS` - selects whether RTS is normal or forced for a given channel. Selections are:

         1.   Normal = channel RTS follows DTE RTS.

         2.   Forced = channel RTS is forced on.

•   `RTS/CTS Delay Time` - the delay time is selectable from 0 to 75 ms.

•   `DTE Rate` - the DTE rate is selectable for 64kbps or 128kbps.

•   `V.54 RDL` - Remote Digital Loopback pattern selection.

613 Configuration

See Figure 4-3, below.
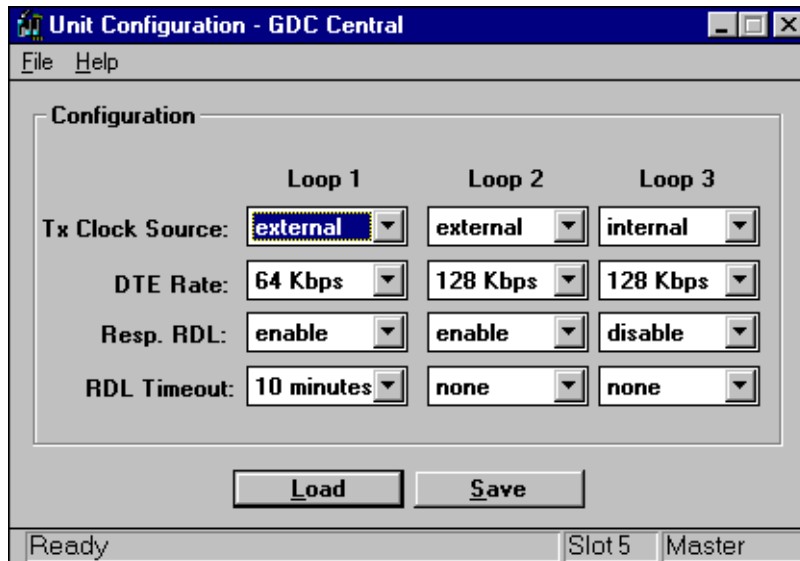
Figure 4-3   SC613 Unit Configuration

•   `TX Clock Source` - Option for the loop master transmit clock source.

•   `DTE Rate` - Options the DTE interface to a K-bit per second rate.

•   `Resp. RDL` - Selects loop remote loopback response.

•   `RDL Timeout` - Selects loop remote loopback time-out.

611 Configuration

See Figure 4-4, below
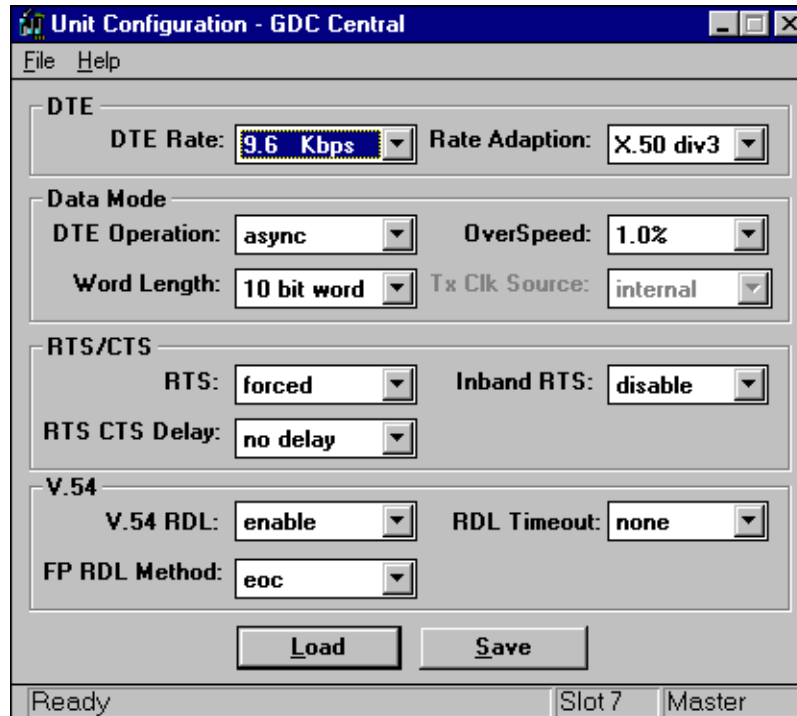
Figure 4-4   SC611 Unit Configuration

DTE

- DTE Rate - Options the DTE interface to a K-bit per second rate.

- Rate Adaption - Selects DTE rate adaption scheme.

Data Mode

- DTE Operation - Selects DTE mode of operation.

- Word Length - Selects the word length for async operation.

- OverSpeed - Selects overspeed for async operation.

- Tx Clk Source - Option for the loop master transmit clock source.

RTS/CTS

- RTS - Selects source of RTS.

- RTS CTS Delay - Selects RTS-to-CTS delay.

- Inband RTS - Selects source of DCD.

V.54

- V.54 RDL - V.54 to apply RDL configuration method.

- FP RDL Method - Selects the front panel RDL method.

- RDL Timeout - Selects loop remote loopback time-out.

621 Configuration

See Figure 4-5, below.

Figure 4-5 DC621 Unit Configuration

DTE

- DTE Rate - Options the DTE interface to a K-bit per second rate.

- Rate Adaption - Selects DTE rate adaption scheme.

Data Mode

- DTE Operation - Options the DTE interface to a K-bit per second rate.

- Word Length - Selects the word length for async operation.

- OverSpeed - Selects overspeed for async operation.

RTS/CTS

- `RTS` - Selects source of RTS.

- `RTS CTS Delay` - Selects RTS-to-CTS delay.

- `Inband RTS` - Selects source of DCD.

V.54

- `V.54 RDL` - V.54 or PN 127 to apply RDL configuration method

- `FP RDL Method` - Selects the front panel RDL method.

- `RDL Timeout` - Selects loop remote loopback time-out.

4. To save your input, click on the `Save` button.

The following rules apply to the DC621 Unit Configuration Screen:

1. If DTE Operation is set to `Sync`, Word Length and Overspeed are irrelevant.

2. If DTE rate is set to `64` or `128` kbps:

    - Word Length, Overspeed and Rate adaption method are irrelevant.

    - DTE Operation, Async selection is not allowed.

3. If DTE Rate is set to `48` kbps:

    - Word Length and Overspeed are irrelevant.

    - DTE Operation, Async selection is not allowed.

5 Monitor

Introduction

The Monitor function contain the following applications:

- What Are You - displays general information associated with the unit, e.g., Firmware level.

- Statistics - displays loop statistics associated with the unit.

- Alarm Summary - opens an alarm summary window that lets you monitor the state of alarms associated with the unit and permits reporting or masking of these alarms.

- Front Panel - opens a graphic display of the unit's front panel.

What Are You

This application identifies and provides information on the selected unit. *Figures 5-1 through 5-4* show you the What Are You screens for the 616 (Remote options apply to 610 and 612 units), 613, 611, and 621 units respectively. To open the What Are You window:

1. Select a unit from the GDC Shelf display.

2. From the Monitor menu select the `What Are You` option.

   You can also select this option from the Front Panel Status application using the Monitor menu item.

This opens the What Are You window for the unit. The unit is queried for information which is then displayed in the window. To update the window, click on the `Refresh` button.

3. You see four fields on these units:

   - `Product Type` - identifies the product, such as SC616.

   - `Firmware Rev` - identifies the level of firmware.

   - `Serial Number` - identifies the serial number of the unit.

   - `MIB Version` - indicates the MIB version associated with the unit.

   For Units 611 and 621, however, an additional field is displayed:

   - `DTE Card Type` - returns the plug-in DTE card type.

   Remote Options

   - `Option Card` - indicates whether or not an option card is installed.

   - `DTE1 Card Type` - identifies the installed DTE1 Card type.

   - `DTE2 Card Type` - identifies the installed DTE2 Card type.

Figure 5-1   SC616 Unit, What Are You Window
(Remote options apply to the DC610 and DC612 units.)

Figure 5-2   SC613 Unit, What Are You Window

Figure 5-3 SC611 Unit, What Are You Window

Figure 5-4 SC621 Unit, What Are You Window

Statistics

This application accumulates 2B1Q loop statistics for the unit. It can hold up to 24-hours of information. The window presents the information in one hour intervals. To open the Statistics window:

1.   Select a unit from the GDC Shelf display.

2.   From the Monitor menu select the `Statistics` option.

      You can also select this option from the Front Panel Status application using the Statistics menu item. This opens the Statistics window for the unit. The unit is queried for information which is then displayed in the window. To update the window, click on the `Refresh` button. *See Figure 5-5, below.*

Figure 5-5   Statistics Window

3.   The following fields appear:

      •   `Category` - indicates the category of the information. You can select the desired category using this field. Categories are: Loop 1, Loop 2, and Loop 3.

      •   `Statistics` - indicates the type of statistic displayed, e.g., Errored Seconds. The options available in this field are dependent upon the option selected in the Category field.

If you select `Loops` 1, 2, or 3 as the Category, the following options are available in this field:

•   `ES` - defined as a second with at least one CRC error event.

•   `SES` - defined as a second with 7 or more CRC error events, or one or more Out Of Frames (OFF).

•   `UAS` - defined as a count of one second intervals when service is not available. Service not available means 10 or more consecutive SESs.

•   `Last 24 Hours` - indicates the 24-hour total for the selected statistic. Note that the total does not include the current 15-minute interval.

Note   *The asterisk denotes the current interval.*

Alarm Summary

This application displays alarm status conditions of the unit. You can also use this window to select those alarms that you want reported and those you do not. The window contains colored text that indicate the state of an alarm., i.e., red indicates an alarm, green indicates no alarm. The Interface drop-down menu lists the loops associated with that particular slot; so, only alarms associated with the selected interface are displayed, e.g., Loop 1 displays alarms associated with Loop 1. *See Figures 5-6 through 5-11 below, which display alarm summary windows for Units 616, 611, 613, 610, 612, and 621 respectively.*
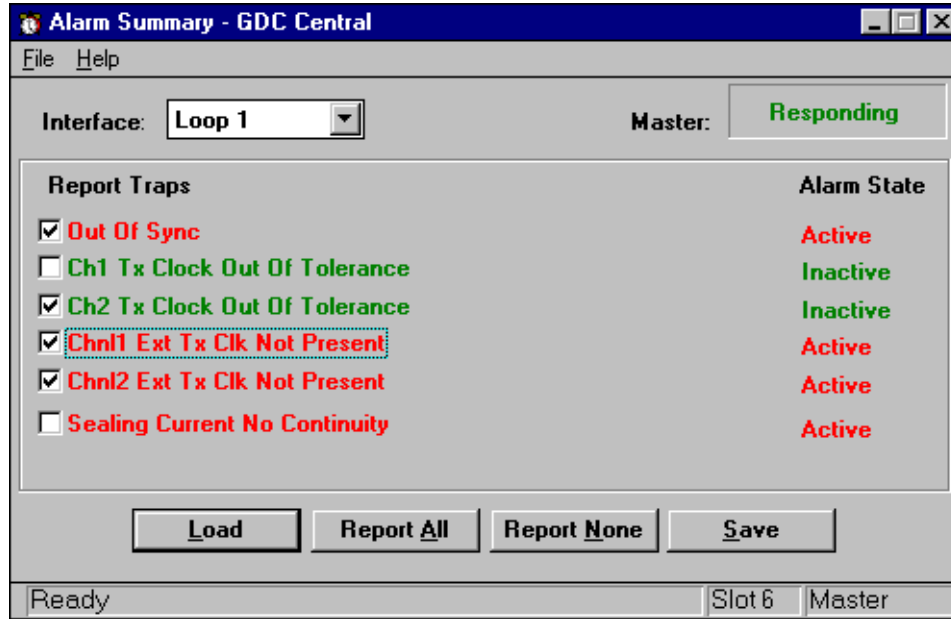
Figure 5-6   Alarm Summary Window, Unit SC616
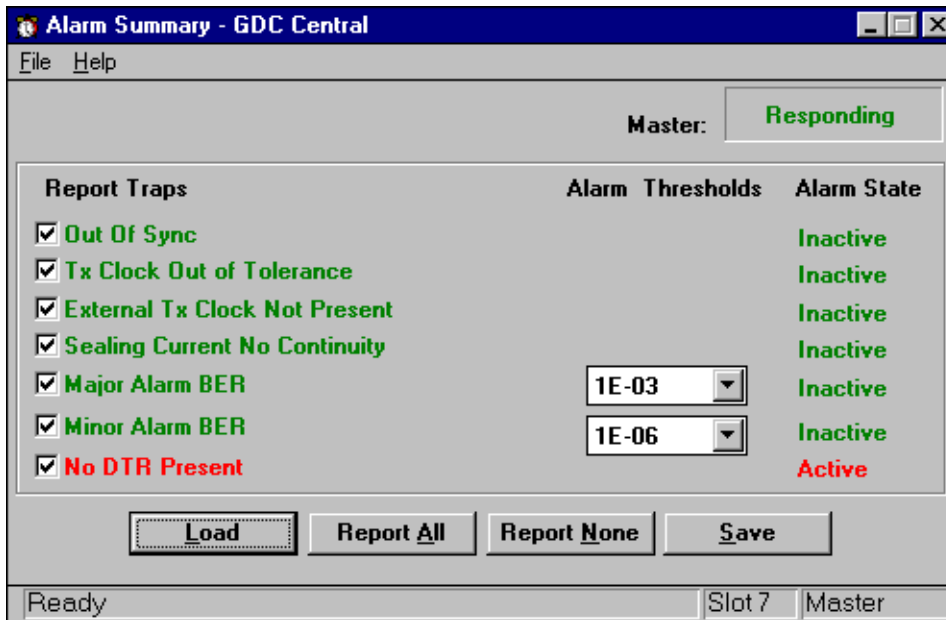
Figure 5-7   Alarm Summary Window, Unit SC611
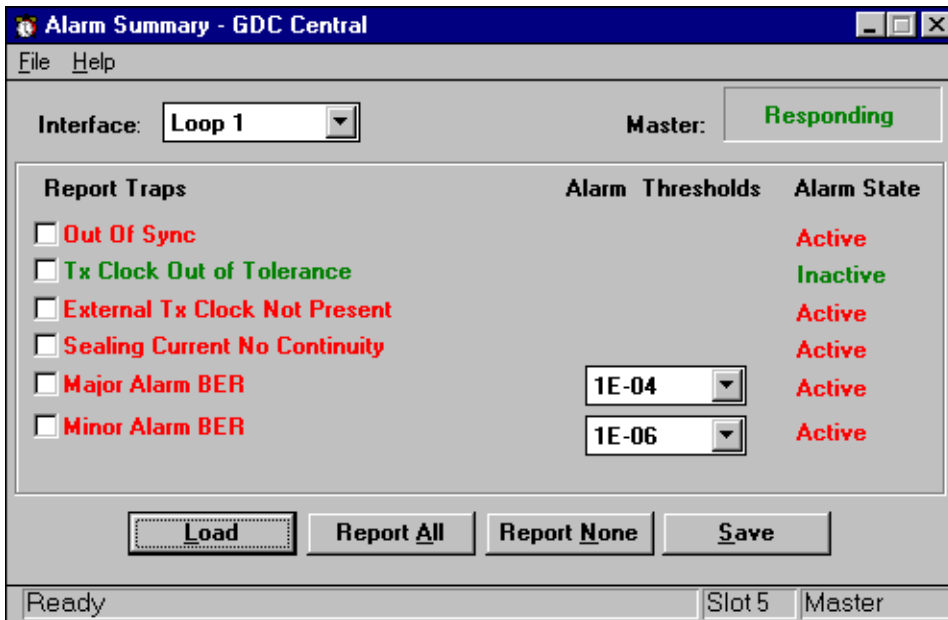
Figure 5-8   Alarm Summary Window, Unit SC613
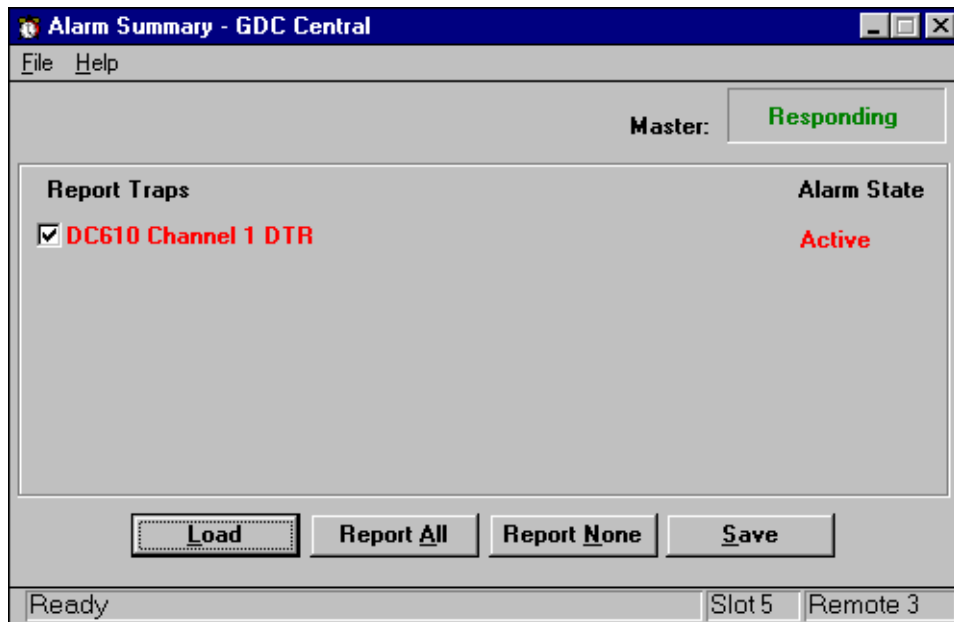
Figure 5-9 Alarm Summary Window, Unit DC610
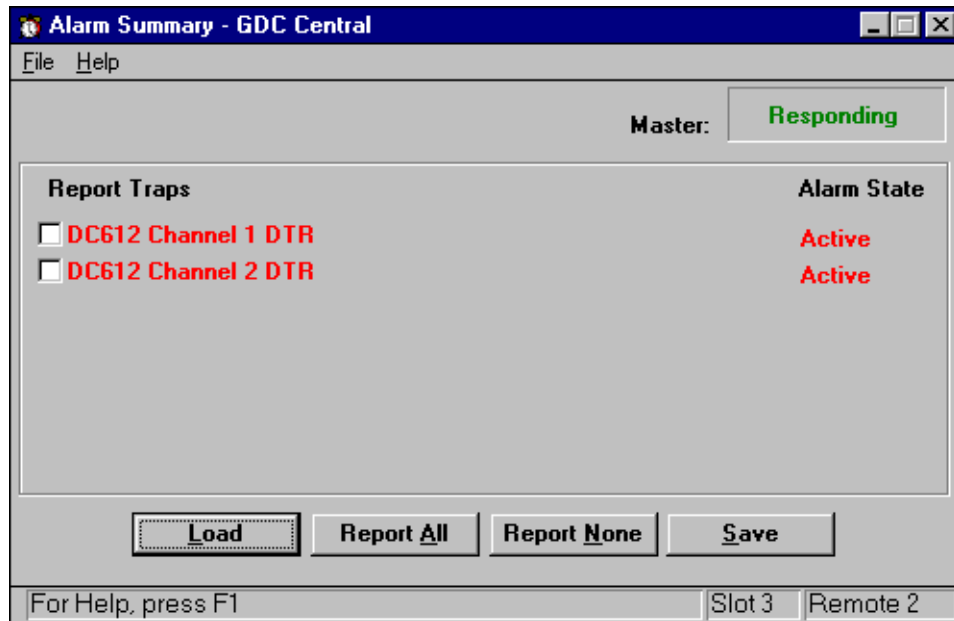
Figure 5-10 Alarm Summary Window, Unit DC612
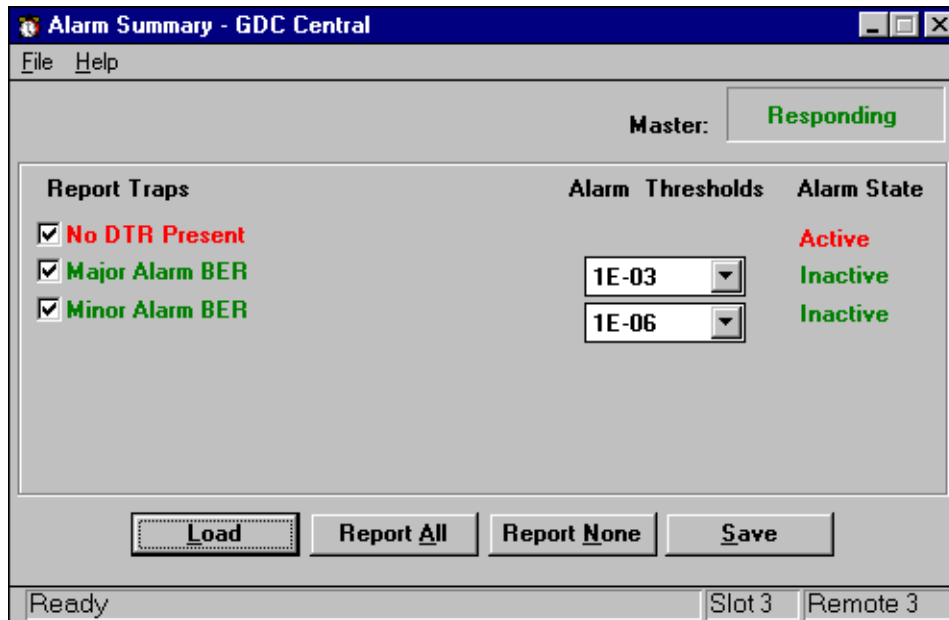
Figure 5-11 Alarm Summary Window, Unit SC621

To open the Alarm Summary window:

1.   Select a unit from the GDC Shelf display.

2.   From the Monitor menu select the `Alarm Summary` option.

      You can also select this option from the Front Panel Status application using the Monitor menu item. This opens the Alarm Summary window for the unit. The unit is queried for information which is then displayed in the window. To refresh the window click on the `Load` button.

3.   Select the Interface, e.g., `Loop 1`, that represents the interface of the alarms that you want to view. *NOTE: Not all units support interface drop down list box.*

4.   To report an alarm, using the mouse, place a check in the appropriate check box. To mask an alarm, remove any check in the check box, i.e., the box must be blank.

      You may use the following buttons when selecting to either report or mask all the alarms in the Alarm Summary window:

          Report All places a check in the corresponding check box for all alarms thereby allowing the reporting of all the alarms in the window.

          Report None removes the checks from all check boxes thereby masking all alarms in the window.

5.   When you are finished click on the `Save` button to store your input.

Front Panel Status

This application lets you display a graphic representation of the front panel of the unit. Each panel displays LEDs that indicates the status of various operations. Each also contains an option button. From the Option button you can select an option associated with the unit, e.g., Configure.

To open the Front Panel window:

1. Select a unit from the GDC Shelf display.

2. From the Monitor menu select the Front Panel option.

   You can also open the Front Panel Status application by double clicking on the card in the GDC shelf.

   This opens the Front Panel window for the unit. The unit is queried for information which is then displayed in the window.

There is a front panel graphic for the Power Supply, and SCM and 2B1Q units which displays the following LEDs (*See Figure 5-12)*:
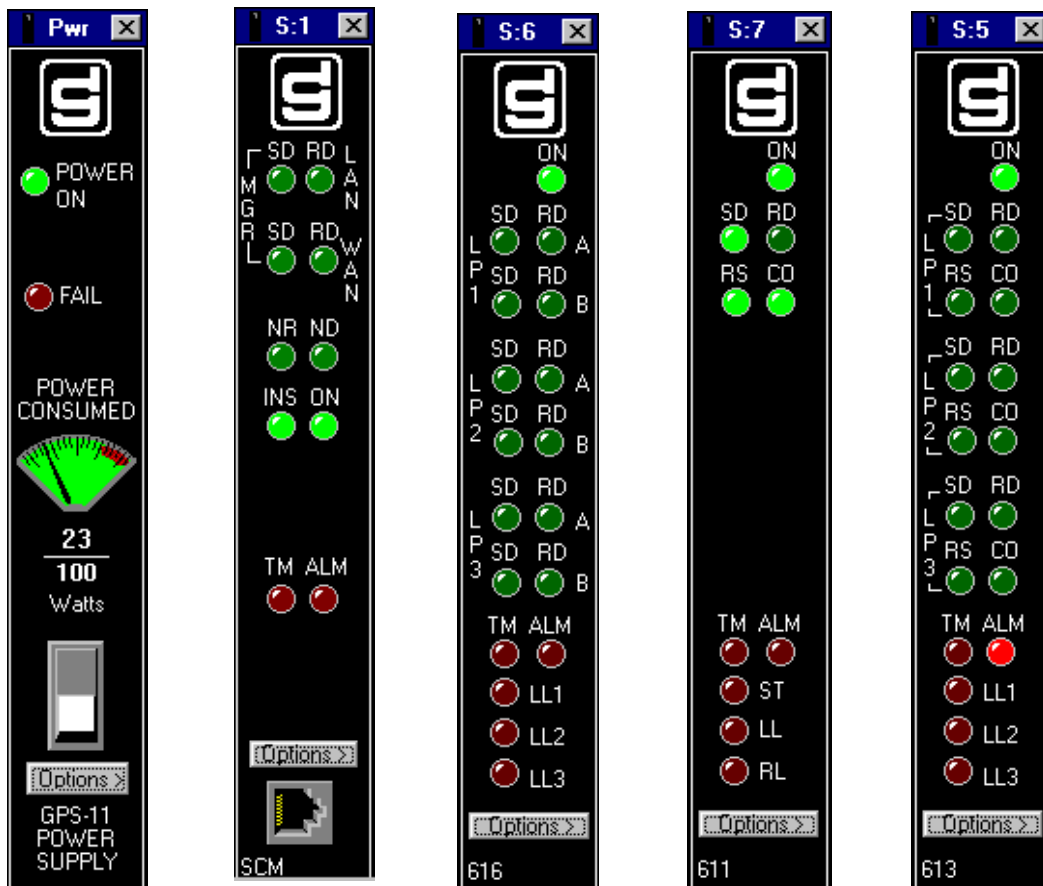
Figure 5-12 Front Panel Status Windows for GPS-11 Power Supply, SCM, 616, 611, and 613

Power Supply (*See Figure 5-12*)

- `Power On` - when illuminated indicates that the supply is on.

- `Fail` - when illuminated indicates a supply failure.

- `Power Consumed` - indicates the number of Watts used by the system.

SCM (*See Figure 5-12)*

- `SD` - when illuminated indicates that data is active.

- `RD` - when illuminated indicates that data is being received.

- `NR` - not used.

- `ND` - not used.

- `INS` - when illuminated indicates that unit is in service.

- `ON` - when illuminated indicates that power is on.

- `TM` (Test mode indicator) - when illuminated indicates that the unit is in test.

- `ALM` (Alarm indicator) - when illuminated indicates alarm severity.

Master Front Panel Status Windows

2B1Q Unit 616 (*See Figure 5-12*)

- `ON` - when illuminated indicates that power is on.

- `SD L1/L2/L3 (A/B)` - when illuminated indicates that data is active for the given loop and channel.

- `RD L1/L2/L3 (A/B)` - when illuminated indicates that data is being received for the given loop and channel.

- `TM` (Test mode indicator) - when illuminated indicates that the unit is in test.

- `ALM` (Alarm indicator) - when illuminated indicates alarm severity.

- `LL1/LL2/LL3` - when illuminated indicates that the given loop is in Line Loopback.

2B1Q Unit 611 (*See Figure 5-12)*
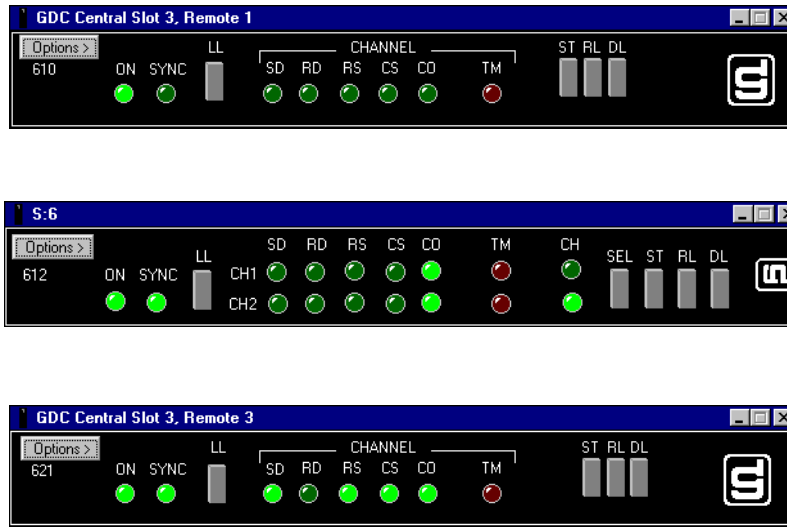
- `ON` - when illuminated indicates that power is on.

- `SD` - when illuminated indicates that data is active for the given loop and channel.

- `RD` - when illuminated indicates that data is being received for the given loop and channel.

- `CO` - when illuminated indicates that data carrier detected is asserted (to DTE).

- `RS` - when illuminated indicates that request-to-send is asserted (by DTE).

- `TM` (Test mode indicator) - when illuminated indicates that the unit is in test.

- `ALM` (Alarm indicator) - when illuminated indicates alarm severity.

- `ST` - when illuminated indicates that unit is in Self-Test.

- `LL` - when illuminated indicates that Line Loopback test is active.

- `RL` - when illuminated indicates that Remote Loopback test is active.

2B1Q Unit 613 (*See Figure 5-12)*

- ON - when illuminated indicates that power is on.

- SD L1/L2/L3 - when illuminated indicates that data is active for the given loop and channel.

- RD L1/L2/L3 - when illuminated indicates that data is being received for the given loop and channel.

- RS L1/L2/L3 - when illuminated indicates that request-to-send is asserted (by DTE) for the given loop and channel.

- CO L1/L2/L3 - when illuminated indicates that data carrier detected is asserted (to DTE) for the given loop and channel

- TM (Test mode indicator) - when illuminated indicates that the unit is in test.

- ALM (Alarm indicator) - when illuminated indicates alarm severity.

- LL1/LL2/LL3 - when illuminated indicates that the given loop is in Line Loopback.

Remote Front Panel Status Windows

Figure 5-13 Front Panel Status Windows for 610, 612, and 621

2B1Q Units 610 and 621 (*See Figure 5-13 - top and bottom panel displays.*)

- ON - when illuminated indicates that power is on.

- SYNC - when illuminated indicates that frame synchronization of the 2B1Q loop signal is acquired.

- CHANNEL SD - when illuminated indicates that data is active for the given loop and channel.

- CHANNEL RD - when illuminated indicates that data is being received for the given loop and channel.

- CHANNEL CO - when illuminated indicates that data is received over channel.

- CHANNEL RS - when illuminated indicates that DTE is ready to send data over channel.

- CHANNEL CS - when illuminated indicates that clear-to-send lead to DTE is on.

- CHANNEL TM (Test mode indicator) - when illuminated indicates that the unit is in test.

2B1Q Unit 612 (*See Figure 5-13 - middle panel display.*)

- ON - when illuminated indicates that power is on.

- SYNC - when illuminated indicates that frame synchronization of the 2B1Q loop signal is acquired.

- CH1/CH2 SD - when illuminated indicates that data is active for the given loop and channel.

- CH1/CH2 RD - when illuminated indicates that data is being received for the given loop and channel.

- CH1/CH2 CO - when illuminated indicates that data is received over for the given loop and channel.

- CH1/CH2 RS - when illuminated indicates that request-to-send is asserted (by DTE) for the given loop and channel.

- CH1/CH2 CS - when illuminated indicates that clear-to send is asserted (by DTE) for the given loop and channel.

- CH1/CH2 TM (Test mode indicator) - when illuminated indicates that the unit is in test.

- CH - when illuminated indicates which channel is active.

6 Administer

Introduction

The Administer menu contains the following applications:

- Maintenance - lets you do basic maintenance operations on the unit.
- Diagnostics - lets you do line loopback tests on the unit.

Maintenance

This application lets you conduct basic maintenance operations on the unit. These operations are:

- Reset Configuration - loads factory defaults to the unit.
- Reset Unit - initiates a board reset. This application disrupts data transfer.
- Inhibit Front Panel - disables the front panel.
- Reset Statistics - resets all statistics to zero for DC610, DC612, DC621, SC611, and SC616. For SC613, statistics are reset on a per-loop basis, using the window in *Figure 6-3*.

To open the Maintenance window:

3. Select a unit from the GDC Shelf display.

4. From the Administer menu select the `Maintenance` option.

5. You can also select the this option from the Front Panel Status application using the Maintain menu item.

6. This opens the Maintenance window for the unit. *Figure 6-1* pertains to the Units 610, 611, 612, 616, and 621; and *Figures 6-2* and *6-3* pertain to Unit 613.

7. Select the desired operation.
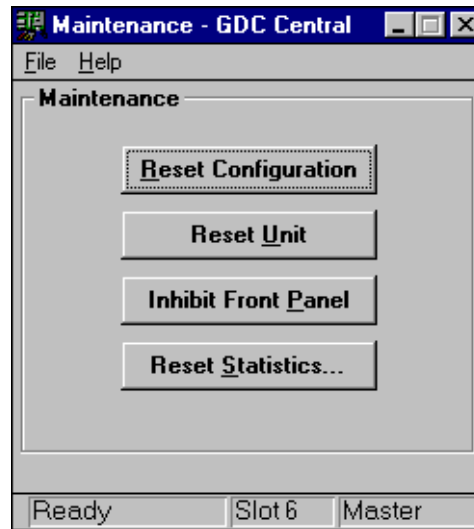
Figure 6-1   Maintenance Window for Units DC610, SC611, SC613, DC612, SC616, and DC621
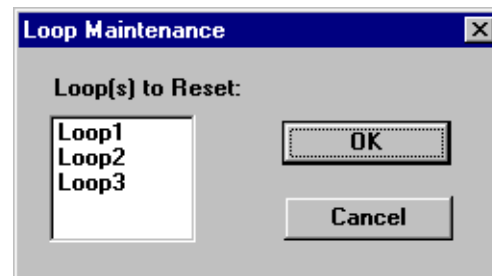
Figure 6-2   Loop Maintenance Window for Unit 613

Diagnostics

This application lets you accomplish the following tests:

`Mst to Rmt ST` - places both the master and remote in Self-Test.

`Rmt to Rmt ST` - places the remote unit in Self-Test. To complete this diagnostic test, Rmt to Rmt ST must also be selected on another circuit.

`Remote Bilateral Loopback` - places the remote in Line Loopback.

`Remote Digital Loopback` - places the remote in Digital Loopback.

`Remote Channel Loopback` - incoming data to the remote DTE is looped back out the remote DTE interface.

`Remote Bilateral Loopback with Self-Test` - places the master in Self-Test and the remote in Line Loopback.

`Remote Digital Loopback with Self-Test` - places the master in Self-Test and the remote in Digital Loopback.

`Local Loopback with Self-Test` - places the master in Self-Test.

`Local Bilateral Loopback` - places the master in Line Loopback.

For further information on these tests, consult your hardware documentation.

To conduct a diagnostic test:

1. Select a card from the GDC Shelf display.

    Note that all tests on the remotes require that you select the appropriate card in the shelf.

2. From the Administer menu select the `Diagnostics` option.

    You can also select this option from the Front Panel Status application using the `Diagnose` option button. This opens the Diagnostics window for the unit.

    See *Figure 6-3,* below.
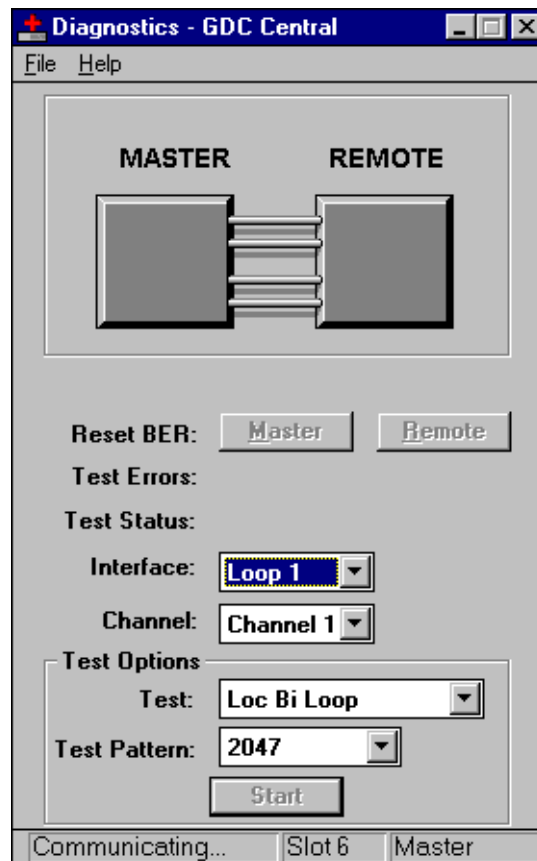
Figure 6-3   Diagnostics Window

3. In the Interface field, select the loop that you want to perform the test on.

4. In the Channel field, select the channel that you want to perform the test on.

5. In the Select Test field, select the test that you want to perform.

6. In the Test Pattern field, select a test pattern, `2047` or `511`.

7. To begin the test, click on the Start button. Information is reported in the following fields:

   Once the test begins, the Stop button replaces the Start button. If you want to stop the test before its normal end, click the Stop button.

8. If applicable to the test, reset the Self Test Error count for the master or remote by clicking on the appropriate buttons. These buttons apply to the SC611, SC613, and SC621 only.

Upgrade Firmware

This application allows firmware to be downloaded to units which have flash upgradeable PROMs.

To upgrade one or more units of the same type:

1. Select the SCM unit from the GDC Shelf window.

2. From the Administer menu select the Upgrade Firmware option. See *Figure 6-4*.
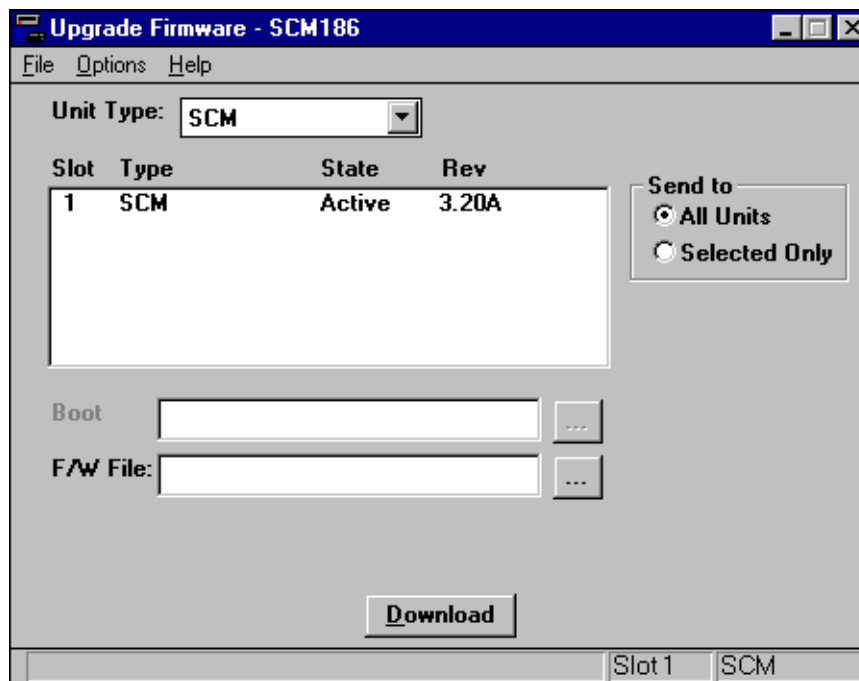
Figure 6-4   Upgrade Firmware Window

You can also select this option from the SCM Front Panel Status application by selection the Upgrade Firmware menu item.

3. Select the type of unit you wish to upgrade using the Unit Type drop-down list. The listbox will update and show units of that type along with their current firmware revisions.

4. If you want all units of that type to be upgraded, select the All Units option button. If you want to upgrade only one unit, highlight that unit in the listbox, and select the Selected Only option button.

5. Certain products require a special boot file to be loaded prior to the actual firmware download. The V.34 and Dual V.34 product families require this step. Type in the full pathname for the file containing the boot code image. You can also select the "..." button and browse for the file using a standard windows File Open dialog.

6. Type in the full pathname for the file containing the firmware code image. You can also select the "..." button and browse for the file using a standard windows File Open dialog.

7. If you wish to delay the start time for the firmware upgrade, select "Start Delay" from the Options menu. Then select one of the delay values: 1, 2, 4, 8, 12, and 18 hours.

8. Select the Download button to initiate the download. Progress is displayed on a progress gauge. When the code download is complete, a check is made to verify that the download was successful. The status of the verification process is displayed in the listbox at the end of each entry. "Pass" or "Fail" will be displayed.

Index

General DataComm