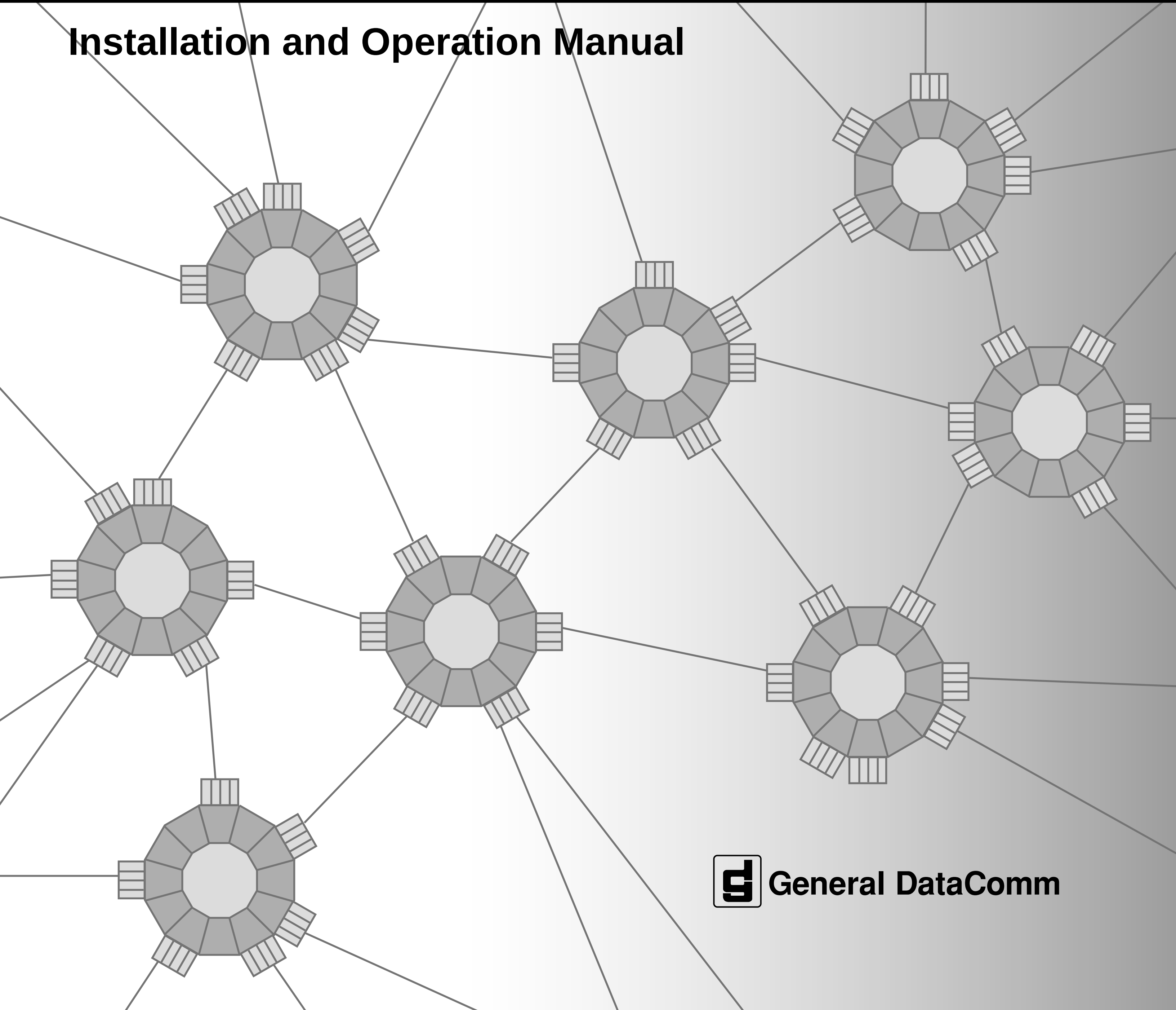
048R303-000
January 2002
Issue 8

SpectraComm Manager Card®

Installation and Operation Manual



General DataComm

048R303-000
Issue 8
January 2002

SpectraComm Manager Card ®

Installation and Operation Manual

Copyright

This publication and the software it describes contain proprietary and confidential information. No part of this document may be copied, photocopied, reproduced, translated or reduced to any electronic or machine-readable format without prior written permission of General DataComm, Inc. The information in this document is subject to change without notice. General DataComm assumes no responsibility for any damages arising from the use of this document, including but not limited to, lost revenue, lost data, claims by third parties, or other damages. If you have comments or suggestions concerning this manual, please contact:

General DataComm, Inc.
Technical Publications
6 Rubber Avenue
Naugatuck, Connecticut USA 06770
Telephone: 1 203 729-0271

Trademarks

All brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Documentation

Revision History

Issue	Date	Description of Change
1 - 4	-	Initial Release and Updates
5	Dec. 1997	Enhancements to SCM terminal interface function
6	Oct. 1999	General updates and corrections
7	Jun. 2001	Added RADIUS authentication and remote SCM IP configuration
8	Jan. 2002	Overview of TEAM-managed SC/UAS network elements; General updates and corrections; Added SC5506 OCU-DP and SC5516 DS0-DP elements

Related Publications

Description	Part Number
SpectraComm/UAS Shelf and Enclosure Installation and Oper. Manual	010R302-REV
SpectraComm 2000 Shelf Installation and Operation Manual	010R358-REV
TEAM Core Software Operation Manual	058R720-VREF
Operation Manual(s) for each individual SCM-compatible network element	Refer to www.gdc.com for specific element Publications.
TEAM Operation Manual(s) for each TEAM-managed network element	

`-REV` designates the most current hardware manual revision (**`-000`**, **`-001`**, etc.)
`-VREF` designates the latest software version, (**`-V420`** is Version 4.2.0).
In addition to the publications listed, always read the Release Notes supplied with your products.

Table of Contents

Preface

Chapter 1: Introduction and Specifications

Chapter 2: Installation and Setup

Chapter 3: SCM Configuration

Chapter 4: SCM Operation

Chapter 5: SNMP Programming

Appendix A:Maintenance

Appendix B:SCM with RADIUS

Appendix C:Canned Configurations

Preface

Scope of this Manual

This manual describes installation and operation of the SpectraComm Manager (SCM) Card which monitors and managers network devices. This document is intended for network operators and installers and assumes a working knowledge of data communication equipment.

The information in this manual has been carefully checked and is believed to be entirely reliable. However, as General DataComm improves the reliability, function and design of its products, it is possible that information may not be current. Check the General DataComm website at **`http://www.gdc.com`** for updated product information or contact your General DataComm field representative.

General DataComm, Inc.
6 Rubber Avenue
Naugatuck, Connecticut, USA 06770
Tel: 1 203 729 0271

Safety Information

This manual should be read in its entirety and all procedures completely understood before installing or operating the unit. The notes that appear throughout this manual must be read prior to any installation or operating procedure. Examples of notes used in this manual are shown below.

Note *A note provides essential operating information not readily apparent which you should be particularly aware of. A note is typically used as a suggestion.*

Important *Indicates an emphasized note. It is something you should be particularly aware of; something not readily apparent. Important is typically used to prevent equipment damage.*

Precautions

The CAUTION, WARNING, and DANGER statements that appear throughout this manual are intended to provide critical information for the safety of both the service engineer and operator, and enhance equipment reliability. The definitions and symbols for such statements comply with ANSI Z535.2, American National Standard for Environmental and Facility Safety Signs, and ANSI Z535.4, Product Safety Signs and Labels, issued by the American National Standards Institute.

⚠ **CAUTION** *Indicates a potentially hazardous situation which, if not avoided, may result in minor to moderate injury. It may also be used to alert against unsafe practices.*

⚠ **WARNING** *indicates an imminently hazardous situation which, if not avoided, could result in death or serious injury.*

⚠ **DANGER** *indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.*

Safety Guidelines

Under proper conditions, this unit will operate reliably and safely in your network. If any component is improperly handled or installed, equipment failure or personnel hazard may occur. Use caution and common sense when installing network wires. Use the following guidelines, especially when unsafe conditions exist or when potentially hazardous voltages are present:

- Repairs must be performed by qualified service personnel only.
- To reduce the risk of electrical shock, do not operate equipment with the cover removed.
- Never install network jacks in a wet location unless the jack is designed for that location.
- Never touch uninsulated network wires or terminals unless the network line is disconnected at the network interface.
- Never install network wiring during an electrical storm.

Antistatic Precautions

Electrostatic discharge (ESD) results from the buildup of static electricity and can cause computer components to fail. ESD occurs when a person whose body contains a static buildup touches a computer component. The SCM card may contain static-sensitive devices that are easily damaged. Proper handling, grounding and precautionary ESD measures are essential. Keep parts and cards in antistatic packaging during transport or when not in use. When handling always use antistatic floorpads, workbenchpads and 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 screw driver or paper clip to set switches.

Compliance

FCC Part 15 Compliance

This device complies with Part 15 of the FCC rules. Operation is subject to the following conditions:

1. This device may NOT cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Electromagnetic Compatibility: Canada

This Class A digital apparatus complies with Canadian ICES-003.

La Compatibilité d' Eléctro-magnetique

Cet appareil numerique de la classe A est conforme a la norme NMB-003 du Canada.

EC Declaration of Conformity

We:
General DataComm Limited
Molly Millars Lane
Wokingham, Berkshire RG41 2QF, United Kingdom

On behalf of:
General DataComm Inc.
6 Rubber Avenue
Naugatuck, Connecticut 06770, U.S.A.

The products to which this declaration relates are in conformity with the following relevant harmonized standards, the reference numbers of which have been published in the Official Journal of the European Communities.

Electromagnetic Compatibility

EN 55022: 1994

Specification for limits and methods of measurement of radio interference characteristics of information technology equipment.

EN 50082-1: 1992

Generic immunity standard Part 1 Residential, Commercial, and Light Industry.

Safety

EN 60950: 1995 A1 through A3

Low Voltage Directive relating to electrical equipment designed for use within certain voltage limits.

Deutschland

Überblick Sicherheit

Bitte lesen sie dieses Handbuch komplett durch und stellen sie sicher, daß sie alle Vorschriften verstehen, bevor sie das Gerät installieren oder betreiben. Die Hinweise in diesem Handbuch müssen vor Installation oder Betrieb gelesen werden. Beispiele für Hinweise sehen sie hier.

Hinweis

Ein Hinweis enthält wichtige Informationen zum Betrieb, die nicht auf den ersten Blick ersichtlichsind, und die zu beachten sind. Ein Hinweis dient als Vorschlag.

Wichtig

Bedeutet einen besonders wichtigen Hinweis. Darauf sollten sie besonders achten, da dies nicht offensichtlich ist. *Wichtige Hinweise dienen im Allgemeinen dazu, Schäden am Gerät zu vermeiden.*

Die Hinweise CAUTION (VORSICHT), WARNING (WARNUNG) und DANGER (GEFAHR), welche im Handbuch erscheinen, enthalten entscheidende Informationen für die Sicherheit sowohl des Servicepersonals als auch der Bediener. Diese Hinweise erhöhen die Zuverlässigkeit der Anlage. Die folgenden Definitionen und Symbole für VORSICHT, WARNUNG und GEFAHR, wie sie in diesem Handbuch auftreten, sind gemäß ANSI Z535.2, Amerikanischer Nationaler Standard für Sicherheitszeichen für Umwelt und Anlagen, und ANSI Z535.4, Produkt-Sicherheits-Zeichen und Beschriftungen, ausgegeben vom American National Standards Institute.

VORSICHT *bedeutet eine potentiell gefährliche Situation, die wenn sie nicht vermieden wird, zu leichten oder mittelschweren Verletzungen führen kann.*

WARNUNG *bedeutet eine drohende gefährliche Situation, die wenn sie nicht vermieden wird, zu schweren Verletzungen oder zum Tode führen kann.*

GEFAHR *bedeutet eine drohende gefährliche Situation, die wenn sie nicht vermieden wird, zwangsläufig zu schweren Verletzungen oder zum Tode führt.*

Sicherheitsrichtlinien

Unter normalen Umständen arbeitet die Anlage sicher und zuverlässig in ihrem Netzwerk. Falsche Handhabung oder Installation von Bestandteilen kann zu Ausfällen oder Gefahren für den Bediener führen. Seien sie vorsichtig und beachten sie die allgemeinen Regeln bei der Installation der Netzwerkkabel. Beachten sie die folgenden Hinweise, besonders bei unsicheren Umständen oder potentiell gefährlichen Spannungen:

- Reparaturen dürfen nur von qualifiziertem Servicepersonal ausgeführt werden.
- Zur Vermeidung elektrischer Schläge darf die Anlage nicht mit geöffneter Abdeckung betrieben werden.
- Niemals Netzwerkstecker in feuchter Umgebung installieren, es sei denn der Stecker ist dafür ausgelegt.
- Niemals unisolierte Netzwerkdrähte oder Klemmen berühren, es sei denn das Netwerk ist am Interface abgeschaltet.
- Niemals Netzwerk bei elektrischem Gewitter verdrahten.

Service Support and Training

VITAL Network Services is a leading single-source, data communications organization which provides network service and support for General DataComm customers throughout the world. Vital Network Services provides the support and training required to install, manage and maintain your GDC equipment. Training courses are available at centers in the US, UK, France, Singapore and Mexico, as well as at a customerís site.

For more information on VITAL Network Services or for technical support assistance, contact VITAL Network Services

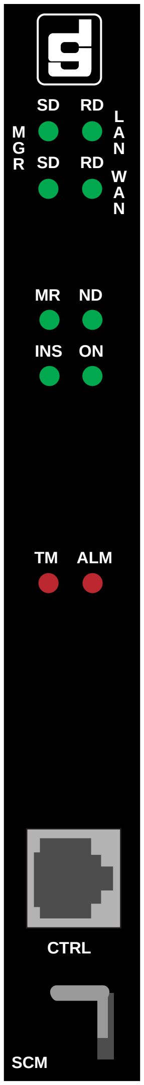
VITAL Network Services World Headquarters		
6 Rubber Avenue	Telephones:	Faxes:
Naugatuck, Connecticut 06770 USA	1 800 243 1030	1 203 723 5012
	1 888 248 4825	1 203 729 7611
http://www.vitalnetsvc.com	1 203 729 2461	

VITAL Network Services Regional Sales and Service Offices:

North American Region Office 6 Rubber Avenue Naugatuck, Connecticut 06770 USA Telephones: 1 800 243 1030 1 888 248 4825 1 203 729 2461 1 800 361 2552 (French Canadian) Training: 1 203 729 2461 Faxes: 1 203 723 5012 1 203 729 7611	**Central America, Latin America** VITAL Network Services Periferico Sur 4225, Desp. 306 C.P. 14210, Mexico D.F., Mexico Telephone: 52 5 645 2238 Training: 52 5 645 2238 Fax: 52 5 645 5976
Europe, Middle East, Africa VITAL Network Services Molly Millars Close Molly Millars Lane Wokingham, Berkshire RG41 2QF UK Telephone: 44 1189 657200 Training: 44 1189 657240 Fax: 44 1189 657279	**Asia Pacific** VITAL Network Services 501 Orchard Road 05-05 Wheelock Place, Singapore 238880 Telephone: 65 735 2123 Training: 65 735 2123 Fax: 65 735 6889

Chapter 1: Introduction and Specifications

System Overview



The SpectraComm Manager card (SCM) is the shelf controller and network management interface to all network access elements in a SpectraComm or UAS shelf. The SCM card provides TCP/IP-based centralized management and uses the Simple Network Management Protocol (SNMP), a proxy agent for the network elements in the shelf. These functions are also performed for the remote units which communicate with the SCM-managed elements in the shelf.

An SCM card and its corresponding IP address can control one network element in a SpectraComm 2000 shelf, up to 15 co-located network elements in a single SpectraComm/UAS shelf, and up to 31 elements in a dual shelf.

With additional software, the SCM can provide management through TEAM applications (Total Enterprise Access Management), and can allow capable SpectraComm modems to open a client service session for RADIUS security.

Features and Benefits

- Supports Ethernet, serial PPP and serial DBU connectivity;
  supports Telnet connectivity for capable network elements.
- Provides a front panel control port configured as a EIA-561 DCE interface or as a VT100-compatible terminal connection.
- Acts as SNMP proxy agent for network elements under its control.
- Creates and maintains defined MIB objects.
- Locally manages up to 15 local network elements in one SpectraComm/UAS Shelf, or up to 31 on two shelves. Can manage up to 1024 network elements.
- Polls network elements for alarm and status change notification.
- Performs SNMP control for TEAM-managed elements according to their respective MIBs.
- Supports TFTP firmware download to the SCM and to network elements.
- Supports dial-backup recovery to preserve communication with network manager.
- Provides option for redundant SCMs.
- Provides Auto Configuration for capable network elements.
- Provides RADIUS (Remote Authentication Dial-In User Service) security.
- Supports remote configuration of SCM IP addressing

Theory of Operation

All management and security communications are directed to the SCM's IP address. The SCM card relays commands and responses between management applications, hardware components, and enabled software, using a slot addressing scheme to communicate over the shelf backplane with the other components. The SCM is transparent to the application software packages which operate as though they were communicating directly with the hardware units.

The SCM provides control and monitoring functions via the SpectraComm backplane for up to 15 co-located network elements in a single SC/UAS Shelf, or for up to 31 elements when two shelves are linked together. It also controls and monitors remote elements linked by a Diagnostic Communication Channel (DCC) to the elements located with the SCM card.

The SCM MIB tables allow user access to configuration, operation, and status data on the network elements for which the SCM card is responsible. An SNMP network manager can query and act upon the MIB tables. When the network manager requires action by the network elements, the SCM card issues the appropriate GDC Management Protocol commands over the shelf backplane, using a slot/line/drop address scheme to identify the communicating network elements.

Note *Table 1-1 and Table 1-2 list all of the SCM-compatible network elements and the SCM functions they support.*

Network Element Discovery

The SCM card performs Discovery on network elements to identify compatible network elements located in its shelf and to store element information in its local database. This information includes the element type, configuration checksum, serial number, alarm status, and equipment status. The user can access this information by means of the SCM Management Information Base (MIB).

The SCM initially performs Discovery at power up by polling all shelf slots (2 in a SpectraComm 2000 shelf, 15 in a single-shelf installation or 31 in a two-shelf installation). From that initial poll, the SCM card identifies each slot with one of the following status conditions:

- Active (containing an SCM-compatible network element)
- Inactive (empty or containing incompatible equipment)

After the initial Discovery, the SCM card polls the active slot addresses for alarms and statistical data and also polls one inactive slot. By reducing the frequency at which it polls inactive slots, the SCM card can continuously monitor as rapidly as possible and still discover newly installed SCM-compatible equipment.

Note *Refer to Chapter 3, SCM Configuration for additional information on Discovery and Autodiscovery of network elements.*

Auto Configuration

The SCM can auto-configure a new or replacement network element when the element is installed in a previously configured shelf slot and when that element type supports auto-configuration.

Firmware Downloading

The SCM provides a Firmware Download function for network elements in the shelf and any associated remotes when those units support firmware downloading.

Note *Refer to Appendix A: Firmware Downloading for detailed information and procedures*

SCM Interfaces/Connectivity

The SpectraComm Manager card occupies one slot in a SpectraComm or UAS Shelf. The standard installation environment for the SCM card is a SpectraComm/UAS Shelf backplane with a back panel DB25F connector (LAN port) and two back panel RJ45 jacks (WAN ports) which provide the routine communications with an SNMP network manager. Typically, the upper WAN port is the active WAN connection. The lower DBU WAN port asserts control whenever its Carrier Detect input is ON, indicating that the modem has an active connection. These interfaces are described in detail below. Refer to *Chapter 2, Installation and Setup* and *Chapter 3, SCM Configuration* for detailed information on configuring the interface ports for various installation configurations.

Note *The WAN ports and the CTRL ports communicate with an SNMP network manager under the Point-to-Point Protocol (PPP).*

LAN Interface

The LAN interface is provided by the back panel DB25F connector for the shelf slot of the SCM card. With the appropriate adapter, this port can access an Ethernet LAN for connecting to LANs using 10BASE-T (twisted pair) or 10BASE-2 (coaxial) wiring. During LAN connectivity, the two LEDs on the front panel, **LAN Send Data** and **LAN Receive Data**, indicate the activity of the SCM card on the interface.

WAN Interface

The WAN interface is provided by the upper of the two back panel RJ45 jacks for shelf slot of the SCM card. This port is an EIA-561 configured as a DCE interface (EIA-232 signal levels through an RJ45 jack) and supports a permanent connection to the network manager, either through a cable or through a dedicated link (i.e., a multiplexer channel). During WAN connectivity, the two LEDs on the front panel, **WAN Send Data** and **WAN Receive Data**, indicate the activity of the SCM card on the interface.

Dial Backup WAN Interface

The Dial Backup (DBU) WAN interface is provided by the lower of the two back panel RJ45 jacks for the shelf slot of the SCM card. This port is an EIA-561 configured as a DTE interface (EIA-232 signal levels through an RJ45 jack) and supports temporary management connection to an auto-answer modem installed in the same shelf (i.e., SpectraComm V. F 28.8/33.6). A DBU connection through this port allows the SCM card to communicate with its network manager if its usual communication link is lost. During DBU WAN connectivity, the two LEDs on the front panel, **WAN Send Data** and **WAN Receive Data**, indicate the activity of the SCM card on the interface.

Note *An option switch on the SCM determines whether the WAN port operates at 19.2 kbps or 9.6 kbps.*

Control Interface

The Control (CTRL) interface is provided by the RJ45 jack located on the SCM front panel. This port is an EIA-561 configured as a DCE interface and supports direct cable connection to a local SNMP network manager or connection to a VT100-compatible terminal. As an SNMP port, the CTRL port functions like the back panel WAN port for temporary connection during setup or troubleshooting. As a terminal port (the default), the CTRL port accesses the SCM menus for configuring the subnet mask, gateway, community name, Telnet login, network elements and the IP address of the SCM card.

Note *An option switch on the SCM card selects the SNMP or terminal port function of the CTRL interface.*

Supported Shelf Systems

The SCM card can control network elements residing in three types of GDC shelf systems: a SpectraComm shelf, a SpectraComm 2000 shelf and a UAS shelf. In each shelf system, the SCM provides the SNMP management and IP address for the network elements in the shelf. The figure below illustrates a sample of network elements in managed shelves. For the detailed information on any shelf system or any of their associated network elements, refer to the accompanying product manuals and Release Notes.

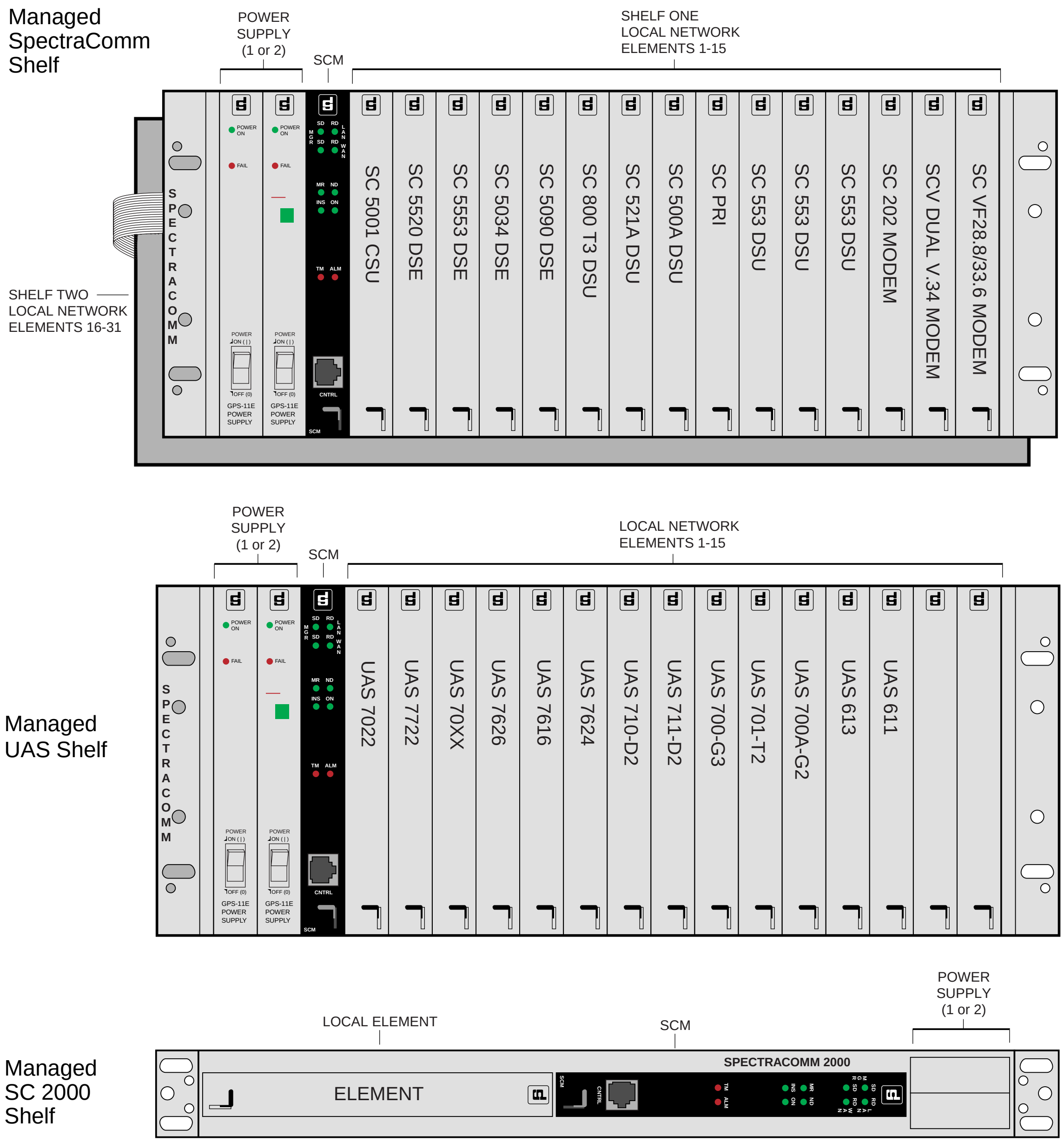


Figure 1-1 Managing Network Elements in GDC Shelf Systems.

Note *Typically, the SCM can be installed in any SpectraComm/UAS shelf slot. However, in SC/UAS shelves equipped with a Telco 50-pin backplane, the SCM can only be installed in Slot 1 or Slot 16.*

Supported Network Elements

The tables below lists the network elements supported by the SCM in a SpectraComm or UAS shelf system and also indicate which elements support features such as Auto Configuration, Auto Discovery, Firmware Download, and a Master/Remote functionality.

Table 1-1 lists elements intended for use in a SpectraComm shelf with an SCM card at Ver. 5.x.x. *Table 1-2* lists elements intended for use in a UAS shelf with an SCM card at Ver. 7.x.x.

Note *Network elements should be in housed in the proper shelf system and the SCM card must be at the proper application version for the shelf in which it resides.*

Note *If both SpectraComm and UAS elements are needed in your network, you will need separate shelves and SCMs with the appropriate version of SCM application code. Otherwise, some network element features will not be supported.*

Table 1-1 SCM-controlled Elements in SpectraComm Shelf System

Managed Network Elements	TEAM Applications	Telnet/Craft w/SCM	Standalone Craft	Discover Remotes	Auto Config	Firmware Download	Can be Master or Remote
SCM Version 5.x.x	TEAM Core	✔				✔	
SC 202 Modem	TEAM 202				✔		✔
SC V.F 28.8/33.6 Modem	TEAM V.34	✔				✔	✔
SC V.34 4-Port Modem	TEAM V.34	✔				✔	✔
SC V.34 DBU	TEAM V.34	✔				✔	✔
SC Dual V.34 Modem	TEAM Dual V.34	✔					✔
SC 5001 T1 LTU	TEAM 5001	✔			❄		
SC 5002 E1 LTU	TEAM 5002	✔			❄	✔	
SC 521 All Rate DDS DSU	TEAM 521	✔			✔	✔	
SC 521A DSU	TEAM 521A	✔	✔		✔	✔	✔
SC 521A/S DSU	TEAM 521A	✔	✔		✔	✔	✔
NMS 510 DSU	TEAM 521A						Remote only
NMS 520 DSU	TEAM 521A						Remote only
SC 5034 DSE	TEAM 5034/90	✔					
SC 5090 DSE	TEAM 5034/90	✔				✔	
SC 553 T1/FT1 DSU	TEAM SC 553	✔	✔	✔	✔	✔	✔
SC 5506 OCU-DP	TEAM 5506/5516	✔			✔	✔	
SC 5516 DS0-DP	TEAM 5506/5516	✔			✔	✔	
SC 5520 DSE	TEAM 5520	✔			❄	✔	
SC 5553 DSE	TEAM 5553	✔				✔	
SC 800 T3 DSU	TEAM 800 T3	✔	✔	✔	✔	✔	✔

Note ❄ *Auto Configuration of the SC 5001, SC 5002 and SC 5520 consists of Highway Configuration information only.*

Table 1-2 SCM-controlled Elements in UAS Shelf System

Managed Network Element	TEAM Application	Telnet/Craft w/SCM	Standalone Craft	Discover Remotes	Auto Config	Firmware Download	Can be Master or Remote
SCM Version 7.x.x	TEAM Core	✔				✔	
SC 2011 DATX	TEAM 2011						
SC V.F 28.8/33.6 Modem	TEAM V.34	✔				✔	✔
SC V.34 4-Port Modem	TEAM V.34	✔				✔	✔
SC V.34 DBU	TEAM V.34	✔				✔	✔
SC Dual V.34 Modem	TEAM Dual V.34	✔					✔
SC 611 NTU	TEAM 600						
SC 613	TEAM 600						
SC 616 LTU	TEAM 600						
DC 610 NTU	TEAM 600						Remotes only
DC 612 NTU	TEAM 600						Remotes only
DC 621 NTU	TEAM 600						Remotes only
GT 128 NTU	TEAM 600		✔		✔		✔
700G2, 700G3	TEAM 700		✔				
700AG2, 700AG2NZ, 701T2, 702G2, 710D2, 711D2	TEAM 700		✔	✔	✔		✔
720G1, 720G2, 721T2, 730D1, 730D2, 731D2,	TEAM 700		✔				Remotes only
GT1020, GT1030, GT1033 Multi-Rate, GT2020, GT2030,	TEAM 700		✔				Remotes only
7001, 7002	TEAM 7000	✔			✔		
7022	TEAM 7000	✔			✔	✔	
7616, 7616MP, 7616NZ	TEAM 7600	✔		✔	✔	✔	
7624	TEAM 7600	✔			✔		
7626	TEAM 7600	✔		✔	✔	✔	
7722	TEAM 7700	✔		✔	✔	✔	
7723 MR	TEAM 7600	✔		✔	✔	✔	

TEAM (Total Enterprise Access) Management

The SCM card itself is managed by the TEAM Core application, which is also responsible for the Discovery and Mapping functions of TEAM Applications within the HP OpenView framework. TEAM software consists of integrated core and individual applications for network elements on the HP OpenView Network Management platform. TEAM applications use Simple Network Management Protocol (SNMP) to configure and control the operation of SpectraComm devices through the SCM card that shares the same shelf. The applications can also control remote network elements under local control.

All of the TEAM application interfaces use the HP OpenView APIs (Application Programmer Interfaces) to integrate with HP OpenView Windows and other network management applications. Menu items are accessed via pulldown menus from the appropriate HP OpenView submap or from a Front Panel toolbar. For detailed information, refer to the GDC TEAM Core documentation and to the TEAM documentation that accompanies the individual products. The workstation that runs the TEAM applications must also be running the TEAM CORE application for managing the SCM.

TEAM applications employ SNMP to:

- Discover and display every GDC device in a SpectraComm shelf
- Manage individual local and remote devices using the SCM IP address(es)
- Configure the SCM and network elements
- Monitor the operation via Alarm Detail and Front Panel displays
- Diagnose suspected problems using local tests, remote loopbacks, and/or self test patterns
- Make connections via Telnet/PPP and MIB browser

Note *TEAM management of the SCM card is documented in the TEAM Core Operation Manual and Release Notes. TEAM management of an individual network element is described in its associated TEAM Operation Manual and Release Notes, i.e., TEAM 521A Operation Manual and TEAM 521A Release Notes.*

RADIUS Dial-in Access Option

RADIUS (Remote Authentication for Dial-In User Service) is an optional software feature for the SCM that permits a GDC SpectraComm modem (SC V.28.8/33.6 or SC DualV.34) to provide a secure dial-in serial connection for the remote management of network elements. When enabled in the SCM by a RADIUS Client Key purchased from General DataComm, RADIUS will authenticate user names, encrypted passwords, and challenged prompts coming from the modem and through the SCM card over the shelf management bus. Communication from the SCM to the customer-supplied RADIUS server can be conducted along a 10Base-T Ethernet interface, a 10Base-2 Ethernet interface, or a 9600/19200 serial PPP interface.

The SCM card emulates a Network Access Server by functioning as a client for RADIUS. The client passes the user name and password data to a user-configured, customer-supplied RADIUS server. If capable, the server will also authenticate challenged replies. The RADIUS server communicates its authentication results to the SCM which then instructs the modem to grant access or cut off the call. Transactions between the SCM and the RADIUS server are validated through the use of a shared secret which is never sent over the network. The figure below is typical of a RADIUS-protected network. Refer to Appendix B, SCM with RADIUS for detailed RADIUS information and procedures.

Note *The SpectraComm modems (SC V.28.8/33.6 or SC DualV.34) must be optioned at the factory for RADIUS. Refer to your modem documentation for more information.*

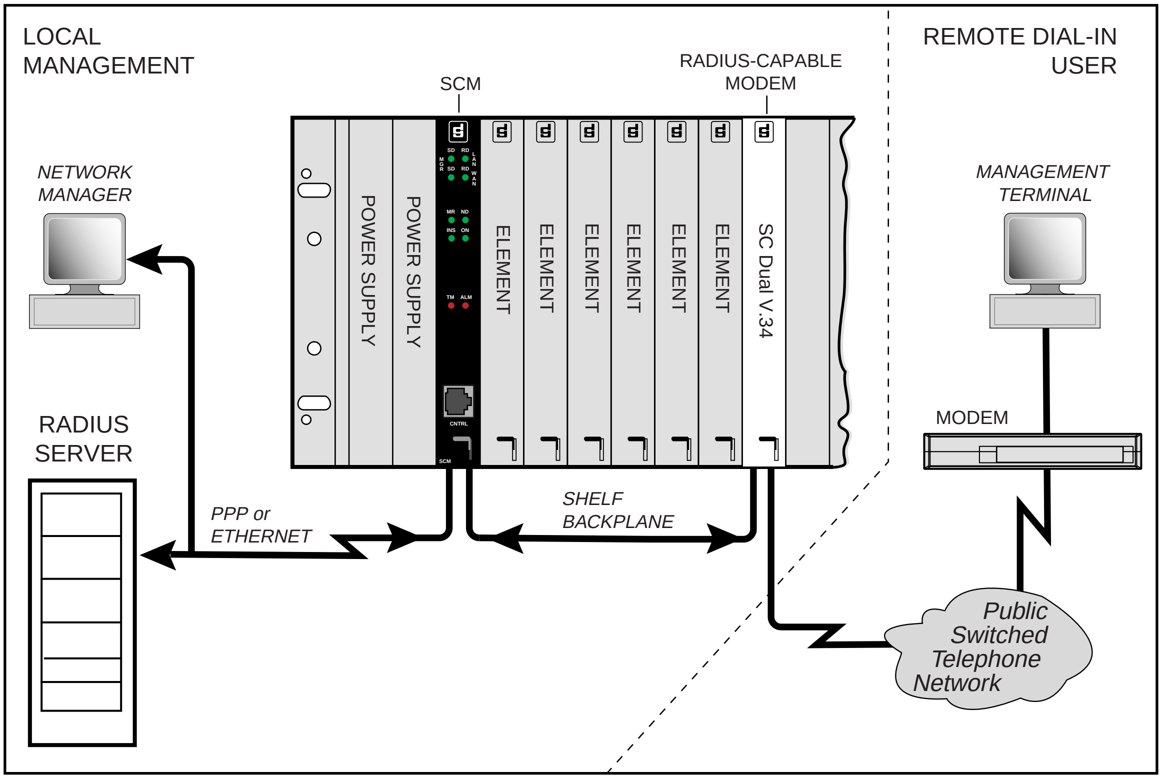


Figure 1-2 A Typical Deployment of RADIUS in a SC/UAS Network

Technical Specifications

The following table describes the physical, operational, and environmental specifications for the SpectraComm Manager card. Conforming to these specifications ensures maximum system performance and reduces the chances of mechanical breakdown and personnel hazard.

Table 1-3 SpectraComm Manager Card Specifications

Specification	**Description**
Physical Dimensions	Width: 178 mm (7.0 in.) Height: 21 mm (0.81 in.) Depth: 241 mm (9.5 in.) Weight: 0.28 kg (10 oz. Shipping weight: 0.74 kg (1 lb 10 oz)
Internal On-board Power Supply	22 VAC, 60Hz, 24 VA
Voltage/Frequency	Refer to the appropriate SpectraComm/UAS Shelf Manual for requirements
Fusing	Refer to the appropriate SpectraComm/UAS Shelf Manual for requirements
Power Dissipation	6 Watts maximum, each
Non-operating Temperature	-25 to 70 degrees C (-9 to 158 degrees F)
Operating Temperature	0 to 50 degrees C (32 to 122 degrees F)
Humidity	5% - 90% non-condensing
Non-operating Altitude	0 m to 12,191 m (0 ft. to 40,000 ft.)
Operating Altitude	0 m to 3,047 m (0 ft. to 10,000 ft.) Derate by one degreeC/1000 feet above sea level.
Safety Compliance	UL listed and CSA approved.
Compatibility	Compliance with Bell Pub. 62310 and ANSI T1.410 standards

Chapter 2: Installation and Setup

Installation Overview

The SCM card is a rackmount product intended for use in a GDC SpectraComm shelf, a GDC UAS shelf or in a SpectraComm 2000 shelf. This chapter provides procedures for installing the SCM card, making power connections, performing pre-operational checks, and making system connections. If this is your first installation of the SCM, be sure to read the previous sections of this manual to understand the optimal functioning of the SCM product as it applies to your network.

Shelf Installation Guidelines

- Locate the shelf unit in a ventilated area where the ambient temperature does not exceed 122 degrees F (50 degrees C).
- Do not install the shelf unit directly above equipment such as power supplies, which generate large amounts of heat.
- To install the SpectraComm/UAS Shelf, refer to Operating and Installation Instructions for SpectraComm/UAS Shelf and Enclosure, GDC P/N 010R302-000.
- When the SCM card controls two shelves, the communications buses of the shelf backplane must be connected with two ribbon cables: one connecting their XA19 connectors, the other connecting their XA20 connectors.

SCM Card Installation Guidelines

- The SCM card installed in a SpectraComm shelf system requires SCM Application Version 5.xx to manage the network elements. In a UAS shelf system, the SCM card requires Application Version 7.xx.
- An SCM card may be installed in any slot in a SpectraComm/UAS Shelf. The SCM card requires two RJ45 connectors in Zone 1 and a DB25 F connector in Zone 3 on the SpectraComm/UAS Shelf backplane
- Perform the option setups, connections and pre-operation checks in their entirety as described in this chapter.

Unpacking Instructions

The SCM card and components are shipped in shock-absorbent packing within a corrugated box. *Table 2-1* and *Table 2-2* list the standard SCM and optional SCM equipment. Some components will not be required/supplied for your network installation.

Remove each component from the box and perform a thorough inspection. If any component appears damaged, contact the shipper immediately. All damaged components must be retained until an inspection by the shipper has been completed. If it is necessary to re-package and return the unit, use the original box and packing material

Standard Equipment

Table 2-1 Standard Equipment Checklist

Description	Connectivity	Part Number
SpectraComm Manager Card, with Ver 5.x.x (in a SpectraComm shelf system)	LAN, WAN, DBU WAN (PPP, Ethernet)	058P150-002
SpectraComm Manager Card, with Ver 7.x.x (in a UAS shelf system)		058P150-003
Adapter, 10BASE-T, twisted pair	LAN interface	029H209-001
Adapter,10BASE-2, coaxial	LAN Interface	058B033-001
Cable, Interface, 10BASE2, coaxial	LAN Interface (5, 15, and 30 meter lengths)	S-125H003-001 S-125H004-001 S-125H005-001
Cable, Interface, RJ45-toRJ45	WAN Control (CTRL) port (7, 14, and 25 foot lengths)	830-028-807 830-028-814 830-028-825
Adapter, RS232 DB25 male to RS561 8-pin modular jack	VT-100 compatible terminal	029H210-001
Adapter, DB9 female to RS561 8-pin modular jack	PC terminal emulator	029H211-001
SCM MIB	*Refer to TEAM Core Release notes for latest version.*	

Shelf Systems and Optional Equipment

The table below lists additional systems and products used with the SCM. Unless otherwise stated in the table, each shelf system includes the following components:

- base shelf and two mounting brackets (19/23-inch standard) with mounting hardware
- one power supply
- one power supply blank front panel
- one or two Zone 1 connector panels
- one 16-slot DB25 Zone 3 connector panel

Table 2-2 Shelf Systems and Optional Equipment

Associated SCM and Shelf Products	Description	Part Number
Shelf System, SpectraComm MS-2 Model 1, 100/120 VAC	Two 8-slot, dual RJ45 Zone 1 connector panels	010M054-001
Shelf System, SpectraComm MS-2 Model 2, -48 VDC	Two 8-slot, dual RJ45 Zone 1 connector panels	010M055-001
Shelf System, SpectraComm MS-2 Model 3, 220/240 VAC, International	Two 8-slot, dual RJ45 Zone 1 connector panels	010M056-001
Shelf System, SpectraComm/UAS MS-2 Model 7, 100/120 VAC	Universal Zone 1 connector panel	010M073-001
Shelf System, SpectraComm/UAS MS-2 Model 8, 220/240 VAC	Universal Zone 1 connector panel	010M074-001
Shelf System, SpectraComm/UAS MS-2 Model 9, -48 VDC, -60 VDC	Universal Zone 1 connector panel	010M075-001
Shelf System, SpectraComm MS-2 Model 10, -48 VDC with redundant power supplies	Two 8-slot, dual RJ45 Zone 1 connector panels	010M070-001
Shelf System, SpectraComm MS-2 Model 11, -48 VDC with redundant power supplies	One 16-slot, 50-pin/wire wrap Zone 1 connector panels	010M071-001
Shelf System, SpectraComm/UAS MS-2 Model 12, -48 VDC, -60 VDC with redundant power supplies	Universal Zone 1 connector panel	010M076-001
Cable, 30-pin Flat	J52 to J52	029H509-001
Cable, 40-pin Flat	J51 to J51	029H510-001
Cable, 50-pin Power	J49 to J49	024H607-001
Adapter, DB25 male to RJ45 female	CTRL port Modem	029H215-001
Kit, Zone 1 (Z1-S-B)	8-slot blank rear panel	010K341-001
Kit, Zone 1 (Z1-S-16DRJ45)	8-slot dual RJ45 connector panel	010K342-001
Kit, Zone 3 (Z1-S-DB25)	16-slot DB25 connector panel	010K339-001
RADIUS Security Client Key (Remote Authentication Dial In User Service) Purchased by the customer to activate downloaded RADIUS firmware in a non-RADIUS SCM card. *Refer to* *Appendix B, SCM with RADIUS* for details.		058U150-D01

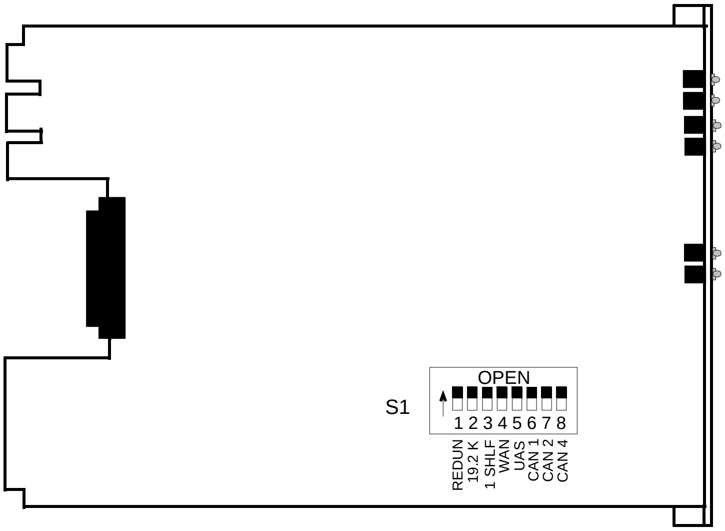
Note *Refer to the GDC website for latest software and MIB information:*
`ftp://ftp.gdc.com/pub/mibc/shelfCtrlr/scm/scm.html`

Note *The SCM WAN port is not accessible when installed in SpectraComm Shelf MS-2 Model 11 (010M071-001).*

SCM Installation

Setting SCM Card Options

The SCM has five options (S1-1 through S1-5) which can be set on the card at the **S1** switch. These switch settings are described in the table below. Three additional settings are for UAS systems customized for canned configurations (refer to *Appendix C, Canned Configurations* for details.



Note:
Switches Shown
in Default Positions

Table 2-3 SCM Card Option Switch Setting

Switch	Label	Option	Action
S1-1	REDUN	**Open**	Sets the SCM as the primary controller.
		Closed	Sets the SCM as the redundant controller.
S1-2	19.2 K	**Open**	Sets operating speed for the WAN and DBU WAN ports to 9.6 kbps.
		Closed	Sets operating speed for the WAN and DBU WAN ports to 19.2 kbps.
S1-3	SHLF	**Open**	Sets the SCM for controlling two SpectraComm/UAS shelves.
		Closed	Sets the SCM for controlling a single SpectraComm/UAS shelf.
S1-4	WAN	**Open**	Sets the SCM front panel CTRL port for a connection with a VT100-compatible terminal.
		Closed	Sets the SCM front panel CTRL port for a WAN connection to an SNMP network manager.
S1-5	UAS	**Open**	Sets the SCM for operation of a SpectraComm shelf.
		Closed	Sets the SCM for operation of a UAS shelf.
S1-6 to S1-8	CAN 1,2 4 Switches	For use In special UAS shelves. Unless instructed by your GC field representative, set all of these switches to **Open** to disable the SCM CAN function.	

Note *After the initial discovery of a two-shelf system, if S1-3 is changed from* **Open** *to* **Closed***, the SCM continues to communicate with second shelf elements, but will not detect newly installed elements there.*

Note *If you select one of the canned configurations and the SCM is not in slot 16, the* **ALM** *LED on the SCM front panel will illuminate continuously.*

Pre-Operational Checks

Power-up occurs when the card is inserted into the shelf, the SCM LEDs illuminate and the SCM performs a self-test. The tables below describe the LED status on the front panel during power-up sequences. If the SCM fails any power-up test, refer to *Service Support and Training on page xi*.

The SCM card indicates a successful power-up by turning off the LEDs in the following order: LAN SD, LAN RD, and then the others in rapid succession. Only the INS and ON LED remain illuminated. *Table 2-4* describes the status of the INS LED for primary or Redundant SCMs.

Table 2-5 describes LED status is a successful power-up. In a failed power-up, LED status will indicate problems detected during the self-test (*Table 2-6*).

Table 2-4 SCM Front Panel In Service (INS) Status Indications

INS LED	Primary SCM	Secondary SCM
ON	Active	Active
OFF	Sleep	Standby

Table 2-5 Successful Power-Up

LAN SD	LAN RD	WAN SD	WAN RD	NR	ND	INS	ON	TM	ALM	Power-Up Status
ON	ON	ON	ON	ON	ON	ON	ON	ON	ON	Power On reset state.
OFF	ON	ON	ON	ON	ON	ON	ON	ON	ON	I/O initialized.
OFF	OFF	ON	ON	ON	ON	ON	ON	ON	ON	PROM checksum test complete.
OFF	OFF	OFF	OFF	OFF	OFF	ON	ON	ON	ON	SCC3. Ethernet, RAM non-extended test complete.
OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	OFF	OFF	SCM active mode (non-redundant)

Table 2-6 Failed Power-Up

LAN SD	LAN RD	WAN SD	WAN RD	NR	ND	INS	ON	TM	ALM	Power-Up Failure
ON	ON	ON	ON	ON	ON	ON	ON	ON	ON	I/O Init/watchdog fail
OFF	ON	ON	ON	ON	ON	ON	ON	ON	ON	PROM checksum fail
OFF	OFF	ON	ON	ON	ON	ON	ON	ON	ON	RAM 5555/AAAA test pattern fail
OFF	OFF	OFF	OFF	ON	ON	ON	ON	ON	ON	RAM address test 5555/AAAA pattern fail
OFF	OFF	OFF	ON	OFF	ON	ON	ON	OFF	OFF	RAM address test 5555 pattern fail
OFF	OFF	OFF	ON	ON	OFF	ON	ON	ON	ON	RAM walking 1s data line fail
OFF	OFF	OFF	ON	ON	ON	OFF	ON	ON	ON	SCC3 internal micro loopback fail
OFF	OFF	OFF	OFF	OFF	ON	ON	ON	ON	ON	LAN internal write fail
OFF	OFF	OFF	ON	OFF	OFF	ON	ON	ON	ON	LAN internal read fail
OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF	ON	Serial number or MAC address fail

Note *If the SCM Alarm LED remains on in normal operation (not canned), check that Dip Switches S1-6 through S1-8 are in the* **`Open`** *position. If any canned switches are* **`Closed`** *and SCM is not in Slot 16, the ALM LED remains on.*

Shelf Address Selection

The plug-in modules identify the shelf where they are installed by reading the shelf address. The shelf address jumper, J50, identifies the shelf as either the base shelf or the second shelf.

J50 is located on the rear of the shelf to the left of the power supply section. Use needle-nose pliers to place the shorting plug on the center and upper pins (Address 0) for a base shelf, or on the center and lower pins (Address 1) for the second shelf.

Note *Before selecting the shelf address, turn off the power supply and remove primary (input) power from the shelf.*

Installing the SCM Card

1. Ensure that the desired switch options have been set on the SCM card S1.
2. Ensure all pre-operational check are completed and the front panel displays a successful power-up seqence.
3. Insert the card into its slot with the GDC logo on top, then slide it in until it makes contact.
4. Pull down the ejector tab and firmly push the module in until it seats in the rear connectors.
5. Proceed to make the required card and shelf connections for your network as described next.

SCM Connections

The SCM card supports management communication through the backplane LAN, WAN, and DBU WAN ports and its front panel CTRL port. Table 2-7 shows connections in a two shelf system.

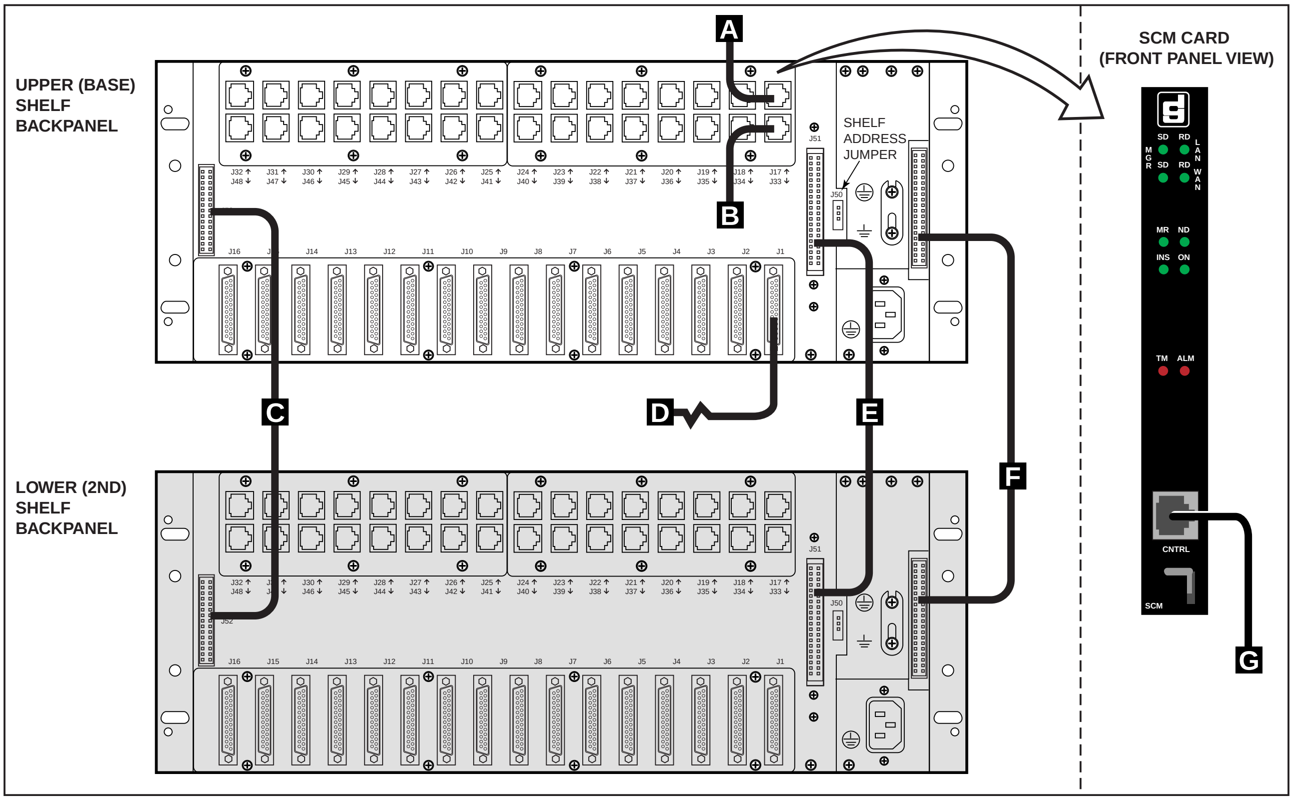


Table 2-7 Typical SCM Card Connections

Item	Location	Interface / Port	Description	Cables	Adapters
A	J17	WAN	To SNMP Network Manager, RJ45 to RJ45	830-128-XXX	029H210-001 029H211-001
B	J33	DBU WAN	J33 to modem, RJ45 to RJ45	830-128-XXX	029H210-001
C	J52 to J52	Shelf-Shelf	30-pin flat cable	029H509-001	-
D	J1	LAN	10BASE-T, twisted pair	S-078H010-XXX S-078H011-XXX	029H209-001
			10BASE-2, coaxial	S-125H003-001 S-125H004-001 S-125H005-001	058B033-001
E	J51 to J51	Shelf-Shelf	40-pin flat cable	029H510-001	-
F	J49 to J49	Shelf-Shelf	50-pin Power cable	024H610-002 (AC) 024H610-001 (DC)	-
G	Front Panel	CTRL	RJ45 to RJ45 to terminal or WAN	830-028-XXX	029H210-001 029H211-001

Note *When SCM is connected to a server, use crossover cable/adapters. When SCM is connected to a hub, use straight-thru cable/adapters. For connectivity in RADIUS systems, refer to Appendix B, SCM with RADIUS .*

LAN Port Connections

The SpectraComm Manager card supports connection to a DIX Ethernet LAN through either twisted pair or coaxial cabling. Each LAN medium requires an appropriate adapter on the Zone 3 DB25 F connector for the SCM card shelf slot. The LAN port for Slot 1 is connector J1 and the LAN port for Slot 16 is connector J16.

- The 10BASE-T (twisted pair) adapter is Part No. 029H209-001
- The 10BASE-2 (coaxial) adapter is Part No. 058B033-001

The table below describes the pins/signals for the DB25 connector and the LAN adapters.

Table 2-8 LAN Port Pinouts

DB25 Pin #	Connection	LAN Type	Function
1	Open		
2	TXO+		Transmit Positive
3	TXO-		Transmit Negative
4	RXI+	10BASE-T	Receive Positive
5	RXI-		Receive Negative
6	Ground		
7	Ground		
8	---		
9	---	Not used	
10	---		
11	Ground		
12	+5 V (fused)		Adapter power
13	+5 V (fused)		Adapter power
14	RX+		Receive Positive
15	RX-	10BASE-2	Receive Negative
16	CD+		Carrier Detect Positive
17	TX-		Transmit Negative
18	TX+		Transmit Positive
19	CD-		Carrier Detect Negative
20	---		
21			
22			
23			
24			
25	RTS		Request To Send From the terminal

Note *The SCM card detects the LAN adapter type at power-up. If the adapter is changed between 10 Base-T and 10 Base-2, the card must be re-powered.*

WAN Port Connection

The SCM card can be connected to an SNMP network manager through its WAN port. The connection employs the Point-to-Point Protocol (PPP). The network manager connected in this way may either be at the same location as the SCM card or be connected to it by a dedicated communication link such as a multiplexer channel.

The WAN port is the upper of the two RJ45 jacks associated with the SCM card slot in the SpectraComm/UAS Shelf. The SCM card uses the connector to present an EIA-561 DCE interface. Electrical signalling format is the same as that used for TIA/EIA-232F. The card presents a DCE interface at the WAN port so that a straight-through cable can be used to connect to a local SNMP network manager, which presents a DTE interface.

The WAN port operates at either 19.2 kbps or 9.6 kbps (switch selectable on the pc card). It supports asynchronous operation, 8 data bits, no parity, and 1 stop bit. When the network manager communicates with the WAN port through a dedicated communication link, you must use a crossover cable if the communication equipment at the SCM card site cannot provide a DTE interface.

The table below describes the pin/signals for the WAN port connectors and their pinouts. Refer to Table 2-9 for the pins/signals for the WAN port cable adapters.

Table 2-9 WAN Port Pinouts

Pin	Signal	Direction
1	Ring Indicator	Not used
2	Carrier Detect	From SCM card
3	Data Terminal Ready	To SCM card
4	Signal Ground	Common
5	Receive Data	From SCM card
6	Send Data	To SCM card
7	Clear To Send	From SCM card
8	Request To Send	To SCM card

Note *The SCM WAN ports are not accessible when the SCM is installed in the Model 11 SpectraComm Shelf (010M071-001), which has a 50-pin/wire wrap Zone 1 connector panel.*

Note *Shelf potential WAN ports are connectors J17 (Slot 1) through J32 (Slot 16).*

DBU WAN Port Connection

The SCM card can be connected to an SNMP network manager through its WAN port. The connection employs the Point-to-Point Protocol (PPP). The network manager connected in this way may either be at the same location as the SCM card or be connected to it by a dedicated communication link such as a multiplexer channel. The WAN port is the upper of the two RJ45 jacks associated with the SCM card slot in the SpectraComm/UAS Shelf. The SCM card uses the connector to present an EIA-561 DCE interface.

Electrical signalling format is the same as that used for TIA/EIA-232F. The card presents a DCE interface at the WAN port so that a straight-through cable can be used to connect to a local SNMP network manager, which presents a DTE interface.

The table below describes the pin/signals for the DBU WAN port connectors and their pinouts. Refer to Table 2-10 for the pins/signals for the WAN port cable adapters.

Table 2-10 DBU WAN Port Pinouts

Pin	Signal	Direction
1	Ring Indicator	To SCM card
2	Carrier Detect	To SCM card
3	Data Terminal Ready	From SCM card
4	Signal Ground	Common
5	Receive Data	To SCM card
6	Send Data	From SCM card
7	Clear To Send	To SCM card
8	Request To Send	From SCM card

Note *Do not use a modem that maintains Carrier Detect in a constant ON condition with the DBU WAN port. The constant state of Carrier Detect would prevent the SCM card from switching between the two WAN ports.*

Note *Shelf potential DBU WAN ports are connectors J33 (Slot 1) through J48 (Slot 16).*

CTRL Port Connection

The SCM card can be connected directly to either a local SNMP network manager or a VT100-compatible terminal through its front panel CTRL (Control) port. The connection employs the PPP protocol. The CTRL port functions as a temporary connection while performing configuration or diagnostics. The CTRL port is a RJ45 jack that presents an EIA-561 DCE interface.

Electrical signalling format is the same as that used for TIA/EIA-232F. The card presents a DCE interface at the CTRL port so that a straight-through cable can be used to connect to the network manager or terminal, which employes a DTE interface. CTRL port operating speed is always 9.6 kbps.

The table below describes the pin/signals for the DBU WAN port connectors and their pinouts. Refer to Table for the pins/signals for the WAN port cable adapters.

Table 2-11 CTRL Port Pinouts

Pin	Signal	Direction
1	Ring Indicator	Not used
2	Carrier Detect	From SCM card
3	Data Terminal Ready	To SCM card
4	Signal Ground	Common
5	Receive Data	From SCM card
6	Send Data	To SCM card
7	Clear To Send	From SCM card
8	Request To Send	To SCM card

Special Installation Considerations

Adapter Considerations

A cable (Part No. 830-028-8XX) is supplied for making connections at the WAN port, the DBU WAN port, or the CTRL port. This cable is equipped with an RJ45 plug connector at each end. Two adapters are available for attaching the cable to a network manager, terminal, or communication device that does not have an EIA-561 port:

- RJ45-to-DB25M adapter (GDC P/N 029H210-001)
  Description: Connects DBU WAN to modem or WAN to terminal with DB25
- RJ45-to-DB9F adapter (GDC P/N (Part No. 029H211-001)
  Description: Connects WAN to PC terminal with DB9

WAN / DBU WAN Port Considerations

- When the network manager communicates with the WAN port through a dedicated communication link, you must use a crossover cable if the communication equipment at the SCM card site cannot provide a DTE interface.
- The DBU WAN port is designed to respond to switched network connections initiated from the SNMP network manager site and cannot itself initiate switched network connections. Connect it to an auto-answer modem.
- The DBU WAN port and the WAN port employ circuitry in common on the SCM card. When Carrier Detect goes on at the DBU WAN port, the SCM card automatically disables the WAN port. When Carrier Detect goes off, the SCM card disables the DBU WAN port and re-enables the WAN port.

SCM Power-Down Considerations

The SCM card stores factory-installed and user-entered data such as IP addresses, subnet masks, and special operational data such as the RADIUS Client Key. If the SCM card is not powered for extended periods, the on-board capacitor will become depleted and this data stored in memory will be lost. When the SCM card is put back in service and powered up, the user will have to re-enter the network data. In RADIUS systems, the user will also have to re-install the RADIUS Client Key, enable RADIUS, and re-configure RADIUS for the network.

Note *For details on re-installing a lost RADIUS Client Key and all associated RADIUS setups, refer to SCM RADIUS Field Upgrade in Appendix B.*

Chapter 3: SCM Configuration

SCM Interface Overview

This chapter describes the procedures for configuring the SCM for the desired interfaces. The SCM card is controlled by SNMP management or via its terminal interface. The terminal interface is accessed at a VT100-compatible terminal or a computer using the Telnet protocol. The terminal interface must be used to configure the IP addresses and subnet masks required by the SCM for both SNMP and Telnet communications.

In order for the SCM card to communicate with an SNMP manager, each port must have an IP address for recognizing incoming messages and identifying outgoing messages. In those installations where management communication must pass through a router between the manager and the SCM card, you must configure the card with the IP address of the router. The following paragraphs explain how to acquire IP addresses, and configure the SCM ports in various network arrangements using the front panel and backplane interfaces: LAN, WAN, DBU WAN and CTRL.

IP Addressing the Interfaces

On the SCM card, the LAN port and CTRL port each have an individual address. The WAN port and DBU WAN port share an address. Each of these addresses are associated with a subnet mask which is a number that is used to identify a subnetwork so that IP addresses can be shared on a local area network. A subnet mask differentiates the IP address so that there is a distinction between a port's subnet address and its individual address.

Note *When creating IP addresses for LAN and WAN ports, the WAN IP address must have a higher network number.*

Manually Configured IP Addressing

Manually configured IP addresses and subnet masks are established by the user locally at the terminal interface or remotely via a Telnet session. IP addresses are stored in SCM nonvolatile memory and retained when there is no power to the card. For each port, the original default address is 0.0.0.0 and the default subnet mask is 255.255.255.0. Refer to the tables that follow for typical network deployments and IP addressing via the terminal interface or a Telnet session. IP configuration procedures are described later in this chapter in the IP Address Menu section.

Auto Discovered IP Addressing

Auto discovered addresses are determined by the SCM through the active interface port. They are stored in SCM volatile memory and lost any time the SCM card is powered down. When power is applied to the SCM, and if the address in nonvolatile memory for the active communication port is 0.0.0.0, the card attempts auto discovery through the port. Auto discovery is disabled when any other address is stored in the nonvolatile memory.

When the active port is either WAN, DBU WAN or CTRL, Auto discovery uses IPCP during the negotiation of a PPP link. When the active port is LAN, Auto discovery uses RARP.

Single LAN Management

In a single LAN environment, the SNMP network manager and one or more SCM cards are connected to the same LAN segment. All communication between the network manager and the SCM card(s) takes place over the Ethernet link.

Each SCM card can communicate independently using its own set of MAC and IP addresses. The IP addresses of the manager and the SCM card LAN port should be set for the same subnetwork. The SCM does not need to route packets in this type of LAN environment, and no SCM Gateway address is required. Table 3-1 and the associated figure provide an example of a single LAN environment and its IP addressing.

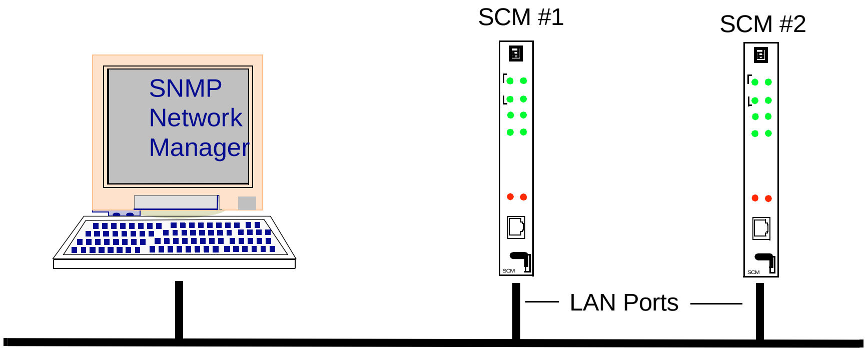


Table 3-1 Typical Single LAN Environment

LAN Management	Example IP Addressing	
SNMP Network Manager	IP Address	192.9.200.1
SCM Card 1	LAN IP Address	192.9.200.2
	Subnet Mask	255.255.255.0
SCM Card 2	LAN IP Address	192.9.200.3
	Subnet Mask	255.255.255.0

Note *There must be a RARP server on the same LAN segment as the SCM. The RARP table of the server must be pre-configured with the SCM MAC address (see inside SCM front panel) and the LAN port IP address.*

Segmented LAN Management

In a segmented LAN environment, the SNMP network manager and one or more SCM cards are connected to different LAN segments. All communication on the Ethernet link between the network manager and the SCM card must pass through the router, which acts as the gateway between the two LAN segments.

The SCM card requires a Default Route IP Address which is the IP address of the router. The IP addresses of the manager and the SCM card LAN port should each be set for its own subnetwork. Table 3-2 and the associated figure provide an example of a single LAN environment and its IP addressing.

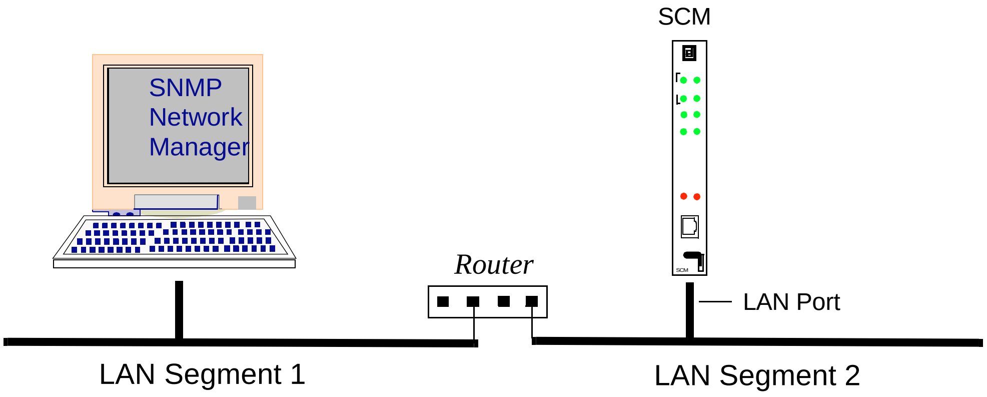


Table 3-2 Typical Segmented LAN Environment

LAN Management	Example IP Addressing	
Router	LAN Segment 1 IP Address	192.9.200.40
	LAN Segment 2 IP Address	192.9.100.40
SCM Card	LAN IP Address	192.9.100.3
	Subnet Mask	255.255.255.0
	Default Route	192.9.100.40

Note *There must be a RARP server on the same LAN segment as the SCM. The RARP table of the server must be pre-configured with the SCM MAC address (see inside SCM front panel) and the LAN port IP address.*

Local WAN Management

In a local WAN environment, the SNMP network manager communicates with one or more SCM cards via WAN connections. Each SCM card communicates with the manager independently, employing Point-to-Point protocol (PPP) and using its own IP address.

The IP addresses of the SNMP manager and the SCM card WAN port should be set for the same subnetwork. Thus, a Default Route address for the SCM is not required. Table 3-4 and the associated figure provide an example of a local WAN environment and its IP addressing.

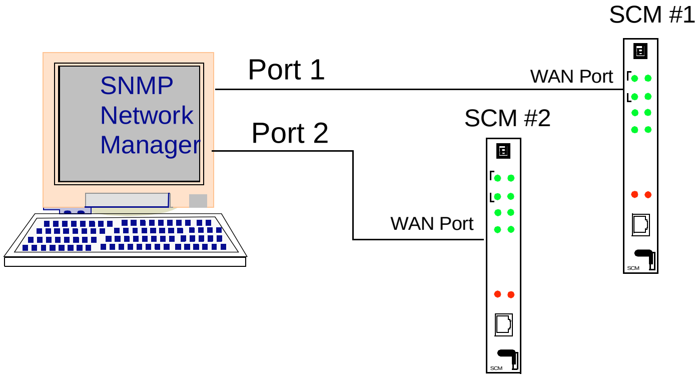


Table 3-3 Typical Local WAN Environment

WAN Management	Example IP Addressing	
SNMP Network Manager	Port 1 IP Address	192.9.10.1
	Port 2 IP Address	192.9.20.1
SCM Card 1	WAN IP Address	192.9.10.2
	Subnet Mask	255.255.255.0
SCM Card 2	WAN IP Address	192.9.20.3
	Subnet Mask	255.255.255.0

Single WAN Management

In a single WAN environment, the SNMP network manager communicates with one SCM card via one WAN connection, then communicates with one or more SCM cards through a private 10Base-2 Ethernet link. Each SCM card communicates with the manager independently, employing Point-to-Point protocol (PPP) and using its own IP address.

The IP addresses of the SNMP manager and the SCM card WAN port should be set for the same subnetwork. Thus, a Default Route address for the SCM is not required. Table 3-4 and the associated figure provide an example of a local WAN environment and its IP addressing.

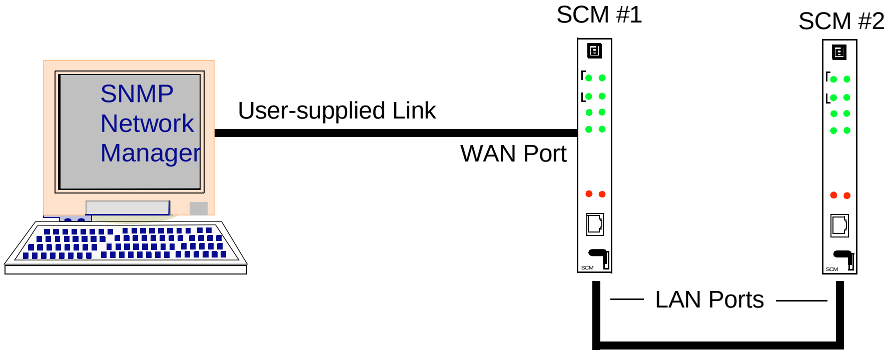


Table 3-4 Typical Single WAN Environment

WAN Management	Example IP Addressing	
SNMP Network Manager	IP Address	192.9.10.1
SCM Card 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 Card 2	LAN IP Address	192.9.200.3
	Subnet Mask	255.255.255.0
	Default Route IP Address	192.9.200.2

Dial Backup WAN Management

In a Dial Backup (DBU) WAN environment, the SNMP network manager communicates with an SCM card via a WAN connection and also furnishes a Dial Backup (DBU) WAN connection.

The WAN and DBU WAN ports share common resources on the SCM card; thus only one port can be active at a time. If a PPP session is in progress through the WAN port when the DBU WAN port DCD signal activates, the existing session is interrupted. A new PPP session must be established each time the state of DCD changes at the DBU WAN port.

The IP addresses of the manager and the SCM card WAN ports should be set for the same subnetwork. Thus, no SCM Default Route address is required. Table 3-5 and the associated figure provide an example of a DBU WAN environment and its IP addressing.

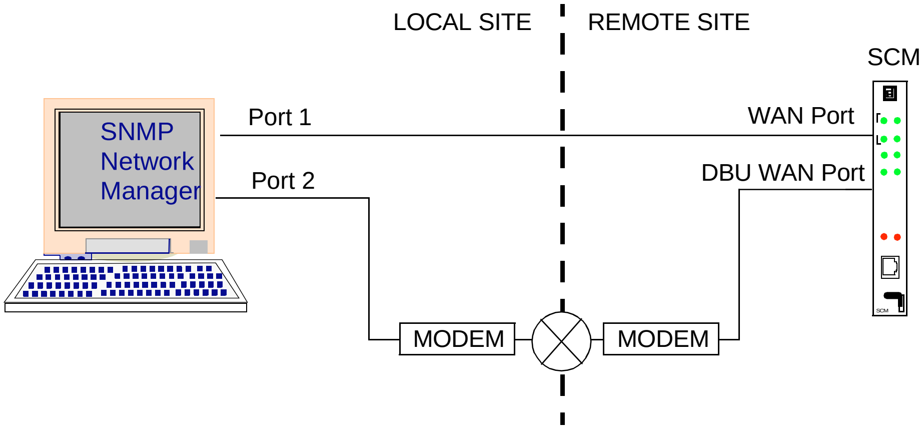


Table 3-5 Typical DBU WAN Environment

Management	Example IP Addressing	
SNMP Network Manager	Port 1 IP Address	192.9.10.1
	Port 2 IP Address	192.9.10.2
SCM Card	WAN IP Address	192.9.10.3
	Subnet Mask	255.255.255.0

Note *The SCM will use the WAN IP address for both the WAN and the DBU WAN ports.*

Segmented WAN Management

In this type of WAN environment, the SNMP network manager and the SCM card communicate through a terminal server on the LAN where the SNMP manager is connected. The connection from the terminal server to the SCM is made through the SCM card WAN port.

The WAN port IP address should be the same as the Segment 2 IP address of the terminal server. The WAN port subnet mask should be set for a Class B subnet. Table 3-6 and the associated figure provide an example of WAN/LAN environment and its IP addressing.

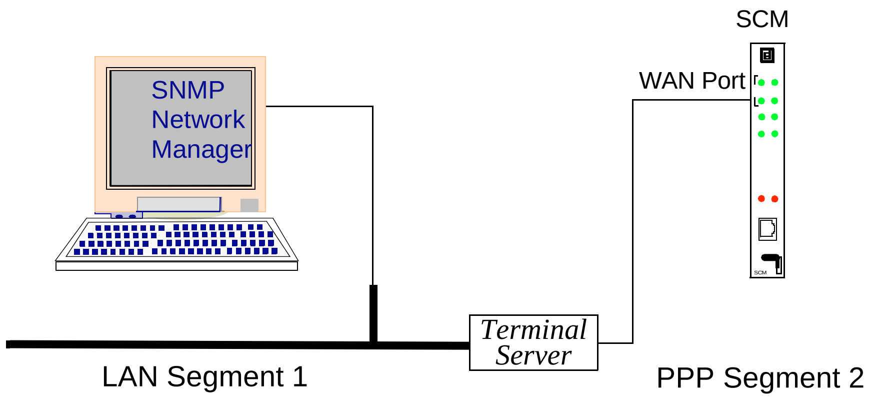


Table 3-6 Typical Segmented WAN Environment

SNMP Network Manager	IP Address	192.9.200.1
Terminal Server	Segment 1 IP Address	192.9.200.40
	Segment 2 IP Address	192.9.100.40
SCM Card	WAN IP Address	192.9.100.40
	Subnet Mask	255.255.255.0

SCM Redundancy Management

In a SpectraComm/UAS system that supports redundancy, there is a primary SCM and a standby (redundant) SCM. The redundant SCM takes over when the primary SCM is not functioning properly. Each SCM has its own separate connection to the LAN and unique IP address by which it can be addressed. Figure 3-1 shows a typical single shelf and a typical shelf pair equipped with SCM Redundancy.

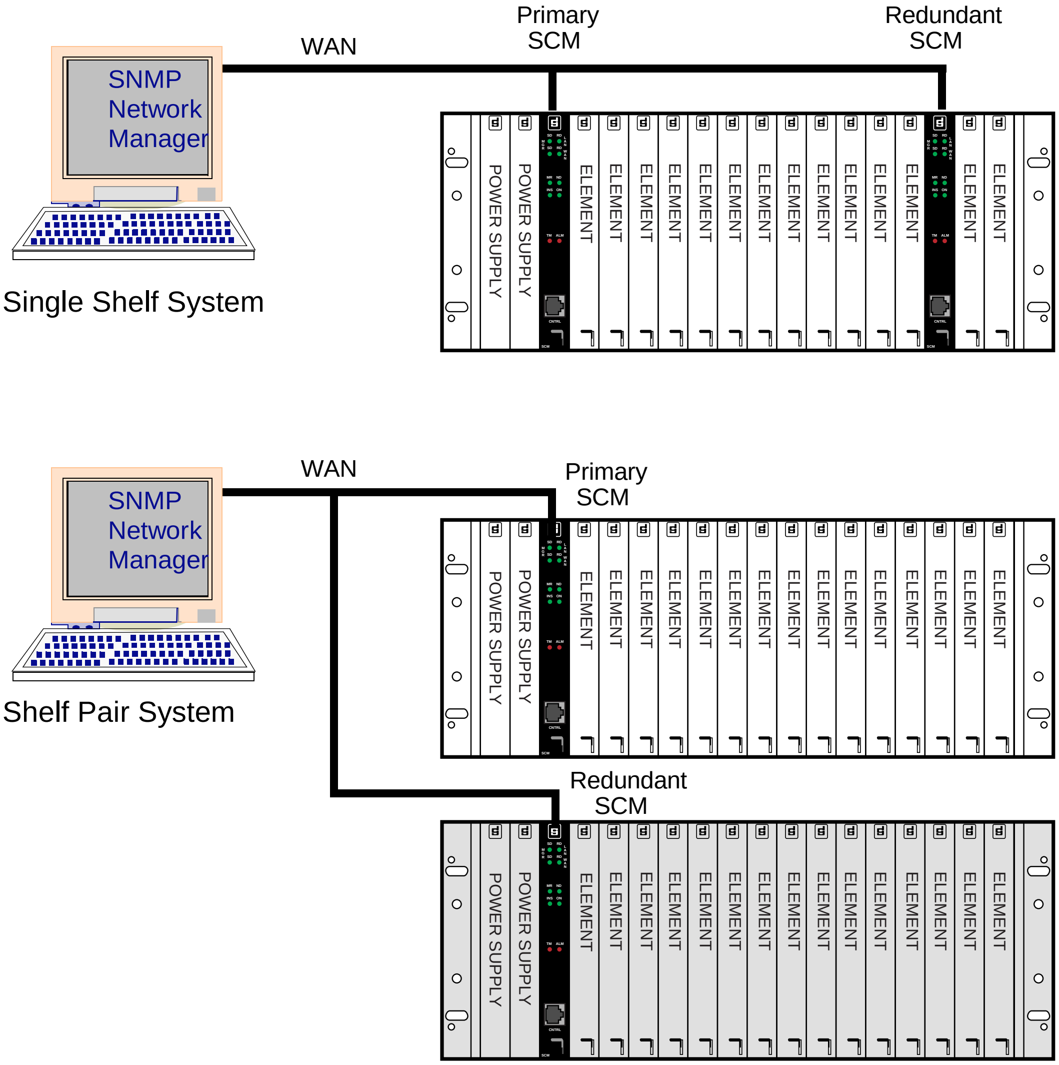


Figure 3-1 SpectraComm/UAS Systems with SCM Redundancy

Activating SCM Redundancy

To activate Redundancy in a single or double shelf system, set the dip switch on one SCM card for primary and set the other SCM for standby. There can only be one primary and one standby assignment in each shelf or shelf pair.

When the primary SCM is in control and the redundant SCM is in standby, communications between the primary SCM and the redundant SCM occurs on the management bus (the method of communicating with the network elements). Thus, to the primary SCM, the redundant SCM looks like a network element and appears in its node table.

Swapping SCM Redundancy

There are three methods, described below, for swapping the SCMs from their dip switch settings of primary to a standby:

- Alive Trap Swap
- Automatic Swap
- Manual Swap

Active Trap Swap

In an Alive Trap swap, the primary SCM sends a trap to the SNMP manager every [n] minutes, based on the value set in the scmAliveTrapInterval MIB variable. When the SNMP manager does not receive the trap on schedule, it commands the redundant SCM to become primary SCM through the scmOperatingMode MIB variable.

Automatic Swap

In an Automatic swap, the redundant SCM automatically takes over as the primary SCM. This occurs when the primary SCM does not communicate with the redundant SCM for longer than the time period indicated in the **scmRedundantTimeOut MIB** variable.

Manual Swap

In a Manual swap, the operator initiates a command to the redundant SCM, causing it to switch from Standby mode to Active mode, forcing the primary SCM into Sleep mode. This command can be issued to the redundant SCM from one of two interfaces:

- From the TEAM Core software application,
  via the **Redundant SCM Options->Operating Mode**
- From the SCM terminal interface,
  via the Master Table **Switch to Active Mode**

Note *In an Automatic swapping of the SCM, the default value of the* ***scmAliveTrapInterval MIB*** *variable is zero. At this value, no automatic swapping will be performed.*

Note *For detailed redundancy procedures, refer to Chapter 2, Installation and Setup for the switch location on the SCM card; refer to Chapter 3, SCM Configuration for Master Table procedures.*

SCM Redundancy Restoral Procedure

When the redundant SCM has asserted control, a hardware reset must be performed on the primary SCM before it can resume control. Follow these steps to return the SCMs to their normal modes of operation:

1. Perform a hardware reset on the primary SCM by power cycling the SCM, i.e., removing the card from the shelf, then putting it back.
2. At the SCM Configuration screen, use **Configuration->Navigate->Redundant SCM Options** to command the active redundant SCM to return to Standby Operating Mode.
3. At the SCM Configuration screen, use **Configuration->File->Save to Unit** to save this mode selection to the redundant SCM.

OR:

1. Remove power from both the primary and redundant SCM cards. Then, power-up the primary SCM, and then power-up the redundant SCM.

Front Panel CTRL Port Management

The diagram below shows how to hook up a local terminal, or hook up a remote terminal using a modem. Table 3-7 details the cables [C#] and adapters [A#] use in the diagram. Refer to Table B-5 for initialization strings in the Answer and Originate modems.

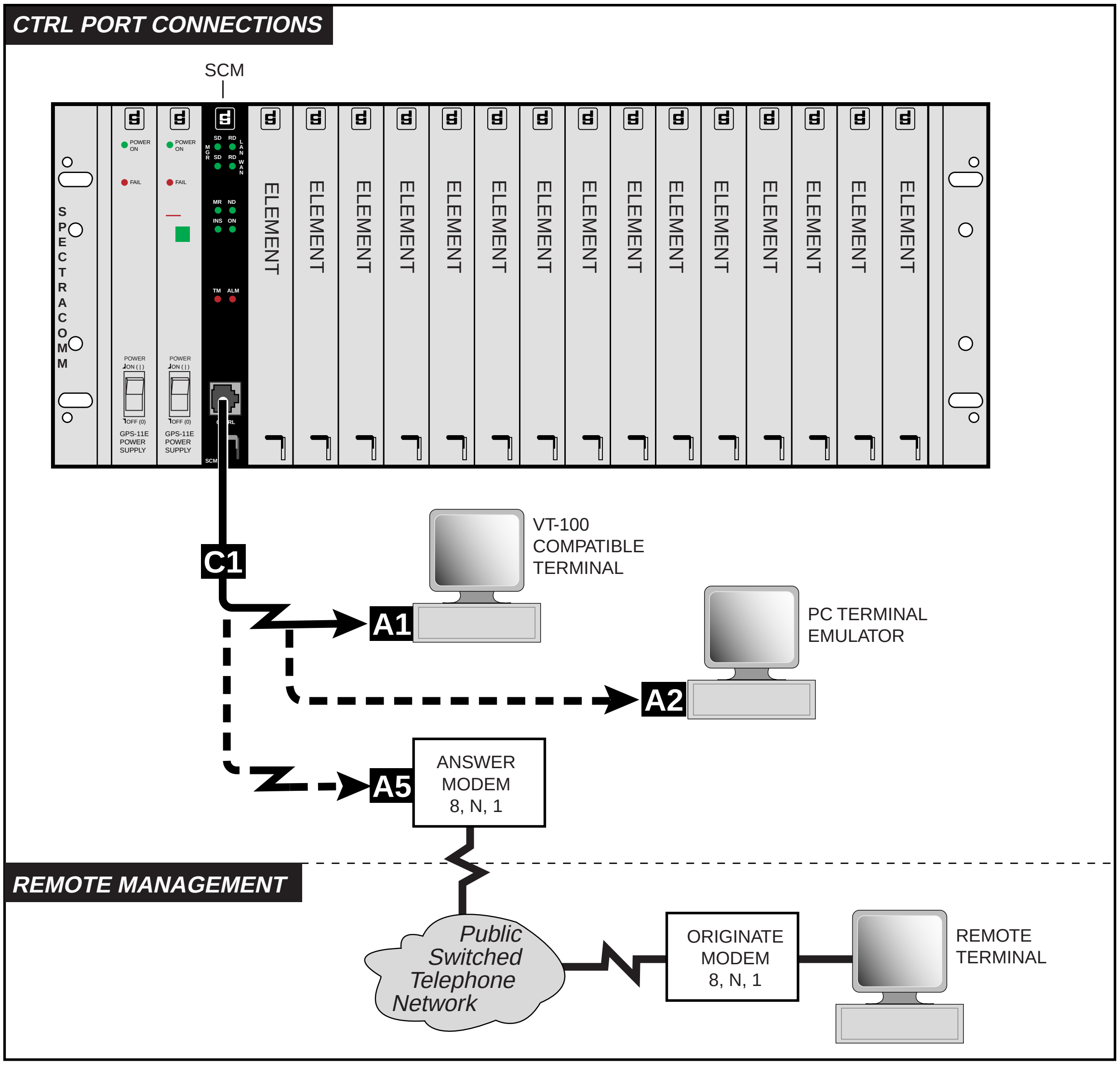


Table 3-7 Front Panel CTRL Management

Cable/Adapter	Location	Description	Part Number
C1	SCM CTRL Port	RJ45 to RJ45 cable, S/T, non-keyed	830-128-807
A1	Terminal	RS232 DB25 male to RS561 adapter	029H210-001
A2	Terminal	DB9 female to RS561 adapter	029H211-001
A5	Answer Modem	DB25 male to RJ45 female adapter	029H215-001

Note *For the highest level of security it is recommended that a CTRL port modem be hooked up for limited and specific purposes and not for continuous remote management.*

SCM Configuration

At the front panel CTRL port, the user can access a Main Menu and subordinate menus/screens to configure the desired interfaces and prepare the SCM for operation. Screen descriptions and associated procedures are provided below.

Note *When using a Telnet interface, only the Element Access function is displayed at the Main Menu. To access the IP address function remotely, access IP Address*

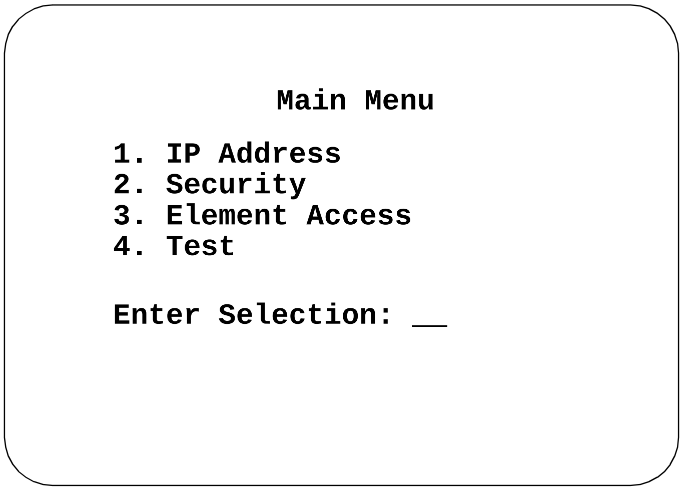
Remote SCM Configuration

1. Connect to the LAN or WAN.
2. Telnet to the SCM which will prompt you for a login.
3. Perform the login sequence as described in this chapter in the *Security Screen* procedure.
4. After the SCM verifies the login sequence and authorizes the dial in user, the Shelf Inventory screen appears.
5. Proceed to *Chapter 4: SCM Operation Overview* for detailed shelf and network element information and procedures.

Local SCM Configuration

1. Connect a VT100-compatible terminal to the front panel CTRL port.
2. Set Switch S1-4 on the card to the **Open** position. This is the factory default which allows the terminal to function with the SCM card.
3. At the terminal screen, press **Enter**. The terminal screen will display the Main Menu (shown below) along with read-only SCM information. Table 3-8 describes the menu selections.

Note *The first screen to appear is always the last screen used in a previous session. To return to the Main Menu, back out of the displayed screen until the Main Menu appears*



```
              Main Menu

     1. IP Address
     2. Security
     3. Element Access
     4. Test

     Enter Selection: __
```

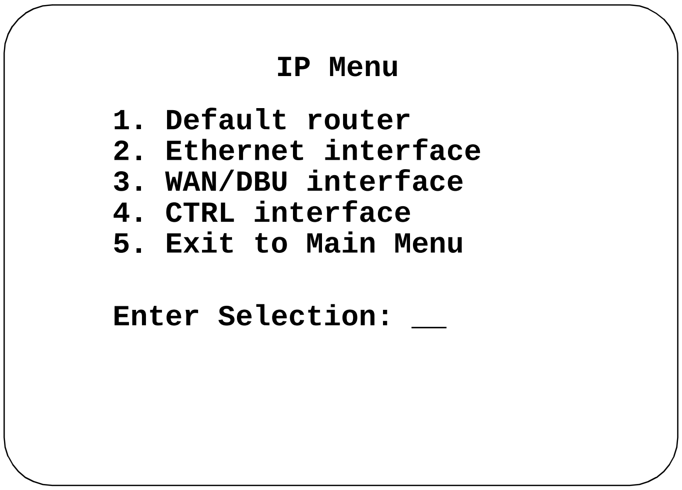
Table 3-8 Main Menu Selections

Menu Item	Description
1. IP Address	Advances to the IP Address menu for setting addresses at any interface.
2. Security	Advances to the Security screen for community name, telnet and port security.
3. Element Access	Accesses the terminal interface to control the SCM and all compatible network elements installed in the SpectraComm/UAS shelf with it.
4. Test	Password-protected test function. For use by authorized GDC personnel only.

Note *On capable systems, the Main Menu contains a hidden submenu for configuring and enabling the optional RADIUS software. Refer to Appendix B, SCM with RADIUS for details.*

IP Address Menu

At the Main Menu, press **1** to access the IP Menu. This menu allows the user to manually configure IP address information in the SCM card from the terminal interface. Table 3-9 describes the menu selections. IP address procedures follow the table.



```
                IP Menu

      1. Default router
      2. Ethernet interface
      3. WAN/DBU interface
      4. CTRL interface
      5. Exit to Main Menu

      Enter Selection: __
```

Table 3-9 IP Menu Selections

Menu Item	Description
1. Default router	Configures the IP address for the default router.
2. Ethernet interface	Configures the IP address for the LAN ports.
3. WAN/DBU interface	Configures the IP address for the WAN or DBU WAN ports.
4. CTRL interface	Configures the IP address for the CTRL port.
5. Exit to Main Menu	Returns to the Main Menu

Changing IP Addressing

1. Access the Main Menu as described above.

2. At the Main Menu, type **1** and press **Enter**. The IP menu appears.

3. At the IP menu, press **1** to configure the address and subnet mask for a default router, if needed. Then, select **L** (LAN), **W** (WAN), or **C** (CTRL). Otherwise, press **2**, **3**, or **4** to configure the LAN, WAN/DBU or CTRL ports with an IP address and a subnet mask.

4. Depending on your selection, the next screen displays the selected interface/router, and one of the following status messages:

Message	Description
Waiting for RARP address	The nonvolatile address is 0.0.0 and the SCM card has not yet received an address from a RARP server.
Using RARP IP Address	The nonvolatile address is 0.0.0 and the SCM card is using the displayed address, received from the RARP server.
Using non-volatile ram IP address	The card is using a manually configured address.

5. The screen then displays the current nonvolatile address, the default address of 0.0.0.0 or a manually entered address, as shown below:

```
Non-volatile IP Address:xxx.xxx.xxx.xxx

Enter address:__
```

6. Press **Enter** to leave the displayed address current as shown. To enter a new address type in the address and then press Enter.

Note *If any part of the address you enter is outside the valid range (0 - 255), an* ***INVALID ADDRESS*** *message is displayed. If you enter 0.0.0.0 in place of a previously configured address, the SCM card tries Auto Discovery to determine an address.*

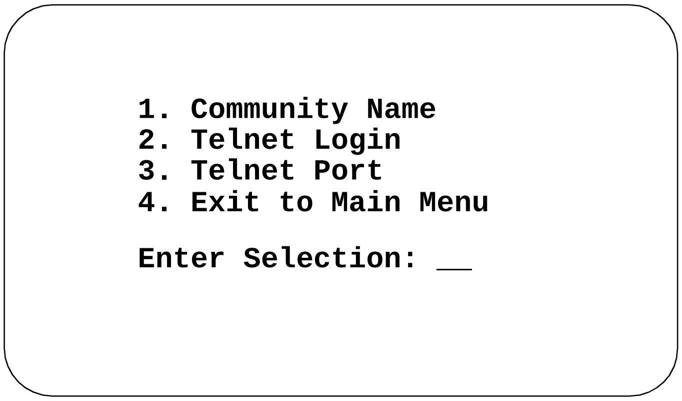
7. When you press Enter in the above step, the screen then displays the current Non-volatile submask (Default is 255.255.255.0), as shown below:

```
Non-volatile submask:xxx.xxx.xxx.xxx

Enter address:__
```

8. Press **Enter** to leave the displayed address current as shown. To enter a new address type in the address, then press Enter. The screen then returns to the IP Menu.
9. Repeat this procedure until all required interfaces have the desired addresses and submasks.

Security Screen

At the Main Menu, press **2** to access the Security screen. This screen allows the super-user to control the access to the network elements. Table 3-10 describes the screen selections. Security procedures follow the table.



```
1. Community Name
2. Telnet Login
3. Telnet Port
4. Exit to Main Menu

Enter Selection: __
```

Table 3-10 Security Selections

Selection	Description
1. Community Name	Display or change the Super User Community Name which is used to read/ write any MIB object. DEFAULT: **scmadmin**
2. Telnet Login	Display or change the Telnet login password. DEFAULT: **scmadmin**
3. Telnet Port	Display or change the Telnet port number. DEFAULT: **23**
4. Exit to Main Menu	Returns to the Main Menu

Security Considerations

- The Telnet login password cannot be changed via a Telnet connection. It can only be changed at the Security screen via a CTRL port.
- **IMPORTANT!** For a higher degree of security, it is strongly recommended that the Telnet password be changed from the default to some other unique textstring. The highest degree of security is achieved by disabling Telnet communication.
- Telnet connectivity can be disabled via TEAM management, if available. As an alternative, you can disable Telnet connectivity with a MIB browser at the SNMP object **scmTelnet** in the scmMaster group in GDCSCM-MIB. The default value of **scmTelnet** is (**1**) enable. If set to (**2**) disable, all Telnet connections to the SCM are refused.

Security Configuration Procedures

1. Press **1** to display the Super User Community Name. Press **Enter** to leave the name unchanged, or type up to 32 characters at the prompt to change the Name, then press **Enter**.
2. Press **2** to display the Telnet Login password. Press **Enter** to leave the password unchanged, or type up to 32 characters at the prompt to change the password, then press **Enter**.
3. Press **3** to display the Telnet port number. Press **Enter** to leave the port number unchanged, or type up to five digits at the prompt to change the port number, then press **Enter**.

Element Access Function

The Element Access function allows the user to employ a series of screens to identify the network elements in a shelf or pair of shelves that are co-located in the shelf with the SCM. From these screens the user can select and control network elements or the SCM itself. The Element Access function is also available via Telnet connection.

In either a CTRL port or a Telnet connection, the initial screen displayed is the Shelf Inventory screen, which identifies the devices installed in the shelf (or pair of shelves) that contains the SCM. At the Shelf inventory screen, you can select the network element, including the SCM itself, to which you need access.

Note *Refer to Chapter 4, SCM Operation for detailed information on the Element Access screens and their associated functions.*

Element Access via the CTRL Port

1. Access the Main Menu from the CTRL port as described above.
   (The operating speed is 9600 bps.)
2. At the Main Menu, type **3** and press **Enter**. The Shelf Inventory screen appears.
   Proceed to *Chapter 3, SCM Configuration* : *SCM Operation Overview* for detailed shelf and network element information.

Operational Checks

The following paragraphs provide information on identifying and correcting common minor problems that may occur with the SCM. Before investigating a problem, check connectivity basics:

- Check that the SCM is plugged into the SpectraComm/UAS shelf correctly.
- Check that the power to the SpectraComm/UAS Shelf is on and that the POWER ON LED is lit.
- Check that all cables are properly connected.
- Check that all switch settings are in their proper positions.
- Check that all LEDs on the front panel of the SCM except INS and ON are Off.

Unable To Communicate via LAN

Network manager communication problems on the LAN may result from the following causes:

- IP Address not set correctly in SCM.
- IP Address for the SCM in the network manager not correct.
- Cables not installed.
- Default Route not set when router exists.

Solutions

1. Connect a VT100-compatible terminal to the CTRL port to check the IP Address in the SCM and ensure the value is correct. If using RARP, ensure that the MAC-to-IP Address is mapped correctly at the network manager or server.

2. Check to make sure that the Subnet Field of the IP Address on the network manager matches that of the SCM.

3. Use a VT100-compatible terminal connected to the CTRL port to check that the Subnet Mask of the SCM LAN port is set correctly.

4. When a router exists, use a VT100-compatible terminal connected to the CTRL port to set the Default Route in the SCM.

Additional Checks for this Condition

- If SNMP communications to the SCM are still not available at this point, perform ping to determine whether the SCM is communicating on the network.

- If ping works, use TFTP to determine the mode of operation.

- If TFTP mode indicates application, walk the system group in MIB-II.

- If communications are still not available, contact your GDC representative.

Note *The INS LED will be Off when primary SCM is in sleep mode or when redundant SCM is in standby mode.*

Unable To Communicate via WAN

- Network manager communication problems on the WAN may result from the following causes:

- IP Address not set correctly in SCM.

- IP Address for the SCM in the network manager not correct.

- Cables not installed.

Solutions

1. If SNMP communications to the SCM are still not available at this point, perform ping to determine whether the SCM is communicating on the network.

2. Use a VT100-compatible terminal connected to the CTRL port to check the IP Address in the SCM and ensure the value is correct.

3. Check to make sure that the Subnet Field of the IP Address on the network manager matches that of the SCM.

4. Make sure that the link connection is established.

Note *If communications are still not available, contact your GDC representative.*

Unable To Communicate with Network Elements

Communication problems involving a specific network element may result from the following causes:

- Data set not properly seated in the SpectraComm/UAS Shelf.
- Data set not working properly.

Solutions

1. Physically re-seat the data set card.
2. Consult the data set user manual and verify that the card is functioning properly.
3. Check the network element's status in the SCM slot table. The status should be Active.

Note *If the status is inactive or active with errors, contact your GDC representative.*

TRAPs Not Being Received

Problems with TRAPS not being received at a network manager may result an improper setup of the SCM trap address table (i.e., incorrect entries by the network manager).

Solutions

1. Verify that the IP address and UDP port number of the network manager are correct.
2. Verify that the community name where traps are to be received is correct.

Unable to Write to MIB

When MIB variables can be read but not written, it may be caused by the Community name having been defined with read-only access.

Solutions

1. Check the community name being used on the network manager against that defined in the SCM.
2. If the community name exists, set its access to read-write. If the community name does not exist, create an entry.

Chapter 4: SCM Operation

SCM Operation Overview

Once the SCM is configured for the desired communication interfaces, several management functions can then occur between the SCM card and the network manager:

This chapter describes these management operations in the screens which are accessed through the Element Access menus and screens and through the SCM menus and screens. Management operations can be performed as follows:

- via one front panel session at a time
- in up to four simultaneous Element Access Telnet sessions
- via multiple simultaneous Element Access terminal interface sessions
- in a SCM Firmware Download session.

Note *The response times of the individual terminal interface sessions can be affected by the number of sessions taking place simultaneously.*

Note *There is a ten-minute inactivity timer on terminal interface functions. If you do not type any characters for ten minutes, the SCM closes the session.*

Connectivity Limitations

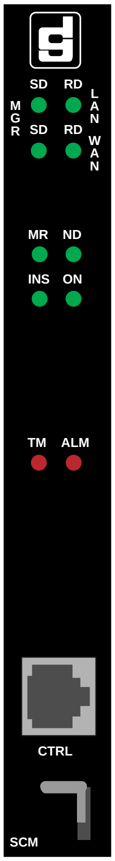
Although the SCM can conduct multiple simultaneous communications, other network elements can engage in only one terminal interface session at a time. If you select a slot (not the SCM) while the network element is already engaged in a session, the SCM responds with the following message:

```
A session with [Slot #] is currently active (Press Enter).
```

Front Panel Management

The SCM front panel informs the user how the various network and interface operations are performing. Table 4-1 describes the SCM Front Panel and the actions of the LED indicators.

Table 4-1 SCM Front Panel Features

SCM Front Panel	LED / Port	Description
 SD RD M G R L A N SD RD W A N MR ND INS ON TM ALM CTRL SCM	LAN SD LAN Send Data	Flashes GREEN when sending management data through the LAN interface.
	LAN RD LAN Receive Data	Flashes GREEN when receiving management data through the LAN interface.
	WAN SD WAN Send Data	Flashes GREEN when sending management data through the WAN or the WAN DBU ports.
	WAN RD WAN Receive Data	Flashes GREEN when receiving management data through the WAN or the WAN DBU ports.
	ND Network Data	Flashes GREEN when the SCM is sending data to a network element through the backplane.
	NR Network Response	Flashes GREEN when the SCM is receiving data from a network element through the backplane.
	ON	Illuminates GREEN when Power is ON.
	INS In Service	Illuminates GREEN when the SCM is active. Flashes GREEN while SCM is in boot mode.
	TM Test Mode	Illuminates RED during the Power-on Self test
	ALM Alarm in Shelf	Illuminates RED when an alarm condition is detected.
	CTRL port	RJ45 Control port for EIA-561 signaling: Provides connectivity to an SNMP network manager or a VT-100-compatible terminal.

Element Access Management

Element Access is launched after a successful user login via a Telnet connection or when Element Access is selected at the Main Menu. All SCM management functions for network elements, including the SCM card are then provided by a series of grouped menus, screens and tables.

The first screen to appear is the Shelf Inventory screen, which depicts all network elements in the shelf or shelves. The user can select a SCM or a non-SCM network element from the Shelf Inventory screen for management. When the SCM card is selected, the Main SCM Menu appears. The the Main SCM Menu and its subordinate menus/screens are described in the paragraphs below.

Note *If a shelf has a redundant SCM, it cannot be accessed through the primary SCM even though the redundant SCM appears in the primary SCM's Shelf Inventory. To perform terminal interface functions on a redundant SCM while it is in Standby mode you must either make a connection to its front panel CTRL port or Telnet to its IP address.*

Element Identification

In order to use the Element Access screens for a terminal interface session, a network element must be identified in the SCM by its slot number in the shelf. According to the functionality of the element, it may be necessary to also specify a Line number and/or a Drop number. These identifying numbers are described below.

Slot Number
The Slot number identifies a network element by its physical slot location in the shelf (1 - 16) or in the shelf pair (1 - 32). You must always select a slot number to access an element.

Line Number
A Line number is required with a slot number in order to access an element when the element supports more than one communication link. Each line is treated as a separate device, so the user must select a line number working with a multi-line device.

Drop Number
A Drop number is required with a slot number to access one or more dedicated remote units which are associated with a shelf element. If a shelf element supports remote units, the user can specify a drop number to access the remote units.

Circuit ID
A Circuit ID is used to identify an element according to a slot number (1 - 32) and a user-configured Name and ID.

Note *The Dual V.34 modems and the SC 5034 DSEs each support two links. To access these network elements, you must specify an appropriate line number.*

Note *The master unit located in the shelf with the SCM site is always Drop 0.*

Element Access Screens

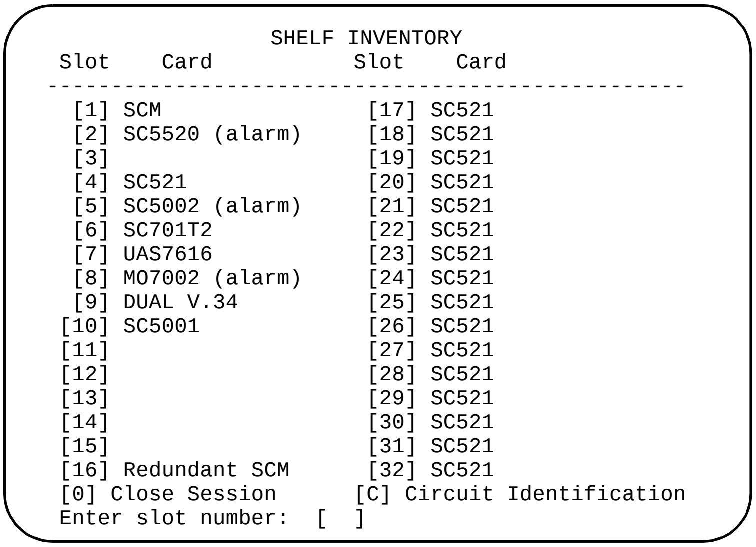
The SCM provides four screens which navigate the user into a terminal interface session. The Shelf Inventory screen is always the initial point of entry for accessing any element by its slot number. Other access screens are launched only when the user selects an element that requires a line number, drop number and/or a circuit identifier. Each screen and its associated functions are described below.

Note *On Element Access screens a plus (**+)** sign next to the slot number indicates a device that has one or more dedicated remotes associated with it. An Alarm tag next to the factory-assigned card description, i.e.,* ***SC5520 (alarm)****, indicates an alarm condition.*

Note *A device displayed in the Shelf Inventory may not necessarily support a terminal connection via the SCM.*

Shelf Inventory Screen

The Shelf Inventory screen displays the current population of the shelf or shelf pair that contains an SCM. The SCM detects the elements installed with it and creates the inventory automatically: up to 16 in a single shelf and up to 32 in a shelf pair. Figure 4-1 illustrates a typical Shelf Inventory screen from a shelf pair installation of the SCM. When the SCM is configured for one shelf, slots 17 - 32 will not be present.



```
                  SHELF INVENTORY
 Slot    Card           Slot    Card
--------------------------------------------------
  [1] SCM                [17] SC521
  [2] SC5520 (alarm)     [18] SC521
  [3]                    [19] SC521
  [4] SC521              [20] SC521
  [5] SC5002 (alarm)     [21] SC521
  [6] SC701T2            [22] SC521
  [7] UAS7616            [23] SC521
  [8] MO7002 (alarm)     [24] SC521
  [9] DUAL V.34          [25] SC521
 [10] SC5001             [26] SC521
 [11]                    [27] SC521
 [12]                    [28] SC521
 [13]                    [29] SC521
 [14]                    [30] SC521
 [15]                    [31] SC521
 [16] Redundant SCM      [32] SC521
 [0] Close Session      [C] Circuit Identification
 Enter slot number:  [  ]
```

Figure 4-1 Typical Shelf Inventory Screen (Shelf Pair shown)

Shelf Inventory Screen Procedure

1. At the Shelf Inventory screen, select a slot number to access the terminal interface of the desired network element.

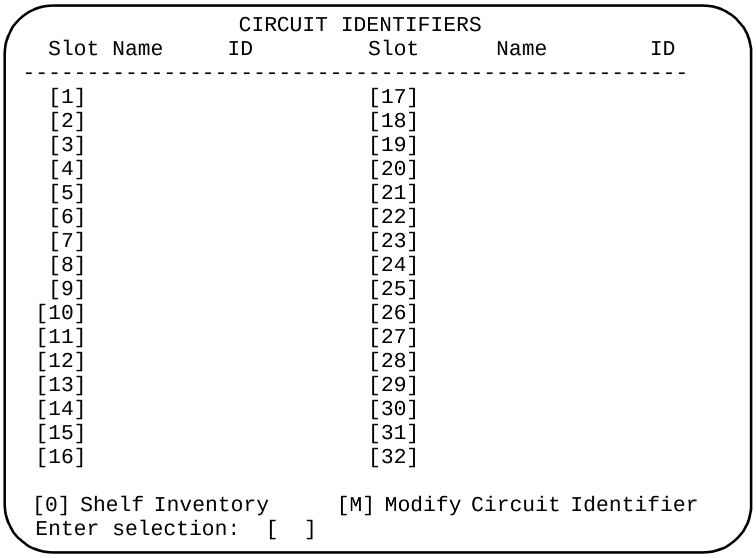
2. Press **C** to display that element's Circuit Identifiers screen.

3. To return to the Shelf Inventory screen from any other terminal interface screen, simultaneously press **CTRL-C**.

4. Press **0** to dismiss the Shelf Inventory screen. In a CTRL port session, the SCM Main Menu appears. In a Telnet session, the session is terminated.

Circuit Identifiers Screen

The Circuit identifiers screen is launched from the Shelf inventory screen and allows the user to establish identifiers for network elements. Instead of displaying the device's factory-assigned name, a user-configured Name and ID are displayed for each device. Slots 1 - 32 are always displayed regardless of the actual shelf configuration. *Figure 4-2* illustrates a typical Circuit Identifiers screen.



```
                      CIRCUIT IDENTIFIERS
  Slot Name     ID          Slot      Name        ID
----------------------------------------------------
  [1]                        [17]
  [2]                        [18]
  [3]                        [19]
  [4]                        [20]
  [5]                        [21]
  [6]                        [22]
  [7]                        [23]
  [8]                        [24]
  [9]                        [25]
 [10]                        [26]
 [11]                        [27]
 [12]                        [28]
 [13]                        [29]
 [14]                        [30]
 [15]                        [31]
 [16]                        [32]

 [0] Shelf Inventory      [M] Modify Circuit Identifier
 Enter selection:  [  ]
```

Figure 4-2 Typical Circuit Identifier Screen

Selection and Deletion Procedures

1. At the Shelf Inventory screen, press **C** to display the Circuit Identifiers screen.
2. If desired, begin a terminal session at once by selecting the desired slot number and then pressing **Enter**.
3. To delete a network element from the screen, press **M**. At the prompt, select the slot number for the element to be deleted. Press **D**(elete Identifier) and then press **Enter** to complete the deletion. Repeat this step for all unwanted network elements.
4. Press **0** to dismiss the Modify menu and return to the Circuit Identification screen.

Name and ID Modification Procedures

1. At the Circuit Identifier screen, press **M**.
2. At the prompt, enter the slot number for the element to be renamed, then press **Enter**.
3. Press **1** and enter a new Name at the prompt (up to 12 characters), then press **Enter**.
4. Press **2** and enter a new ID at the prompt (up to 20 characters), then press **Enter**. Repeat Steps 2 though 4 to modify identifiers for other elements.
5. Press **0** to dismiss the Modify menu and return to the Circuit Identifiers screen. To return to the Shelf Inventory screen from the Circuit Identifiers screen, simultaneously press **CTRL-C**.

Line Selection Screen

A network element, such as the SC5034 DSE or a Dual V.34 modem, has the capability of supporting multiple network connections or of functioning as two modems on a single card. Each connection and function is considered as a separate device by the SCM, requiring its own configuration and individual monitoring. When you select a multi-line network element from the Shelf Inventory or Circuit Identifiers screen, the Line Selection screen appears and prompts for more information. A typical instance is described in the Line Selection procedure below.

Line Selection Procedure

1. At the Shelf Inventory or Circuit Identifiers screen, select the desired multi-line device. The Line Selection screen appears.
2. Select the line you intend to work with (**`Line 1`** or **`Line 2`**).
3. Press **`Enter`** to begin a terminal session with that network element.
4. Select **`0`** to return to the Shelf Inventory screen.

Note *The Line Selection screen will display a plus (**`+)`** sign next to the selection number if there are one or more dedicated remotes associated with the line.*

Drop Inventory Screen

A network element may have one or more dedicated remote units associated with it. Such elements are tagged with a **+** sign on the Shelf Inventory or Circuit Identifiers screen, and when selected, the Drop Inventory screen appears. This screen lists a Master (in the shelf with the SCM) and any Remotes that may be accessible through it. A typical instance is described in the Drop Inventory procedure below.

Line Selection Procedure

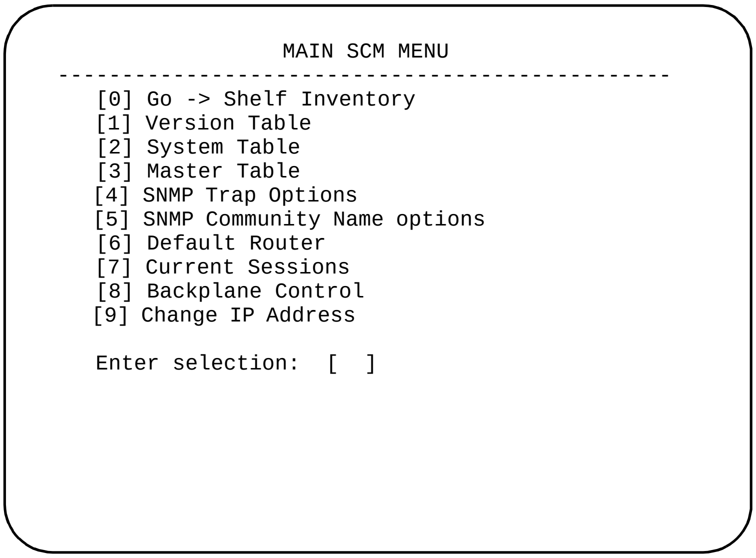
1. At the Shelf Inventory or Circuit Identifiers screen, select the desired network element which has associated remote(s). The Drop Inventory screen appears.
2. From the Drop Inventory list, select a Drop number to select the individual network element you intend to work with. Press **`Enter`** to begin a terminal session with that network element.
3. Select **`S`** to return to the Shelf Inventory screen.

Note *The Drop Inventory screen will always assigns Drop 0 to the Master device, which is located in the shelf with the SCM.*

The Main SCM Menu Screens

When you select an SCM from a Shelf Inventory screen or Circuit Identifiers Screen, you can command several functions that are available in the SCM from a series of menus and tables. The Main SCM menu is the first screen displayed. Table 4-2 and the following paragraphs describe each menu selection and the associated subscreens.

Note *A redundant SCM cannot be accessed through the primary SCM even though the redundant SCM appears in the primary's Shelf Inventory.*



```
                    MAIN SCM MENU
------------------------------------------------
   [0] Go -> Shelf Inventory
   [1] Version Table
   [2] System Table
   [3] Master Table
   [4] SNMP Trap Options
   [5] SNMP Community Name options
   [6] Default Router
   [7] Current Sessions
   [8] Backplane Control
   [9] Change IP Address

   Enter selection:  [  ]
```

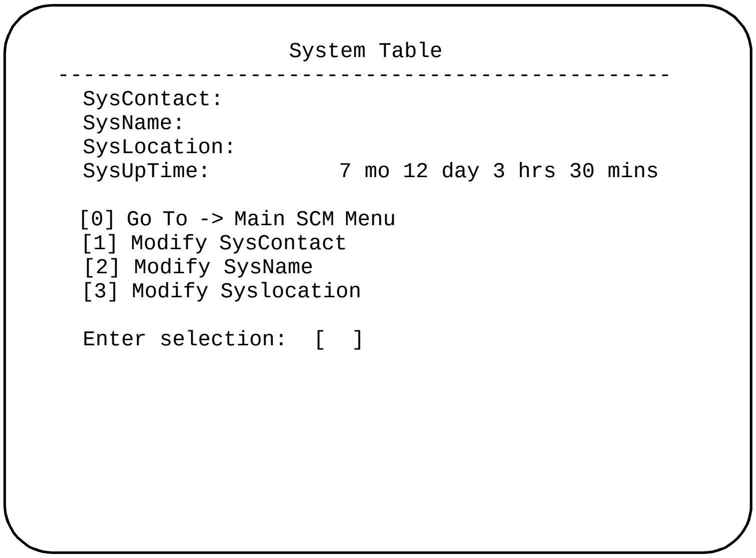
Table 4-2 The SCM Main Menu

Selection	Description
[0] Go -> Shelf Inventory	Returns to the Shelf inventory screen.
[1] Version Table	Displays read-only data on the serial number of the SCM and version numbers of the SCM operating code.
[2] System Table	Advances to the System Table data and related menu items.
[3] Master Table	Advances to the Master Table data and related menu items.
[4] SNMP Trap Options	Advances to the SNMP Trap Options configuration screen.
[5] SNMP Community Name Options	Advances to the SNMP Community Name Options configuration screen.
[6] Default Router	Advances to the Default Router configuration screen.
[7] Current Sessions	Advances to the current Telnet/Element Access session.
[8] Backplane Control	Advances to the Backplane Control menu and screens.
[9] Change IP Address	Advances to the Change IP Address screen.

Note *When a redundant SCM is in Standby mode, the Backplane Control selection is not applicable.*

System Table Screen

The System Table and its related menu is displayed when you select **2** from the Main SCM Menu. System Table information is part of the **System group** in the RFC1213-MIB. *Table 4-3* and the paragraphs below describe its use.



```
                  System Table
 ------------------------------------------------
   SysContact:
   SysName:
   SysLocation:
   SysUpTime:          7 mo 12 day 3 hrs 30 mins

   [0] Go To -> Main SCM Menu
   [1] Modify SysContact
   [2] Modify SysName
   [3] Modify Syslocation

   Enter selection:  [  ]
```

Table 4-3 The System Table Screen

Display/Selection	Description
SysContact	The contact person for the managed node and the method of contact.
SysName	An assigned name for the managed node. Typically, the fully qualified domain name of the node is used for SysName.
SysLocation	The physical location of the node. (e.g., telephone closet, 3rd floor)
SysUpTime	A read-only display of the time since the network management portion of the system was last re-initialized.
[0] Go To -> Main SCM Menu	Dismisses the System table and returns to the SCM Main menu.
[1] Modify SysContact	Select [1], [2], or [3] to modify the associated System Table information.
[2] Modify SysName	
[3] Modify SysLocation	

System Table Procedure

1. To modify System Table information, type **1** and press **Enter**. A highlight appears on the Modify SysContact field. Edit contents as desired, then press **Enter**.

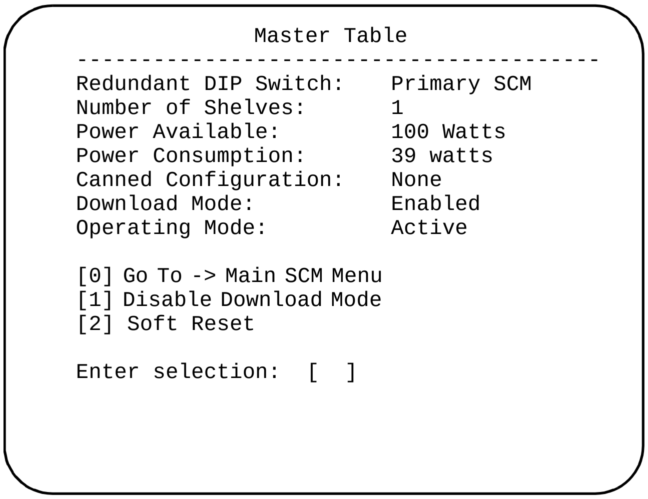
2. Type **2** and press **Enter**. A highlight appears on the Modify SysName field. Edit contents as desired, then press **Enter**.

3. Type **3** and press **Enter**. A highlight appears on the Modify SysLocation field. Edit contents as desired, then press **Enter**.

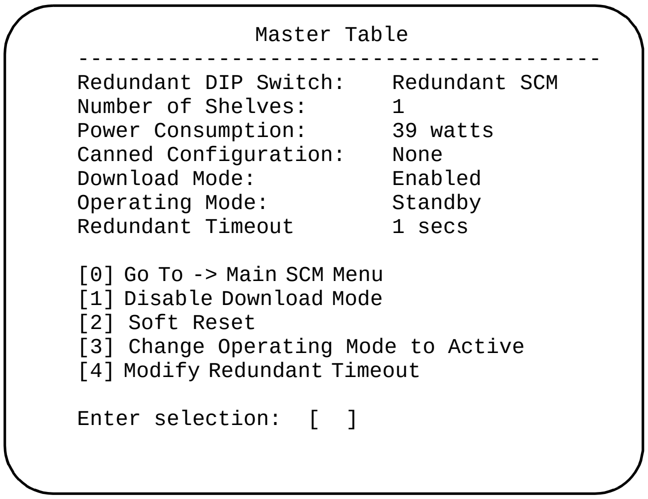
4. Press **0** to return to the Main SCM menu.

Master Table Screen

The Master Table and its related menu is displayed when you select **3** from the Main SCM Menu. The Master Table information is part of the **scmMaster** group in the GDCSCM-MIB. Depending on how the Redundancy Dip Switch is set on the SCM card, the Master Table will display slight differences. The example below illustrates typical Master Table screens for a Primary SCM and for a Redundant SCM. *Table 4-4* and paragraphs below describe their use.



```
              Master Table
-----------------------------------------
Redundant DIP Switch:   Primary SCM
Number of Shelves:      1
Power Available:        100 Watts
Power Consumption:      39 watts
Canned Configuration:   None
Download Mode:          Enabled
Operating Mode:         Active

[0] Go To -> Main SCM Menu
[1] Disable Download Mode
[2] Soft Reset

Enter selection:  [  ]
```



```
              Master Table
-----------------------------------------
Redundant DIP Switch:   Redundant SCM
Number of Shelves:      1
Power Consumption:      39 watts
Canned Configuration:   None
Download Mode:          Enabled
Operating Mode:         Standby
Redundant Timeout       1 secs

[0] Go To -> Main SCM Menu
[1] Disable Download Mode
[2] Soft Reset
[3] Change Operating Mode to Active
[4] Modify Redundant Timeout

Enter selection:  [  ]
```

Table 4-4 The System Table Screen

Display/Selection	SCM Setting	Description
Redundant DIP Switch	Prim/Stdby	Displays the current SCM setting as set at DIP Switch S1: **Primary** or Redundant
Number of Shelves	Prim/Stdby	Displays the number of shelves for which the SCM is configured: **1** or 2
Power Available	Primary	Displays the total amount of power available to the shelf or shelves.
Power Consumption	Prim/Stdby	A read-only display of the time since the network management portion of the system was last re-initialized.
Canned Configuration	Prim/Stdby	In special UAS shelves only: Displays the current setting of the canned configuration DIP switches: 1 - 7, or **None**. *Refer to Appendix C for details.*
Download Mode	Prim/Stdby	Displays whether SCM will permit Trivial File Transfer protocol (TFTP) for downloading code: **Enabled** or Disabled
Operating Mode	Prim/Stdby	Displays the operating mode of the SCM in its control of the management bus: **Active**, Standby, or Sleep
Redundant Timeout	Standby	Displays the number of seconds a redundant SCM will tolerate the absence of express polls from the primary SCM before the redundant SCM takes control of the management bus.
[0] Go To -> Main SCM Menu	Prim/Stdby	Dismisses the Master table and returns to the SCM Main Menu.
[1] Disable Download Mode	Prim/Stdby	*See Procedures below.*
[2] Soft Reset	Prim/Stdby	Commands the SCM to perform a software reset. Entered defaults, configurations, and firmware upgrades are not lost.
[3] Change Operating Mode to Active	Standby	*See Procedures below.*
[4] Modify Redundant Timeout	Standby	*See Procedures below.*

Download Mode Procedure

The Download Mode setting can be changed by the user for both a primary and a redundant SCM. This permits the SCM to support TFTP downloading of code to those network elements which are download-capable. When **Disabled** at the Master Table screen, the user will not be able to place the SCM in boot mode, download code to the SCM or network elements. This procedure is described below.

1. The factory default for the Download Mode is **Enabled**.
2. To disable Download mode in a primary or redundant SCM, press **1** at the Master Table screen, then press **Enter**. TFTP downloading attempts will be denied.
3. Repeating these keypresses will toggle the Download mode between **Enabled** and **Disabled**.
4. Press **0** to return to the Main SCM Menu.

Note *When Download Mode is disabled, any attempts to download will result in a TFTP error response. The response indicates that the download request has been denied. For detailed Downloading procedures, refer to Appendix A.*

Operating Mode Procedure

The Operating Mode identifies the degree to which an SCM is controlling the communication along the management bus. The table below defines the various Operating Modes for both primary and redundant SCMs. On a redundant SCM, the user can change the Operating Mode between Standby and Active. This procedure is described after the table.

Operating Mode	At a Primary SCM	At a Redundant SCM	Action/Description
Active Mode	Factory default	User-selectable, or selected when Primary times out.	When in Active mode, the primary or redundant SCM has full control of the shelf and its elements.
Standby Mode	Not available	Factory default	When in Standby mode, a redundant SCM card has been properly configured via its DIP switch, but is not currently in control of the management bus.
Sleep Mode	Set by a mode change at the redundant SCM	Not available	When a redundant SCM changes operating mode from Standby to Active, the primary SCM is forced into Sleep mode, and the redundant SCM takes full control of the management bus.

1. To change the Operating Mode of a redundant SCM from Standby Mode, press **3** at the Master Table screen, then press **Enter**. This places the redundant SCM into Active mode and forces the primary SCM into sleep mode.
2. To restore the SCMs to their normal modes of operation, you must perform a hardware reset on the SCMs as described in the SCM Redundancy Restoral Procedure, *Chapter 3, SCM Configuration* .
3. Press **0** to return to the Main SCM Menu.

Note *For a primary SCM, the Operating Mode field is read-only and cannot be changed by the user.*

Changing Redundant Timeout

The Redundant Timeout field identifies the amount of time a redundant SCM can remain in Standby Mode before the timeout occurs. On a redundant SCM, this field allows the user to control whether a redundant SCM will switch to Active mode or how quickly it will do so when a timeout condition exists on the shelf.

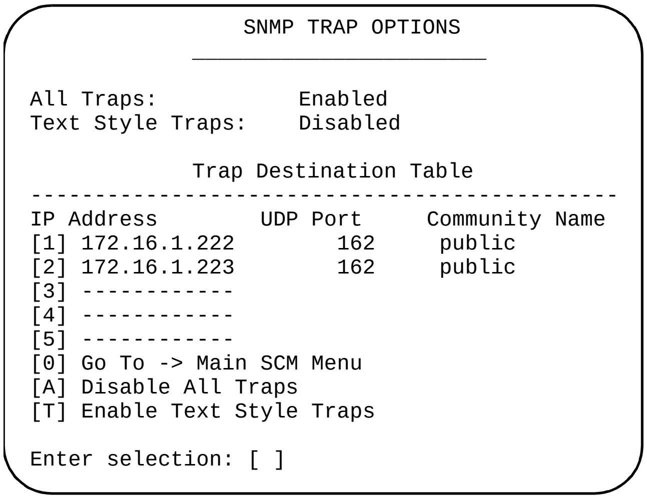
A timeout condition is caused when the redundant SCM has not received express polls from the primary SCM for longer than the user-set timeout interval, indicating that the primary SCM is not conducting operations normally at the management bus. In this case, the timeout may be adjusted so that the redundant SCM takes control of the management bus. This procedure is described below.

1. The default timeout value is **`0`**. At this setting, the redundant SCM ignores any interruption of communication from the primary SCM and does not take control of the management bus.
2. To ensure the redundant SCM responds, you must change the Redundant Timeout interval to a non-zero value.
3. At a redundant SCM, press **`4`** at the Master Table screen, then press **`Enter`**. A highlight appears at the Redundant Timeout field.
4. Type in a value from 1 - 300 seconds, and then press **`Enter`**.
5. Press **`0`** to return to the Main SCM Menu.

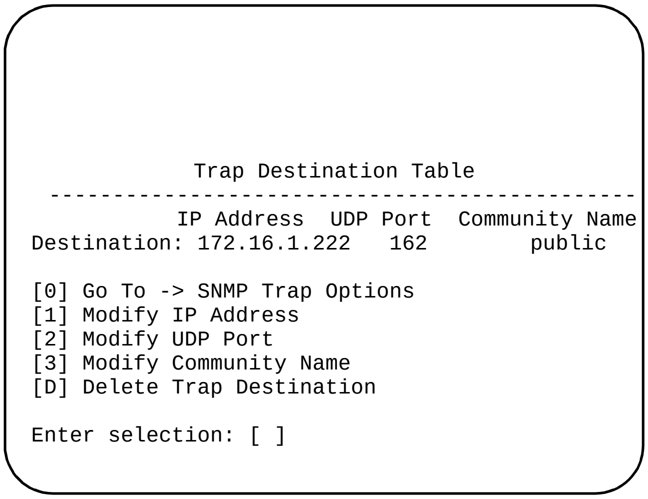
Note *The Redundant Timeout field is only available at the Master Table of the redundant SCM.*

SNMP Trap Options Screen

The SNMP Trap Options screen is displayed when you select **4** from the Main SCM menu. Traps are used to send unsolicited information to a network manager such as extraordinary events or alarms. To send/receive traps, the Trap Destination Table must be completed. Up to five Trap destinations can be set up and enabled in the SCM with the IP address and UDP port of the network manager. Table 4-5 and the following paragraphs describe selections for each menu and submenu.



```
                 SNMP TRAP OPTIONS
              _______________________

All Traps:             Enabled
Text Style Traps:      Disabled

             Trap Destination Table
----------------------------------------------
IP Address         UDP Port     Community Name
[1] 172.16.1.222         162     public
[2] 172.16.1.223         162     public
[3] ------------
[4] ------------
[5] ------------
[0] Go To -> Main SCM Menu
[A] Disable All Traps
[T] Enable Text Style Traps

Enter selection: [ ]
```



```
                Trap Destination Table
 ----------------------------------------------
          IP Address   UDP Port  Community Name
Destination: 172.16.1.222   162        public

[0] Go To -> SNMP Trap Options
[1] Modify IP Address
[2] Modify UDP Port
[3] Modify Community Name
[D] Delete Trap Destination

Enter selection: [ ]
```

Table 4-5 SNMP Trap Options Screen Selections

Screen	Display/Selection	Description
SNMP Trap Options screen	All Traps	Read-only status of all traps; changes dynamically when Selection [A] is Enabled or Disabled.
	Text Style Traps	Read-only status of all text-style traps; changes dynamically when Selection [T] is **`Enabled`** or Disabled.
	Destinations [1] through [5]	Selects the IP address of a trap destination and advances to a subscreen for modifying trap options for that destination.
	[0] Go To -> Main SCM Menu	Returns to the SCM Main menu.
	[A] Disable All Traps	Globally toggles all traps as all **`Enabled`** or all Disabled.
	[T] Enable Text Style Traps	Toggles only the text-style traps as all **`Enabled`** or all Disabled.
Destination subscreens	Destination	Displays the selected destination's IP address, and the default or entered values for the UDP port and Community named.
	[0] Go To -> SNMP Trap Options	Returns to the SNMP Trap Option screen, saving all changes.
	[1] Modify IP Address	Opens an entry field which prompts for a valid IP address.
	[2] Modify UDP Port	Opens an entry field which prompts for a UDP port address. Default: **`162`**
	[3] Modify Community Name	Opens an entry field which prompts for a community name of up to 32 characters. Default: **`public`**
	[D] Delete Trap Destination	Deletes the selected destination entirely from the Trap Destination Table and returns to the SNMP Trap Options screen.

Note *A trap destination must have a valid IP address entered before other fields in the Trap Option screen can be accessed. Trap destinations appear in the order they were configured. When a destination is deleted, destinations below it move up in the table.*

Modify IP Address Procedure

1. At the SNMP Trap options screen, use the Trap Destination Table to select a destination for change (**1** through **5**). A subscreen appears for modifying the trap options for that destination.
2. Press **1** to modify the IP address. An entry prompt appears. If the IP address displayed is correct as is, press **Enter** to dismiss the prompt.
3. If the IP address is blank or incorrect, type a new valid IP address at the prompt, then press **Enter**. The new address is inserted at the Destination field, and the Trap Destinations table will be updated.
4. Press **0** to return to the SNMP Trap Options screen. The Trap Destinations Table will reflect the latest changes.

Note *The SCM will only accept IP addresses that are within the valid format and range of values.*

Modify UDP Procedure

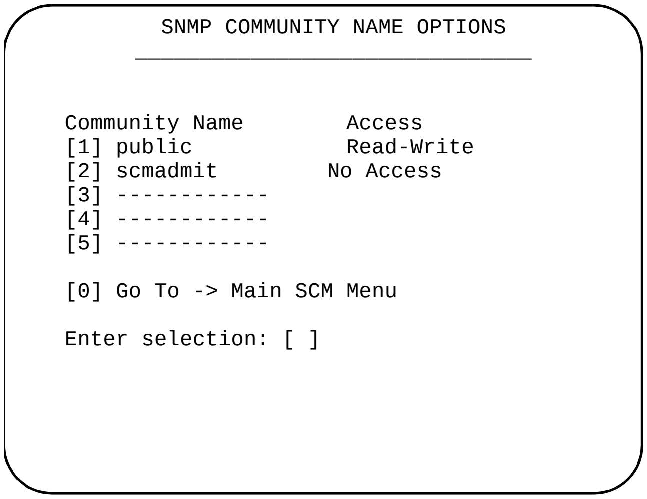
1. At the SNMP Trap options screen, use the Trap Destination Table to select a destination for change (**1** through **5**). A subscreen appears for modifying the trap options for that destination.
2. The default UDP port number is **162**. If the port number is correct as is, press **Enter** to dismiss the prompt.
3. To modify the port number, press **2**. An entry prompt appears.
4. Type the new port number at the prompt, then press **Enter**. The new port number is inserted at the Destination field, and the Trap Destinations table will be updated.
5. Press **0** to return to the SNMP Trap Options screen.

Modify Community Name Procedure

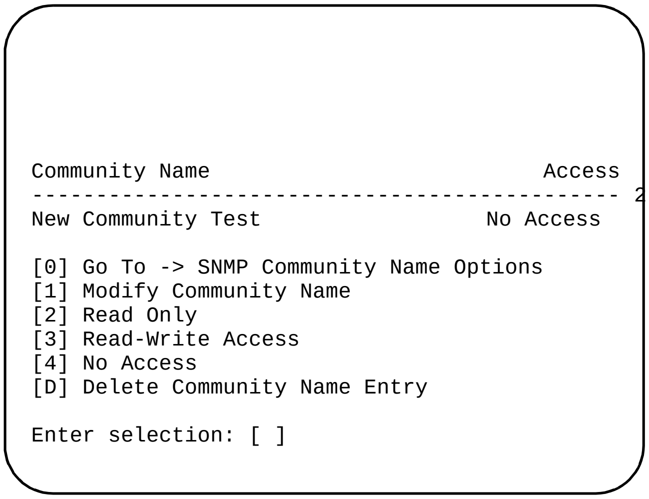
1. At the SNMP Trap options screen, use the Trap Destination Table to select a destination for change (**1** through **5**). A subscreen appears for modifying the trap options for that destination.
2. The default Community name is **public**. If the Community name is correct as is, press **Enter** to dismiss the prompt.
3. To modify the Community name, press **3**. An entry prompt appears.
4. Type the new Community name at the prompt, then press **Enter**. The new name is inserted at the Destination field, and the Trap Destinations table will be updated.
5. Press **0** to return to the SNMP Trap Options screen.

SNMP Community Name Options Screen

The SNMP Community Names Option screen is displayed when you select **5** from the Main SCM menu. Up to five community names can be defined to restrict access to an agent by either allowing or denying write access to the SCM MIB. *Table 4-6* and the following paragraphs describe selections for each menu and submenu.



```
            SNMP COMMUNITY NAME OPTIONS
        _______________________________


   Community Name        Access
   [1] public            Read-Write
   [2] scmadmit         No Access
   [3] ------------
   [4] ------------
   [5] ------------

   [0] Go To -> Main SCM Menu

   Enter selection: [ ]
```



```
Community Name                           Access
---------------------------------------------- 2
New Community Test                   No Access

[0] Go To -> SNMP Community Name Options
[1] Modify Community Name
[2] Read Only
[3] Read-Write Access
[4] No Access
[D] Delete Community Name Entry

Enter selection: [ ]
```

Table 4-6 SNMP Community Names Options Selection

Screen	Display/Selection	Description
SNMP Community Name Options screen	Community Names [1] through [5]	Selects a community name and advances to a subscreen for modifying that name and its access status. Default community name: **`public`** Default access: **`Read Only`**
	[0] Go To -> Main SCM Menu	Dismisses the Community Names Option screen and returns to the SCM Main menu.
Community Name subscreens	Community Name	Displays the selected community name and its current access privilege, if any.
	[0] Go To -> SNMP Community Name Options	Returns to the SNMP Community Name Options screen, saving all changes.
	[1] Modify Community Name	Opens a entry field which prompts for a community name up to 32 characters.
	[2] Read Only Access	Assigns read-only access to the selected community name.
	[3] Read-Write Access	Assigns read-write access to the selected community name.
	[4] No Access	Denies access to the selected community name.
	[D] Delete Community Name Entry	Deletes the selected community name entirely from the Community Name Table and returns to the SNMP Community Name Options screen.

Note *A Community Name must be established before the selections for changing access status or deleting a name can be accessed by the user. When a blank community name is selected, its subscreen will only display* **`No Access`** *until the user defines a new name.*

Modify Community Name Procedure

1. At the SNMP Community Name screen, use the Community Name Table to select an entry for change (**`1`** through **`5`**). A subscreen appears for modifying the options for that entry.
2. Press **`1`** to modify the Community name. An entry prompt appears. If the name displayed is correct as is, press **`Enter`** to dismiss the prompt.
3. If the name field is blank or incorrect, type a new valid IP address at the prompt, then press **`Enter`**. The new name is inserted at the name field, and the Community Name table will be updated.
4. Press **`0`** to return to the SNMP Community Name Options screen, which will reflect the latest changes.

Note *A Community Name must be entered before other Community Name options can be selected for change.*

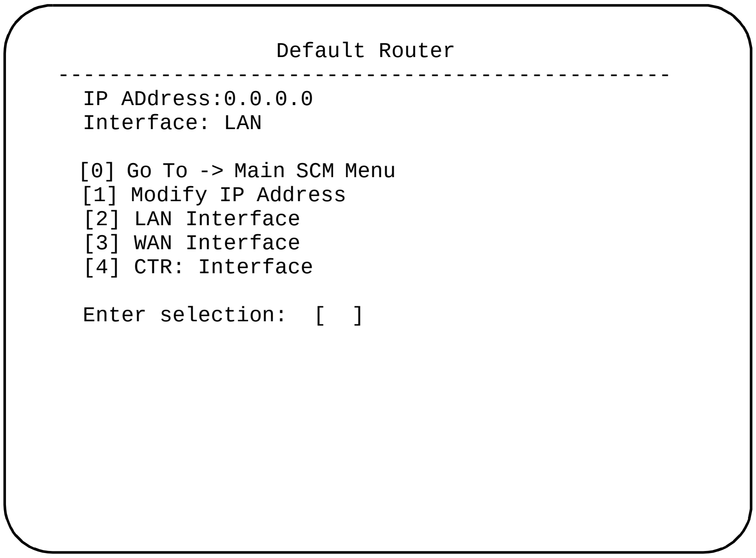
Modify Access Status Procedure

1. Select a Community name entry as described above.
2. To set an access status for a trap destination, perform the one of the following actions:
   - Press **`[2] Read Only Access`** to permit read only privileges to the selected community name, then press **`Enter`**.
   - Press **`[3] Read-Write Only Access`** to permit read and write privileges to the selected community name, then press **`Enter`**.
   - Press **`[4] No Access`** to deny read, write and view privileges to the selected community name, then press **`Enter`**.

Note *The access status options [***`2`***] through [***`4`***] are displayed at the Community Name subscreen only when a Community name has been established for a table entry.*

Default Router Screen

The Default Router screen is displayed when you select **6** from the Main SCM menu. The screen provides the means for identifying the router through which the SCM communicates and the interface it employs for communications. Table 4-7 and the following paragraphs describe each selection.



```
                  Default Router
------------------------------------------------
  IP ADdress:0.0.0.0
  Interface: LAN

 [0] Go To -> Main SCM Menu
 [1] Modify IP Address
 [2] LAN Interface
 [3] WAN Interface
 [4] CTR: Interface

  Enter selection:  [  ]
```

Table 4-7 The Default Router Selections

Display/Selection	Description
IP Address	Displays the current configuration for the default router IP address.
Interface	Displays the SCM interface currently selected for communication with the default router.
[0] Go To -> Main SCM Menu	Dismisses the Default Router screen and returns to the SCM Main menu.
[1] Modify IP Address	Opens a prompt for modifying the IP address for the default router.
[2] LAN Interface	Instructs the SCM to communicate with the default router through its LAN port.
[3] WAN Interface	Instructs the SCM to communicate with the default router through its WAN port.
[4] CTRL Interface	Instructs the SCM to communicate with the default router through its CTRL port.

Modify Default Router IP Procedure

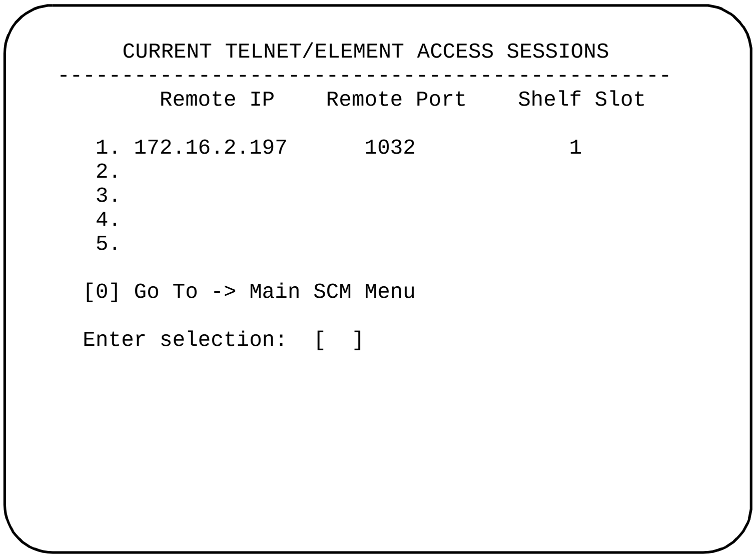
1. Press **1** at the Default Router screen. An entry prompt appears on the screen. If the name displayed is correct as is, press **Enter** to dismiss the prompt.

2. To modify the IP address for the default router, type the new address at that prompt and press **Enter**. The new IP address is inserted in the IP Address display line for the default router.

Note *The SCM accepts only input in the valid IP address format and range of values.*

Current Sessions Screen

Selection **7** in the SCM Main Menu accesses the Current Telnet/Element Access Sessions screen. which provides information about Element Access sessions that are in progress. *Table 4-8* and the following paragraphs describe each selection.



```
     CURRENT TELNET/ELEMENT ACCESS SESSIONS
------------------------------------------------
        Remote IP     Remote Port     Shelf Slot

   1. 172.16.2.197      1032            1
   2.
   3.
   4.
   5.

  [0] Go To -> Main SCM Menu

  Enter selection:  [  ]
```

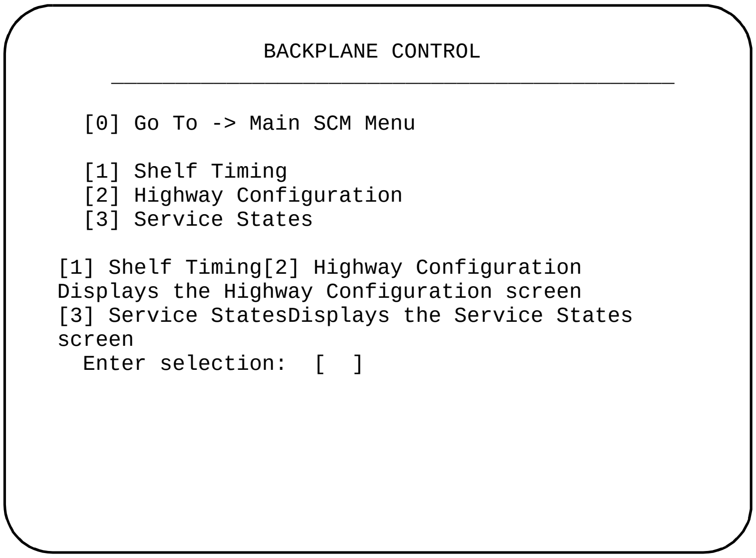
Table 4-8 The Current Sessions Selections

Display/Selection	Description	Field Details
Current Sessions [1] through [4]	Displays information on up to four Telnet sessions that can be active simultaneously.	Remote IP field: Displays the Remote IP address of the host that has initiated the session. Remote Port field: Displays the host communication port being used. Shelf Slot field: Displays the slot number of the SpectraComm/UAS device being accessed through the SCM.
Current Session [5]	Reserved for the displayed information of an active CTRL port session.	
[0] Go To -> Main SCM Menu	Dismisses the Current Sessions screen and returns to the SCM Main menu.	

Backplane Control Screen

Selection **8** in the SCM Main Menu accesses the Backplane Control menu. This function is only valid when the SCM is controlling shelf components that exchange data on the backplane data highways; for example, the line terminating units and data set emulators that make up a SpectraComm/UAS system. *Table 4-9* and the following paragraphs describe selections for each menu and submenu.

.



```
                    BACKPLANE CONTROL
      ____________________________________________

     [0] Go To -> Main SCM Menu

     [1] Shelf Timing
     [2] Highway Configuration
     [3] Service States

   [1] Shelf Timing[2] Highway Configuration
   Displays the Highway Configuration screen
   [3] Service StatesDisplays the Service States
   screen
     Enter selection:  [  ]
```

Table 4-9 The Current Sessions Selections

Selection	Description
[0] Go To -> Main SCM Menu	Dismisses the Current Sessions screen and returns to the SCM Main menu.
[1] Shelf Timing	Advances to the Shelf Timing Screen
[2] Highway Configuration	Advances to the Highway Configuration Screen
[3] Service States	Advances to the Service States Screen.

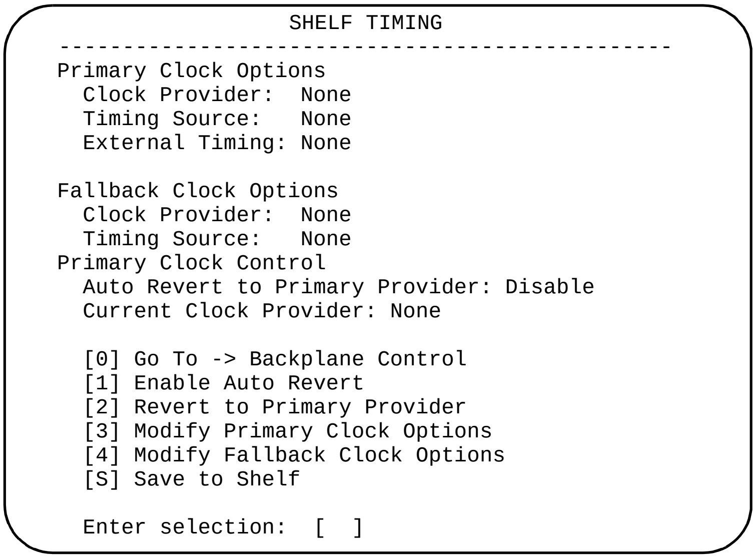
Special Considerations

- Backplane Control is not a valid function when the shelf is populated with individual units such as SC 521 DSUs or SC 553 DSUs.
- Backplane Control is not selectable from the SCM Main Menu of a redundant SCM while it is in Standby mode. In that mode the SCM does not communicate on the backplane and thus does not have any information about the other devices that populate its shelf. When a redundant SCM switches to Active mode, it interrogates the other devices in its shelf; thus, the Backplane Control selection would appear again in the SCM Main Menu.

Backplane Control: Shelf Timing

Press **1** at the Backplane Control menu to access the Shelf Timing screen, shown below. *Table 4-10* describes each field and selection.

.



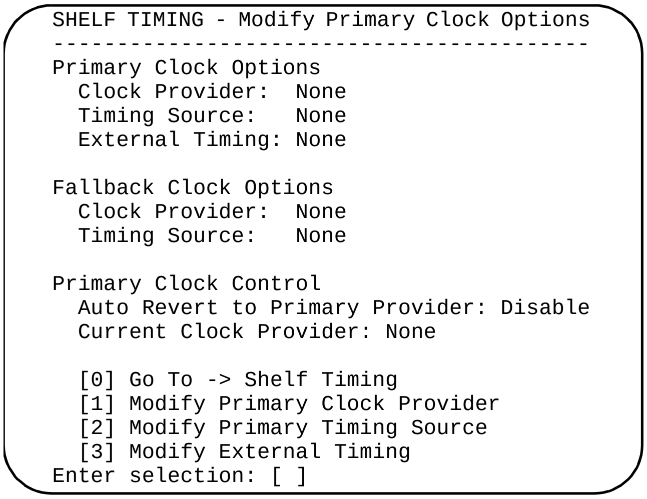
```
                      SHELF TIMING
------------------------------------------------
Primary Clock Options
  Clock Provider:  None
  Timing Source:   None
  External Timing: None

Fallback Clock Options
  Clock Provider:  None
  Timing Source:   None
Primary Clock Control
  Auto Revert to Primary Provider: Disable
  Current Clock Provider: None

  [0] Go To -> Backplane Control
  [1] Enable Auto Revert
  [2] Revert to Primary Provider
  [3] Modify Primary Clock Options
  [4] Modify Fallback Clock Options
  [S] Save to Shelf

  Enter selection:  [  ]
```

Table 4-10 The Current Sessions Selections

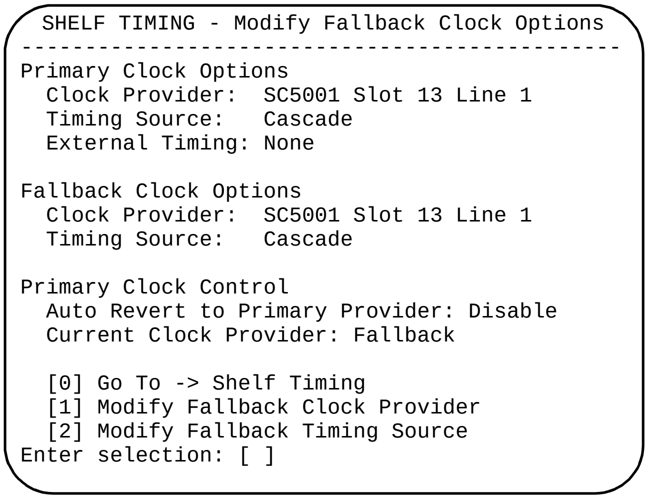
Display / Selection	Field	Description
Primary Clock Options	Clock Provider	Displays the LTU that supplies timing for the other network element sin the shelf.
	Timing Source	Displays the timing source for the LTU: Network, Internal or External.
	External Timing	Displays the DSE that gets the external timing from its DTE.
Fallback Clock Options	Clock Provider	The LTU that provides timing for the other network elements in the shelf when the primary clock cannot
	Timing Source	The LTU that supplies timing for the other network element sin the shelf.
Primary Clock Control	Auto Revert to Primary Provider	When Enabled, the system returns from the fallback to the primary clock as soon as the primary clock is available. When Disabled, a user command is required for clock control to revert from the fallback to the primary clock.
	Current Clock Provider	Displays the clock currently providing shelf timing: Primary or Fallback.
[0] Go To -> Backplane Control	Dismisses the Shelf Timing screen and returns to the Backplane Control menu. Pending changes are discarded unless Save to Shelf is performed first.	
[1] Enable Auto Revert	Toggles Auto Revert from Enable to Disable.	
[2] Revert to Primary Provider	When Auto Revert is Disabled, this selection commands a switchback from Fallback to Primary clock timing for the shelf.	
[3] Modify Primary Clock Options	Advances to the Modify Primary Clock screen.	
[4] Modify Fallback Clock Options	Advances to the Modify Fallback Clock screen.	
[S] Save to Shelf	Saves changed settings to the SCM. Pending changes are indicated with an asterisk (*) and will be discarded unless saved to shelf.	

Modify Primary or Fallback Clock

Press **3** in the Shelf Timing menu to access the Modify Primary Clock screen.
Press **4** to access the Modify Fallback Clock screen. Both screens are shown below. The top half of these screens reference the same timing information as found on the Shelf Timing menu. The lower half of the screens each contain specific selections for configuring the primary or the fallback clock. *Table 4-11* and the following paragraphs describe selections in both screens.



```
SHELF TIMING - Modify Primary Clock Options
------------------------------------------
Primary Clock Options
  Clock Provider:  None
  Timing Source:   None
  External Timing: None

Fallback Clock Options
  Clock Provider:  None
  Timing Source:   None

Primary Clock Control
  Auto Revert to Primary Provider: Disable
  Current Clock Provider: None

  [0] Go To -> Shelf Timing
  [1] Modify Primary Clock Provider
  [2] Modify Primary Timing Source
  [3] Modify External Timing
Enter selection: [ ]
```



```
 SHELF TIMING - Modify Fallback Clock Options
-----------------------------------------------
Primary Clock Options
  Clock Provider:  SC5001 Slot 13 Line 1
  Timing Source:   Cascade
  External Timing: None

Fallback Clock Options
  Clock Provider:  SC5001 Slot 13 Line 1
  Timing Source:   Cascade

Primary Clock Control
  Auto Revert to Primary Provider: Disable
  Current Clock Provider: Fallback

  [0] Go To -> Shelf Timing
  [1] Modify Fallback Clock Provider
  [2] Modify Fallback Timing Source
Enter selection: [ ]
```

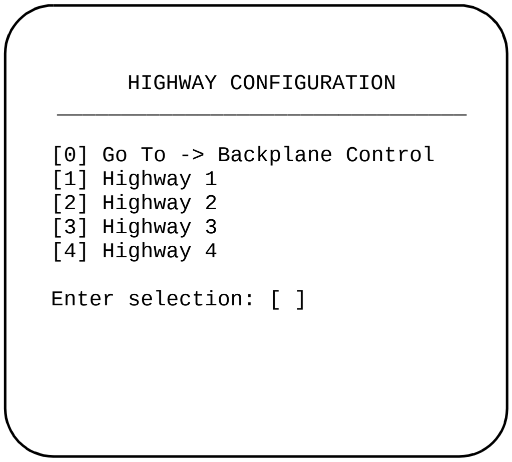
Table 4-11 Primary and Fallback Clock Modification Screens

Screen	Display/Selection	Description
Modify Primary Clock	[0] Go To -> Shelf Timing	Dismisses the Modify Primary Clock screen and returns to the Shelf Timing menu.
	[1] Modify Primary Clock Provider	Toggles through a selectable list of shelf units which are capable of providing a clock.
	[2] Modify Primary Timing Source	Toggles through a selectable list of clock sources: Network, Internal External, Cascade.
	[3] Modify External Timing	Toggles through a selectable list of units capable of passing timing to the shelf from a DTE.
Modify Fallback Clock	[0] Go To -> Shelf Timing	Dismisses the Modify Fallback Clock screen and returns to the Shelf Timing menu.
	[1] Modify Fallback Clock Provider	Toggles through a selectable list of shelf units which are capable of providing a clock.
	[2] Modify Fallback Timing Source	Toggles through a selectable list of clock sources: Network, Internal External, Cascade.

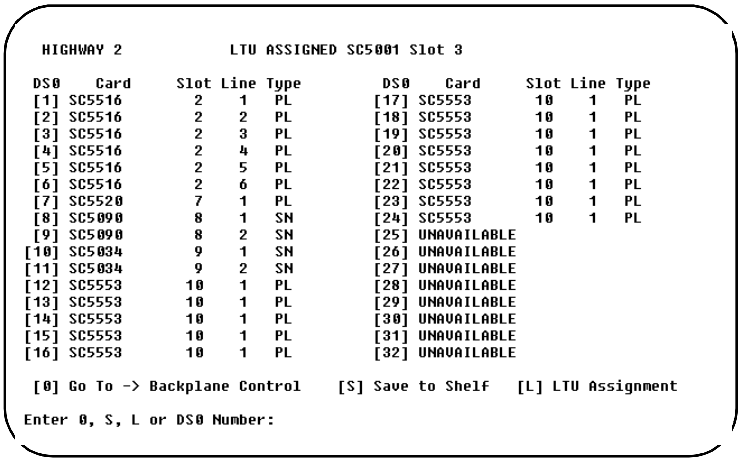
Note *When the External Timing Source option is selected for a unit, you must also enable the Auto Revert to Primary Provider option for that unit.*

Backplane Control: Highway Configuration

Press **2** in the Backplane Control menu to access the Highway Configuration screen. This screen is used to make highway assignments for product cards that use a SC 5001 or SC 5002 LTU. When a highway is selected from the Highway Configuration screen, a corresponding DS0/card slot configuration screen appears. *Table 4-12* describes both screens, with highway configuration procedures following the table.



```
HIGHWAY CONFIGURATION
─────────────────────────────────────────
[0] Go To -> Backplane Control
[1] Highway 1
[2] Highway 2
[3] Highway 3
[4] Highway 4

Enter selection: [ ]
```



```
 HIGHWAY 2            LTU ASSIGNED SC5001 Slot 3

 DS0    Card     Slot Line Type        DS0    Card     Slot Line Type
 [1] SC5516        2    1   PL        [17] SC5553       10    1   PL
 [2] SC5516        2    2   PL        [18] SC5553       10    1   PL
 [3] SC5516        2    3   PL        [19] SC5553       10    1   PL
 [4] SC5516        2    4   PL        [20] SC5553       10    1   PL
 [5] SC5516        2    5   PL        [21] SC5553       10    1   PL
 [6] SC5516        2    6   PL        [22] SC5553       10    1   PL
 [7] SC5520        7    1   PL        [23] SC5553       10    1   PL
 [8] SC5090        8    1   SN        [24] SC5553       10    1   PL
 [9] SC5090        8    2   SN        [25] UNAVAILABLE
[10] SC5034        9    1   SN        [26] UNAVAILABLE
[11] SC5034        9    2   SN        [27] UNAVAILABLE
[12] SC5553       10    1   PL        [28] UNAVAILABLE
[13] SC5553       10    1   PL        [29] UNAVAILABLE
[14] SC5553       10    1   PL        [30] UNAVAILABLE
[15] SC5553       10    1   PL        [31] UNAVAILABLE
[16] SC5553       10    1   PL        [32] UNAVAILABLE

 [0] Go To -> Backplane Control    [S] Save to Shelf   [L] LTU Assignment

Enter 0, S, L or DS0 Number:
```

Table 4-12 Highway Configuration Screens

Screen	Display/Selection	Description
Highway Configuration screen	[0] Go To -> Backplane Control	Returns to the Main SCM menu.
	[1] through [4] Highway Assignment	Advances to the configuration screen for the selected highway: **1**, **2**, **3** or **4**.
DS0/Card Slot Configuration screen	DS0 Assignment [0] through [32]	Select **1 - 24** when the shelf LTU is a SC 5001 (T1) or None. Select **0 - 31** when the shelf LTU is a SC 5002 (E1).
	Card Assignment	Displays the device type assigned to that DS0/timeslot. A DS0 number is **Available** when the LTU permits an assignment. *(See Note below.)*
	Slot Number	Displays the physical location of the device in the shelf.
	Line	Displays the channel or timeslot number.
	Type	Displays the line type of the device as detected by the SCM: **PL** (private line) or **SN** (switched network)
	[0] Go To -> Backplane Control	Returns to the Backplane Control menu. Pending changes are discarded unless they are saved to shelf first.
	[S] Save to Shelf	Saves changed settings to the SCM. Pending changes are indicated with an asterisk ***** and will be discarded unless saved to shelf.
	[L] LTU Assignment	Select from SC 5001 or SC5002 LTUs installed in the shelf, or None.

Note *When a SC 5001 (T1) LTU is selected, DS0 numbers 25 through 32 are* **Unavailable**.
When a SC 5002 (E1) LTU is selected, DS0 numbers 0 and 16 are labeled as **Unavailable**.

Highway Configuration Procedure

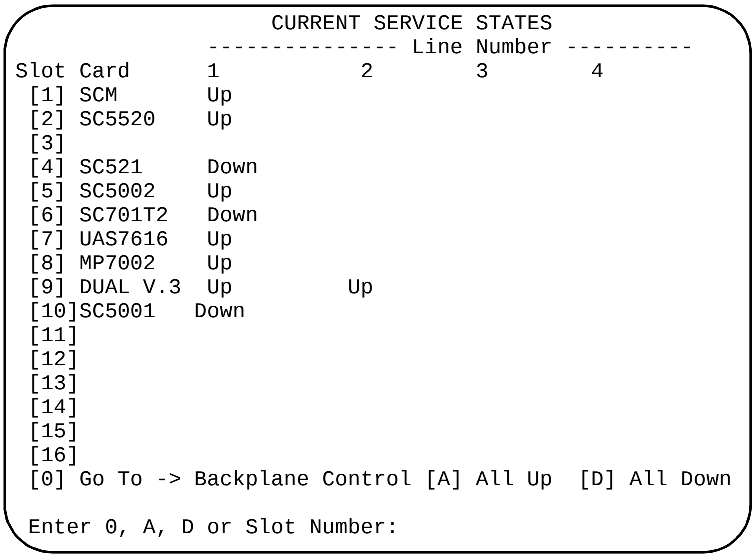
Product cards that use a SC 5001 (T1) LTU or a SC 5002 (E1) LTU use highway assignments configured by the user, as described below.

1. Check that the product cards and the associated LTUs (SC 5001s or SC 5002s) are securely installed in the SpectraComm shelf.
2. At the Highway Configuration menu, select the first highway (**`1 - 4`**) for configuration. A list of up to 32 DS0 numbers appear. (Availability depends on the LTU type.)
3. To assign a LTU to the selected highway, press **`L`** and then press **`Enter`**. A highlight appears at the LTU Assignment field.
4. Use the **`Up/Down`** arrows to scroll through the LTUs installed in the shelf, then press **`Enter`** to make the selection. The LTU and its shelf slot number will display as the assigned LTU for that highway.
5. You can now assign product cards to the selected LTU on this highway. Begin by selecting an available DS0 number (**`1 - 32`**).
6. Use the **`Up/Down`** arrows to scroll through the valid product cards in the shelf, then press **`Enter`** to make the selection. The DS0 field displays the product card, shelf slot number, line number and line type as detected by the SCM.
7. For products that support multiple channels (lines), the following conditions apply:
   - The SC 5034 is a two-channel card; one or both channels of a specific card can be selected for DS0 numbers on any of the four highways.
   - The SC 5090 is a two-channel card; one or both channels of a specific card can be selected for DS0 numbers on any of the four highways.
   - The SC 5553 is a 24-channel card; one or up to 24 channels of a specific card can be selected for DS0 numbers on the same highway. Do not split DS0 assignments between highways.
   - The SC 5520 is a single channel card; the channel of a specific card can be selected for a DS0 number on any one highway.
   - The SC 5506 card is a six-channel card; one or up to 6 channels of a specific card can be selected for DS0 numbers on a single highway. Do not split DS0 assignments between highways.
   - The SC 5516 card is a six-channel card; two, four or all six channels of a specific card can be selected for DS0 numbers. Consecutive DS0 numbers are required for each pair of channels selected. All DS0 assignments must be on the same highway.
8. Repeat Steps 5 through 7 for other product cards in the shelf, as needed.
9. When all desired LTU and DS0 assignments have been made for that highway, press **`S`** to save the assignments to the shelf.
10. To select another highway for configuration, press **`0`** to return to the Highway Configuration menu. Repeat the Steps 2 through 9 until all highways are configured as needed.

Backplane Control: Service States

Press **3** at the Backplane Control menu to access the Current Service States screen, shown below. *Table 4-13* describes each field and selection.

.



```
                    CURRENT SERVICE STATES
               --------------- Line Number ----------
Slot Card      1           2        3        4
 [1] SCM       Up
 [2] SC5520    Up
 [3]
 [4] SC521     Down
 [5] SC5002    Up
 [6] SC701T2   Down
 [7] UAS7616   Up
 [8] MP7002    Up
 [9] DUAL V.3  Up          Up
 [10]SC5001   Down
 [11]
 [12]
 [13]
 [14]
 [15]
 [16]
 [0] Go To -> Backplane Control [A] All Up  [D] All Down

 Enter 0, A, D or Slot Number:
```

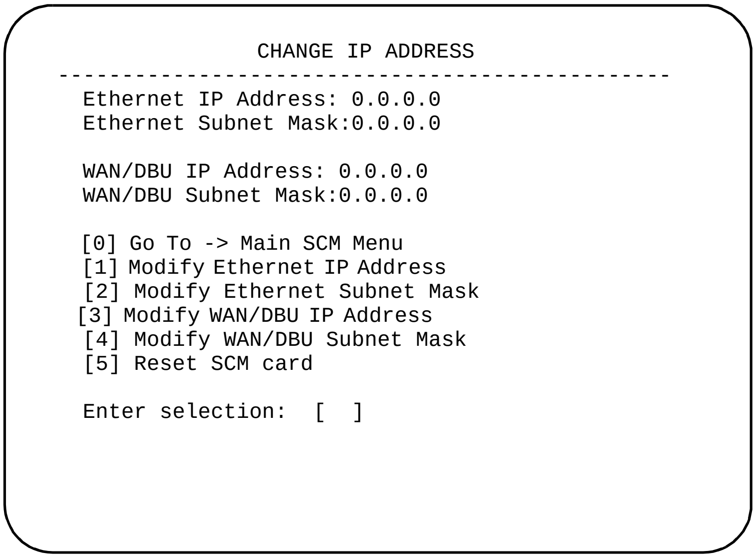
Table 4-13 The Service States Screen

Display / Selection	Description
Slots [1] through [16]	Selects a slot row in order to set the service state. When row is highlighted, arrow keys toggle state between Up and Down.
Card	Displays the device type installed in the slot.
Line	Indicates devices that support multiple channels.
[0] Go To -> Backplane Control	Dismisses the Service States screen and returns to the Backplane Control menu.
[A] All Up	Sets the state for all units to All Up (In Service)
[D] All Down	Sets the state for all units to All Down (Out of Service), except for the SCM.

Note *The SCM card will not respond to the* **`All Down`** *command or to the individual arrow toggle to* **`All Down`**. *These commands are not valid for the SCM.*

Change IP Address Screen

Selection **9** in the SCM Main Menu accesses the Change IP Address screen, shown below. This screen shows the current Ethernet and WAN/DBU IP addresses/masks and allows the user to make changes from a terminal (CTRL port) interface or via a Telnet connection. *Table 4-14* and the following paragraphs describe each selection. Procedures follow the table.



```
                    CHANGE IP ADDRESS
------------------------------------------------
  Ethernet IP Address: 0.0.0.0
  Ethernet Subnet Mask:0.0.0.0

  WAN/DBU IP Address: 0.0.0.0
  WAN/DBU Subnet Mask:0.0.0.0

  [0] Go To -> Main SCM Menu
  [1] Modify Ethernet IP Address
  [2] Modify Ethernet Subnet Mask
 [3] Modify WAN/DBU IP Address
  [4] Modify WAN/DBU Subnet Mask
  [5] Reset SCM card

  Enter selection:  [  ]
```

Table 4-14

Display/Selection	Description
Ethernet IP Address Ethernet Subnet Mask	Displays the current configuration for the Ethernet IP address and subnet mask.
WAN/DBU IP Address WAN/DBU Subnet Mask	Displays the current configuration for the WAN/DBU IP address and subnet mask.
[0] Go To -> Main SCM Menu	Dismisses the Change IP Address screen and returns to the SCM Main menu.
[1] Modify Ethernet IP Address	Opens a prompt for modifying the Ethernet IP address.
[2] Modify Ethernet Subnet Mask	Opens a prompt for modifying the Ethernet subnet mask.
[3] Modify WAN/DBU IP Address	Opens a prompt for modifying the WAN/DBU IP address.
[4] Modify WAN/DBU Subnet Mask	Opens a prompt for modifying the WAN/DBU subnet mask.
[5] Reset SCM card	Commands the SCM to perform a software reset. Entered configurations are not lost.

Procedures

To change the SCM LAN and WAN IP addressing/subnet masks, perform the following steps:

1. For a CTRL port session skip to Step 3.
   For a Telnet session, connect the LAN or WAN, telnet to the SCM and perform the login sequence as described in *Chapter 3, SCM Configuration : Operational Checks* .
2. At the Shelf Inventory screen, select the SCM slot number. At the Main SCM menu, press **9** to change the IP addressing. The Change IP Address screen appears, as shown above.
3. At the Change IP Address screen, press **1** to modify the Ethernet IP address. An entry prompt appears. If the IP address displayed is correct as is, press **Enter** to dismiss the prompt.
4. If the IP address is blank or incorrect, type a new valid IP address at the prompt, then press **Enter**.
5. The new IP address is inserted in the Ethernet IP Address display line.
6. Repeat Steps 3 through 5 for any additional IP addresses/masks changes, as required.
7. When all changes are entered, press 5 to reset the SCM card. This causes the new IP addresses/masks to take effect. The current Telnet connection will close.
8. Make a new Telnet connection to the SCM card using the new IP address.

Note *Resetting the SCM card in the last step of this procedure will drop the Telnet connection. Unless your PC or UNIX Telnet software has timed out, the screen will appear to be hung up.Use the new IP address for all new Telnet sessions.*

Note *The SCM accepts only input in the valid IP address format and range of values.*

Chapter 5: SNMP Programming

SNMP Programming Overview

The following SNMP programming topics will assist the user in using the Management Information Bases (MIBS) to perform specialized management and configuration of the SCM and the network elements.

Using MIB Browsers

The SCM supports the SNMP standard MIBs, RFC 1213 and RFC 1215. To use these objects, you must load them onto your target system. To operate on the SCM MIB using a MIB browser, perform the following steps:

1. Load/Compile MIB files as defined in MIB browser manual.
2. Use the files from the SCM MIB diskette for the target system (DOS/UNIX).
3. Load the file **`GDCMACRO.MIB`** first.
4. Then load **`GDCSCM.MIB`** next.
5. Finally, load other network element MIBs.
6. Once loaded, you can access the objects by using the MIB browser's **`get`**, **`get-next`** and **`set`** commands. These commands allow you to walk the MIB tree in both the industry-standard branches as well as the GDC private enterprise branch (**`498`**).

Trap and Node Table Errors

The following errors can occur when reading, adding to, or deleting entries from a Trap Table, Node Table, or Community Name Table.

Table 5-1 Table Errors

Errors	Description
noSuch	Occurs if the instance (IP address or UDP port is incorrect. Occurs if a get is performed on a non-existent entry Occurs if an attempt is made to add and entry where no variable binding with the community name exists. Occurs if the super-user name is not used to access the Community name table.
genError	Occurs if the Trap Address table is full.
badValue	Occurs if the value of any variable binding is not within the allowable range.

SCM MIB General information

This section provides general information on several groups or objects in the SCM MIB which can be useful to the user.

SCM Version Table

In the GDCSCM-MIB, there are variables in a Version group that are used to report on the **`scmMIBVersion`**, **`scmBootVersion`**, and **`scmApplVersion`**. These variables read-only and indicate the current version operating in the SCM.

SCM Slot State Table

In a read-only MIB table, **`scmSlotState`**, the SCM holds the current state of all the network elements co-located in the shelf. This table is not held in non-volatile RAM, therefore all rows in the table are created at every power-up and no row creation is possible by the user. The SCM initially tags all network elements in the shelf as inactive and then determines which ones are active. *Table 5-2* defines the possible values of **`scmSlotState`**:

Table 5-2 Slot State Values

Value	Description
inactive	The network element does not respond to express polls on the backplane. If active or active with errors at any time, it takes three non-responses to a poll for the NE to become inactive
active error	Communication errors are detected in response to an express poll.
Active	The network element responds properly to all express polls.

Note *Communication errors are defined as checksum errors in messages across the backplane*

Network Element Index

Network elements are accessed through an index related to their address. This index, called the **`SCinstance`**, is an unsigned 32-bit integer. The index is defined as **`ssllddxx`**, as follows:

```
index = (ss * 16777216) + (ll * 65536) + (dd * 256) + xx
```

where:

- **`ss`** is the slot number in the SpectraComm/UAS shelf
  Values are 1 through 32 (two-shelf system), 1 through 16 (one-shelf system)
- **`ll`** is the line associated with the slot
  Values are 1 - 128.
- **`dd`** = the drop defined off of the line
  Values are 0 - 31.
- **`xx`** is used to define interfaces on some network elements
  Values are 0 - 255.
  An element that supports only one interface in its MIB always sets this to zero.

Note *The SCM furnishes the variable* ***`scmShelfnumber`*** *to indicate to the network manager whether the system is a one-shelf or a two-shelf system.*

Master Table Group

In the GDCSCM-MIB, there are variables in a Master group that are used for several overall functions, as described in *Table 5-3* below.

Table 5-3 Master Table Values

Value	Description
scmMasterTimeout	Sets the management bus timeout.
scmAlarmScan	Globally turns off alarm scan on all network elements under the SCM’s control.
scmTime	Sets the time for internal timekeeping purposes.
scmDate	Sets the date.
scmRedundant	Indicates whether the SCM is operating as a Primary or Redundant.
scmShelfNumber	Indicates whether the SCM is operating in a one- or two-shelf system.
scmReset	Resets the SCM card in the shelf.
scmPowerAvail	Determines the total power (in watts) available to the shelf. This is done by summing the output power of all the power supply cards.
scmDefaultConfig	Allows the Non Volatile Configuration to be set to a factory default state.
scmPowerConsum	Determines how much power (in watts) is consumed by all of the network elements in the shelves managed by the SCM. This is done by summing the output power of all active cards in the SCM node table.
scmCannedConfig	Reads the DIP switches and reports the current canned configuration settings.
scmNetworkElementRealTime	Sets the real time of the network elements.
scmLoadCode	Determines if TFTP code downloading to the SCM or to any network element is permitted.
scmOperatingMode	In a redundant system, determines the operating mode of an SCM on the management bus.
scmAliveTrapInterval	In a redundant system, sets the interval (secs) at which the SCM send traps to show how long it has been alive.
scmRedundantTimeout	In a redundant system, sets the interval (secs) after which the SCM takes control of the management bus.
scmTelnet	Determines if Telnet to the SCM is permitted.
scmTextAlarmTraps	Enables or Disables the text format for alarm traps received from the managed network elements. When set to enable, the SCM sends **`scmTextAlarmTrap`** messages.

Note *Do not change the scmAlarmScan default value unless instructed by a GDC representative.*

Node Table Group

In the GDCSCM-MIB, there are variables in a Node group that are used for several overall functions, as described in *Table 5-4* below.

Table 5-4 Node Table Values

Node Variable	Description	Defaults
scmNodeIndex	Address of the network element in the table used by all other node variables.	**-**
scmNodeType	Type of network element.	**-**
scmNodeConfigCs	The last available checksum given to the SCM from the network element.	**zero**
scmNodeStatus	Status of the network element. An invalid status deletes the entry from the table.	**Valid**
scmNodeAlarmScan	Determines if the network element should be scanned for alarm information. If set to OFF, no traps are sent for the element and alarms are discarded.	**ON**
scmNodeLevel	Determines the timeout (secs) for command response information. Formula for the timeout is 2 * level.	**1**
scmNodeConfigChecksumStatus	Indicates that the configuration checksum is the table matches the one in the network element.	**Incorrect**
scmNodeCurrentAlarms	Alarm information of the network element. The number of bytes is element-dependent.	**NULL**
scmNodeSerialNumber	Serial number of the network element. Can be used to set the address of the element when required.	**NULL**
scmNodeAdminStatus	Desired status of the network element.	**DOWN**
scmNodeOperStatus	Actual status of the network element.	**DOWN**

Adding to the Node Table

The Node table requires a network element index to add, delete, or view the entries in the Node table. In addition, the type of network element is required before an entry can be added to the Node table.

Example: When a SNMP set is performed on the variable **scmNodeType** using a instance, an entry is added into the table as follows:

```
scmNodeType.83951616 = vfast
```

This furnishes an entry for Slot 5, Line 1 and Drop 0. When a get is performed to read the variables, the following states are returned:

```
scmNodeIndex.83951616 = 83951616

scmNodeType.83951616 = vfast

scmNodeConfigCs.83951616 = 0

scmNodeStatus.83951616 = valid

scmNodeAlarmScan.83951616 = On

scmNodeLevel.83951616 = 1
```

```
scmNodeConfigChecksumStatus.83951616 = incorrect

scmNodeCurrentAlarms.83951616 = 0

scmNodeSerialNumber.83951616 = valid serial number

scmNodeAdminStatus.83951616 = down

scmNodeOperStatus.83951616 = down
```

Special Considerations

- If multiple sets are done to add an entry, all possible set fields can be SET.
- If an error occurs while setting any of the variable bindings, the error is brought to the attention of the network manager, and no entry is added in the table.
- A NULL serial number can be specified to allow entries to be added for which the serial number is currently not known. If this is done and the network element is added at a later date, it is not guaranteed that the element address is correct and enabled to talk to the SCM.
- For a remote network element, the serial number of the element must be set through the network manager when you install it for setting the element address.

Adding Nodes via the SCM

The SCM uses two methods to add shelf network elements to the Node Table:

- An added element is detected when it is plugged into the shelf.
- Added network elements are detected when the SCM is powered up.

When a network element is plugged into the shelf, the element sends the necessary information for the SCM to determine the network element type. The SCM then sets the element address to its slot number, Line 1, Drop, 0, and adds the element to its Node table.

If an SCM needs to be replaced, the new SCM detects the active network elements in the shelf when it powers up. The SCM adds active shelf elements to the Node table. Since the element addresses were set previously by the replaced SCM, the serial number can be retrieved from the element.

Deleting from the Node Table

To delete a node entry from the table, the **`scmNodeStatus`** needs to be set to invalid:

```
scmNodeStatus.83951616 = invalid
```

Note *If a network element is deleted from the Node table, the SCM does not add it to the Node table again until either the SCM or the element is re-powered.*

Community Name MIB General Information

Up to five traps can be defined as destinations when the user specifies destination IP address, UDP port, Community Name and access privilege. The traps can then be enabled to send unsolicited information to the destination (a network manager).

Trap Table Group

In the **GDCMN-MIB**, there are variables in a Trap Group which are used to add, delete and view the trap destination definitions. The Trap group is located in non-volatile RAM, so it does not have to be created at every power-up of the SCM.

Table 5-5 Trap Address Table Variables

Variable	Definition	Defaults
cmnTrapGlobal	Globally enables or disables traps on the SCM.	**Enabled**
cmnTrapAddrNumber	Indicates the maximum amount of SNMP Network Manager IP addresses the table can hold.	**5**
cmnTrapAddrIPDest	The IP address where the trap is to be sent.	**-**
cmnTrapAddrUDPDest	The UPD port where the trap is to be sent	**-**
cmnTrapAddrCommunity	The community name to use when sending a trap.	**public**
cmnTrapAddrStatus	The status of the row entry: Valid status allows the entry to be read from the table. Invalid status deletes the entry from the table.	**Valid**

Note *IP address and UDP port must be set before a Community name can be added, deleted or viewed.*

Note *When replacing SCMs, manually delete trap destinations which are no longer needed.*

Trap Table Guidelines

- To add a entry into the trap table, the community name for a TRAP to this manager is required.

  For Example:
  When a SNMP **set** is performed on the variable **cmnTrapAddrCommunity** using an instance, an entry is added to the table, **cmnTrapAddrCommunity.192.9.10.2.162 = test**, using an IP Address of 192.9.200.2 and a UDP port of 162).

  When a **get** is performed to read the variables, the following statements are returned:

  ```
  cmnTrapAddrIpDest.192.9.10.2.162 = 192.9.10.2

  cmnTrapAddrUdpDest.192.9.10.2.162 = 162

  cmnTrapAddrCommunity.192.9.10.2.162 = "test"

  cmnTrapAddrStatus.192.9.10.2.162 = valid
  ```

- To change **cmnTrapAddrCommunity**, a set can be performed to another community name:

  ```
  cmnTrapAddrCommunity.192.9.10.2.162 = newname
  ```

- To delete trap entry from the table, set **cmnTrapAddrStatus** to invalid:

  ```
  cmnTrapAddrStatus.192.9.10.2.162 = invalid.
  ```

Supported Traps

The following traps are supported by the SCM:

Table 5-6 Standard Traps

Trap Type	Trap	Description
Standard Traps	coldstart	Sent when the first network interface is determined to be up.
	linkUP	Sent when any other network interface comes up or changes its state.
	linkDOWN	Sent only on interfaces where an SNMP manager exists and when a network interface goes down or changes its state.
	authenticationFailure	Sent whenever an SNMP command is received with an incorrect community name.
SCM-specific Traps	scmAliveTrap	Sent every [*n*] minutes based on the value in the MIB object **`scmAliveTrapInterval`**. No trap is sent if value is zero. Sent when values are changed for **`scmOperatingMode`** or **`scmRedundantTimeOut`**.
	scmAlarmTrap	Sent whenever a network element detects a change in its alarm information.
	scmPowerSupplyTrap	Sent when there is a change in the amount of power available to the shelf, i.e., when a power supply fails or is replaced.
	scmConfigChksumTrap	Sent when the configuration of a network element's checksum changes during a terminal interface session. Notifies the network manager of terminal interface activities.
	scmAlarmTextTrap	If enabled in the Master Table, this trap is sent when the SCM receives an alarm from a network element that supports text-style traps. *(See example message below.)*

Note *The* ***`authenticationFailure`*** *TRAP can be masked individually through the MIB-II variable* ***`snmpEnableAuthenTraps`****.*

Note *The* ***`scmAlarmTrap`*** *can be masked in the Node Table by turning off a network element's alarm scan or by turning off all alarm traps through the SCM MIB.*

Note *EXAMPLE: A text-style trap message takes the following format:*

```
Productname: Slot [n] Drop [x] AlarmName is [Active or Inactive].
```

Community Names Group Table

In the GDCCMN-MIB there are variables in a Community Name group that allow a user to add, delete and view the community names held in the **`cmnCommunityTable`**. This function is available only when write access is assigned. The SCM community name table is located in non-volatile RAM, so it does not have to be re-created every time the SCM is powered up.

You must set at least one community name with read-write access in the Community Name table before any other MIB objects can be set using the SCM card. Use the super-user community name to set the first, privileged, community name, and then use that privileged community name to set all other MIB objects. The variable in the Community Names MIB are described in Table 5-7.

Table 5-7 Community Name Table Variables

Variable	Description	Defaults
cmnCommunityIndex	Entry number in the table	-
cmnCommunityName	String (up to 32 characters) that holds the community name	-
cmnCommunityAccess	Indicates the access privilege assigned to that community name: Read only, Read-write, or No access	**`NoAccess`**
cmnCommunityStatus	Valid or Invalid	**`valid`**

Community Name Table Guidelines

- The Community Name table requires an index from 1 through [n] in order to add, delete, or view the entries in the Community Name table, where [n] is **`cmnCommunityNumber`**. In addition, super-user community name must be used in order to add/delete an entry.
- To add a entry into the Community name table, a community name is required.

  For Example:
  when a SNMP **`set`** is performed on the variable **`cmnCommunityName`** using an index, an entry is added to the table, **`cmnCommunityName.2=test`**, using an index of 2.

  When a **`get`** is performed to read the variables, the following statements are returned:

  ```
  cmnCommunityName.2 = test

  cmnCommunityAccess.2 = noAccess

  cmnCommunityStatus.2 = valid
  ```

- To change **`cmnCommunity`**Access, a set can be performed to one of the following:

  ```
  readOnly

  readWrite access

  cmnCommunityAccess.2 = readWrite.
  ```

- To delete a community name entry from the table, set **`cmnCommunityStatus`** to invalid:

  ```
  cmnCommunityStatus.2 = invalid.
  ```

Note *The superuser community name can be accessed and changed through the front panel CTRL port.*

MIB-II Groups

MIB-II is defined in the Internet document RFC 1213, Management Information Base for Network Management of TCP/IP-based internets. RFC 1213, together with companion memos (RFC 1155 and RFC 1157) provides a simple, workable architecture and system for managing TCP/IP-based internets, and the Internet community in particular. The SCM supports the following MIB-II groups: Address Translation Group, IP Group, ICMP Group, UDP group, Transmission Group, TCP group, and SNMP group. The SCM does not support the EGP Group.

Note *RFC 1155 describes the structure of management information, and RFC 1157 describes the network management protocol for TCP/IP-based internets.*

SNMP IP Routing Table

In the MIB-II there is an IP routing table that contains an entry for each route known to the SCM. The main function of this table is to equate an out-going IP packet with a route that provides the physical interface port. The routing table can be built via SNMP if there is an existing IP connection to one of the ports. The routing table is stored in volatile memory, so it is lost if the SCM is re-powered.

IP Route Creation

A route in the IP routing table can be created through SNMP by sending a single PDU with ipRouteNextHop, ipRouteMask, and ipRouteIpindex set. The instance is calculated by ANDING ipRouteNextHop with ipRouteMask. Other variables may be set in the same PDU, but ipRouteNextHop, ipRouteMask, and ipRouteIpindex must be set in the same PDU as a minimum for creation. Variables not set in the PDU take default values.

Example:
The route has a next hop IP address of 192.9.200.26, a subnet mask of 255.255.0.0 and an if index of 1. The route instance is calculated as (192.9.200.26 & 255.255.0.0) which is 192.9.0.0. The user does a set of ipRouteNextHop.192.9.0.0 = 192.9.200.26, ipRouteMask.192.9.0.0 = 255.255.0.0 and ipRouteIpindex.192.9.0.0 =1. This causes a route of 192.9.0.0 to be created, which points to the LAN port (index of 1).

IP Route Modification

A route in the IP routing table can be modified through SNMP by setting the ipRoute variable that is pointed to by the instance of the route. A route cannot be modified if its route type is direct. In the SCM the LAN, CTRL, and DBU WAN ports are configured as direct routes and cannot be modified through SNMP.

Example:
The route instance is 0.0.0.0 with type = 4. User does a set of ipRouteType.0.0.0.0 = 3. This causes the route type to change to 3. Once the type is changed to 3, (direct type) it cannot be modified.

IP Route Deletion

A route in the IP routing table can be deleted through SNMP by setting its ipRouteType to **`invalid`**.

Example:
The route instance is 0.0.0.0. User does a set of ipRouteType.0.0.0.0 = 2. This causes the route to be deleted and removed from the routing table.

Note *A zero value cannot appear to the left of a non-zero value in the mask. For example, 255.255.0.0 is a valid mask; 255.0.255.0 is not a valid mask.*

Other MIB Groups

System Group

All objects in the system group are supported as specified in the RFC.

Table 5-8 System Group Variables

Variable	Description
sysDescr	Returns a string in the form of the SpectraComm Manager (SCM) Version 1.00B. This is the version of the SCM code that is currently running.
sysObjectID	Returns the Object IDentifier (OID) for the scmMaster branch of the MIB tree. The object scmMaster is set to: **`iso.org.dod.internet.private.enterprises.gdc.sc.scm`** which in numerical form is: **`1.3.6.1.4.1.498.3.6`**
sysContact	These objects are all stored within the SCMs non-volatile memory area. The default value for each is a zero length, null string.
sysName	
sysLocation	
sysServices	Returns the value of 72. This represents a node offering services at layers 4 (end-to-end) and 7 (applications).

Interface Group Table

The **`ifNumber`** object returns the value 3 for the three available interfaces. The rows described in the **`ifTable`** contain read-only objects. The table that is indexed by **`ifIndex`** pertains to the following interfaces:

ifIndex	Interface
1	LAN
2	WAN/DBU
3	MBUS
4	CTRL

Appendix A: Maintenance

Overview

This section describes the procedures for maintaining the firmware in the SCM and also in the network elements in the shelf. Before performing a firmware download, read the firmware download guidelines and definitions provided below.

Firmware Definitions

The SCM card can operate under two distinct versions of firmware: the Boot code or the Application code. The type of code can be determined from the SCM cards front panel INS (In Service) indicator, which flashes or illuminates according to the code currently running:

- INS indicator flashes green when the SCM card is in Boot mode.
- INS indicator illuminates steadily when the card is in Application mode.

Another means of identifying the running code is via a VT100-compatible terminal connected to the front panel CTRL port. When the SCM card is powered up, the startup screen displays the type of operating code currently running on the card.

Switching Operating Codes

The user must place the SCM card in Boot mode in order to load Application code into the SCM memory. In Boot mode, SCM card can communicate over a LAN or WAN using TFTP protocol. However, while in Boot mode, the SCM cannot perform SNMP communications, such as access and poll network elements. Therefore, after the Application code is loaded, the user must use a Trivial File Transfer Protocol (TFTP) command to put the card back into Application mode.

Getting Files

The SCM acts only as a TFTP server, waiting for a client’s request to receive files (**`GET`**) or send files (**`PUT`**). All files returned by the **`GET`** command are ascii-based and should be retrieved in netascii mode. The following commands get their associated files from the SCM:

`APPLVER` - gets the Application software version. The value returned is the same as the SNMP variable scmApplVersion found in the SCM MIB. In Application mode it determines if a new software download is necessary. In Boot mode, the string of 0.00 is returned.

`BOOTVER` - gets the Bootrom software version. The value returned is the same as the SNMP variable scmBootVersion found in the SCM MIB.

`SCMBOOT` - instructs the SCM to go into Boot mode. If the SCM is already in Boot mode, no further action occurs. The string OK is returned.

`SCMMODE` - indicates the SCM current operating mode. One of the following strings are returned:

`APPLICATION` - the SCM is operating from application code.

`BOOT` - the SCM is operating from boot code. The INS LED blinks during BOOT mode.

`DOWNLOAD` - the SCM is currently downloading new application code.

Firmware Download Guidelines

FTP Time-Outs

During a read request cycle where the network manager is getting files from the SCM, it is the network manager's responsibility to determine a reasonable time-out and retry count for obtaining the file. The suggested values are a time-out of five seconds with a retry count of three.

During a write request cycle where the network manager is putting a download file to the SCM, the SCM uses a fixed-value time-out if data stops appearing in mid-transfer. After that time-out expires, the UDP ephemeral port connection is destroyed, and any further attempts to communicate with that port results in an ICMP port unreachable response.

TFTP Error Conditions

- Any duplicate packets received is acknowledged and discarded.
- Any data packet that arrives out of sequence as determined by the block number field is acknowledged and discarded.
- Attempting to **`GET`** any file name other than those previously described in the **`GET`** files section results in an error code of 1 (**`File not found`**) as defined by RFC 1350.
- Attempting to **`PUT`** any file name other than those previously described in the PUT files section results in an error code of **`1`**.
- Attempting to **`PUT`** a valid network element file name for an element that is not responding results in the same error code. In all cases, the connection is dropped.
- Attempting to **`PUT the SCMCODE.DWL`** file in netascii mode results in the response **`TFTP Not In OCTET Mode`**.
- Attempting to **`PUT`** the S**`CMCODE.DWL`** file when the SCM is not in boot mode results in the response **`SCM Not In Boot Mode`**.
- Attempting two simultaneous **`PUT`** sessions cause an error message of **`Download Already In Progress`**.

Note *The code version number is formatted as x.yz where x is a major revision, y is a minor revision, and z is a typographical revision.*

Note *All file names recognized by the SCM are case insensitive. The size for each file is a single line, terminated by a carriage return/line-feed sequence.*

Special Considerations

When RADIUS is enabled at the SCM, the network manager should schedule maintanence procedures such as firmware downloads during low peak hours.

Downloading SCM Program Code

SCMCODE.DWL is the actual code that is downloaded into the application area of the SCM memory. It is a binary file and must be sent with the transfer mode set to binary. The SCM resets and performs its normal start-up procedure after some time-out at the end of the download. As long as the code checksum is correct, the SCM runs the application code. The network manager can check the current version of the APPLICATION code before it does a download to see if the latest version is already installed and operational.

SCM Download Procedure

The following procedure and flow chart shows the sequence that should be followed to download new program code to an SCM.

1. Start a TFTP session by connecting to the SCM.
2. Get the file SCMBOOT in ascii mode from the SCM.
3. Wait for the SCM to re-establish the link.
4. Start a new TFTP session to the SCM.
5. Put the SCMCODE.DWL file in binary mode to the SCM.

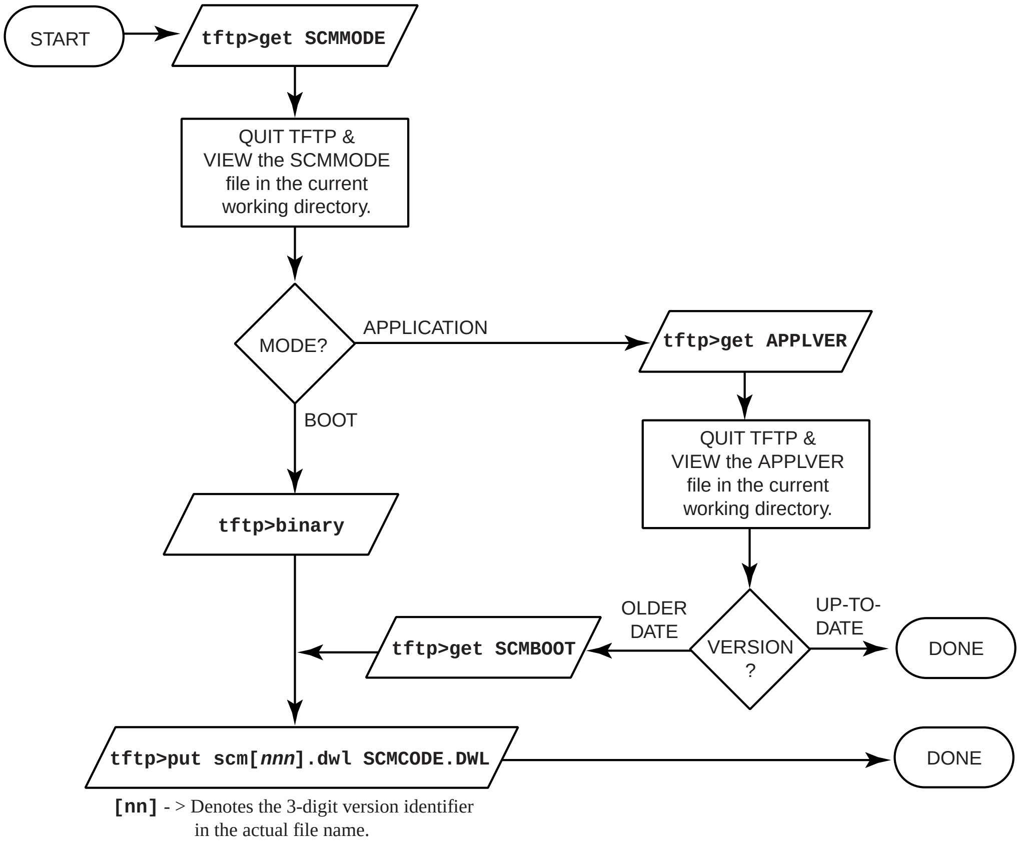

START
tftp>get SCMMODE
QUIT TFTP & VIEW the SCMMODE file in the current working directory.
MODE?
APPLICATION
BOOT
tftp>get APPLVER
QUIT TFTP & VIEW the APPLVER file in the current working directory.
tftp>binary
OLDER DATE
VERSION ?
UP-TO-DATE
DONE
tftp>get SCMBOOT
tftp>put scm[nnn].dwl SCMCODE.DWL
DONE
[nn] - > Denotes the 3-digit version identifier in the actual file name.

Figure A-1 Sequence for Downloading SCM Application Code

Downloading Network Element Firmware

The SCM card supports the download of operating code to the network elements installed with it in the SpectraComm/UAS shelf. The SCM uses TFTP to send code to network elements. Network elements may be updated individually (by address) or as a group (by product code). Downloaded code is buffered in the SCM and delivered to the network elements by way of the shelf backplane.

Note *When updated individually, network elements can report errors during the code transfer. However, group updates (Broadcast) can report no errors until the entire transfer has been completed. Refer to Table A-1 for interpretations of TFTP Error Messages.*

Downloading Guidelines

The download procedure for network elements is similar to downloading code to the SCM. It consists of two processes: send Boot code to network elements, and then send Application code to **`<applicPP.PP>`** (the SCM knows the address).

1. Prepare the network elements for downloading application code.

   - Which elements for downloading application code?
   - Each unit verifies its Product code with request.
   - A local file (on client) is named to send as a request.
   - The network elements may store the contents of the download request file (it might be needed to download application, etc.).

2. Download the application code.

   - A local file (on client) is named as application.
   - Each unit verifies its Product code with request.
   - Single address network element can report errors.

File Naming Conventions

The remote file naming convention serves two basic purposes:

1. Defines the destination address when sending Boot Code (All numbers are in HEX).

   - Single Address: **`<SSLLDDPP.PP>`** where

```
SS      Slot          (1 - 20)
LL      Line          (1 - 3A)
DD      Drop          (0 - 1F)
PP.PP   Product Code(0 to FFFF)
```

   - Product Specific Broadcast: <brdcstPP.PP> where

```
PP.PP   Product Code(0 to FFFF)
```

2. Defines the type of file when sending Application Code.

Application Code: **`<applicPP.PP>`** where Operational Checks

```
PP.PP   Product Code(0 to FFFF)
```

Network Element Download Procedure

1. Open TFTP session using the IP of the SCM.
2. Type: **`bin`**
3. Type: put <local request file> **`SSLLDDPP.PP`**
4. Repeat Step 3 to set up several network elements (but not all of them) at once.

   or

5. Type: **`put <local request file> brdcstPP.PP`**
6. Type: **`put <local application file> applicPP.PP`** to send application to a single card.
7. Type **`<local application file> applbrPP.PP`** to send application to all NE(s) selected in Step 4 or in Step 5.
8. Type: **`q`**

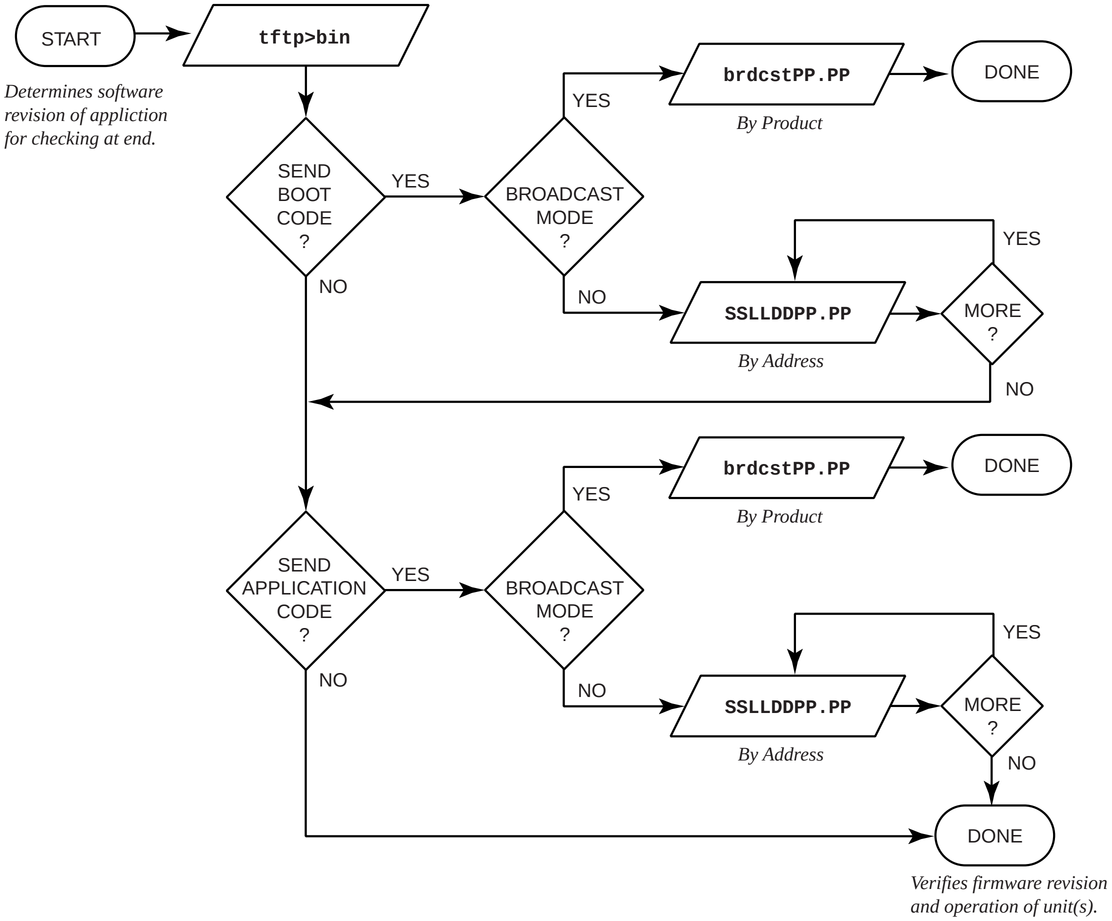


Figure A-2 Sequence for Downloading Code to Network Elements

Error Messages

Table A-1 FTFP Error Messages

Error Code	Message	Interpretation
0	Cannot get this file while in Download mode	While a file is downloading you cannot GET the applver file or use scmboot to instruct the SCM to go into BOOT mode.
0	Download already in progress	A file is currently being downloaded to the SCM.
0	Error erasing FLASH	The FLASH memory could not be erased while trying to download a file.
0	Error writing to FLASH	While downloading a file to the SCM, no more data could be written to the FLASH memory.
0	Invalid application checksum	The application checksum was incorrect following a download.
0	Invalid mode	Returned if the mode during a TFTP GET is not "netascii."
0	SCM not in BOOT mode	Returned if a download to the SCM is attempted while it is any mode but BOOT.
0	TFTP not in OCTET mode	Returned if a download to the SCM is attempted while TFTP is not in octet or binary mode.
1	File not found	Returned if the filename to GET or PUT does not match the filename that resides in the SCM.
5	Unknown transfer ID	Returned if the source transfer ID does not match the source transfer ID established during the read or write request.
0	Invalid product code	No NE exists for the product code. A different NE is present at this address.
0	Not ready	The NE replied that it was busy and could not complete.
0	Not in download mode	The NE was asked to accept an application file before it was placed in download mode.
0	Bad NE code Checksum	After downloading the application code, the NE replied that the checksum verification failed.
0	SNMP setting deny access	The SNMP object `scmCodeDownload` was set to: disable(2). To download code to the SCM or to any NE(s), it must be set to enable(1)
0	NE not responding	The SCM did not get a response form the NE. No NE is at that address.
0	Invalid address	The slot, line, and/or drop were of range, where the ranges are Slot (1-32), Line (1-128), and Drop (0-31).

Table A-2 VT100 Error Messages

Message	Interpretation
Invalid Address	The SCM accepts only values between 0 and 255 as input for an IP address or subnet mask.
Invalid Password	The correct password must be entered to access the Test Menu.
Route Already Exists, Input Not Accepted	The route that results from the IP address and/or subnet mask entered for a port or gateway must be unique. The SCM ANDS together address and mask input, then compares the resulting route with existing routes. If a match occurs, the input is rejected. A route defined as zero is not compared, and so is always accepted.

Appendix B: SCM with RADIUS

Remote Authentication for Dial-In Users (RADIUS)

GDC's Remote Authentication for Dial-In Users Service (RADIUS) is an optional software feature for the SCM. A shelf system protected by RADIUS security consists of a customer-supplied RADIUS server, a GDC SpectraComm Manager (SCM) card equipped with RADIUS, and either a GDC SpectraComm Dual V.34 modem or a GDC SpectraComm V.28.8/33.6 modem. Either type of RADIUS-capable modem must be optioned at the factory for RADIUS.

RADIUS Operation Overview

- The modem conducts a client service session for RADIUS security, prompting the user for a user name and password. This information passes to the secure RADIUS server via the SCM.
- The SCM emulates a Network Access Server, operating as a client of the RADIUS server. The client is responsible for passing information to a RADIUS server and then acts upon the returned response.
- The RADIUS server communicates with the SCM to authenticate the dial-in caller.

Once a dial-in caller is authenticated through the user name and password, the RADIUS server may then send an additional Challenge which prompts for the caller's unique Challenge reply. Network access is then either granted or denied.

Modem and RADIUS Password Overview

It is important to distinguish between the two types of security passwords. With RADIUS, the caller is prompted for the **`password`** that is stored with the user name at the RADIUS server. RADIUS user name/password procedures are described in RADIUS Configuration Procedures later in this in this Appendix. *RADIUS passwords can be upper/lower case alphanumeric characters.*

If RADIUS becomes disabled, the modem will activate Online Security and prompt the caller for a **`cell password`** stored in the modem. For more information on Online Security cell passwords, refer your RADIUS-capable modem manual. *Cell passwords must be uppercase characters only.*

RADIUS Communication Overview

A RADIUS server can communicate with the SCM through several interface options, both locally and across the Public Switched Network. The following tables and their associated diagrams show the cables and adapters required for each RADIUS connectivity option:

- Table B-1: SCM RADIUS via the LAN interface (10Base-T)
- Table B-2: SCM RADIUS via the LAN interface (10Base-2)
- Table B-3: SCM RADIUS via the WAN interface (Direct Serial PPP)
- Table B-4: SCM RADIUS via the DBU WAN interface (modem/serial PPP)

Note *In order to configure an SCM for RADIUS, you must connect a terminal to the SCM Front Panel CTRL port.*

SCM RADIUS Connectivity

The following diagrams illustrate the options for connecting the SCM with RADIUS through its LAN port, WAN port, DBU WAN port and the SCM front panel CTRL port. Each diagram identifies cables and adapters for those interfaces. Ensure that the appropriate connections are in place and operational before proceeding with the RADIUS procedures in this Appendix.

Note *To hook up a remote terminal at the SCM's Front Panel CTRL port using a modem, refer to Chapter 3: Front Panel CTRL Port Management .*

RADIUS Communication via LAN (10Base-T)

The diagram below shows the required connectivity for RADIUS setup and communication along the LAN (10Base-T) interface. *Table B-1* details the cables [C#] and adapters [A#] used in the diagram.

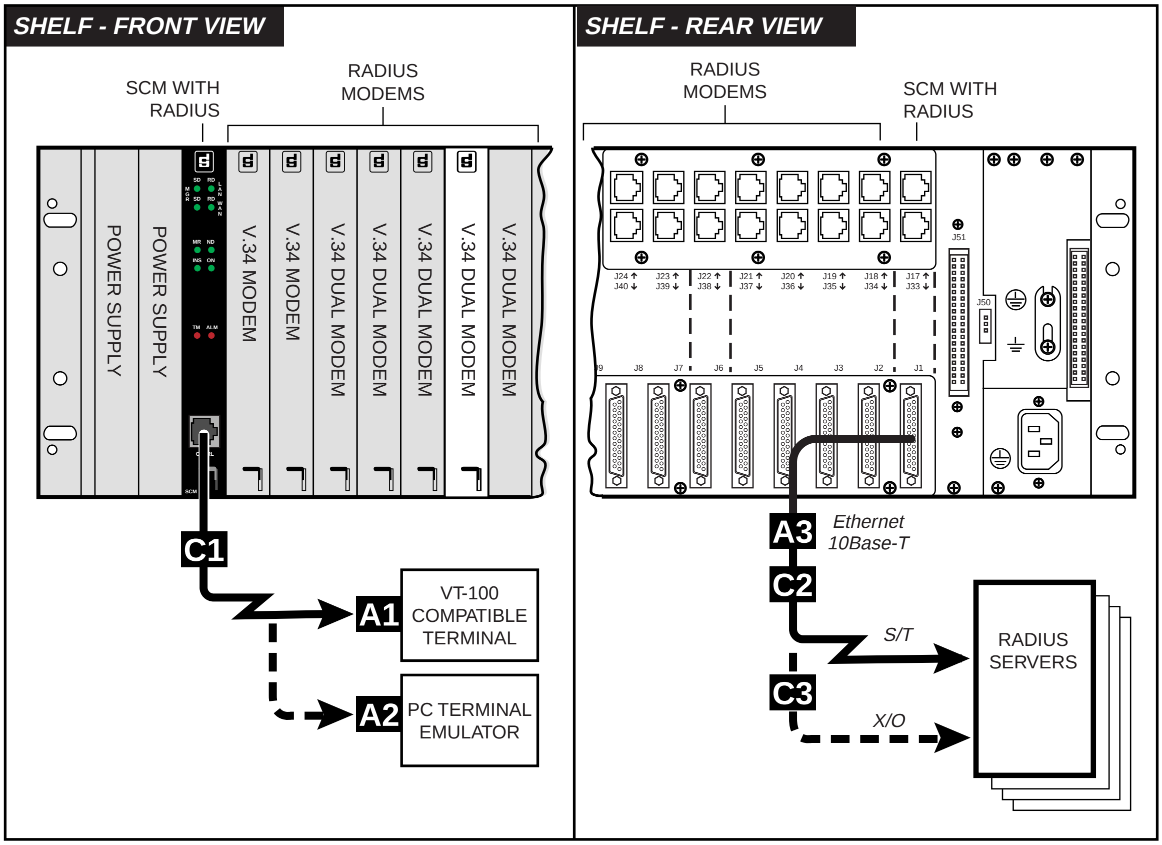


Table B-1 Typical LAN Connections in a SCM-RADIUS Shelf (10Base-T)

Cable/Adapter	Location	Description	Part Number
C1	CTRL Port	RJ45 to RJ45 cable, S/T, non-keyed	830-128-807
C2	J1	CAT5 patch cable, straight-thru	S-078H10-XXX
C3		CAT5 patch cable, crossover	S-078H11-XXX
A1	Terminal	RS232 DB25 male to RS561	029H210-001
A2	Terminal	DB9 female to RS561	029H211-001
A3	J1	LAN interface adapter, twisted pair, 10Base-T	029H209-001

RADIUS Communication via LAN (10Base-2)

The diagram below the options for connecting the SCM with RADIUS through its LAN (10Base-2) interface. *Table B-2* details the cables [C#] and adapters [A#] used in the diagram.

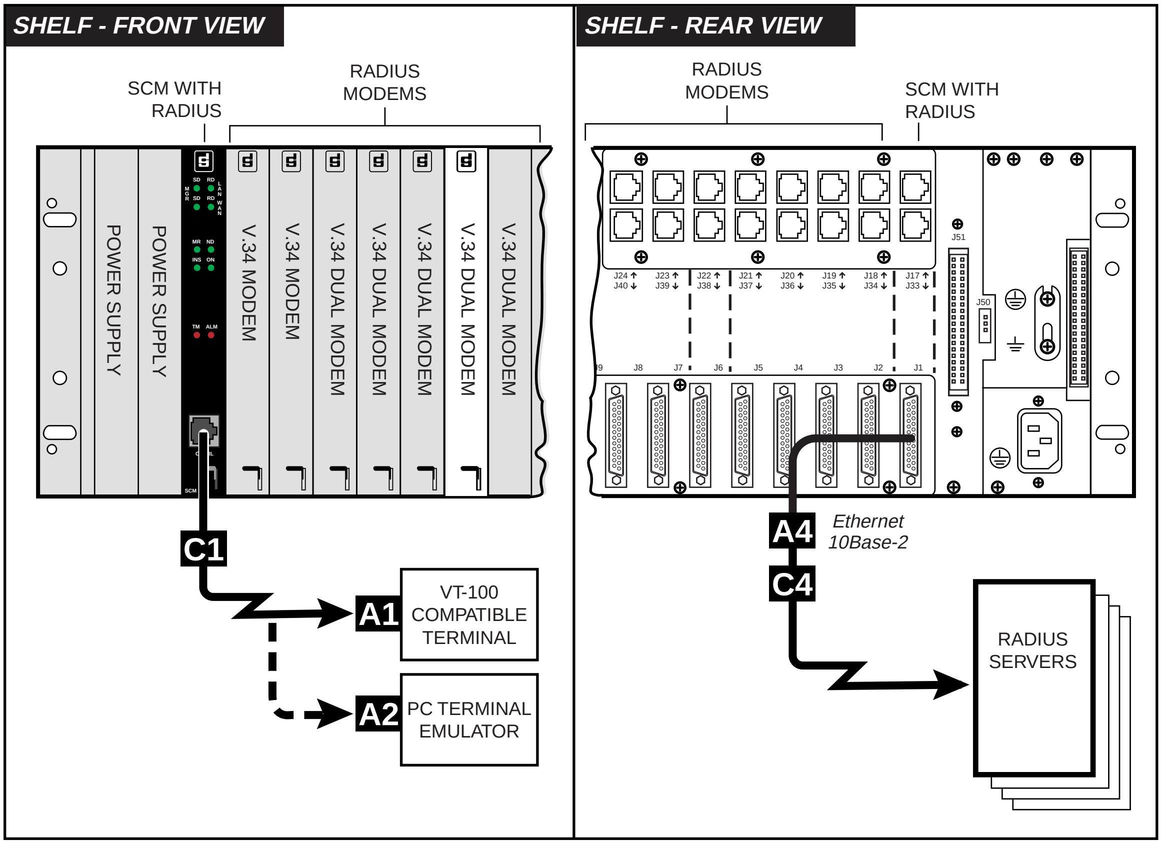


Table B-2 Typical LAN Connections in a SCM-RADIUS Shelf (10Base-2)

Cable/Adapter	Location	Description	Part Number
C1	SCM CTRL Port	RJ45 to RJ45 cable, S/T, non-keyed	830-128-807
C4	J1	LAN interface cable, coaxial, 5 meters	S-125H003-001
		LAN interface cable, coaxial, 15 meters	S-125H004-001
		LAN interface cable, coaxial, 30 meters	S-125H005-001
A1	Terminal	RS232 DB25 male to RS561	029H210-001
A2	Terminal	DB9 female to RS561	029H211-001
A4	J1	LAN interface adapter, coaxial, 10Base-2	058B003-001

RADIUS Communication via WAN

The diagram below the options for connecting the SCM with RADIUS through its WAN interface. *Table B-3* details the cables [C#] and adapters [A#] used in the diagram.

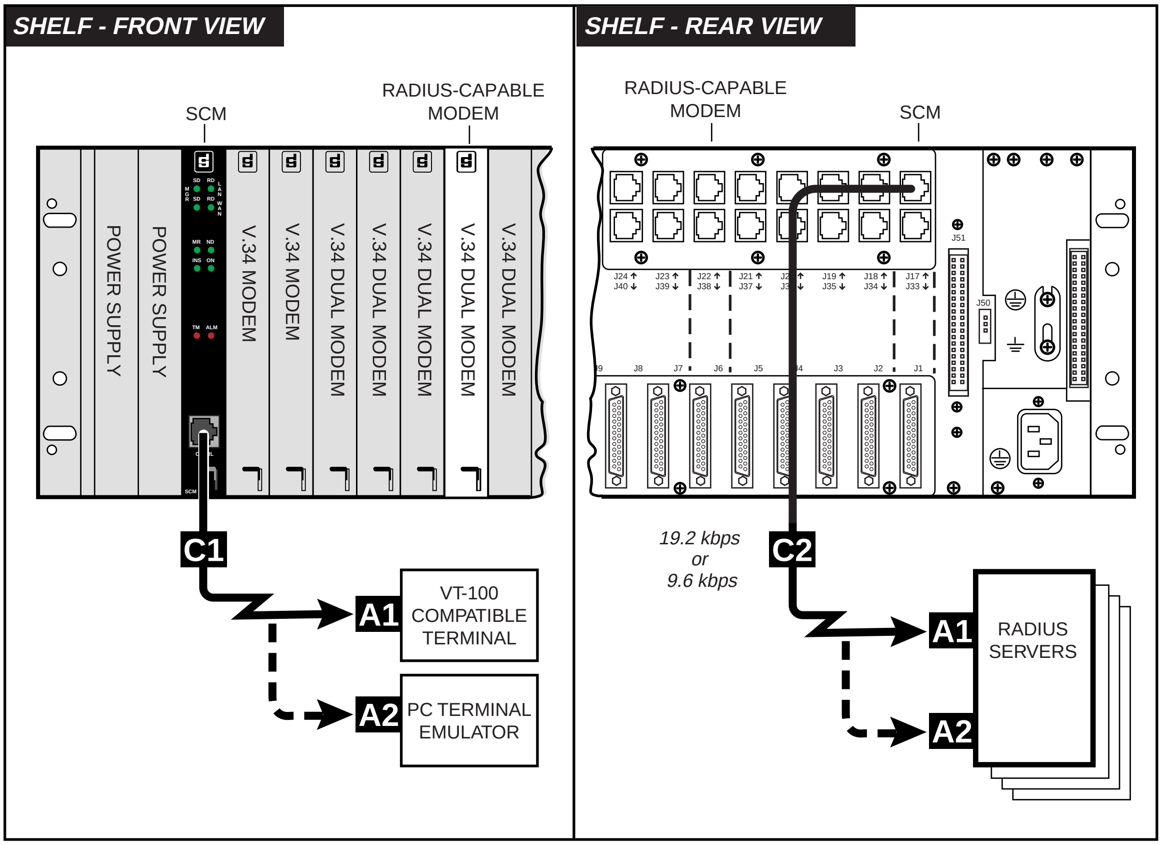


Table B-3 Typical WAN Connections in a SCM-RADIUS Shelf

Cable/Adapter	Location	Description	Part Number
C1	SCM CTRL Port	RJ45 to RJ45 S/T cable, non-keyed	830-128-807
C2	J17	RJ45 to RJ45 S/T cable. non-keyed	830-128-807
A1	Terminal or Server	RS232 DB25 male to RS561	029H210-001
A2	Terminal or Server	DB9 female to RS561	029H211-001

RADIUS Communication via DBU WAN

The diagram below shows how to connect a RADIUS server to the SCM via the DBU WAN interface. Table B-4 details the cables [C#] and adapters [A#] used in the diagram. Table B-5 provides modem initialization strings and modem commands.

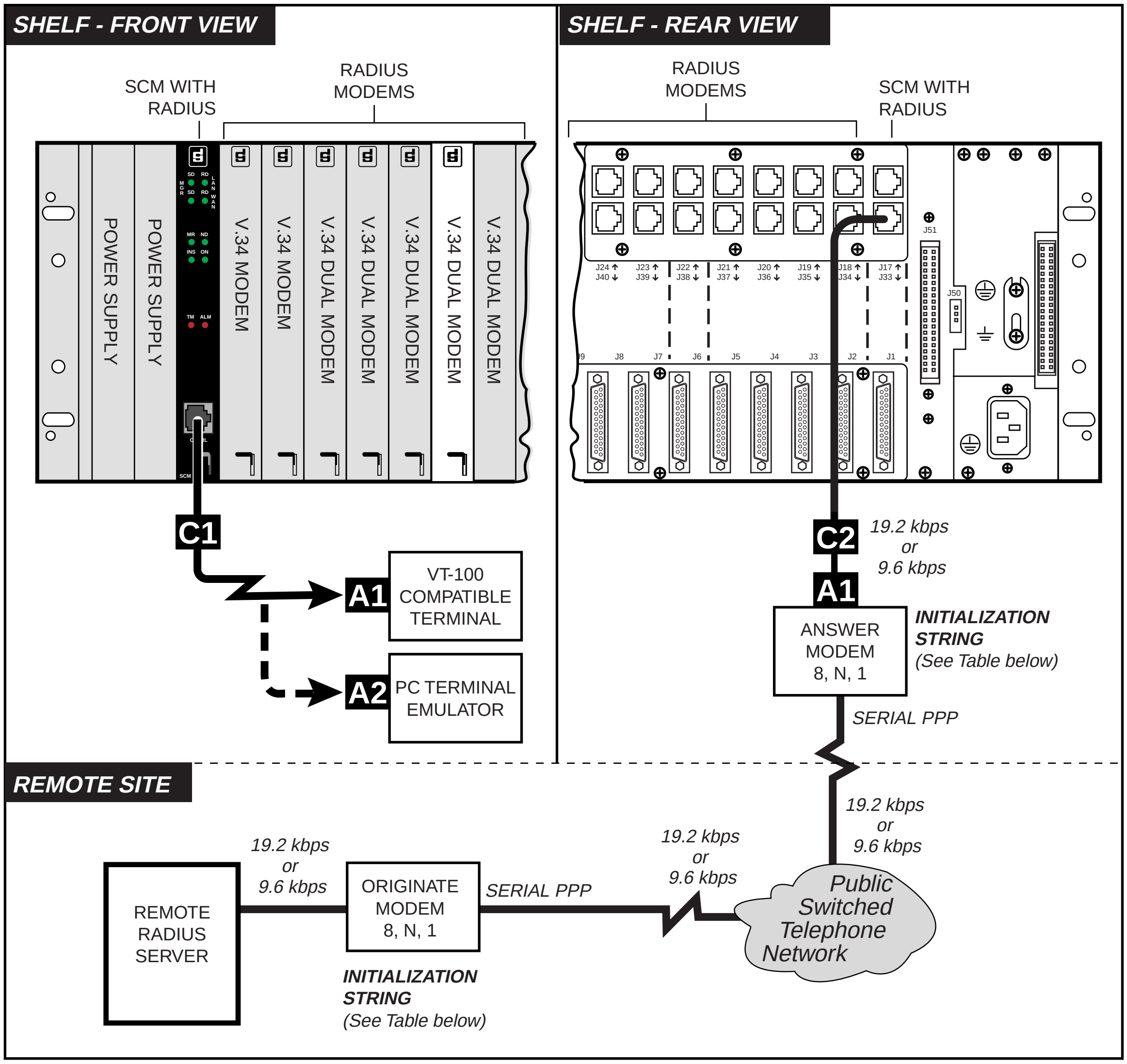


Table B-4 Typical DBU WAN Connections in a SCM-RADIUS Shelf

Cable/Adapter	Location	Description	Part Number
C1	SCM CTRL Port	RJ45 to RJ45 S/T cable, non-keyed	830-128-807
C2	J33	RJ45 to RJ45 S/T cable, non-keyed	830-128-807
A1	Terminal or Modem	RS232 DB25 male to RS561 adapter	029H210-001
A2	Terminal or Modem	DB9 female to RS561 adapter	029H211-001

Table B-5 Initialization Strings and Modem Commands

Command Descriptions	
&F	Factory Default Modem
%C0	Disable Compression
&D0	Ignore DTR (Force DTR On)
&G7	Maximum DCE Rate: 9600 bps
&G11	Maximum DCE Rate: 19200 bps
%K1	Disable Character Abort
\Q0	No Flow Control
\V0	Connect Message, V.F. Speed and Protocol
\R0	Disable Asymmetrical Rates
\T7	Lock DTE Speed to 9600 bps
\T11	Lock DTE Speed to 19200 bps
&H1	V34 only
&W	Save Options
E0	Disable Local Echo
Q1	Put In Quiet Mode

Modem/Speed	MODEM Initialization Strings
Answer Modem at 19200 bps	**AT&F%C0&D0&G11%K1\Q0\R0\T11&H1&W<CR>** **ATE0Q1&W<CR>**
Answer Modem at 9600 bps	**AT&F%C0&D0&G7%K1\Q0\R0\T7&H1&W<CR>** **ATE0Q1&W<CR>**
Originate Modem at 19200 bps	**AT&F%C0\V0&G11\T11&W<CR>**
Originate Modem at 9600 bps	**AT&F%C0\V0&G7\T7&W<CR>**

Note *Make sure the SCM speed is optioned at DIP Switch S1-2 to match the modem speed.*

SCM RADIUS Field Upgrade

An SCM with RADIUS installed at the factory will have RADIUS enabled in the SCM. An SCM in the field can be upgraded to RADIUS capability by the factory or by the user. The preferred method is to return the SCM card to General DataComm for a factory upgrade. This ensures that the SCM has RADIUS fully installed, enabled and identified on the card.

As an alternative, the user can upgrade an existing SCM in the field to support RADIUS by taking the following actions:

- Download and install the latest SCM code (for a SpectraComm or UAS shelf)
- Purchase a RADIUS Client Key to enable the feature (GDC P/N 058U150-D01)
- Activate the RADIUS Client Key in the SCM
- Configure RADIUS in the SCM

Note *IMPORTANT! Make sure to complete basic SCM configuration procedures prior to installing and configuring RADIUS. Refer to Chapter 3: SCM Configuration for accessing and using SCM configuration screens.*

Acquire RADIUS Code and Client Key

1. Download the latest SCM code by using:

```
ftp://ftp.gdc.com/pub/mibs/shelfCtrlr/scm/scm.html
```

2. The download file (.dwl) is binary and should be saved to your local disk to be sent to the intended SCM via TFTP.

Note *To download the SCM with RADIUS code, follow the Downloading SCM Program Code procedure described in Appendix A.*

3. Have ready the SCM’s 16-digit serial number and then contact GDC Customer Support to purchase a RADIUS Client Key for the intended SCM.

   The SCM serial number starts with **`0018`** and can be found printed on the SCM card’s EPROM-U4 or displayed onscreen at the SCM’s Version Table (Telnet or CTRL port).

Note *IMPORTANT! Only use the serial number printed on the EPROM label on the SCM card or as displayed at the terminal interfaces. Do not use the SCM serial number which is displayed at the SNMP interface via the TEAM windows.*

4. Perform all of the RADIUS configuration procedures below, using the RADIUS Client Key. The acquired Client Key will fully activate RADIUS for one single, specific SCM.

Note *Keep the RADIUS Client Key in a secure location in the event that the SCM loses them from memory. This can occur when the SCM is un-powered for an extended period.*

RADIUS Configuration Procedures

The SCM Control Port terminal interface provides a Main Menu which contains the hidden RADIUS menus and screens. Procedures for each RADIUS menu function are provided below.

Note *IMPORTANT! If you have installed RADIUS via firmware download to the SCM, you must acquire a RADIUS Client Key from General DataComm to proceed with RADIUS configuration.*

Note *IMPORTANT! To ensure RADIUS security, it is strongly recommended that you disable the Remote Configuration feature on the RADIUS modem (**AT*R1**).*

Note *IMPORTANT! To ensure the integrity of RADIUS security, it is strongly recommended that the default SCM Telnet password be changed from **scmadmin** to some other unique password. This will prevent unauthorized users from making a Telnet connection to the SCM and disabling security on the modems (refer to Chapter 3: Security Screen procedure). As an alternative, Telnet communication can be disabled with a MIB browser or via TEAM management, if available.*

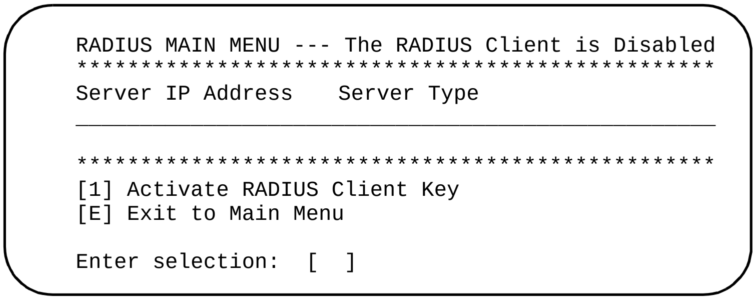
Accessing the RADIUS Main Menu

Whether factory-installed or user-installed, RADIUS must be configured by the user according to the specific network management needs. RADIUS configuration can only be performed at the front panel CTRL port.

1. Connect a VT100-compatible terminal to the front panel CTRL port.
2. Ensure that Switch S1-4 on the card is set to the **Open** position. This is the factory default which allows the terminal to function with the SCM card.
3. The terminal screen will display the Main Menu when you press **Enter**.
   If the terminal screen is blank, press **Enter** to refresh the screen.

Note *If some other screen beside the Main Menu displays, back out of the screen(s) until the terminal screen displays the Main Menu.*

4. At the Main Menu, press the key combination **CTRL-R**, then press **Enter**.
5. At the prompt, type the RADIUS password in all lower case as follows: **validate**, then press **Enter**.
6. If RADIUS has been user-installed via firmware download, the RADIUS Main menu will appear as shown below with limited selections available. If RADIUS has been factory-installed, or if it has already been activated, skip to step 10.



```
RADIUS MAIN MENU --- The RADIUS Client is Disabled
**************************************************
Server IP Address    Server Type
__________________________________________________

**************************************************
[1] Activate RADIUS Client Key
[E] Exit to Main Menu

Enter selection:  [  ]
```

7. Press **1** to activate the RADIUS Client Key.

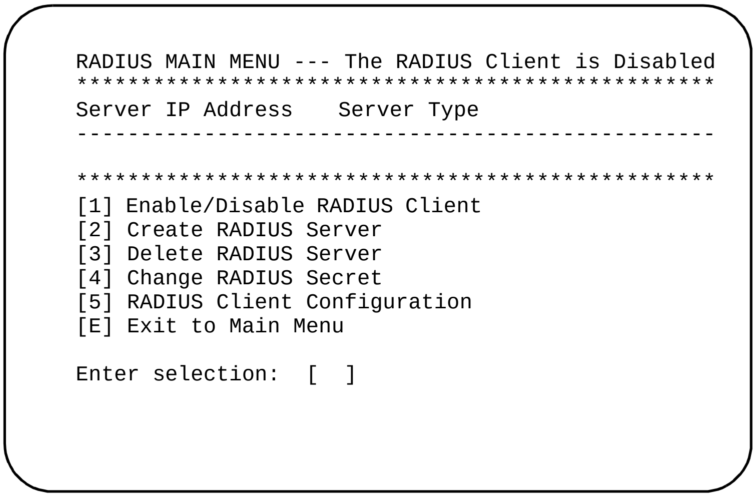
8. At the prompt, enter the 24 alpha-numeric characters, separated at intervals by spaces.

Note *You can only use a RADIUS Client Key for its specific SCM and the Key must be entered exactly with no errors, corrections or backspaces. Otherwise, the screen will refresh and the following message will display:* ***`Error: key must have 24 ascii characters separated by spaces. Format: #### #### #### #### #### ####`***

9. When the SCM has successfully decoded and activated the Client Key, the following message will display:

```
Key Activated Successfully
 Please Enable and Configure RADIUS Client
```

10. The full RADIUS Main Menu appears, as shown below. Initially, the screen will display the status of the RADIUS client and RADIUS menu items. No server data will be displayed until servers are created via this menu. Table B-6 describes the menu selections, with procedures following the table.



```
RADIUS MAIN MENU --- The RADIUS Client is Disabled
**************************************************
Server IP Address    Server Type
--------------------------------------------------

**************************************************
[1] Enable/Disable RADIUS Client
[2] Create RADIUS Server
[3] Delete RADIUS Server
[4] Change RADIUS Secret
[5] RADIUS Client Configuration
[E] Exit to Main Menu

Enter selection:  [  ]
```

Table B-6 RADIUS Main Menu

Display / Selections	Description
RADIUS Client Status	Read-only display of the RADIUS Client: Enabled or Disabled.
[1] Enable/Disable RADIUS Client	Opens a Enabled/Disable menu and entry field. *Procedures and precautions described below.*
[2] Create RADIUS Server	Opens an entry field for creating up to six RADIUS servers with their associated IP addresses, server types, and Secrets. *Procedure described below.*
[3] Delete RADIUS Server	Opens an entry field for deleting a RADIUS server by its IP address. *Procedure described below.*
[4] Change RADIUS Secret	Selects a RADIUS server by its IP address in order to change the Secret shared between the SCM and the RADIUS server(s). *Procedure described below.*
[5] RADIUS Client Configuration	Advances to a Configuration screen for setting several operation and parameters of the RADIUS Client. *Procedure described below.*
[E] Exit to Main Menu	Exits the RADIUS Main Menu, and returns to the Main Menu.

Enabling RADIUS Client

1. At the RADIUS Main Menu, press **1**, then press **Enter**.
2. At the prompt, press **1** and then press **Enter** to enable RADIUS Client.
3. Press **E** to return to the RADIUS Main Menu. The RADIUS Client Status will now display **Enabled**.

Disabling RADIUS Client

Disabling the RADIUS Client will prevent users from logging in unless cell passwords are configured in the modems.

1. At the RADIUS Main Menu, press **1**, then press **Enter**.
2. At the prompt, press **2** and then press **Enter** to disable RADIUS Client.
3. Press **E** to return to the RADIUS Main Menu. The RADIUS Client Status will now display **Disabled**.
4. The next dial in caller will have to wait 60 seconds while the RADIUS modem tries a RADIUS login. The modem will request an On-line Security cell password.

Note *Entering a cell password in a RADIUS modem by using the* **%P** *commands can compromise RADIUS security and should only be performed by the supervisor in emergency conditions when all servers are not responding, or if the SCM is down.*

Create RADIUS Server

Up to six RADIUS servers can be created using the Create RADIUS Server selection. The first server created will be the Default RADIUS server used by the SCM. To create the first server, perform the following steps:

1. At the RADIUS Main Menu, press **2**, then press **Enter**. The screen displays the following:

```
Port# Translation: 1812 or 1645 = Authentication
Enter Server IP Address,Port,Secret:
```

2. At the prompt, type the server IP address, the Port number, and the Secret in one text string, separated by commas as show in this example: **###.###.###.###,NNN,Secret**

   where:

   ###.###.###.### *represents the IP address for the RADIUS server*

   NNN *represents the Authentication Port number (1812 or 1645)*

   Secret *represents the textstring (up to 16 upper/lower case alphanumeric characters) shared between the SCM and the RADIUS server*

Note *Use Port 1645 for Windows NT servers; use Port 1812 for all other servers.*
For more information, refer to the documentation which accompanied your server.

3. Press **Enter** to complete the RADIUS server entry. The RADIUS Main Menu refreshes with the new server data added to the table.

4. The first server entered becomes the default RADIUS server. Repeat steps 1 - 3 to create up to five redundant servers, as needed. If you attempt to create more than six RADIUS servers in total, the following message appears:

```
RADIUS Server Table is full
```

Note *Redundant RADIUS servers take over the authentication tasks when the Default server does not respond to the SCM. Refer to Redundant RADIUS Servers for a theory of operation and important configuration guidelines.*

Delete RADIUS Server

1. At the RADIUS Main Menu, press **3**, then press **Enter**.
2. At the prompt, type in IP address of the RADIUS server, then press **Enter** to delete the RADIUS server. The RADIUS Main Menu refreshes with the server removed from the table.

Change RADIUS Secret

1. At the RADIUS Main Menu, press **4**, then press **Enter**. The screen displays the following:

```
Enter Server IP Address,Old Secret,New Secret
```

2. At the prompt, type the server IP address, the old Secret and the new Secret in one text string, separated by commas as shown in this example:

```
###.###.###.###,OLDSecret,NEWSecret
```

where:

###.###.###.### *represents the IP address for the RADIUS server*

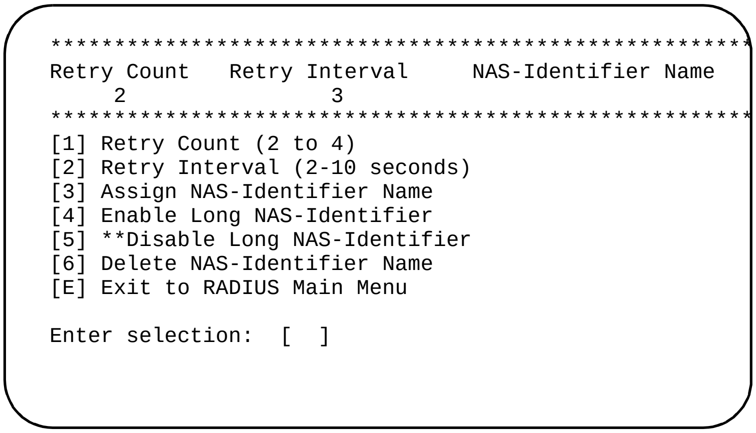
OLDSecret *represents the old shared secret (up to 16 characters)*
NEWSecret *represents the new shared secret* **Secret**
(up to 16 upper/lower case alphanumeric characters)
shared between the SCM and the RADIUS server

3. Press **Enter** to complete the RADIUS server entry. The RADIUS Main Menu refreshes and with the new secret available to the system.
4. Ensure that the customer-supplied RADIUS server is using the same Secret as entered at the SCM. Refer to your server documentation for more information.

Note *If the old Secret is lost/forgotten, you will need to delete the associated RADIUS server and re-create at the RADIUS Main Menu it in order to assign a new Secret to that server.*

Configuring RADIUS Client

At the RADIUS Main Menu, press **5** to access the RADIUS Client Configuration menu, described below. Detailed explanations, as needed, follow the table.



```
*******************************************************
Retry Count   Retry Interval     NAS-Identifier Name
     2                3
*******************************************************
[1] Retry Count (2 to 4)
[2] Retry Interval (2-10 seconds)
[3] Assign NAS-Identifier Name
[4] Enable Long NAS-Identifier
[5] **Disable Long NAS-Identifier
[6] Delete NAS-Identifier Name
[E] Exit to RADIUS Main Menu

Enter selection:  [  ]
```

Table B-7 RADIUS Client Configuration Selections

Display / Selections	Description
Retry Count	Read-only display of the Retry Count. DEFAULT: **2**
Retry Interval	Read-only display of the Retry Interval, in seconds. DEFAULT: **3**
NAS-Identifier Name	Read-only display of the shelf name or, if enabled, the specific network element location (shelf:slot:chan) that a user is dialing in on.
[1] Retry Count (2 to 4)	After the first try, the number of times the SCM will retry a RADIUS server for authentication. If the server does not respond after the last try, the SCM tries a redundant RADIUS server(s), if any.
[2] Retry Interval (2-10 seconds)	The number of seconds between the SCM's attempts to contact a RADIUS server for validation.
[3] Assign NAS-Identifier name	A RFC2138 standards-based Network Access Server identifier, up to 20 alpha-numeric characters, that identifies only the shelf that the caller is dialing in to.
[4] Enable Long NAS-Identifier [5] Disable Long NAS-Identifier	Enable or **Disable** a long name format used to identify the exact location of the hardware in the shelf that a caller is dialing in to. A double-asterisk will appear next to selection [4] or [5] to indicate whether the Long NAS-Identifier Name has been Enabled or Disabled.
[6] Delete NAS-Identifier Name	Clears the NAS-Identifier Name from the Client Configuration.
[E] Exit to RADIUS Main Menu	Exits the RADIUS Client Configuration screen, and returns to the RADIUS Main Menu.

Note *When multiple redundant RADIUS servers are created, it is recommended that the user set minimum values for the Retry Count and the Retry Interval to avoid modem timeout. Refer to Figure B-2 for examples and recommendations in typical situations.*

NAS-Identifier Names

The NAS Identifier is defined by RFC2138 and is unique to the NAS Client. This name is used to identify the location of the NAS Client that is communicating with callers attempting to dial into the network.

- When the user assigns a NAS-Identifier Name and sets the Long NAS-Identifier Name field to **`Disable`**, that entry becomes the only identifying name for the shelf where the NAS Client resides.

- When the user assigns a NAS-Identifier Name and sets the Long NAS-Identifier Name field to **`Enable`**, that entry becomes part of a detailed identifier for the NAS Client.
  A Long NAS-Identifier is sent as:

  `NAS_Indentifier:slot[#]:[A` *or* **`B]`**

  where: **`NAS_Identifier:`** is the shelf name.
  `slot[#]:` is the slot location in the shelf.
  `A` *or* **`B`** : refers to the separate modems (Dual V.34 modems only)

Note *The Long NAS Identifier option should only be used if the customer-supplied RADIUS server is capable of employing it. Refer to your server documentation for more information.*

RADIUS in Operation

Once RADIUS has been fully enabled and configured at the SCM, as described above, it is ready to authenticate dial-in users through the user names and passwords. RADIUS can also authenticate callers with an additional Challenge prompt from the RADIUS server. The following guidelines and procedures describe RADIUS in operation.

Note *Not all servers support Challenge. Refer to your server documentation to determine server capability.*

RADIUS Server Checklist

Check the following readiness list to make sure the customer-supplied RADIUS server is ready for operation. Refer to your server's documentation for setup and operation instructions.

✔ Ensure that the SCM IP Address has been entered at each RADIUS server.

✔ When creating user names and passwords, be aware of the limits imposed by your server and by the SCM. The SCM allows up to 25 upper/lower case alphanumerics for a user name and up to 25 upper/lower case alphanumerics for a password. The SCM also allows up to 16 upper/lower case alphanumerics for the Secret. As a rule, use as many characters as your server allows, without exceeding the limits imposed by the SCM.

✔ For each RADIUS server, ensure that the Secret created at the server is the same as the Secret entered at the SCM's RADIUS Main Menu for that server. Upper and lowercase alpha numeric characters are permitted.

✔ When creating a server at the SCM RADIUS Main Menu, ensure that the port number you enter (1812 or 1645) matches the port number (or platform) for that RADIUS server.

Note *When setting up a RADIUS server for Challenge authentication, you may use as many upper/lower case alphanumeric characters as your server allows but not more than 85 characters for the server's Challenge prompt, and not more than 50 characters for the caller's Challenge reply. These limits are imposed by the RADIUS modem and should not be exceeded.*

RADIUS Modem Checklist

Check the following readiness list to make sure the RADIUS modems are ready for RADIUS operation. Refer to your modem documentation for setup and operation instructions.

✔ Ensure the modem supports RADIUS authentication. The Product Code field at the modem's ATI4 screen will display `SEC` in modems that support RADIUS.

✔ Ensure that the modem has been configured for RADIUS. Use the modem's `AT %S2` command to option the modem for RADIUS Security. Save the configuration with by typing `AT &W` and then press `Enter`.

✔ Determine whether Remote Configuration will be allowed. The highest level of RADIUS security is achieved when Remote Configuration is disabled at the modem with the `AT *R1` command. Save this configuration by typing `AT &W` and then press `Enter`.

✔ Determine whether cell passwords will be stored in the modem. If so, cell passwords must be uppercase only. The highest level of RADIUS security is achieved when no cell passwords are stored in the modem. This ensures that if all RADIUS servers fail or if the SCM fails, all dial-in access to the network will be denied until the servers and/or SCM are back online. Refer to the information on the `%P` command in your modem manual.

✔ Turn off the modem's escape code characters by typing `AT S2=128` and then press `Enter`.

RADIUS Authentication Sequence

The following sequence is the basic order of operation that occurs when a caller dials in to a RADIUS-secured system. Be sure to read the final paragraphs on Special Conditions which provide additional RADIUS information and guidelines for maintaining the highest level of security during special network conditions.

1. A caller dials in to a modem in the shelf, and the modem prompts for a user name.
2. The caller has a total of 60 seconds to type the user name and press **`Enter`**. The modem will re-prompt the caller at 20-second intervals until a user name is entered, or until the 60-second interval ends. If a name has not been entered, the caller will be disconnected.
3. With a user name entered, the modem then prompts for a user password.
4. The caller has 60 seconds to type the password and press **`Enter`**. The modem will re-prompt the caller at 20-second intervals until a password is entered, or until the 60-second interval ends. If a password has not been entered, the caller will be disconnected.

Note *If your user name or password entry is interrupted by a modem re-prompt, always continue with the entry from the point of the interruption. DO NOT re-enter the user name or password from the beginning.*

5. When a user name and password have been entered, the SCM employs the shared Secret for the Default RADIUS server and then sends the user name and the encrypted password across the Ethernet/PPP link to the Default RADIUS server.

Note *The Default RADIUS server is the first server created at the RADIUS Main Menu. For detailed information on the sequence of operation when a Default server fails, refer to Redundant RADIUS Servers .*

6. When the responding RADIUS server receives the user name and password from the SCM, the user name and password is checked for authenticity.
7. If the RADIUS server was not able to authenticate the user name and password, the server tells the SCM to instruct the modem to disconnect the caller.

Note *Depending on server capability, an* **`Access Denied`** *transaction may be saved to a log file.*

8. If the RADIUS server was able to authenticate the user name and password, one of the following sequences will occur, depending on whether the server is capable of Challenge authentication.

RADIUS without Challenge

8A. The RADIUS server sends an Accept message to the SCM.

8B. The SCM instructs the modem to display an Access Granted message to the caller.

RADIUS with Challenge

8A. The RADIUS server sends a Challenge prompt to the caller.

8B. The caller has two minutes to type the Challenge reply and press **`Enter`**. The modem re-prompts the caller at 40-second intervals until a reply is entered, or when the two minutes lapse. If a reply has not been entered, the server denies access to the caller.

8C. If the caller enters a Challenge reply that the RADIUS server cannot authenticate, the server tells the SCM to instruct the modem to disconnect the caller.

8D. If the caller enters a Challenge reply that the RADIUS server can authenticate, the server sends an sends an Accept message to the SCM.

8E. The SCM instructs the modem to display an Access Granted message to the caller.

Note *The RADIUS server will wait a total of 120 seconds for the caller to type in a Challenge reply. At 40-second intervals, the modem will re-prompt if the entry was not completed.*

If your Challenge entry is interrupted by a modem re-prompt, always continue with the entry from the point of the interruption. DO NOT re-enter the user name or password from the beginning.

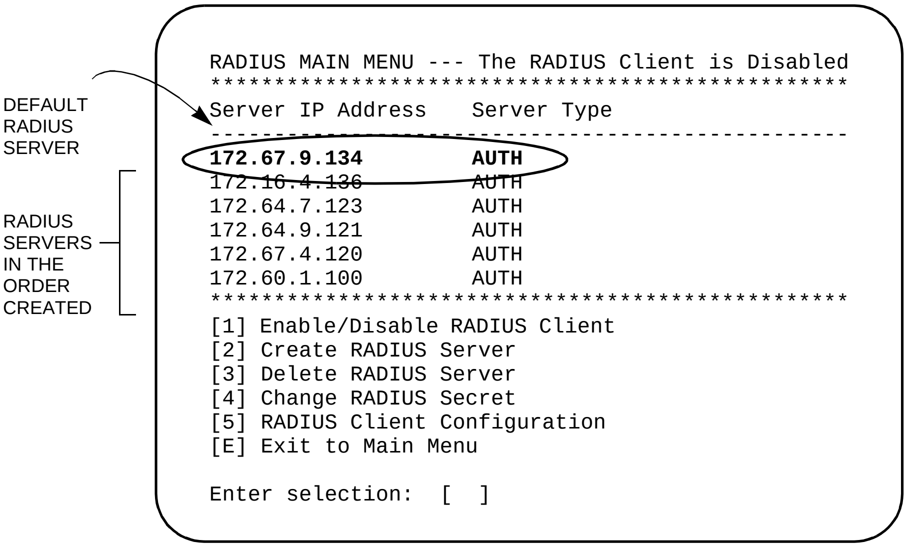
9. With Access Granted, the dial-in caller is allowed access without further RADIUS control or monitoring.

Special Conditions

The section describes RADIUS operation under various network conditions and configurations. Read this section completely in order to configure RADIUS for optimal performance.

Redundant RADIUS Servers

When you create the first RADIUS server, it appears as the first entry on the Main RADIUS Menu. This position in the list causes it to be Default RADIUS server that the SCM will try to communicate with for authenticating dial-in users (*Figure B-1*). When you create additional RADIUS servers, they will also appear in the RADIUS server list and will function as redundant RADIUS servers.



```
RADIUS MAIN MENU --- The RADIUS Client is Disabled
***************************************************
Server IP Address    Server Type
---------------------------------------------------
172.67.9.134         AUTH
172.16.4.136         AUTH
172.64.7.123         AUTH
172.64.9.121         AUTH
172.67.4.120         AUTH
172.60.1.100         AUTH
***************************************************
[1] Enable/Disable RADIUS Client
[2] Create RADIUS Server
[3] Delete RADIUS Server
[4] Change RADIUS Secret
[5] RADIUS Client Configuration
[E] Exit to Main Menu

Enter selection:  [  ]
```

Figure B-1 Default and Redundant RADIUS Servers

Theory of Operation

When the Default server does not respond to the SCM's authentication request, the SCM will pause for a short interval and retry the request to the Default server. The duration of the interval and number of retries are determined by the user at the Client Configuration screen.

If the Default server still does not respond after the last retry, the SCM will then try to communicate with the next RADIUS server in the list. This process repeats until one of the RADIUS servers responds to the SCM. The SCM will continue to communicate to this redundant server for every subsequent authentication, even when the Default RADIUS server returns to service.

Note *In order to reset the SCM to communicate with the Default RADIUS server, you must power-cycle the SCM or perform a soft reset at the Main SCM Menu Master Table screen.*

Note *It is possible for the modem to timeout while the SCM is trying to find a responding RADIUS server for authentication. Modem timeout should be avoided by configuring the RADIUS Client with lower values for Retry Count and Retry Interval, as shown in Figure B-2.*

Configuring Redundant Radius Servers

By creating one or more redundant RADIUS server, the system is prepared for a possible failure in the Default RADIUS server. If this occurs, the SCM will retry the Default server two or more times before trying to authenticate a dial-in caller with the next server on the RADIUS server list.

If two or more servers fail, the SCM may exceed the 60-second timer in the modem before it finds a responding server. This can be avoided by setting lower values for the Retry Count and Retry Interval. In *Figure B-2*, this situation is demonstrated in two cases: Case 1 results in modem timeout and failed RADIUS authentication; Case 2 results in successful RADIUS authentication.

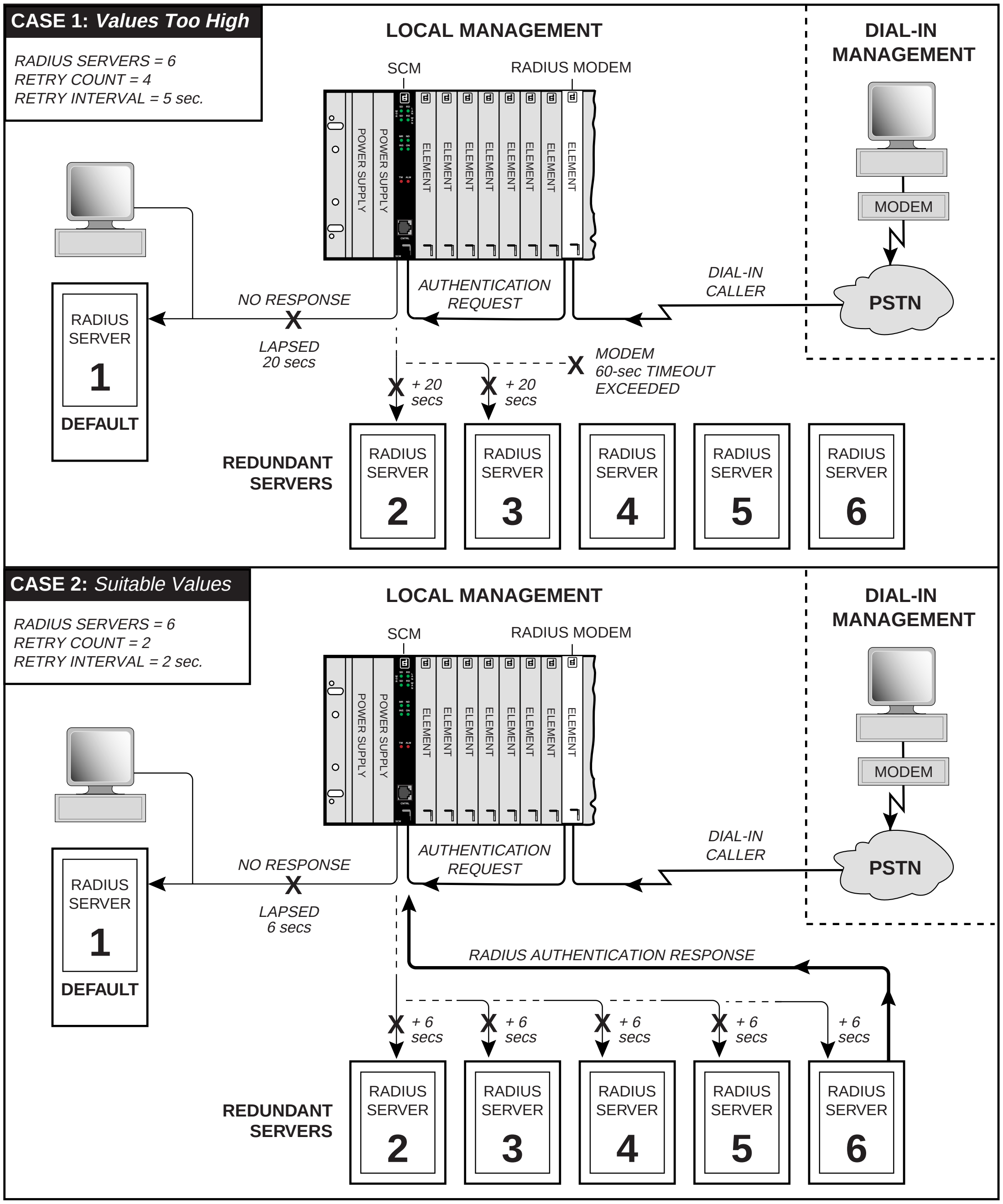


Figure B-2 Optimal Use of Redundant RADIUS Servers

SCM and RADIUS Server Failure

RADIUS authentication can not occur if any of following conditions exist at the local site:

- all RADIUS servers fail to respond to the SCM
- the SCM card fails
- the SCM card is removed from the shelf
- the RADIUS Client is disabled at the RADIUS Main Menu

When any of these situations occur, the modem will not be able to receive a RADIUS authentication response. After 60 seconds without a RADIUS authentication response, the modem will assume a Forced Online Security control of the network. This will stay in affect until the failed/disabled conditions have been corrected.

Forced Online Security provides a limited degree of security to the network when RADIUS authentication is disrupted by the user or by component failure. The user can control the level of security available during such disruptions by opting to store or remove cell passwords in RADIUS modems. This is special sequence of operation is described below.

Note *IMPORTANT! Cell passwords in the modem should only be entered in the RADIUS modems by the supervisor or an authorized network administrator according to network management preferences in the event of SCM failure, or when all RADIUS servers have failed.*

Removing cell passwords from the RADIUS modems ensures the highest level of security by refusing all access to the network until the SCM and/or the RADIUS servers are put back online.

Entering cell passwords in the RADIUS modems allows access to the network if SCM or RADIUS servers fail.

Note *Refer to the RADIUS modem manual for detailed information on Online Security and the use of cell passwords in the modem.*

Forced Online Security Sequence

For clarity, it is assumed that in the sequence below, the caller would be entering correct user name, password, or Challenge response at the first modem prompt and within the first 20-second interval.

1. A caller dials in to a RADIUS modem in the shelf, and the modem begins its prompts for a RADIUS user name, and a RADIUS password.
2. During this period, the SCM fails, is removed from the shelf, or all RADIUS servers fail. This prevents the modem from receiving an authentication response from the server.
3. The modem waits for 60 seconds and then begins a Forced Online Security sequence. In this sequence, the modem will attempt to authorize a caller by using a cell password stored in the modem.
4. The modem prompts the caller for a cell password. The chart below describes the two final paths of a Forced Online Security sequence, based on whether cell passwords were stored in the modem or not.

No Cell Passwords Stored in Modem		**Cell Passwords Stored in Modem**	
4A.	The caller has 60 seconds to type a cell password and press **Enter**. The modem re-prompts the caller at 20-second intervals until a cell password is entered, or when the minute lapses.	4A.	The caller has 60 seconds to type a cell password in all uppercase characters, and press **Enter**. The modem re-prompts the caller at 20-second intervals until a cell password is entered, or when the minute lapses.
4B.	If a cell password has not been entered, the call is disconnected. If the caller enters a cell password and presses **Enter**, the call is disconnected at once.	4B.	If a cell password has not been entered, the call is disconnected. If the caller enters a cell password and presses **Enter**, the modem attempts to match the entry with its stored cell passwords.
		4C.	If the modem finds no match for the entry, or if the cell password was entered with any lowercase characters, the modem denies access to the caller.
		4D.	If the modem finds a match to the entry, the modem grants access to the caller.

5. With Access Granted, the dial-in caller is allowed access without further RADIUS or Online Security control or monitoring.

SCM Maintenance

When the network manager maintains the SCM or any network element via firmware download, RADIUS authentication requests from the modem will queue behind that task. Where possible, such maintenance procedures should be scheduled during low peak hours to avoid delays in RADIUS authentication. Otherwise, the user should be aware of modem functionality during such delays.

If the delay exceeds 60 seconds, the RADIUS modem will take one of the following actions:

- activate Online Security with the cell passwords stored in the modem
- disconnect the call if no cell passwords are available

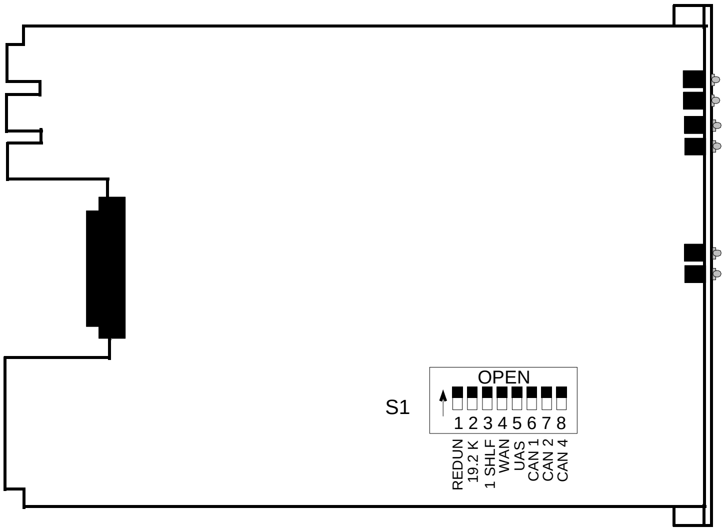
Appendix C: Canned Configurations

Canned Configuration Overview

The SCM has three options (S1-6 through S1-8) which can be set on the card at the **S1** switch. In special UAS shelves only, the user can set these switches in combination in order to configure shelf elements with one of seven canned configurations stored in memory. When all positions are set to OPEN, this function is disabled.

Setting Canned Configuration Switches

Table C-1 locates the switch positions and shows switch combinations for each available setting.

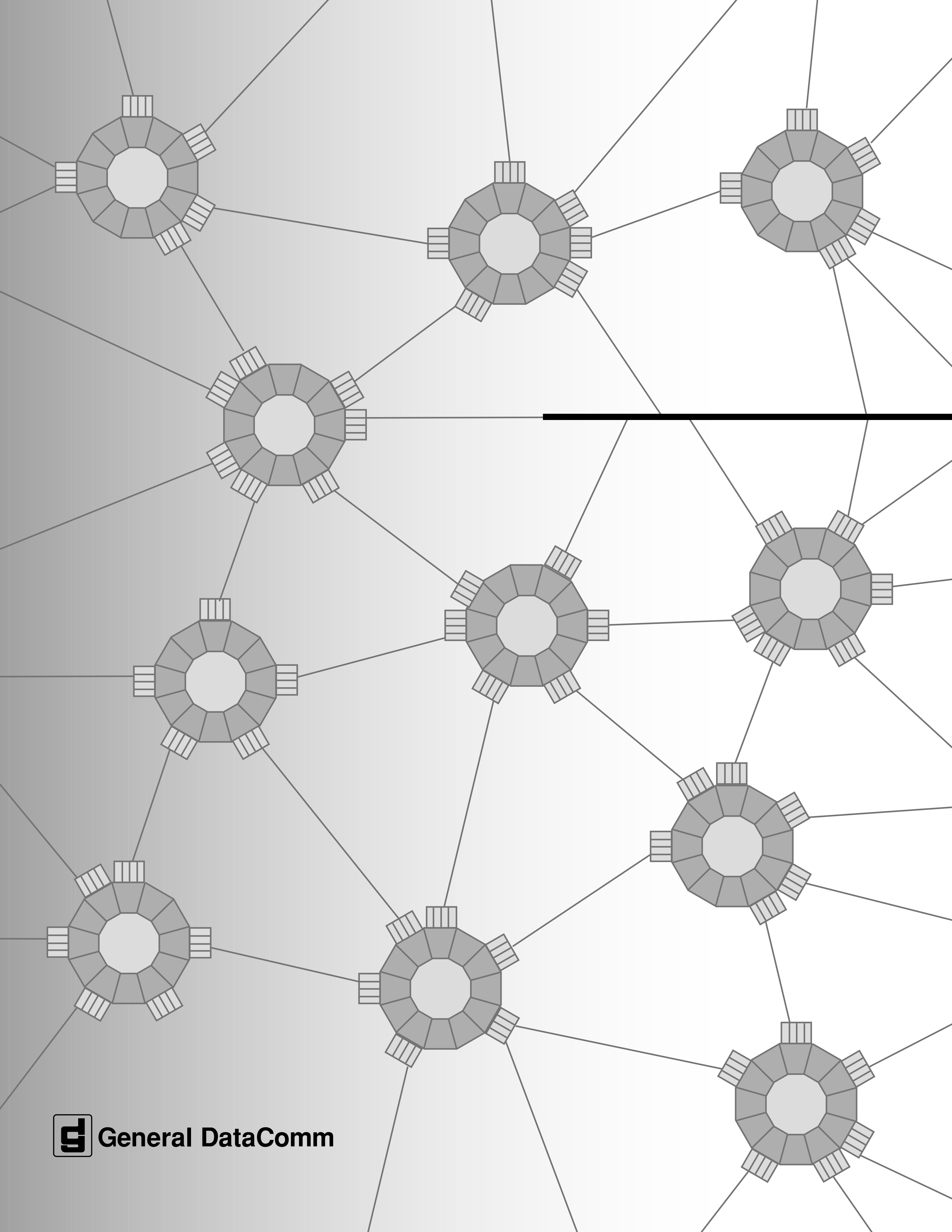


Note:
Switches Shown
in Default Positions

Table C-1 Switch Settings for UAS Canned Configurations

Canned Configuration	S1-6 CAN1	S1-7 CAN2	S-18 CAN4
NONE	Open	Open	Open
1	Closed	Closed	Open
2	Open	Open	Open
3	Closed	Closed	Open
4	Open	Open	Closed
5	Closed	Closed	Closed
6	Open	Open	Closed
7	Closed	Closed	Closed

Note *If you select one of the canned configurations and the SCM is not in slot 16, the ALM LED on the SCM front panel will illuminate continuously.*



General DataComm