

# SCM-16

---

Secure Console Manager

**Firmware Version 4.02  
and Higher**

## **User's Guide**





## **Warnings and Cautions:**



### **INSTALLATION INSTRUCTIONS**

#### **SECURE RACKING**

---

If Secure Racked units are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered.

1. The ambient within the rack may be greater than room ambient. Installation should be such that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 45°C. Consideration should be given to the maximum rated ambient.
2. Installation should be such that a hazardous stability condition is not achieved due to uneven loading.

#### **INPUT SUPPLY**

---

1. Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.
2. When installing 48 VDC rated equipment, it must be installed only per the following conditions:
  - A. Connect the equipment to a 48 VDC supply source that is electrically isolated from the alternating current source. The 48 VDC source is to be connected to a 48 VDC SELV source.
  - B. Input wiring to terminal block must be routed and secured in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.
  - C. A readily accessible disconnect device, with a 3 mm minimum contact gap, shall be incorporated in the fixed wiring.

#### **GROUNDING**

---

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit.

## **No Serviceable Parts Inside; Authorized Service Personnel Only**

---

Do not attempt to repair or service this device yourself. Internal components must be serviced by authorized personnel only.

- **Shock Hazard - Do Not Enter**

## **Disconnect Power**

---

If any of the following events are noted, immediately disconnect the unit from the outlet and contact qualified service personnel:

1. If the power cord becomes frayed or damaged.
2. If liquid has been spilled into the device or if the device has been exposed to rain or water.

# Table of Contents

---

|                                                                       |            |
|-----------------------------------------------------------------------|------------|
| <b>1. Introduction</b>                                                | <b>1-1</b> |
| <b>2. Unit Description</b>                                            | <b>2-1</b> |
| 2.1. Front Panel                                                      | 2-1        |
| 2.2. Back Panel                                                       | 2-2        |
| <b>3. Getting Started</b>                                             | <b>3-1</b> |
| 3.1. Hardware Installation                                            | 3-1        |
| 3.1.1. Apply Power to the SCM-16                                      | 3-1        |
| 3.1.2. Connect your Control Device to the SCM-16                      | 3-1        |
| 3.2. Communicating with the SCM-16                                    | 3-2        |
| <b>4. Hardware Installation</b>                                       | <b>4-1</b> |
| 4.1. Connecting Power to the SCM Unit                                 | 4-1        |
| 4.1.1. AC Powered Units                                               | 4-1        |
| 4.1.2. DC Powered Units                                               | 4-1        |
| 4.2. Connecting the Network Cable                                     | 4-2        |
| 4.3. Connecting Devices to the SCM                                    | 4-2        |
| <b>5. Configuration</b>                                               | <b>5-1</b> |
| 5.1. Communicating with the SCM Unit                                  | 5-1        |
| 5.1.1. The Text Interface                                             | 5-1        |
| 5.1.2. The Web Browser Interface                                      | 5-4        |
| 5.2. System SetUp Port                                                | 5-5        |
| 5.3. Configuration Menus                                              | 5-5        |
| 5.4. Defining System Parameters                                       | 5-7        |
| 5.4.1. The Real Time Clock and Calendar                               | 5-8        |
| 5.4.2. The Invalid Access Lockout Feature                             | 5-10       |
| 5.4.3. The Audit Log                                                  | 5-12       |
| 5.4.4. Callback Security                                              | 5-13       |
| 5.5. User Accounts                                                    | 5-14       |
| 5.5.1. Supervisor Access                                              | 5-15       |
| 5.5.2. Port Access                                                    | 5-15       |
| 5.6. Managing User Accounts                                           | 5-16       |
| 5.6.1. Viewing User Accounts                                          | 5-17       |
| 5.6.2. Adding User Accounts                                           | 5-19       |
| 5.6.3. Modifying User Accounts                                        | 5-20       |
| 5.6.4. Deleting User Accounts                                         | 5-21       |
| 5.7. Port Configuration                                               | 5-22       |
| 5.7.1. Port Modes                                                     | 5-22       |
| 5.7.2. RS232 Port Configuration Menus                                 | 5-24       |
| 5.7.3. Network Port Configuration Menu                                | 5-30       |
| 5.7.4. Implementing IP Security                                       | 5-40       |
| 5.7.4.1. Adding IP Addresses to the Allow and Deny Lists              | 5-42       |
| 5.7.4.2. Linux Operators and Wild Cards                               | 5-43       |
| 5.7.4.3. IP Security Examples                                         | 5-44       |
| 5.8. Copying Parameters to Several RS-232 Ports (Text Interface Only) | 5-45       |
| 5.9. Save User Selected Parameters                                    | 5-47       |

**6. The Status Screens ..... 6-1**

6.1. The Port Status Screen (/S) ..... 6-1

6.2. The Port Diagnostics Screen (/SD) ..... 6-2

6.3. The Network Status Screen (/SN)..... 6-4

6.4. The Port Parameters Screens (/W) ..... 6-6

**7. Operation ..... 7-1**

7.1. Any-to-Any Mode ..... 7-1

7.1.1. Port Connection and Disconnection..... 7-1

7.1.1.1. Connecting Ports ..... 7-1

7.1.1.2. Disconnecting Ports ..... 7-3

7.1.2. Defining Hunt Groups ..... 7-5

7.2. Passive Mode ..... 7-6

7.3. Buffer Mode ..... 7-7

7.3.1. Reading Data from Buffer Mode Ports ..... 7-7

7.3.2. Port Buffers ..... 7-8

7.4. Modem Mode..... 7-9

**8. Telnet & SSH Functions..... 8-1**

8.1. Network Port Numbers ..... 8-1

8.2. SSH Encryption ..... 8-1

8.3. The Direct Connect Feature ..... 8-2

8.3.1. Standard Telnet Protocol and SSH..... 8-2

8.3.2. Configuration ..... 8-2

8.3.3. Connecting to an RS232 Port using Direct Connect ..... 8-3

8.3.4. Terminating a Direct Connect Session..... 8-4

**9. The Syslog Feature ..... 9-1**

9.1. Configuration ..... 9-1

9.2. Criteria for Generating a Syslog Message ..... 9-3

9.3. Testing Syslog Configuration..... 9-4

**10. SNMP Traps ..... 10-1**

10.1. Configuration: ..... 10-1

10.2. SNMP Trap Message ..... 10-2

10.3. How and When SNMP Traps are Sent: ..... 10-2

10.4. Testing the SNMP Trap Function..... 10-3

**11. Saving and Restoring Configuration Parameters ..... 11-1**

11.1. Sending Parameters to a File ..... 11-1

11.2. Restoring Saved Parameters..... 11-2

**12. Upgrading SCM Firmware ..... 12-1**

**13. Command Reference Guide..... 13-1**

13.1. Command Conventions ..... 13-1

13.2. Command Summary ..... 13-2

13.3. Command Set..... 13-3

**Appendices:**

**A. RS232 Port Interface ..... Apx-1**

**B. Specifications..... Apx-2**

**C. Customer Service ..... Apx-3**

**Index.....Index-1**

## List of Figures

|       |                                                       |       |
|-------|-------------------------------------------------------|-------|
| 2.1.  | Instrument Front Panel                                | 2-1   |
| 2.2.  | Instrument Back Panel (Model SCM-16)                  | 2-2   |
| 3.1.  | The Port Status Screen (Text Interface)               | 3-4   |
| 3.2.  | The Port Status Screen (Web Browser Interface)        | 3-4   |
| 4.1.  | Terminal Block Assembly (DC Units Only)               | 4-1   |
| 5.1.  | The Port Status Screen (Text Interface)               | 5-3   |
| 5.2.  | The SCM Main Menu (Web Browser Interface)             | 5-4   |
| 5.3.  | The System Parameters Menu (Text Interface)           | 5-6   |
| 5.4.  | The System Configuration Menu (Web Browser Interface) | 5-6   |
| 5.5.  | The Real Time Clock Menu (Text Interface)             | 5-9   |
| 5.6.  | The Real Time Clock Menu (Web Browser Interface)      | 5-9   |
| 5.7.  | The Create User Menu (Text Interface)                 | 5-18  |
| 5.8.  | The Create User Menu (Web Browser Interface)          | 5-18  |
| 5.9.  | Port Configuration Menu (Text Interface)              | 5-23  |
| 5.10. | Port Configuration Menu (Web Browser Interface)       | 5-23  |
| 5.11. | Network Parameters Menu (Supervisor Mode Only)        | 5-31  |
| 5.12. | Network Configuration Menu (Web Browser Interface)    | 5-31  |
| 5.13. | Network Parameters Menu (Web Browser Interface)       | 5-32  |
| 5.14. | Network Port Parameters Menu (Web Browser Interface)  | 5-34  |
| 5.15. | SNMP Parameters Menu (Web Browser Interface)          | 5-37  |
| 5.16. | IP Security Menu (Text Interface)                     | 5-41  |
| 5.17. | IP Security Menu (Web Browser Interface)              | 5-41  |
| 5.18. | The Copy Port Parameters Menu                         | 5-45  |
| 6.1.  | Port Status Screen (Sample Data Shown)                | 6-1   |
| 6.2.  | Port Diagnostics Screen                               | 6-3   |
| 6.3.  | Network Status Screen                                 | 6-4   |
| 6.4.  | Port Parameters Screen (RS232 Port Shown)             | 6-6   |
| 6.5.  | Port Parameters Screen (Network Port Shown)           | 6-6   |
| A.1.  | RS232 Port Interface                                  | Apx-1 |





# 1. Introduction

---

The SCM-16 Secure Console/AUX Management Switch provides in-band and out-of-band access to RS-232 console ports and maintenance ports on UNIX servers, routers and any other network elements which have a serial console port. System administrators can access the SCM-16 via TCP/IP network, using SSH or Telnet, or out-of-band via modem or local terminal.

The SCM features two separate command interfaces; a convenient, user-friendly web browser interface, and a simple, command driven text interface.

## **Intelligent Port Selection**

Each of the SCM's sixteen serial ports can be individually accessed by number, name or group via SSH or Telnet sessions. The SCM-16 also allows direct connections using TCP port assignments. Each SCM serial port can be separately configured using simple menu driven commands to set the port password, data rate, flow control and other operating parameters.

The full matrix capability of the SCM-16 allows you to easily connect any two ports on the switch, even when the ports are using different communications settings. Ports can also be connected or disconnected by a third party with supervisor rights, and system managers can swap various RS232 devices between ports at a remote location.

## **Security and Colocation Features**

Secure Shell (SSHv2) encryption and address-specific IP security masks prevent unauthorized access to command and configuration functions. The SCM-16 also provides two different levels of user security; the Supervisor level and the Non-Supervisor level. The Supervisor level, which is intended for use by system managers and other administrators, provides complete access to all SCM port connection / disconnection functions, operating features and configuration menus, and also allows access to any port on the switch. The Non-Supervisor level is ideal for colocation applications, since users are only permitted to view status and connect to the ports allowed by their password.

## Capture Buffer

The "Buffer Mode" allows individual ports to capture and store incoming data, such as error and status messages received from attached console ports. This "snapshot" of the last 32K of data received is stored in memory, and can be viewed, saved, or erased by the system operator at any time.

Console messages, which are stored in the SCM port buffers, can be sent to a remote location via SYSLOG, or an SNMP message can be generated to alert administrators when new console messages are received. This is particularly useful in the event that an "alarm error" or other critical data is sent from a specific console port during non-connect periods.

## Configuration Backup

Once you have configured the SCM to fit your application, parameters and options can be saved to an ASCII text file on your PC. This allows you to quickly restore user-selected parameters if unit configuration is accidentally altered or deleted. Saved parameters can also be uploaded to other SCM units. This allows rapid set-up when several units will be configured with identical or similar parameters.

## Typographic Conventions

---

|                            |                                                                                                                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>^</b> (e.g. <b>^X</b> ) | Indicates a control character. For example, the text " <b>^X</b> " (Control X) indicates the <b>[Ctrl]</b> key and the <b>[X]</b> key must be pressed simultaneously. |
| <b>COURIER FONT</b>        | Indicates characters typed on the keyboard.<br>For example, <b>/E</b> or <b>/P 02</b> .                                                                               |
| <b>[Bold Font]</b>         | Text set in bold face and enclosed in square brackets, indicates a specific key.<br>For example, <b>[Enter]</b> or <b>[Esc]</b> .                                     |
| <b>&lt; &gt;</b>           | Indicates required keyboard entries:<br>For Example: <b>/P &lt;n&gt;</b> .                                                                                            |
| <b>[ ]</b>                 | Indicates optional keyboard entries.<br>For Example: <b>/W [n]</b> .                                                                                                  |

## 2. Unit Description

### 2.1. Front Panel

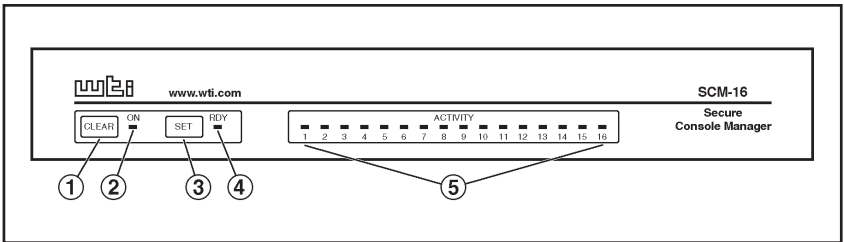


Figure 2.1: Instrument Front Panel

- ① **CLEAR:** Restarts the SCM without changing user-selected parameter settings.  
**Note:** When Clear is pressed, all ports will be disconnected.
- ② **ON:** Lights when AC Power is applied.
- ③ **SET:** Used to Initialize the SCM to default parameters. To initialize the SCM, press and hold the SET button for approximately five seconds.

#### Notes:

- During initialization, all port LEDs will flash ON three times.
  - After initialization, all command-selected parameters will be cleared, and the SCM will revert to the default parameters. The default "super" user account will also be restored.
- ④ **RDY:** (Ready) Flashes to indicate unit is operational.
  - ⑤ **ACTIVITY LEDs:** A series of sixteen LEDs, which light to indicate data activity at the corresponding port.

## 2.2. Back Panel

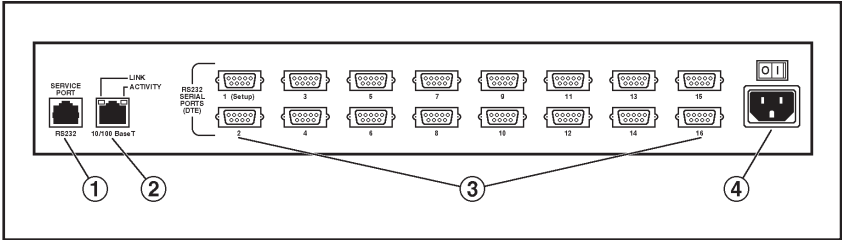


Figure 2.2: Instrument Back Panel (Model SCM-16)

- ① **Service Port:** For factory use only.
- ② **Network Port:** An RJ45 Ethernet port for connection to your 10Base-T, TCP/IP network. Note that the SCM features a default IP address (192.168.168.168). This allows you to connect to the unit without first assigning an IP address. Note that the Network Port also includes two, small LED indicators for Link and Data Activity. For more information on Network Port configuration, please refer to Section 5.7.3.  
**Note:** When connecting the SCM to a 100BaseT interface, most router switches will autosense to determine if the device is 100BaseT or 10BaseT, and then configure the interface accordingly. If your router switch does not autosense, your network interface port must be manually set to 10BaseT.
- ③ **RS232 Serial Ports:** For connection to console ports on target devices. Standard DB9 connectors configured as DTE ports. The RS232 ports are similar to a serial port on a PC. When connecting a modem, use a standard serial cable. When connecting a PC or other DTE device use a null modem cable.
- ④ **Power Components:** The Power Switch and Power Cable Receptacle (AC Units) or Terminal Block Assembly (DC Units.) For more information, please refer to Section 4.1.

## 3. Getting Started

---

This section provides a brief demonstration of basic SCM capabilities, and describes a simple "walk-through" that can be performed to determine if the unit is operating properly. In order to take full advantage of the features provided by this unit, it is recommended that you should complete the entire Installation and Configuration sections after performing this Quick Start procedure.

### 3.1. Hardware Installation

---

#### 3.1.1. Apply Power to the SCM-16

Refer to the safety precautions listed at the beginning of this User's Guide, and then connect the unit to an appropriate power source. Note that the AC version of the SCM-16 is designed for 100 to 240 VAC, 50/60 Hz operation and features an auto sensing power supply, and that the DC model (the SCM-16DC) is designed for -48 VDC operation.

When power is applied to the SCM-16, the ON LED should light, and the RDY LED should begin to flash. Note however, that the boot up procedure may take up to two minutes; this delay is due to the time required to generate SSH keys.

#### 3.1.2. Connect your Control Device to the SCM-16

The SCM-16 can either be controlled via local PC Serial Port, external modem, or TCP/IP network. In order to connect ports or select parameters, commands are issued to the SCM-16 via either the Network Port or RS232 Setup Port. Note that it is not necessary to connect to both the Network and Setup Ports, and that the Setup Port can be connected to either a local PC or an external modem.

- **Network Port:** Connect your 10Base-T or 100Base-T network interface to the SCM-16 10/100Base-T Network port.
- **Console Port:** Use the supplied null modem cable to connect your PC COM port to the SCM-16 Set-Up Port (RS232).
- **External Modem:** Use a standard AT Style modem cable to connect your external modem to a vacant SCM-16 RS232 Port. Note that although if necessary, a modem can be installed at RS232 Port 1, it is recommended to keep this port free to allow access by a local user.

## 3.2. Communicating with the SCM-16

---

Once your Network Cable, Local PC COM port and/or external modem have been connected to the SCM-16, you can then use an SSH Client, communications program or web browser to access command mode and communicate with the unit. When properly configured, the SCM-16 will allow command mode access via Telnet, Web Browser, SSH client, modem, or local PC. However, in order to ensure security, both Telnet and Web Browser access are disabled in the default state. To enable Telnet and/or Web Browser access, please refer to Section 5.

### Notes:

- Default SCM-16 communications parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this Quick Start procedure, it is recommended to configure your communications program to accept the default parameters.
- The SCM-16 features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network access to command mode, providing that you are contacting the SCM-16 from a node on the same subnet. When attempting to access the SCM-16 from a node that is *not* on the same subnet, please refer to the User's Guide for further configuration instructions.

#### 1. Access Command Mode:

- Via Local PC:** Start your communications program (e.g., Hyperterminal) and then press **[Enter]**. Wait for the connect message, and then proceed to Step 2.
- Via SSH Client:** Start your SSH client, then enter the default IP address (192.168.168.168) for the SCM-16 and invoke the connect command.
- Via Web Browser:** Make certain that Web Browser access has been enabled as described in Section 5.7. Start your JavaScript enabled web browser, enter the default SCM-16 IP address (192.169.168.168) in the Web Browser address bar, and then press **[Enter]**.
- Via Telnet:** Make certain that Telnet access has been enabled as described in Section 5.7. Start your Telnet client, and enter the SCM's default IP address (192.168.168.168).

- e) **Via Modem:** Make certain that your external modem is connected to an SCM-16 port which is configured for Modem Mode, and then use your communications program to dial the number for the phone line connected to your external modem.
- 2. **Username / Password Prompt:** A message will be displayed, which prompts you to enter your username and password.. The default username is “**super**” (all lower case, no quotes), and the default password is also “**super**”. If a valid username and password are entered, the SCM-16 will display either the Main Menu (Web Browser Interface) or the Port Status Screen (SSH, Telnet, or Modem) as shown in Figures 3.1 and 3.2.
- 3. **Review Help Menu:** If you are communicating with the SCM-16 via the text interface, type **/H** and press **[Enter]** to display the Help Menu, which lists all available SCM-16 commands.
- 4. **Creating Connections Between Ports:** The SCM-16 can perform two types of connections; Resident Connections and Third Party Connections.

**Note:** Ports are connected and disconnected using commands that are issued via the Text Interface.

- a) **Resident Connection:** Your resident port (e.g. Port 1) issues a **/C** command to connect to a second port.
  - i. To connect Port 1 to Port 2, type **/C 2 [Enter]**. While Port 1 is connected, the SCM-16 will not recognize commands issued at Port 1. However, the unit will recognize a Resident Disconnect Sequence issued at Port 1 or Port 2.
  - ii. Issue the Resident Disconnect Sequence (Logoff Sequence); type **^X** (press **[Ctrl]** and **[X]** at the same time).
- b) **Third Party Connection:** Your resident port (e.g. Port 1) issues a **/C** command to create a connection between two other ports.
  - i. To connect Port 2 to Port 3, type **/C 2 3 [Enter]**.
  - ii. While Ports 2 and 3 are connected, Port 1 will still recognize SCM-16 commands. Type **/S [Enter]** to display the Port Status Screen. The "STATUS" column should now list Ports 2 and 3 as connected, and Port 1 as "Free".

PORT STATUS:  
Site ID: (undefined)

02/12/2007 06:42:41 GMT (GMT+0000)

| PORT | NAME        | USERNAME | STATUS | MODE | BUFFER COUNT |
|------|-------------|----------|--------|------|--------------|
| 01   | (undefined) |          | Free   | Any  | 0            |
| 02   | (undefined) |          | Free   | Any  | 0            |
| 03   | (undefined) |          | Free   | Pass | 0            |
| 04   | (undefined) |          | Free   | Pass | 0            |
| 05   | (undefined) |          | Free   | Pass | 0            |
| 06   | (undefined) |          | Free   | Pass | 0            |
| 07   | (undefined) |          | Free   | Pass | 0            |
| 08   | (undefined) |          | Free   | Pass | 0            |
| 09   | (undefined) |          | Free   | Pass | 0            |
| 10   | (undefined) |          | Free   | Pass | 0            |
| 11   | (undefined) |          | Free   | Pass | 0            |
| 12   | (undefined) |          | Free   | Pass | 0            |
| 13   | (undefined) |          | Free   | Pass | 0            |
| 14   | (undefined) |          | Free   | Pass | 0            |
| 15   | (undefined) |          | Free   | Pass | 0            |
| 16   | (undefined) |          | Free   | Pass | 0            |

Enter /H for command menu.  
SCM>

Figure 3.1: The Port Status Screen (Text Interface)



Figure 3.2: The Port Status Screen (Web Browser Interface)



- iii. Issue a Third Party Disconnect command to disconnect Ports 2 and 3; type **/D 2 [Enter]**. The unit will display the "Are you Sure (y/n)?" prompt. Type **y** and press **[Enter]** to disconnect.
  - iv. Type **/S [Enter]** to display the Port Status Screen. The "STATUS" column should now list Ports 2 and 3 as "Free".
5. **Exit Command Mode:** When you have finished communicating with the unit, it is important to always log off using the appropriate SCM-16 command, rather than simply closing your Telnet or communications program. When you log off properly, this ensures that the unit has completely exited from command mode, and is not waiting for the inactivity timeout to elapse before allowing additional connections. To exit command mode, type **/x** and press **[Enter]**.

This completes the Quick Start Guide for the SCM-16. Prior to placing the unit into operation, it is recommended to refer to the remainder of this User's Guide for important information regarding advanced configuration capabilities and more detailed operation instructions. If you have further questions regarding the SCM-16 unit, please contact WTI Customer Support as described in Appendix C.



## 4. Hardware Installation

### 4.1. Connecting Power to the SCM Unit

The SCM is available in both AC and DC powered versions. When connecting AC or DC power to the SCM, proceed as follows:



- Before attempting to install this unit, please review the warnings and cautions listed at the front of the user's guide.
- This device should only be operated with the type of power source indicated on the instrument nameplate. If you are not sure of the type of power service available, please contact your local power company.
- Reliable earthing (grounding) of this unit must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than directly to the branch circuit.

#### 4.1.1. AC Powered Units

Plug the power cable (supplied with the unit) into the receptacle on the SCM back panel. Then, connect the power cable to an appropriate, grounded outlet. The SCM features a self adjusting power supply that automatically adapts to power supplies between 90 and 250 VAC. Press the Power Switch ON. The ON LED should light and the RDY LED should begin to flash.

#### 4.1.2. DC Powered Units

When connecting the SCM to your DC Power source, first remove the protective cover from the terminal block, attach the wires from the -48 VDC power source to the screw terminals, connect the ground line to the labeled ground screw, and then replace the protective cover.

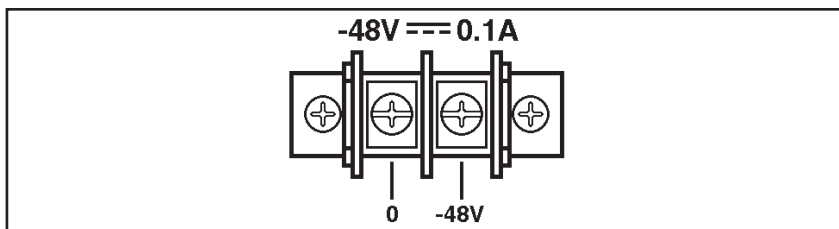


Figure 4.1: Terminal Block Assembly (DC Units Only)

## 4.2. Connecting the Network Cable

---

The Network Port is an RJ45, 10BaseT Ethernet Jack, for connection to a TCP/IP network. Note that the SCM features a default IP Address (192.168.168.168.) Providing that you are communicating with the unit from a node on the same subnet, this allows you to contact the SCM without first accessing command mode to assign an IP address.

When installing the SCM in a working network environment, it is recommended to assign the IP Address, Gateway Address, and Subnet Mask as described in Section 5.7.3.

**Note:** When connecting the SCM to a 100BaseT interface, most router switches will autosense to determine if the device is 100BaseT or 10BaseT, and configure the network interface accordingly. If your router does not autosense, your interface port must be manually set to 10BaseT.

## 4.3. Connecting Devices to the SCM

---

1. Determine which SCM port will be used for connection to the new device (e.g. Port 3).
2. Use an appropriate DB9 cable to connect the RS232 serial port on the device to a DB9 port on the SCM.
  - a) **External Modems and other DCE Devices:** Use a standard serial modem cable.
  - b) **PCs and other DTE Devices:** Use a null modem cable.
3. Access the SCM command mode and select communication parameters for each SCM port as described in Section 5.7.2.

## 5. Configuration

---

### 5.1. Communicating with the SCM Unit

---

In order to configure the SCM, you must first connect to the unit, and access command mode. Note that, the SCM offers two separate configuration interfaces; the Web Browser Interface and the Text Interface.

In addition, the SCM also offers three different methods for accessing command mode; via network, via external modem, or via local console. The Web Browser interface is only available via network, and the Text Interface is available via network (SSH or Telnet), modem or local PC.

#### 5.1.1. The Text Interface

The Text Interface consists of a series of simple ASCII text menus, which allow you to set options and define parameters by entering the number for the desired option using your keyboard, and then typing in the value for that option.

Since the Web Browser Interface and Telnet accessibility are both disabled in the default state, you will need to use the Text Interface to contact the unit via Local PC or SSH connection when setting up the unit for the first time. After you have accessed command mode using the Text Interface, you can then enable Web Access and Telnet access in order to allow future communication with the unit via Web Browser or Telnet. Keep in mind therefore, that you will not be able to contact the unit via web browser or Telnet until you have specifically enabled those options.

Once Telnet Access is enabled, you will then be able to use the Text Interface to communicate with the SCM via local PC, Telnet or SSH connection. If an external modem is installed on one of the SCM's RS232 ports and that port is properly configured, you will also be able to use the Text Interface to contact the unit via modem.

In order to use the Text Interface, your installation must include:

- **Access via Network:** The SCM must be connected to your TCP/IP Network, and your PC must include a communications program (such as HyperTerminal.)
- **Access via Modem:** An external modem must be connected to one of the SCM's RS232 ports, a phone line must be connected to the external modem, and your PC must include a communications program.
- **Access via Local PC:** Your PC must be physically connected to one of the SCM's RS232 ports as described in Section 4.3, and the PC must include a communications program.

To access command mode via the Text Interface, proceed as follows:

**Note:** Command mode *cannot* be accessed via a Buffer Mode Port, Passive Mode Port, or any port that is presently connected to another SCM port.

1. Contact the SCM Unit:

- a) **Via Local PC:** Start your communications program and press [Enter]. Wait for the connect message, then proceed to Step 2.
- b) **Via Network:** The SCM includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit. For more information, please refer to Section 5.7.3.
  - i. **Via SSH Client:** Start your SSH client, and enter the SCM's IP Address. Invoke the connect command, wait for the connect message, then proceed to Step 2.
  - ii. **Via Telnet:** Start your Telnet Client, and then Telnet to the SCM's IP Address. Wait for the connect message, then proceed to Step 2.

**Note:** When communicating with the unit for the first time, you will not be able to contact the unit via Telnet, until you have accessed command mode, via Local PC or SSH Client, and used the Network Parameters Menu (/N) to enable Telnet as described in Section 5.7.3.

| PORT STATUS:               |             |          |                                    |      |              |
|----------------------------|-------------|----------|------------------------------------|------|--------------|
| Site ID: (undefined)       |             |          | 02/12/2007 06:42:41 GMT (GMT+0000) |      |              |
| PORT                       | NAME        | USERNAME | STATUS                             | MODE | BUFFER COUNT |
| 01                         | (undefined) |          | Free                               | Any  | 0            |
| 02                         | (undefined) |          | Free                               | Any  | 0            |
| 03                         | (undefined) |          | Free                               | Pass | 0            |
| 04                         | (undefined) |          | Free                               | Pass | 0            |
| 05                         | (undefined) |          | Free                               | Pass | 0            |
| 06                         | (undefined) |          | Free                               | Pass | 0            |
| 07                         | (undefined) |          | Free                               | Pass | 0            |
| 08                         | (undefined) |          | Free                               | Pass | 0            |
| 09                         | (undefined) |          | Free                               | Pass | 0            |
| 10                         | (undefined) |          | Free                               | Pass | 0            |
| 11                         | (undefined) |          | Free                               | Pass | 0            |
| 12                         | (undefined) |          | Free                               | Pass | 0            |
| 13                         | (undefined) |          | Free                               | Pass | 0            |
| 14                         | (undefined) |          | Free                               | Pass | 0            |
| 15                         | (undefined) |          | Free                               | Pass | 0            |
| 16                         | (undefined) |          | Free                               | Pass | 0            |
| Enter /H for command menu. |             |          |                                    |      |              |
| SCM>                       |             |          |                                    |      |              |

Figure 5.1: The Port Status Screen (Text Interface)

2. **Username / Password Prompt:** A message will be displayed, which prompts you to enter a username and password. The default username is "**super**" (all lower case, no quotes), and the default password is also "**super**".
3. If a valid username and password are entered, the SCM will display the Port Status Screen, shown in Figure 5.1.

**Note:** If the Telnet connection is refused, it is most likely due to one of the following reasons:

- The IP Security feature has denied the connection.
- You are attempting to use an account that permits Supervisor commands to connect to a port that does not permit Supervisor Commands.
- The unit is operating on a 100Base-T network that does not autosense for 10Base-T devices (see Section 4.2).

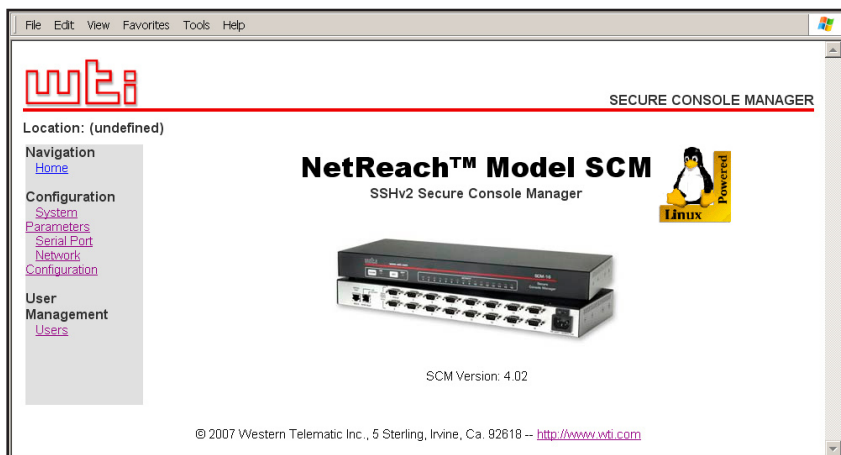


Figure 5.2: The SCM Main Menu (Web Browser Interface)

### 5.1.2. The Web Browser Interface

The Web Browser Interface consists of a series of web forms, which can be used to select configuration parameters and enable/disable SCM operating functions, by clicking on radio buttons and/or entering text into designated fields.

#### Notes:

- The Web Browser Interface cannot be used to connect and disconnect ports; the Web Browser Interface is used only for configuration purposes.
  - In order to use the Web Browser Interface, Web Access must be enabled via the Text Interface Network Parameters Menu (/N), the SCM must be connected to a TCP/IP network, and your PC must be equipped with a JavaScript enabled web browser.
1. Start your JavaScript enabled Web Browser.
  2. Key the SCM's IP address (default = 192.168.168.168) into the web browser's address bar, and press **[Enter]**.
  3. **Username / Password Prompt:** A message box will be displayed which prompts you to enter your username and password. The default username is "**super**" (all lower case, no quotes), and the default password is also "**super**".
  4. If a valid username and password are entered, the SCM Main Menu will appear as shown in Figure 5.2.



---

## 5.2. System SetUp Port

---

Port 1 is reserved as a SetUp Port, and will always permit password protected access to Supervisor commands. Therefore, Port 1 *cannot* be configured as a Buffer Mode Port or Passive Mode Port, because these port modes do not permit access to command mode. In addition, the Supervisor Mode *cannot* be disabled at Port 1.

---

## 5.3. Configuration Menus

---

Although the Web Browser Interface and Text Interface provide two separate means for selecting parameters, both interfaces allow access to the same set of basic parameters, and parameters selected via one interface will also be applied to the other. To access configuration menus, proceed as follows:

- **Text Interface:** Refer to the Help Screen (/H) and then enter the appropriate command to access the desired menu. When the configuration menu appears, key in the number for the parameter you wish to define, and follow the instructions in the resulting submenu.
- **Web Browser Interface:** Click the appropriate button on the left hand side of the Main Menu (Figure 5.2) to access the desired configuration menu. To change parameters, click in the desired field and key in the new value or select a value from the pull-down menu. To apply newly selected parameters, click on the “Change Parameters” button at the bottom of the menu.

The following sections describe options and parameters that can be accessed via each of the configuration menus. Please note that essentially the same set of parameters and options are available to both the Web Browser Interface and Text Interface.

**Note:** Configuration menus are only available when you have logged into command mode using an account and port that permit Supervisor Level commands.

SYSTEM PARAMETERS:

1. User Directory

2. Site-ID:

3. Real Time Clock:

4. Invalid Access Lockout:

5. Audit Log:

6. Callback Security:

7. "/PW" Command:

02/12/2007 06:47:16

On

On - Without Syslog

On - Callback (Without Password Prompt)

Off

Enter: #<CR> to change,

<ESC> exit ...

Figure 5.3: The System Parameters Menu (Text Interface)

File Edit View Favorites Tools Help

wti

REMOTE SITE MANAGER

Location: (undefined)

Navigation

Home

Configuration

System

Parameters

Serial Port

Network

Configuration

User Management

Users

System Configuration

Site-ID: (undefined) Set Site-ID

Audit Log: On - Without Syslog Set Audit Log

"/PW" Command: On Set User PW

Real Time Clock

Configure Invalid Access Lockout

Configure Callback Security

© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>

Figure 5.4: The System Configuration Menu (Web Browser Interface)

---

## 5.4. Defining System Parameters

---

The System Parameters menus are used to define the Site ID Message, set the system clock and calendar, and configure the Invalid Access Lockout feature and Callback feature.

In the Text Interface, the System Parameters menu is also used to create and manage user accounts and passwords. Note however, that when you are communicating with the unit via the Web Browser Interface, accounts and passwords are managed and created via a separate menu that is accessed by clicking on the "Users" link on the left hand side of the menu.

- **Text Interface:** Type **/F** and press **[Enter]**. The System Parameters Menu will appear as shown in Figure 5.3.
- **Web Browser Interface:** Click the "System Properties" link on the left hand side of the SCM Home Screen. The System Parameters menu will be displayed as shown in Figure 5.4.

The System Parameters Menus are used to define the following:

- **User Directory:** This function is used to create, modify and delete user accounts and passwords. As discussed in Section 5.5, user accounts allow you to set the security level for each password as well as determine which ports a user will be allowed to access.

**Note:** The "User Directory" option does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the "Users" link on the left hand side of the configuration menu.

- **Site ID:** A text field, generally used to note the installation site or name for the SCM unit. (Up to 32 chars.; Default = undefined.)

### Notes:

- The Site ID cannot include double quotes.
- The Site ID will be cleared if the SCM is reset to default settings.
- **Real Time Clock:** This prompt provides access to the Real Time Clock menu, which is used to set the clock and calendar, and to enable and configure the NTP (Network Time Protocol) feature as described in Section 5.4.1.
- **Invalid Access Lockout:** If desired, this feature can be used to automatically disable an SCM serial port after a user specified number of unsuccessful login attempts are made. For more information, please refer to Section 5.4.2.

- **Audit Log:** Enables and configures the Audit Log feature, as described in Section 5.4.3. (Default = On - Without Syslog.)
- **Callback Security:** Enables and configures the Callback Security Function as described in Section 5.4.4. In order for this feature to function, a Callback number must also be defined for each desired user account as described in Section 5.6.
- **"/PW" Command:** Enables/Disables the /PW (Change Password) command. When enabled, the /PW command can be issued at the text interface by any user account in order to change that account's password. When disabled, accounts that do not permit Supervisor commands will not be able to change passwords. (Default = Off.)

### 5.4.1. The Real Time Clock and Calendar

The Real Time Clock menu is used to set the SCM's internal clock and calendar. To access the Real Time Clock Menu, proceed as follows:

- **Text Interface:** Type **/F** and press **[Enter]**. The System Parameters menu will appear as shown in Figure 5.3. At the System Parameters menu, type **3** and press **[Enter]** to display the Real Time Clock menu.
- **Web Browser Interface:** Click on the "System Properties" link at the left hand side of the SCM Home Screen to display the System Parameters menu as shown in Figure 5.4. From the System Parameters Menu, click on the "Real Time Clock" link to access the Real Time Clock menu.

The configuration menu for the Real Time Clock offers the following options:

- **Date:** Sets the Month, Date, Year and day of the week for the SCM's real-time clock/calendar.
- **Time:** Sets the Hour, Minute and Second for the SCM's real time clock/calendar. Key in the time using the 24-hour (military) format.

```

REAL-TIME-CLOCK:

1. Date:                      02/12/2007 (Mon)
2. Time:                      06:51:05
3. Time Zone:                 (GMT+0000) GMT (No DST)
4. NTP Enable:                Off
5. Primary NTP IP Address:    (undefined)
6. Secondary NTP IP Address:  (undefined)
7. NTP Timeout:              3 Sec

Enter: #<CR> to change,
      <ESC> for previous menu ...

```

Figure 5.5: The Real Time Clock Menu (Text Interface)

File Edit View Favorites Tools Help

REMOTE SITE MANAGER

Location: (undefined)

Navigation

- Home

Configuration

- System
- Parameters
- Serial Port
- Network
- Configuration

User Management

- Users

Real Time Clock

Date: 02 / 13 / 2007

Time: 00 : 27 : 31

Time Zone: GMT (No DST)

NTP Enable: Off

Primary NTP Address: 0.0.0.0

Secondary NTP Address: 0.0.0.0

NTP Timeout: 03

Change NTP Parameters

© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>

Figure 5.6: The Real Time Clock Menu (Web Browser Interface)

- **Time Zone:** Sets the time zone, relative to Greenwich Mean Time. Note that the Time Zone setting will function differently, depending on whether or not the NTP feature is enabled and properly configured: (Default = GMT (No DST).)
- ◆ **NTP Enabled:** The Time Zone setting is used to adjust the Greenwich Mean Time value (received from the NTP server) to determine the precise local time for the selected time zone.
- ◆ **NTP Disabled:** If NTP is disabled, or if the SCM is not able to access the NTP server, then status screens and activity logs will list the selected Time Zone and current Real Time Clock value, but will not apply the correction factor to the displayed Real Time Clock value.

- **NTP Enable:** When enabled, the SCM will contact an NTP server (defined via the NTP IP Address prompts) once a day, and update its clock based on the NTP server time and selected Time Zone. (Default = Off.)

### Notes:

- The SCM will also contact the NTP server and update the time whenever you change NTP parameters.
- To command the SCM to immediately contact the NTP server at any time, make certain that the NTP feature is enabled and configured, then type **/F** and press **[Enter]**. When the System Parameters menu appears, press **[Esc]**. The SCM will save parameters and then attempt to contact the server, as specified by currently defined NTP parameters.
- **Primary NTP IP Address:** Defines the IP address for the primary NTP server. (Default = undefined.)
- **Secondary NTP IP Address:** Defines the IP address for the secondary, fallback NTP Server. (Default = undefined.)
- **NTP Timeout:** The amount of time in seconds, that will elapse between each attempt to contact the NTP server. When the initial attempt is unsuccessful, the SCM will retry the connection four times. If neither the primary nor secondary NTP server responds, the SCM will wait 24 hours before attempting to contact the NTP server again. (Default = 3 Seconds.)

## 5.4.2. The Invalid Access Lockout Feature

When properly configured and enabled, the Invalid Access Lockout feature will watch all login attempts made at all SCM ports. If a given port exceeds the selected number of invalid attempts, then that port will be automatically disabled for a user-defined length of time. The Invalid Access Lockout feature uses three separate counters to track invalid access attempts:

- **Serial Port Counter:** Counts invalid access attempts at each individual serial port. If the number of invalid attempts at a given port exceeds the user-defined Lockout Attempts value, then that port will be locked.
- **Raw Socket Counter:** Counts invalid attempts to connect to a port via Raw Socket protocol. If the number of invalid attempts at a given port exceeds the user-defined Lockout Attempts value, then Raw Socket connections to that port will be locked.

- **Telnet, SSH and Web Browser Counter:** Counts all invalid attempts to access command mode via Telnet, SSH or Web Browser interface. If the number of cumulative invalid attempts exceeds the user-defined Lockout Attempts value, then the Network Port will be locked.

Note that when an Invalid Access Lockout occurs, you can either wait for the Lockout Duration period to elapse (after which, the SCM will automatically reactivate the port), or you can issue the `/UL` command (type `/UL` and press **[Enter]**) via the Text Interface to instantly unlock all SCM serial ports.

### Notes:

- Invalid Access Lockout parameters, defined via the System Parameters menu, will apply to all SCM serial ports.
- When a Port is locked, an external modem connected to that port will not answer.
- When a given SCM serial port is locked, the other SCM serial ports will remain unlocked, unless the Invalid Access Lockout feature has been triggered at those other ports.
- If any one of the SCM's logical network ports is locked, all other network connections to the unit will also be locked.
- All invalid access attempts at the SCM Network Port are cumulative (the count for invalid access attempts is determined by the total number of all invalid attempts at all 64 logical network ports.) If a valid login name/password is entered at any of the logical network ports, then the count for all SCM logical network ports will be restarted.
- A Port that has been locked by the Invalid Access Lockout feature will still respond to the ping command (providing that the ping command has not been disabled.)

The Invalid Access menus allow you to select the following:

- **Lockout Enable:** Enables/Disables the Invalid Access Lockout feature. (Default = On.)
- **Lockout Attempts:** The number of invalid attempts required to activate the Invalid Access Lockout feature. (Default = 9.)
- **Lockout Duration:** The length of time ports will remain locked when an Invalid Access Lockout occurs. If the duration is set at "Infinite", then ports will remain locked until the `/UL` command is issued. (Default = 30 Minutes.)

### 5.4.3. The Audit Log

This feature allows you to create a record of command activity at all SCM ports. Audit Log records will include the time, date, username, and a brief description of each logged event (e.g., Connect, Login, etc.) The Audit Log is enabled and configured via the System Parameters Menus.

The System Parameters Menus includes three different options for Audit Log configuration; Off (Audit Log disabled), "On with Syslog" and "On without Syslog." When "On with Syslog" is selected, each individual Audit Log record will be sent out to the user-defined Syslog IP Address as a Syslog message at the time that it is generated. The Syslog IP Address is defined via the Network Parameters Menu, as described in Section 5.7.3.

To read or erase the Audit Log, access command mode (via the Text Interface,) using an account and port that permit Supervisor commands, type **/A s**, press **[Enter]** (where **s** is an optional text string that you wish to search for,) and follow the instructions in the resulting submenu. When the **s** (search string) option is included, the **/A** command will return only those records that match the selected search string.

#### Notes:

- The SCM dedicates a fixed amount of internal memory for Audit Log records, and if log records are allowed to accumulate until this memory is filled, memory will eventually "wrap around," and older records will be overwritten by newer records.
- The Audit Log cannot be viewed via the Web Browser Interface.
- When the **s** option is used to search for all records that contain a specific text string, the Delete function will still delete all Audit Log records; the Delete function is not limited to the records that are currently displayed on screen.



#### 5.4.4. Callback Security

The Callback function provides an additional layer of security when callers attempt to access command mode via modem. When this function is properly configured, modem users will not be granted immediate access to command mode upon entering a valid password; instead, the unit will disconnect, and dial a user-defined number before allowing access via that number. If desired, users may also be required to re-enter the password *after* the SCM dials back.

In order for Callback Security to function properly, you must first enable and configure the feature via the System Parameters menus as described in this section, and then define a callback number for each desired user account as described in Section 5.6. To configure and enable the Callback function, proceed as follows:

- **Text Interface:** Type **/F** and press **[Enter]** to access the System Parameters menu, then type **6** and press **[Enter]** to display the Callback Security Menu.
- **Web Browser Interface:** Click the "System Properties" link on the left hand side of the screen to access the System Configuration menu, then click the "Configure Callback Security" link to display the Callback Security Menu.

In both the Text Interface and Web Browser Interface, the Callback Security Menu offers the following options:

- **Callback Enable:** This prompt offers five different configuration options for the Callback Security feature: (Default = On - Callback (Without Password Prompt.)
  - ◆ **Off:** All Callback Security is disabled.
  - ◆ **On - Callback (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt will *not* be displayed when the user's modem answers. If the account *does not* include a Callback Number, that user will be granted immediate access and a Callback will *not* be performed.
  - ◆ **On - Callback (With Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt *will* be displayed when the user's modem answers (accounts that include a Callback Number will be required to re-enter their username/password when their modem answers.) If the account *does not* include a Callback Number, then that user will be granted immediate access and a Callback will *not* be performed.

- ◆ **On - Callback ONLY (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the username/password prompt will *not* be displayed when the user's modem answers. Accounts that *do not* include a Callback Number will *not* be able to access command mode via an SCM modem port.
- ◆ **On - Callback ONLY (With Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the username/password prompt *will* be displayed when the user's modem answers (users will be required to re-enter their username/password when their modem answers.) Accounts that *do not* include a Callback Number will *not* be able to access command mode via an SCM modem port.
- **Callback Attempts:** The number of times that the SCM will attempt to call the Callback number. (Default = 3 attempts.)
- **Callback Delay:** The amount of time that the SCM will wait between Callback attempts. (Default = 30 seconds.)

#### **Notes:**

- After configuring and enabling Callback Security, you must then define a callback phone number for each desired user account (as described in Section 5.6) in order for this feature to function properly.
- When using the "On - Callback (With Password Prompt)" option, it is important to always define a callback number for each user account. Otherwise accounts that do not include a callback number will be allowed to immediately access command mode, and the callback function will not be performed.

## **5.5. User Accounts**

---

Prior to accessing command mode or establishing a Telnet Direct Connection, you will be prompted to enter a username and password. The username and password entered at login determine which port(s) you will be allowed to connect and what type of commands you will be allowed to execute. Each username / password combination is defined within a "user account."

The SCM allows up to 128 user accounts; each account includes a username, password, security level, port access rights, and an optional dialback number.

### 5.5.1. Supervisor Access

In order to protect access to important commands, the SCM allows you to enable or disable Supervisor commands for specific accounts. Accounts that have Supervisor Access enabled, will be allowed access to all configuration menus, review all status screens, and connect to any SCM RS232 port.

When Supervisor Access is disabled, the account will be blocked from changing configuration parameters, access to status screens will be restricted, and the user will only be able to connect to ports specifically allowed by that account.

Note that in the default state, the SCM includes one predefined user account that provides access to Supervisor commands and allows connections with any SCM RS232 port. The default username for this account is **"super"** (lowercase, no quotation marks), and the password for the account is also **"super"**.

#### Notes:

- In order to ensure security, it is recommended that when initially setting up the unit, you should either change the username and password for the default "super" user account, or preferably, a new user account with Supervisor access should be created, and the "super" account should then be deleted.
- If the SCM is reset to default parameters, all user accounts will be cleared, and the default "super" account will be restored.
- If Supervisor commands are disabled at a given port, then accounts that permit Supervisor commands will not be able to access command mode via that port.

In most cases, a password with Supervisor Access can be entered at any port, allowing the user to invoke Supervisor level commands. However, if you wish to completely deny a specific port's access to Supervisor commands (even *with* a password that normally permits them), the Port Parameters menus can disable Supervisor commands at ports 2 through 16, and the Network Port. The Supervisor Mode *cannot* be disabled at Port 1 (System Setup Port.) For a summary of commands and status screens available to Supervisors and non-Supervisors, please refer to Section 13.

### 5.5.2. Port Access

Each account can be granted access to a different selection of ports. Accounts *with* Supervisor access are always allowed to establish connections with all ports, but accounts *without* Supervisor Access can be restricted to a specific port or group of ports. Note also, that several accounts can be allowed access to the same port.

## 5.6. Managing User Accounts

---

The User Directory function is employed to create new accounts, display parameters for existing accounts, modify accounts and delete accounts. Up to 128 different user accounts can be created. The "User Directory" function is only available when you have logged into command mode using an account and port that permit Supervisor commands.

- **Text Interface:** Type **/F** and press **[Enter]** to access the System Parameters Menu. From the System Parameters Menu, type **1** and press **[Enter]** to access the User Directory.
- **Web Interface:** Click the "Users" link on the left hand side of the screen to access the User Directory management menus.

In both the Text Interface and the Web Browser Interface, the user configuration menu offers the following functions:

- **View User Directory:** Displays currently defined parameters for any SCM user account as described in Section 5.6.1.
- **Add Username:** Creates new user accounts, and allows you to assign a username, password, command level, port access rights, and callback number, as described in Section 5.6.2.
- **Edit User Directory:** This option is used to edit account information, as described in Section 5.6.3.
- **Delete User:** Clears user accounts, as described in Section 5.6.4.

### 5.6.1. Viewing User Accounts

The "View User Directory" option allows you to view details about each account, including the ports the account is allowed to access and whether or not the account is allowed to invoke Supervisor commands. The View User option will not display actual passwords, and instead, the password field will read either "defined" or "undefined." Note that the View User Accounts function is only available to users who have accessed command mode using a password that permits Supervisor Level commands. To view account details, proceed as follows:

- **Text Interface:** From the User Directory menu, type **1** and press **[Enter]**. The SCM will display a screen which lists all defined user accounts. Key in the name of the desired account and then press **[Enter]**.
- **Web Browser Interface:** From the User menu, click the "View/Edit User" link. The SCM will display a menu that allows you to select the desired user and directory function. Select the "View User" button, and then click on the down arrow, scroll to the desired username, select the username, and then click "Choose User."

ADD USERNAME TO DIRECTORY:

1. Username:

2. Password:

3. Supervisor Access:

4. Port Access:

(undefined)

Off

| PORT# | PORT NAME   | ACCESS | PORT# | PORT NAME   | ACCESS |
|-------|-------------|--------|-------|-------------|--------|
| 1     | (undefined) | Off    | 9     | (undefined) | Off    |
| 2     | (undefined) | Off    | 10    | (undefined) | Off    |
| 3     | (undefined) | Off    | 11    | (undefined) | Off    |
| 4     | (undefined) | Off    | 12    | (undefined) | Off    |
| 5     | (undefined) | Off    | 13    | (undefined) | Off    |
| 6     | (undefined) | Off    | 14    | (undefined) | Off    |
| 7     | (undefined) | Off    | 15    | (undefined) | Off    |
| 8     | (undefined) | Off    | 16    | (undefined) | Off    |

5. Callback Phone #:

Enter: #<CR> to select,

<ESC> to return to previous menu ...

Figure 5.7: The Create User Menu (Text Interface)

File Edit View Favorites Tools Help



REMOTE SITE MANAGER

Location: (undefined)

Navigation

Home

Configuration

System Properties

Serial Port

Network

Configuration

User Management

Users

Add User

User Name:

Password:

Password Confirm:

Supervisor Access:

Port 1 Access:

Port 2 Access:

Port 3 Access:

Port 4 Access:

Port 5 Access:

Port 6 Access:

Port 7 Access:

Port 8 Access:

Callback Phone #:

Port 9 Access:

Port 10 Access:

Port 11 Access:

Port 12 Access:

Port 13 Access:

Port 14 Access:

Port 15 Access:

Port 16 Access:

Add User

© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>

Figure 5.8: The Create User Menu (Web Browser Interface)

### 5.6.2. Adding User Accounts

The "Add Username" option allows you to create new accounts and assign usernames, passwords, command level, port access rights, and Callback Numbers to each account. Note that the Add User function is only available to users who have accessed command mode using a password that permits Supervisor Level commands. To create new user accounts, proceed as follows:

- **Text Interface:** From the User Directory menu, type **2** and press **[Enter]**. The Add Username menu (Figure 5.7) will be displayed.
- **Web Browser Interface:** From the Edit User menu, click the "Add User" link. The SCM will display the Add User menu (Figure 5.8.)

The Add Username Menu can be used to define the following parameters for each new account:

- **Username:** Up to sixteen characters long, and cannot include non-printable characters. Duplicate usernames are not allowed. (Default = undefined.)
- **Password:** Five to sixteen characters long, and cannot include non-printable characters. Note that passwords are case sensitive. (Default = undefined.)
- **Supervisor Access:** Determines whether the account is allowed to invoke Supervisor commands. (Default = Off.)
- **Port Access:** Determines which port(s) this account will be allowed to create connections with. (Default = All Ports Off.)
- **Callback Number:** Assigns a number that will be called when this user attempts to access command mode via modem at an SCM port, where the Callback Security Function has been enabled as described in Section 5.4.4. (Default = undefined.)

#### Notes:

- If the Callback Number is not defined, then Callbacks will not be performed for this user.
- If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use either of the "On - Callback" options, then this user will be granted immediate access to command mode via modem.
- If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use the "On - Callback ONLY" option, then this user will not be able to access command mode via a Modem Mode port.

### 5.6.3. Modifying User Accounts

The "Edit User Directory" function allows you to edit existing user accounts in order to modify passwords and usernames, or change port access or Supervisor Command capability. Note that the Edit/Modify User function is only available to users who have accessed command mode using a password that permits Supervisor Level commands. To modify a user account, proceed as follows:

- **Text Interface:** From the User Directory menu, type **3** and press **[Enter]**. The SCM will display a screen which lists all user accounts. Key in the name of the account you wish to modify, and press **[Enter]**.
- **Web Browser Interface:** From the User Configuration menu, click the "View/Edit User" link. The SCM will display a menu that allows you to select the user. Select the "Modify User" button, then click the down arrow, scroll to the name of the desired account, select the username, and then click "Choose User" to display the "Modify User" menu.



#### 5.6.4. Deleting User Accounts

This function is used to delete individual user accounts. Note that the Delete User function is only available to users who have accessed command mode using a password that permits Supervisor Level commands. To delete an existing user account, proceed as follows:

- **Text Interface:** From the Users Directory menu, type **4** and press **[Enter]**. The SCM will display a screen which lists all currently defined accounts. Key in the name of the account you wish to delete and press **[Enter]**. The SCM will delete the specified account without further prompting.
- **Web Browser Interface:** From the User Configuration menu, click the "View/Edit Users" link. The SCM will display a menu that lists all currently defined accounts. Select the "Delete User" box, then click the down arrow, scroll to the account you wish to delete, select the account, and then click "Choose User." The SCM will display a screen that lists details for the specified account; click "Delete User" to confirm deletion.

#### Notes:

- Deleted accounts cannot be automatically restored.
- The SCM allows you to delete the default "super" account, which is included to permit initial access to command mode. Before deleting the "super" account, make certain to create another account that permits Supervisor Access. If you do not retain at least one account with Supervisor Access, you will not be able to invoke supervisor level commands.

## 5.7. Port Configuration

---

When responding to prompts, invoking commands, and selecting items from port configuration menus, note the following:

- Configuration menus are only available to accounts and ports that permit Supervisor commands.
- If you are configuring the SCM via modem, modem parameters will not be changed until after you exit command mode and disconnect from the SCM.

### 5.7.1. Port Modes

The SCM offers four different port operation modes:

- **Any-to-Any Mode:** Allows communication between connected ports and permits access to command mode. Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer or Modem Mode Ports by invoking the /C command. The Any-to-Any Mode is available to all ports and is the default Port Mode for Ports 1 and 2.
- **Passive Mode:** Allows communication between connected ports, but does *not* allow access to command mode. Passive Mode Ports can be connected by accessing command mode from a free Any-to-Any or Modem Mode port and invoking the /C command. Passive Mode is not available at Port 1 or the Network Port, and is the default mode at Ports 3 through 16.
- **Buffer Mode:** Allows storage of data received from connected devices. Collected data can be retrieved by accessing command mode from a free Any-to-Any or Modem Mode Port, and issuing the Read Buffer (/R) Command. Furthermore, Buffer Mode ports can also be configured to support the Syslog and SNMP Traps features, discussed in Sections 9 and 10. The Buffer Mode is not available at Port 1 or the Network Port.
- **Modem Mode:** Allows communication between connected ports, permits access to command mode and simplifies connection to an external modem. Modem Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem Mode also allows definition of a Hang-Up String, Reset String, and Initialization String. The Modem Mode is not available at the Port 1 or the Network Port.

For more information on Port Modes, please refer to Section 7.

**PORT PARAMETERS #03:**

|                              |         |                             |         |
|------------------------------|---------|-----------------------------|---------|
| <b>COMMUNICATION SETTING</b> |         | <b>PORT MODE PARAMETERS</b> |         |
| 1. Baud Rate:                | 9600    | 21. Port Name:              |         |
| 2. Bits/Parity:              | 8-None  | 22. Port Mode:              | Passive |
| 3. Stop Bits:                | 1       | 23. DTR Output:             | Pulse   |
| 4. Handshake:                | RTS/CTS | 24. Buffer Params:          | ---     |
|                              |         | 25. Modem Params:           | ---     |

|                           |          |                         |     |
|---------------------------|----------|-------------------------|-----|
| <b>GENERAL PARAMETERS</b> |          | <b>NETWORK SERVICES</b> |     |
| 11. Supervisor Mode:      | Permit   | 31. Direct Connect:     | Off |
| 12. Logoff Char:          | ^X       | Telnet Port:            | --- |
| 13. Sequence Disc:        | One Char | SSH Port:               | --- |
| 14. Inact Timeout:        | Off      | Raw Port:               | --- |
| 15. Command Echo:         | On       | 32. Syslog:             | --- |
| 16. Accept Break:         | On       | 33. SNMP Trap Lv:       | --- |

Enter: "<" previous port,  
">" next port,  
<ESC> exit ...

Figure 5.9: Port Configuration Menu (Text Interface)

The screenshot shows a web browser window with the title "REMOTE SITE MANAGER". The URL bar shows "http://www.wti.com". The page has a navigation menu on the left with links for "Home", "System", "Parameters", "Serial Port", "Network", "Configuration", "User", "Management", and "Users". The main content area displays the "Serial Port 3 Configuration" form. The form contains various settings for the serial port, including Port Name, Baud Rate, Bits/Parity, Stop Bits, Handshake Mode, Port Mode, Supervisor Mode, Logoff Character, Sequence Disconnect, Inactivity Timeout, Command Echo, Accept Break, Direct Connect, Modem Reset String, Modem Init String, Modem Hang-Up String, Periodic Reset Interval, DTR Output, Buffer DateTime, Buffer Connect, Syslog, Facility, Level, and SNMP Trap Level. A "Change Serial Parameters" button is at the bottom of the form.

Location: (undefined)

Navigation: [Home](#)

Configuration: [System](#), [Parameters](#), [Serial Port](#), [Network](#), [Configuration](#)

User Management: [Users](#)

**Serial Port 3 Configuration**

Port Name:

Baud Rate:

Bits/Parity:

Stop Bits:

Handshake Mode:

Port Mode:

Supervisor Mode:

Logoff Character:

Sequence Disconnect:

Inactivity Timeout:

Command Echo:

Accept Break:

Direct Connect:

Modem Reset String:

Modem Init String:

Modem Hang-Up String:

Periodic Reset Interval:

DTR Output:

Buffer DateTime:

Buffer Connect:

Syslog:

Facility:

Level:

SNMP Trap Level:

© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>

Figure 5.10: Port Configuration Menu (Web Browser Interface)

### 5.7.2. RS232 Port Configuration Menus

The Port Configuration Menus are used to select communications parameters and enable/disable options for each RS232 port.

- **Text Interface:** Type **/P n** and then press **[Enter]** (Where **n** is the number or name of the desired RS232 port.) The Port Parameters menu will be displayed as shown in Figure 5.9.
- **Web Browser Interface:** Click the "Serial Port" link on the left hand side of the screen. The Port Selector menu will be displayed. From the Port Selector menu, use the drop down menu to select the desired RS232 Port, and then click the "Select Port" button. The Port Parameters menu will be displayed as shown in Figure 5.10.

The Port Configuration menus allow the following parameters to be defined. Note that all of these parameters are available via both the Text Interface and Web Browser Interface, and that parameters selected via one interface are also applied to the other.

#### Communication Settings:

- **Port Name:** (Up to 16 characters, Default = undefined).

#### Notes:

- Port Names cannot include non-printable characters, the forward slash (/), double quotes ("), asterisks (\*), or blank spaces.
- Port Names must begin with an alphabetic character; Port Names *cannot* begin with a number or punctuation character.
- A Port cannot be named "**N1**" through "**N66**", these names are reserved for the logical Network Ports.
- Port names are case-sensitive.
- **Baud Rate:** Any standard rate from 300 bps to 115.2K bps. (Default = 9600 bps)
- **Bits/Parity:** (Default = 8-None).
- **Stop Bits:** (Default = 1).
- **Handshake Mode:** XON/XOFF, RTS/CTS (hardware), Both, or None. (Default = RTS/CTS).

---

**General Parameters:**

- **Supervisor Mode:** Permits/denies port access to supervisor commands. When enabled (Permit), the port will be allowed to invoke supervisor commands, providing the unit is accessed using an account that permits them. If disabled (Deny), the port may *not* invoke Supervisor commands. (Default = Permit).

**Note:** If the Supervisor Mode is set to "Deny", then user accounts that permit Supervisor commands will not be allowed to access command mode via this port.

- **Logoff Character:** The Logoff Character determines the command(s) or character(s) that must be issued at this port in order to disconnect from a second port. Note that the Logoff Character does not apply to Direct Connections. (Default = ^X)

**Note:** When redefining the Logoff Character, select a character that *does not* normally occur in your data. This prevents the SCM from accidentally disconnecting ports in the middle of a transfer when a character that accidentally matches the Logoff Character is passed.

- **Sequence Disconnect:** Enables/Disables and configures the Resident Disconnect command. This offers the option to disable the Sequence Disconnect, select a one character format or a three character format. (Default = One Character.)

**Notes:**

- When a Resident Connection is initiated, the SCM will list the connected ports, and the command required in order to terminate the connection.
- The One Character Disconnect is intended for situations where the other port should *not* receive the disconnect command. When the Three Character format is selected, the disconnect sequence *will* be passed to the other port.
- When the Three Character format is selected, the Resident Disconnect Sequence will use the "[Enter]**L**L**L**[Enter]", format, where **L** is the selected Logoff Character.

- **Inactivity Timeout:** Enables and selects the Timeout Period for this port. If enabled, the port will disconnect when no additional data activity is detected for the duration of the timeout period. When the port is set for Any-to-Any Mode, Passive Mode, or Buffer Mode, the default setting is "Off." When set for Modem Mode, the default setting is 5 minutes.

**Notes:**

- The Inactivity Timeout value is also applied to Direct Connections.
- The Inactivity Timeout is also applied to non-connected ports that are left in command mode. If the timeout is enabled, and no additional activity is detected, an unconnected port will exit command mode when the Timeout Disconnect expires.
- **Command Echo:** Enables or Disables command echo at this port. (Default = On.)
- **Accept Break:** Determines whether the port will accept breaks received from the attached device, and pass them along to a connected port. When enabled, breaks received at this port will be passed to any port this port is connected to. When disabled, breaks will be refused at this port. (Default = On.)

**Port Mode Parameters:**

- **Port Mode:** The operation mode for this port. Ports 1 and 2 *cannot* be configured as Passive or Buffer Mode ports, and the internal modem port is always configured for Modem Mode. (Port 1 and 2, Default = Any-to-Any Mode; Serial Ports 3 and above, Default = Passive Mode; Internal Modem Port, Default = Modem Mode.)

Depending on the Port Mode selected, the SCM will also display the additional prompts listed in this section. In the Text Interface, these parameters are accessible via a submenu, which will only be active when the appropriate port mode is selected, and in the Web Browser Interface, fields will be "grayed out" unless the corresponding port mode is selected.

- **Any-to-Any Mode / Passive Mode:** Allows the following Mode-specific parameter to be defined:
  - **DTR Output:** Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high. (Default = Pulse.)
- **Modem Mode:** Allows the following mode-specific parameters to be defined:
  - **Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **ATZ**.)
  - **Initialization String:** Defines a command string that can be sent to initialize an external modem to settings required by your application. (Default = **AT&C1&D2S0=1&B1&H1&R2**)
  - **Hang-Up String:** Although the SCM will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined.)
  - **Periodic Reset Value:** Determines how often the Reset String will be sent to the modem at this port.

**Note:** When communicating with the SCM via modem, these parameters will not be changed until after you exit command mode and disconnect.

- **Buffer Mode:** Allows the following mode-specific parameters to be defined:
  - **Buffer DateTime:** Enables/Disables the Time/Date stamp for buffered data. When enabled, the SCM will add a time/date stamp whenever five seconds elapse between data items received. (Default = On.)
  - **Buffer Connect:** When enabled, the SCM will continue to Buffer captured data while you are connected to the Buffer Mode port. (Default = Off.)

## Network Services:

- **Direct Connect:** Direct Connect allows users to access the SCM and automatically create a connection between the Network Port and a specific RS232 port by including the appropriate Telnet port number in the connect command (e.g. Port 5 = 2105). For more information, please refer to Section 8.3. As described below, the Direct Connect feature offers three options. (Default = Off.)
  - **Off:** Telnet users will *not* be able to employ the Direct Connect feature to connect to this port.
  - **On - No Password:** Telnet users *will* be able to employ the Direct Connect feature to connect to this port without entering a password.
  - **On - Password:** Telnet and SSH users will be able to use Direct Connect to connect to this port, but will be required to enter a password before the connection is established.

**Note:** If "On - Password" is selected, and Supervisor commands are disabled at the Network Port, then only accounts that do not permit Supervisor commands will be allowed to establish a direct connection via the Network Port. If Supervisor commands are disabled at a given port, then that port will not allow access by accounts that permit Supervisor commands.

When the Port Parameters menu is accessed via the Text Interface, the menu also lists both Direct Connect port numbers for this port (port numbers are not listed in the Web Browser Interface.)

- **Telnet Port:** The Telnet port number employed to create a Direct Connection to this port using standard Telnet protocol.
- **SSH Port:** When Direct Connect (Item 13) is set at "On - Password", this line will display the Telnet port number used to create a Direct Connection to this port using SSH protocol. For more information, please refer to Section 8.3.
- **Raw Port:** The Telnet port number that is used to create a Direct Connection to this port using Raw Socket protocol.



- **Syslog:** The Syslog feature is used to create records of each buffer event. As event records are created, they are sent to a Syslog Daemon, at an IP address defined via the Network Parameters menu. For more information, please refer to Section 9. The Syslog feature offers three possible settings. (Default = Off)
  - **Off:** Syslog disabled. (Default)
  - **On - Not Connected:** Messages will only be generated when a user is *not* connected to a buffer port (either by /C or direct connect.) This prevents information captured from the attached device from being put into Syslog messages while a user is connected to a buffer port.
  - **On - Always:** *All* captured information will be sent out via Syslog message; whether a user is connected or not.

### Notes:

- Syslog is only available at Buffer Mode Ports.
- This option is not available to RS232 Ports 1 and 2, because Ports 1 and 2 cannot be configured as Buffer Mode Ports.

The Port Parameters menu also offers two additional items used to set the priority of Syslog messages generated by this port:

- **Facility:** The facility under which this port will log messages. (Default = Local\_0.)
- **Level:** The severity (or priority) of messages generated by this port. (Default = Emergency.)
- **SNMP Trap Level:** Enables/disables the SNMP Trap function and sets the byte level that will generate traps at this port. If set to "0" (zero), then SNMP Traps are disabled at this port.

If this value is set between 1 and 32,767, then the SNMP Trap function is enabled, and traps will be sent to the SNMP Managers whenever the buffer for this port reaches the specified level. For more information, please refer to Section 10. (Default = Off.)

### Note:

- The SNMP Trap feature only applies to Buffer Mode Ports.
- This option is not available to RS232 Ports 1 or 2. This is because Ports 1 and 2 are reserved as SetUp Ports, and cannot be configured as Buffer Mode Ports.

### 5.7.3. Network Port Configuration Menu

The Network Parameters Menus are used to select parameters and options for the Network Port. The Network Parameters Menus also allow you to implement IP Security features, which can restrict access based on the user's IP Address.

Although the Web Browser Interface and Text Interface allow definition of essentially the same parameters, parameters are arranged differently in the two interfaces. In the Text Interface, most network parameters are defined via one menu. But in the Web Browser Interface, network parameters are divided between six separate submenus as described in this section. To access the Network Parameters Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]**. The Network Parameters Menu shown in Figure 5.11 will be displayed.
- **Web Browser Interface:** Click on the "Network Configuration" link on the left hand side of the screen. The SCM will display the Network Configuration menu shown in Figure 5.12, which allows you to access the various submenus used to configure the network port.

#### Notes:

- Settings for network parameters depend on the configuration of your network. Please contact your network administrator for appropriate settings.
- The Network Parameters Menu selects parameters for all 16 logical Network Ports.
- When a new IP Address is selected, or the status of the DHCP feature is changed, the unit will disconnect and reconfigure itself with the new values when you exit the Network Parameters Menu. When configuring the unit via Web or Telnet, make certain your DHCP server is set up to assign a known, fixed IP address.
- The Network Parameters menu is only available when you have logged into command mode using an account and port that permit Supervisor commands.

The Network Parameters menu offers the following options. Note that although the descriptions of parameters in this section are arranged according to the Web Browser Interface submenu in which they reside, in the Text Interface, all parameters (except IP Security configuration) are included in one menu.

**NETWORK PARAMETERS:**

|                              |               |                            |             |
|------------------------------|---------------|----------------------------|-------------|
| <b>COMMUNICATION SETTING</b> |               | <b>SERVERS AND CLIENTS</b> |             |
| 1. IP Address:               | 207.212.30.80 | 21. Telnet Access:         | On          |
| 2. Subnet Mask:              | 255.255.255.0 | 22. SSH Access:            | On          |
| 3. Gateway Addr:             | 207.212.30.1  | 23. Web Access:            | Off         |
| 4. DHCP:                     | Off           | 24. SYSLOG IP addr:        | (undefined) |
| 5. IP Security:              | Off           | 25. SNMP Access:           | Off         |
| 6. Static Route:             | Off           | 26. SNMP Trap:             | Off         |
|                              |               | 27. TACACS:                | Off         |
| <b>GENERAL PARAMETERS</b>    |               | 28. RADIUS:                | Off         |
| 11. Supervisor Mode:         | Permit        | 29. PING Access:           | On          |
| 12. Logoff Char:             | ^X            | 30. Raw Socket Access:     | Off         |
| 13. Sequence Disc:           | One Char      |                            |             |
| 14. Inact Timeout:           | 5 Min         |                            |             |
| 15. Command Echo:            | On            |                            |             |
| 16. Accept Break:            | On            |                            |             |

Enter: #<CR> to change,  
<ESC> exit ...

Figure 5.11: Network Parameters Menu (Supervisor Mode Only)

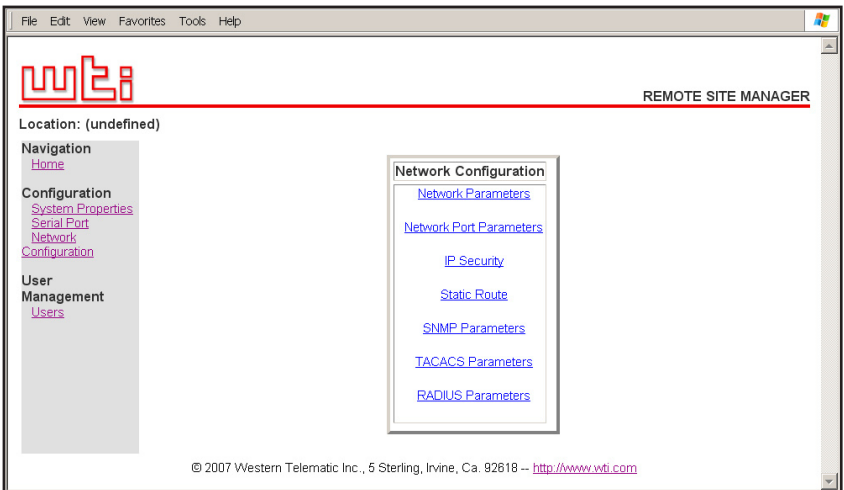


Figure 5.12: Network Configuration Menu (Web Browser Interface)

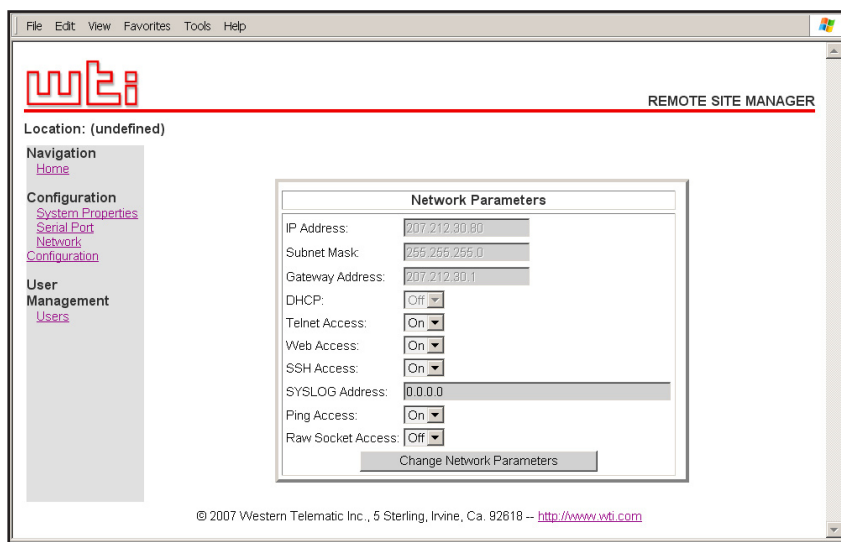


Figure 5.13: Network Parameters Menu (Web Browser Interface)

## Network Parameters

In the Text Interface, these parameters are accessed via the Network Configuration menu (Figure 5.12.) In the Web Browser Interface, these parameters can be found by first clicking the "Network Configuration" link, and then Clicking the "Network Parameters" link to display the Network Parameters menu (Figure 5.13.)

- **IP Address:** (Default = 192.168.168.168.)
- **Subnet Mask:** (Default = 255.255.255.0.)
- **Gateway Address:** (Default = undefined.)
- **DHCP:** Enables/Disables Dynamic Host Configuration Protocol. When this option is "On", the SCM will perform a DHCP request. Note that the MAC address for the SCM is listed on the Network Status Screen. (Default = Off.)

**Note:** Before configuring this feature via Telnet or Web, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the SCM unit.

- **Telnet Access:** Enables/disables Telnet access to the SCM. When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the unit. (Default = On.)
- **Web Access:** Enables/disables the Web Browser Interface. When disabled, users will not be allowed to contact the unit via the Web Browser Interface. (Default = Off.)
- **SSH Access:** Enables/disables SSH communication with the SCM. (Default = On.)
- **SYSLOG IP Address:** The IP Address for the Syslog Daemon that will receive log records generated by the SCM. For more information, please refer to Section 9. (Default = 0.0.0.0.)

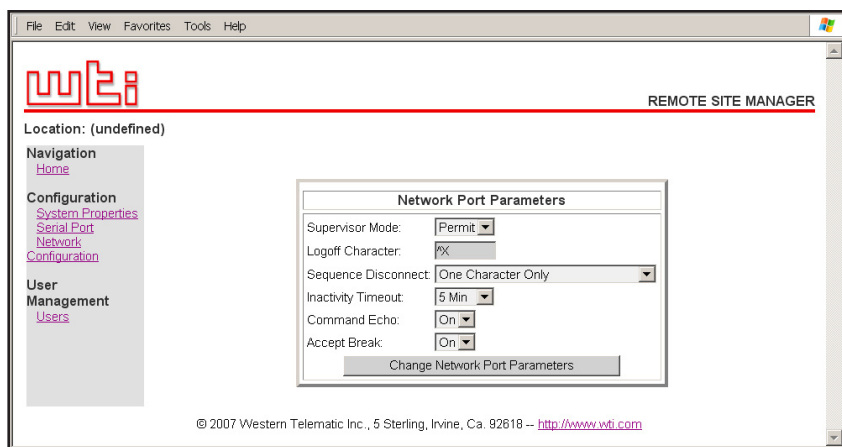


Figure 5.14: Network Port Parameters Menu (Web Browser Interface)

## Network Port Parameters

In the Text Interface, these parameters are found in the Network Configuration menu (Figure 5.12.) In the Web Browser Interface, these parameters are found by first clicking the "Network Configuration" link, and then clicking the "Network Port Parameters" link to display the Network Port Configuration Menu (Figure 5.14.)

- **Supervisor Mode:** Permits or denies access to Supervisor commands. If disabled, the Network port is *not* allowed to invoke Supervisor commands. (Default = Permit).

**Note:** When Supervisor Mode for the Network Port is set to "Deny," accounts that permit Supervisor commands will not be allowed to access command mode via network.

- **Logoff Character:** Defines the Logoff Character for this port. The Logoff Character determines which command(s) must be issued at this port in order to disconnect from a second port. Note that the Logoff Character does not apply to Telnet Direct Connections. (Default = ^X ([Ctrl] plus [X])).

- **Sequence Disconnect:** Enables/Disables and configures the Resident Disconnect command. Offers the option to either disable the Sequence Disconnect, or select a one character, or a three character command format. (Default = One Character).

**Notes:**

- The One Character Disconnect is intended for situations where the destination port should *not* receive the disconnect command. When the Three Character format is selected, the disconnect sequence *will* pass through to the destination port prior to breaking the connection.
  - When Three Character format is selected, the Resident Disconnect uses the format "[Enter]**L****L****L**[Enter]", where **L** is the selected Logoff Character.
- **Timeout Disconnect:** Enables and selects the Timeout Disconnect period for the Network Port. If enabled, and the port does not receive or transmit data for the specified time period, the port will disconnect. (Default = 5 Minutes).
- Note:** The Timeout Disconnect value is also applied to Direct Connections.
- **Command Echo:** Enables or Disables the command echo for the Network Port. (Default = On).
  - **Accept Break:** Determines whether the port will accept breaks received from the attached device, and pass them along to a connected port. When enabled, breaks received at this port will be passed to any port this port is connected to, and sent to the device connected to the other port. When disabled, breaks will be refused at this port. (Default = On.)

## **IP Security**

As described in Section 5.7.4, the IP Security function allows you to restrict command mode access based on the user's IP address. In the Text Interface, IP Security parameters are defined via item 8 in the Network Configuration menu. In the Web Browser Interface, these parameters are found by clicking the "Network Configuration" link, and then Clicking the "IP Security" link. In the default state, IP Security is disabled.

## **Static Route**

The Static Route menu allows you to type in Linux routing commands that will be automatically executed each time that the unit powers up or reboots. In the Text Interface, the Static Route menu is accessed via item 6 in the Network Configuration menu. In the Web Browser Interface, the Static Route menu is accessed by first clicking the Network Configuration link and then clicking the Static Route link.



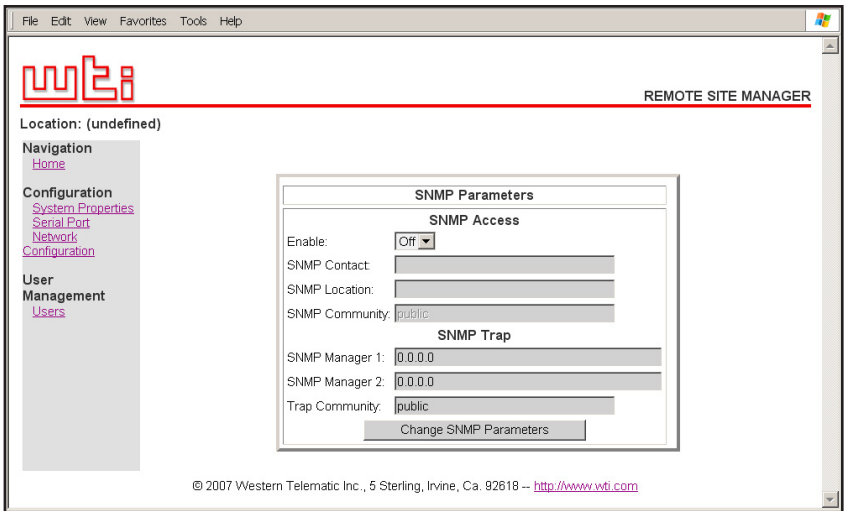


Figure 5.15: SNMP Parameters Menu (Web Browser Interface)

### SNMP Parameters

In the Text Interface, SNMP parameters are found in the Network Configuration menu (Figure 5.12.) In the Web Browser Interface, SNMP parameters can be found by first clicking the "Network Configuration" link, and then clicking the "SNMP Parameters" link to display the SNMP Parameters Menu (Figure 5.15.)

- **SNMP Access (SNMP):** Enables/disables SNMP Polling. (Default = Off.)

**Note:** This item only applies to external SNMP polling of the SCM; it does not effect the ability of the SCM to send SNMP traps.

- **SNMP Manager 1:** The IP Address for the first SNMP Manager. For more information, please refer to Section 10. (Default = Undefined.)
- **SNMP Manager 2:** (Default = Undefined.)
- **SNMP Community:** (Default = Public.)
- **SNMP Contact:** (Default = undefined.)
- **SNMP Location:** (Default = undefined.)

## TACACS Parameters

To access the TACACS Configuration Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to access the Network Configuration Menu. From the Network Configuration Menu, type **12** and press **[Enter]** to display the TACACS Configuration Menu.
- **Web Browser Interface:** Click on the "Network Configuration" link to display the menu shown in Figure 5.10, then click the "TACACS Parameters" link to display the TACACS Configuration Menu.

The TACACS Configuration Menus offer the following options:

- **Enable:** Enables/disables the TACACS feature at the Network Port. (Default = Off.)
- **IP Address 1:** Defines the IP address for your primary TACACS server. (Default = undefined.)
- **IP Address 2:** Defines the IP address for your secondary, fallback TACACS server (if present.) (Default = undefined.)
- **Secret Word:** Defines the shared TACACS Secret Word for both TACACS servers (IP Address 1 and IP Address 2). (Default = undefined.)
- **Fallback Local:** Determines whether or not the SCM will fallback to its own password/username directory when an authentication attempt fails. When enabled, the SCM will first attempt to authenticate the password by checking the TACACS Server; if this fails, the SCM will then attempt to authenticate the password by checking its own internal username directory. (Default = Off.)
- **Authentication Port:** The port number for the TACACS function. (Default = 49.)

---

## RADIUS Parameters

To access the RADIUS Configuration Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to access the Network Configuration Menu. From the Network Configuration Menu, type **13** and press **[Enter]** to display the RADIUS Configuration Menu.
- **Web Browser Interface:** Click on the "Network Configuration" link to display the menu shown in Figure 5.12, then click the "RADIUS Parameters" link to display the RADIUS Configuration Menu.

The RADIUS Configuration Menus offer the following options:

- **Enable:** Enables/disables the RADIUS feature at the Network Port. (Default = Off.)
- **IP Address 1:** Defines the IP address for your primary RADIUS server. (Default = undefined.)
- **Secret Word 1:** Defines the RADIUS Secret Word for the primary RADIUS server (IP Address 1.) (Default = undefined.)
- **IP Address 2:** Defines the IP address for your secondary, fallback RADIUS server (if present.) (Default = undefined.)
- **Secret Word 2:** Defines the RADIUS Secret Word for the secondary RADIUS server (IP Address 3.) (Default = undefined.)
- **Fallback Timer:** Determines how long the SCM will continue to attempt to contact the primary RADIUS Server before falling back to the secondary RADIUS Server. (Default = 3 Seconds.)
- **Fallback Local:** Determines whether or not the SCM will fallback to its own password/username directory when an authentication attempt fails. When enabled, the SCM will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the SCM will then attempt to authenticate the password by checking its own internal username directory. (Default = Off.)
- **Authentication Port:** The port number for the RADIUS function. (Default = 1812.)

#### 5.7.4. Implementing IP Security

The SCM can restrict unauthorized IP addresses from establishing an inbound Telnet connection to the unit. This allows the user to grant Telnet access to only a specific group of IP addresses, or block a particular IP address. In the default state, the SCM accepts incoming IP connections from all hosts.

The IP Security Function employs a TCP Wrapper program which allows the use of standard, Linux operators, wild cards and net/mask pairs to create a host based access control list.

As shown in Figures 5.16 and 5.17, the IP Security configuration menus include "hosts.allow" and "hosts.deny" client lists. Basically, when setting up IP Security, you must enter IP addresses for hosts you wish to allow in the Allow list, and addresses for hosts you wish to deny in the Deny list. Since Linux operators, wild cards and net/mask pairs are allowed, these lists can indicate specific addresses, or a range of addresses to be allowed or denied.

When the IP Security feature is properly enabled, and a client attempts to connect, the SCM will perform the following checks:

1. If the client's IP address is found in the "hosts.allow" list, the client will be granted immediate access. Once an IP address is found in the Allow list, the SCM will not check the Deny list, and will assume you wish to allow that address to connect.
2. If the client's IP address is not found in the Allow list, the SCM will then proceed to check the Deny list.
3. If the client's IP Address *is* found in the Deny list, the client *will not* be allowed to connect.
4. If the client's IP Address *is not* found in the Deny list, the client *will* be allowed to connect, even if the address was not found in the Allow list.

#### Notes:

- If the SCM finds an IP Address in the Allow list, it will not check the Deny list, and will allow the client to connect.
- If both the Allow and Deny lists are left blank, then the IP Security feature will be disabled, and all IP Addresses will be allowed to connect (providing that the proper password and/or SSH key is supplied.)
- When the Allow and Deny lists are defined, the user is only allowed to specify the Client List; the Daemon List and Shell Command cannot be defined.

```

IP SECURITY:

CLIENT LIST FOR "hosts.allow" FILE:
1.
2.
3.
4.
5.
6.
7.
8.

CLIENT LIST FOR "hosts.deny" FILE:
9.
10.
11.
12.
13.
14.
15.
16.

Enter: #<CR> to select menu,
      <ESC> for previous menu ...

```

Figure 5.16: IP Security Menu (Text Interface)

The screenshot shows a web browser window with the title "REMOTE SITE MANAGER". The address bar shows "Location: (undefined)". The left sidebar contains a navigation menu with the following items: "Navigation" (with a link to "Home"), "Configuration" (with links to "System Properties", "Serial Port", "Networks", and "Configuration"), and "User Management" (with a link to "Users"). The main content area displays the "IP Security Parameters" configuration page. This page has a table with two columns: "Allow Host Parameters" and "Deny Host Parameters". Each column contains eight rows, each with a "Mask #X" label and an input field. The "Allow Host Parameters" column has masks #1 through #8, and the "Deny Host Parameters" column has masks #9 through #16. Below the table is a "Change IP Security Parameters" button. At the bottom of the page, there is a copyright notice: "© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>".

| IP Security Parameters        |                                |
|-------------------------------|--------------------------------|
| Allow Host Parameters         | Deny Host Parameters           |
| Mask #1: <input type="text"/> | Mask #9: <input type="text"/>  |
| Mask #2: <input type="text"/> | Mask #10: <input type="text"/> |
| Mask #3: <input type="text"/> | Mask #11: <input type="text"/> |
| Mask #4: <input type="text"/> | Mask #12: <input type="text"/> |
| Mask #5: <input type="text"/> | Mask #13: <input type="text"/> |
| Mask #6: <input type="text"/> | Mask #14: <input type="text"/> |
| Mask #7: <input type="text"/> | Mask #15: <input type="text"/> |
| Mask #8: <input type="text"/> | Mask #16: <input type="text"/> |

Change IP Security Parameters

© 2007 Western Telematic Inc., 5 Sterling, Irvine, Ca. 92618 -- <http://www.wti.com>

Figure 5.17: IP Security Menu (Web Browser Interface)

#### 5.7.4.1. Adding IP Addresses to the Allow and Deny Lists

To add an IP Address to the Allow or Deny list, and begin configuring the IP Security feature, proceed as follows.

##### **Notes:**

- Both the Allow and Deny list can include Linux operators, wild cards, and net/mask pairs.
- In some cases, it is not necessary to enter all four "digits" of the IP Address. For example, if you wish to allow access to all IP addresses that begin with "192," then you would only need to enter "192."
- The IP Security Configuration menu is only available when the Supervisor Mode is active.

1. Access the IP Security Configuration Menu.
  - a) **Text Interface:** Type **/N [Enter]** to display the Network Configuration Menu. From the Network Configuration Menu, type **9 [Enter]** to display the screen shown in Figure 5.16.
  - b) **Web Browser Interface:** Click on "Network Configuration" on the left hand side of the screen. When the Network Configuration menu appears, click on "IP Security" to display the screen shown in Figure 5.17.
2. **Allow List:** Enter the IP Address(es) for the clients that you wish to allow. Note that if an IP Address is found in the Allow list, the client will be allowed to connect, and the SCM will not check the Deny list.
  - a) **Web Browser Interface:** Place the cursor in the first empty field in the parameters menu, then key in the desired IP Address, operators, wild cards, and/or net/mask pairs.
  - b) **Text Interface:** Note the number for the first empty field in the Allow list, then type that number at the command prompt, press **[Enter]**, and then follow the instructions in the resulting submenu.
3. **Deny List:** Enter the IP Address(es) for the clients that you wish to deny. Note that if the client's IP Address is not found in the Deny List, that client will be allowed to connect. Use the same procedure for entering IP Addresses described in Step 2 above.

#### 5.7.4.2. Linux Operators and Wild Cards

In addition to merely entering a specific IP address or partial IP address in the Allow or Deny list, you may also use any standard Linux operator or wild card. In most cases, the only operator used is "EXCEPT" and the only wild card used is "ALL," but more experienced Linux users may note that other operators and wild cards may also be used.

**EXCEPT:**

This operator creates an exception in either the "allow" list or "deny" list.

For example, if the Allow list includes a line which reads "192. EXCEPT 192.255.255.6," then all IP address that begin with "192." will be allowed; except 192.255.255.6 (providing that this address appears in the Deny list.)

**ALL:**

The ALL wild card indicates that all IP Addresses should be allowed or denied. When ALL is included in the Allow list, all IP addresses will be allowed to connect; conversely, if ALL is included in the Deny list, all IP Addresses will be denied (except for IP addresses listed in the Allow list.)

For example, if the Deny list includes a line which reads "ALL EXCEPT 168.255.192.192," then all IP addresses except 168.255.192.192 will be denied (except for IP addresses that are listed in the Allow list.)

**Net/Mask Pairs:**

An expression of the form "n.n.n.n/m.m.m.m" is interpreted as a "net/mask" pair. A host address is matched if "net" is equal to the bitwise AND of the address and the "mask."

For example, the net/mask pattern "131.155.72.0/255.255.254.0" matches every address in the range "131.155.72.0" through "131.155.73.255."

### 5.7.4.3. IP Security Examples

1. **Mostly Closed:** Access is denied by default and the only clients allowed, are those explicitly listed in the Allow list. To deny access to all clients except 192.255.255.192 and 168.112.112.05, the Allow and Deny lists would be defined as follows:
  - Allow List:
    1. 192.255.255.192
    2. 168.112.112.05
  - Deny List:
    1. ALL
2. **Mostly Open:** Access is granted by default, and the only clients denied access, are those explicitly listed in the Deny list, and as exceptions in the Allow list. To allow access to all clients except 192.255.255.192 and 168.112.112.05, the Allow and Deny lists would be defined as follows:
  - Allow List:
    1. ALL EXCEPT 192.255.255.192, 168.112.112.05
  - Deny List:
    1. 192.255.255.192, 168.112.112.05

#### Notes:

- When defining a line in the Allow or Deny list that includes several IP addresses, each individual address is separated by either a space, a comma, or a comma and a space as shown in Example 2 above.
- Take care when using the "ALL" wild card. When ALL is included in the Allow list, it should always include an EXCEPT operator in order to allow the unit to proceed to the Deny list and determine any addresses you wish to deny.



|                                                                                                                                                                                                          |                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| COPY PORT PARAMETERS:                                                                                                                                                                                    |                                                                                                                                       |
| <b>COMMUNICATION SETTING</b><br>1. Baud Rate:<br>2. Bits/Parity:<br>3. Stop Bits:<br>4. Handshake:                                                                                                       | <b>PORT MODE PARAMETERS</b><br>21. Port Name:<br>22. Port Mode:<br>23. DTR Output:<br>24. Buffer Params: ---<br>25. Modem Params: --- |
| <b>GENERAL PARAMETERS</b><br>11. Supervisor Mode:<br>12. Logoff Char:<br>13. Sequence Disc:<br>14. Inact Timeout:<br>15. Command Echo:<br>16. Accept Break:                                              | <b>NETWORK SERVICES</b><br>31. Direct Connect:<br><br>32. Syslog: ---<br>33. SNMP Trap Lv: ---                                        |
| Enter: #<CR> to define parameter.<br>Port 1 and internal modem port restricted values NOT changed,<br>-<CR> to remove all values set, X<CR> to exit WITHOUT copy,<br><ESC> to copy to ports and exit ... |                                                                                                                                       |

Figure 5.18: The Copy Port Parameters Menu

## 5.8. Copying Parameters to Several RS-232 Ports (Text Interface Only)

When the /CP command (Copy Port Parameters) is invoked, the unit will display a menu which allows you to select parameters, and copy them to all or several RS-232 ports. The Copy Port Parameters menu can set all parameters for the specified port(s), or define only a select group of parameters for a specific group of ports.

### Notes:

- The /CP command is not available via the Web Browser Interface.
- The /CP command will *not* copy parameters to the Network Port.
- The /CP command is only available to accounts and ports that permit Supervisor commands.
- The /CP command cannot be used to set Port 1 to Passive or Buffer Mode, or to disable the Supervisor Mode at Port 1.

To copy parameters to all or several RS-232 ports, proceed as follows:

1. Use the Text Interface to enter command mode via an account and port that permit access to Supervisor commands.

2. Invoke the **/CP** command at the command prompt; the menu shown in Figure 5.18 will be displayed. The following options are available:
  - a) **Copy to All Ports:** Type **/CP [Enter]**.
  - b) **Copy to a Range of Ports:** Type **/CP m-n [Enter]**. Where **m** and **n** are port numbers that specify the desired range. For example, to copy parameters to ports 3 through 7, type **/CP 3-7** and press **[Enter]**.
  - c) **Copy to Several Ports:** Type **/CP m,n,x [Enter]**. Where **m**, **n** and **x** are the numbers of the desired ports. For example, to copy parameters to ports 3, 5, and 7, type **/CP 3,5,7 [Enter]**.
  - d) **Combination:** To invoke the **/CP** command in a manner where a range of ports is specified, along with several other ports outside the range, type **/CP m,n,x-z [Enter]**. Where **m**, **n**, **x**, and **z** are port numbers. For example to copy parameters to ports 3 and 5 *plus* ports 7 through 9, type **/CP 3,5,7-9 [Enter]**.
3. **Selecting Parameters:** To select parameters to be copied, key in the number for the desired parameter, press **[Enter]**, then follow the instructions in the submenu.

**Note:** The **/CP** command will only copy the parameters currently displayed by the Copy Port Parameters menu.
4. **Clear Menu:** After defining several parameters, if you wish to clear the **/CP** menu and start again, type **-** (dash) and press **[Enter]**, the menu will be reset.
5. **Exit Without Copy:** To exit from the Copy Parameters menu *without* copying selected parameters, type **x [Enter]**. The SCM will return to the command prompt.
6. **Copy Parameters:** When you have finished selecting parameters, press **[Esc]** to copy the selected parameters.

## **5.9. Save User Selected Parameters**

---

Although this step is optional, it is strongly recommended to save all user-defined parameters to an ASCII file as described in Section 11. This will allow quick recovery in the event of accidental deletion or reconfiguration of port parameters.



# 6. The Status Screens

The Status Screens display connection status and communication parameters for the RS232 ports and the Network Port. There are four different status screens; The Port Status Screen (/S), the Port Diagnostics Screen (/SD), the Network Status Screen (/SN), and the Port Parameters Screens (/W).

**Note:** The status screens discussed in this section are only available via the Text Interface. The status screens cannot be accessed via the Web Browser Interface.

## 6.1. The Port Status Screen (/S)

The Port Status Screen lists the general status of the SCM's sixteen RS-232 ports. To display the Port Status Screen, access the Text Interface command mode and type `/S [Enter]`, the screen will appear as shown in Figure 6.1.

Note that the screen format will vary, depending upon whether the user account permits or denies access to Supervisor commands. If the username entered at login does not allow Supervisor commands, then the Port Status Screen will only display the status of the ports allowed by that account.

PORT STATUS:  
Site ID: (undefined)02/12/2007 12:09:10 UTC (GMT+0000)

| PORT | NAME             | USERNAME | STATUS | MODE   | BUFFER COUNT |
|------|------------------|----------|--------|--------|--------------|
| 01   | Local_PC         |          | Free   | Any    | 0            |
| 02   | Local_Terminal   |          | Free   | Any    | 0            |
| 03   | FTM_Modem        |          | Free   | Any    | 0            |
| 04   | Undefined        |          | Free   | Pass   | 0            |
| 05   | DSL_Router       |          | Free   | Pass   | 0            |
| 06   | (undefined)      |          | Free   | Pass   | 0            |
| 07   | Cisco_2900       |          | Free   | Pass   | 0            |
| 08   | Cisco_2500       |          | Free   | Pass   | 0            |
| 09   | Sun_Netra_t1     |          | Free   | Buffer | 1176         |
| 10   | NPS_Reboot_Unit  |          | Free   | Pass   | 0            |
| 11   | Paradyne_DSU     |          | Free   | Pass   | 0            |
| 12   | (undefined)      |          | Free   | Pass   | 0            |
| 13   | (undefined)      |          | Free   | Pass   | 0            |
| 14   | (undefined)      |          | Free   | Pass   | 0            |
| 15   | File_txt_Any     |          | Free   | Any    | 0            |
| 16   | File_txt_Passive |          | Free   | Pass   | 0            |

Enter /H for command menu.

Figure 6.1: Port Status Screen (Sample Data Shown)

The Port Status Screen lists the following items:

- **Port:** The Port Number.
- **Name:** The user-defined name for each port.
- **Username:** The username that was entered in order to access command mode via this port.
- **Status:** The connect status of each port.
  - If the port is connected to an RS232 port, this column will list the number of the other SCM port in "c-**nn**" format, where "nn" is the number of the SCM port connected to this port (for example, "**C-07**".)
  - If the connected port is listed as "**Nn**" (where "**n**" is a number), this indicates that the SCM RS232 port is connected to the Network port. The numbers indicate which of the available Telnet sessions is being used (for example, "**C-N5**".)
- **Mode:** The user-selected Port Mode.
- **Buffer Count:** The amount of data (in bytes) stored in the buffer for this port.

## 6.2. The Port Diagnostics Screen (/SD)

---

The Port Diagnostics Screen provides more detailed information about each port. To display the Port Diagnostics Screen, access the Text Interface command mode and type **/SD** **[Enter]**, the screen will appear as shown in Figure 6.2.

Note that the screen format will vary, depending upon whether your account permits or denies access to Supervisor commands. If the username entered at login does not allow Supervisor commands, then the Port Diagnostics Screen will only display the status of the ports allowed by that account. Ports that are not assigned to the account will not be displayed.

The Port Diagnostics Screen lists the following items:

- **Port:** The Port Number. If this column contains a plus sign (+) next to the port number, this indicates that the port is allowed to invoke Supervisor commands, providing the user account allows access to these commands.
- **Name:** The user-defined name for each port.

| PORT DIAGNOSTICS:          |             |        |      |     |                                    |      |     |     |  |
|----------------------------|-------------|--------|------|-----|------------------------------------|------|-----|-----|--|
| Site ID: (undefined)       |             |        |      |     | 02/12/2007 06:44:19 GMT (GMT+0000) |      |     |     |  |
| PORT                       | NAME        | STATUS | BAUD | COM | HS                                 | MODE | BUF | CTS |  |
| 01                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Any  | 0   | L   |  |
| 02                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Any  | 0   | L   |  |
| 03                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 04                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 05                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 06                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 07                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 08                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 09                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 10                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 11                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 12                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 13                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 14                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 15                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| 16                         | (undefined) | Free   | 9600 | 8N1 | RTS                                | Pass | 0   | L   |  |
| Enter /H for command menu. |             |        |      |     |                                    |      |     |     |  |
| SCM>                       |             |        |      |     |                                    |      |     |     |  |

Figure 6.2: Port Diagnostics Screen

- **Status:** The connect status for each port.
  - When the port is connected, this column will list the number of the other port connected to this port. If the column contains an asterisk, this indicates the port has accessed command mode.
  - If the connected port is listed as "**Nn**" (where "**n**" is a number), this indicates that the RS232 port is connected to the Network port. The numbers indicate which of the available Telnet sessions is being used (for example, "**C-06**".)
- **Baud:** The baud rate selected for each port.
- **COM:** The Data Bits, Parity, and Stop Bits selected for each port. For example, "8N1" indicates Eight data bits, No parity, and One stop bit.
- **HS:** The handshaking (flow control) mode for each port.
- **Mode:** The user-selected Port Mode.
- **BUF:** The amount of data (in bytes) currently stored in the buffer for this port.
- **CTS:** The High/Low status of the CTS line at the RS232 interface.

```

NETWORK STATUS:                                MAC Address: 00-10-ec-80-92-dd

```

| PORT TCP | PORT STATUS | USERNAME        | PORT TCP | PORT STATUS | USERNAME |  |
|----------|-------------|-----------------|----------|-------------|----------|--|
| -----    |             |                 |          |             |          |  |
| N1       |             | 23 Active super | N17      |             | Free     |  |
| N2       |             | Free            | N18      |             | Free     |  |
| N3       |             | Free            | N19      |             | Free     |  |
| N4       |             | Free            | N20      |             | Free     |  |
| N5       |             | Free            | N21      |             | Free     |  |
| N6       |             | Free            | N22      |             | Free     |  |
| N7       |             | Free            | N23      |             | Free     |  |
| N8       |             | Free            | N24      |             | Free     |  |
| N9       |             | Free            | N25      |             | Free     |  |
| N10      |             | Free            | N26      |             | Free     |  |
| N11      |             | Free            | N27      |             | Free     |  |
| N12      |             | Free            | N28      |             | Free     |  |
| N13      |             | Free            | N29      |             | Free     |  |
| N14      |             | Free            | N30      |             | Free     |  |
| N15      |             | Free            | N31      |             | Free     |  |
| N16      |             | Free            | N32      |             | Free     |  |
| -----    |             |                 |          |             |          |  |

```

Enter <CR> to show more, <ESC> to quit...

```

Figure 6.3: Network Status Screen

### 6.3. The Network Status Screen (/SN)

This screen lists current conditions for the Network Port. To display the Network Status Screen, type **/SN** and press **[Enter]**. The Network Status Screen is only available when you have logged in using an account and port that permit Supervisor commands. Note that the SCM will allow up to sixteen simultaneous inbound Telnet connections.

As shown in Figure 6.3, the Network Status Screen lists the following information:

**Note:** When the Network Status Screen is displayed, the screen will initially show the first 32 Network Ports. Press **[Enter]** to display the remaining Network Ports.

- **MAC Address:** The permanent physical address assigned to the Network Card.
- **Port:** The Network Port Number for each logical TCP Port. For more information, please refer to Section 8.1.



- **TCP Port:** The logical TCP port number to which each Telnet session is connected.
  - Normally, when a Telnet session has been established, this field will list port number 23.
  - If the Telnet Direct Connect function has been employed to connect to an SCM port using standard Telnet protocol (with password), this column will list the virtual TCP port number, ranging from 2101 to 2116.
  - If the Telnet Direct Connect function has been employed to connect to an SCM port using standard Telnet protocol (*without* password), this column will list the virtual TCP port number, ranging from 2301 to 2316.
  - If the Telnet Direct Connect function has been employed to connect to an SCM port using SSH protocol, this column will list the virtual TCP port number, ranging from 2201 to 2216.
- **Status:** The status for each TCP port.
  - If the Status Column reads "Active," this indicates the port has accessed command mode.
  - If this Telnet session is connected to an RS232 Port, this column will read "C-nn," where "nn" indicates the connected port for each Telnet session.
- **Username:** The username that was entered at this port in order to access command mode.

```
PORT PARAMETERS #03:

COMMUNICATION SETTING
1. Baud Rate:          9600
2. Bits/Parity:        8-None
3. Stop Bits:         1
4. Handshake:          RTS/CTS

PORT MODE PARAMETERS
21. Port Name:
22. Port Mode:         Passive
23. DTR Output:        Pulse
24. Buffer Params:     ---
25. Modem Params:      ---

GENERAL PARAMETERS
11. Supervisor Mode:   Permit
12. Logoff Char:       ^X
13. Sequence Disc:     One Char
14. Inact Timeout:     Off
15. Command Echo:      On
16. Accept Break:      On

NETWORK SERVICES
31. Direct Connect:    Off
Telnet Port:          ---
SSH Port:             ---
Raw Port:             ---
32. Syslog:            ---
33. SNMP Trap Lv:     ---

SCM>
```

Figure 6.4: Port Parameters Screen (RS232 Port Shown)

```
NETWORK PARAMETERS:

COMMUNICATION SETTING
1. IP Address:         207.212.30.80
2. Subnet Mask:        255.255.255.0
3. Gateway Addr:       207.212.30.1
4. DHCP:               Off
5. IP Security:        Off
6. Static Route:       Off

SERVERS AND CLIENTS
21. Telnet Access:     On
22. SSH Access:        On
23. Web Access:        Off
24. SYSLOG IP addr:    (undefined)
25. SNMP Access:       Off
26. SNMP Trap:         Off
27. TACACS:            Off
28. RADIUS:            Off
29. PING Access:       On
30. Raw Socket Access: Off

GENERAL PARAMETERS
11. Supervisor Mode:   Permit
12. Logoff Char:       ^X
13. Sequence Disc:     One Char
14. Inact Timeout:     5 Min
15. Command Echo:      On
16. Accept Break:      On

SCM>
```

Figure 6.5: Port Parameters Screen (Network Port Shown)

## 6.4. The Port Parameters Screens (/W)

The /W (Who) command displays more detailed information about an individual SCM port. Rather than listing general connection information for all ports, the Port Parameters screen lists all defined parameters for a specific port.

The Port Parameters Screens are available to accounts that permit Supervisor commands and accounts that do not permit Supervisor commands. Note however, that if your account that does not permit Supervisor commands, the SCM will only display information for the port from which you have logged in.

The /W command can be applied to either an RS232 Port or the Network Port. Figure 6.4 shows the screen displayed when the /W command is applied to an RS232 Port, and Figure 6.5 shows the screen displayed when an account that permits Supervisor commands applies the /W command to the Network Port.

The /W command uses the following format:

**/W *xx* [Enter]**

Where ***xx*** is the desired port number. If the letter "N" is entered in place of a port number, the /W command will display parameters for the Network Port.

**Note:** When command mode is accessed via the Network Port using an account that does not permit Supervisor commands, the /W command will only display the Sequence Disconnect, Logoff Character, and the status of the Accept Break item.



## 7. Operation

---

This section discusses the procedures for connecting and disconnecting ports, and describes the various port modes.

**Note:** The Web Browser Interface cannot be used to connect or disconnect ports. In order to connect or disconnect ports, you must access command mode via the Text Interface.

### 7.1. Any-to-Any Mode

---

Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer, or Modem Mode ports by accessing command mode via the Text Interface and issuing the /C Command. All ports can be configured for Any-to-Any Mode, and it is also the default mode for Ports 1 and 2.

#### 7.1.1. Port Connection and Disconnection

The SCM allows communication between devices without the requirement that both ports use the same communication parameters.

##### 7.1.1.1. Connecting Ports

Two different types of connections can be made between SCM ports; Resident Connections and Third Party Connections.

- **Resident Connections:** Your resident port issues a /C command to connect to a second port. For example, Port 4 issues the /C command to connect to Port 5.
- **Third Party Connections:** (Supervisor Only) Your resident port issues a /C command to create a connection between two *other* ports. For example, Port 1 is your resident port, and Port 1 issues a command to connect Port 2 to Port 3.

#### **Notes:**

- Third Party Connections can only be initiated by accounts and ports that permit Supervisor commands.
- The RS232 Ports cannot employ the /C command to initiate a connection to the Network Port.
- If your account does not permit Supervisor commands, you will only be able to connect to ports allowed by your account. Accounts with Supervisor access are allowed to connect to all RS232 ports.

To Connect ports, proceed as follows:

1. Access command mode via the Text Interface.
2. Invoke the /C command to connect the desired ports.
  - a) **Resident Connect:** To connect your resident port to another port, type `/C xx [Enter]`. Where **xx** is the number or name of the port you want to connect. The SCM will display the numbers of the connected ports, along with the command required in order to disconnect the two ports.

**Example:** To connect your resident port to Port 8, type `/C 8 [Enter]`.

- b) **Third Party Connect:** (Supervisors Only) To connect any two ports (other than your resident port), type `/C xx yy [Enter]`. Where **xx** and **yy** are two port names or numbers. The SCM will display the numbers of the two connected ports.

**Example:** To connect Port 5 to Port 6, access command mode at a third port that permits Supervisor commands (using an account that also permits supervisor commands), and invoke the following command: `/C 5 6 [Enter]`.

### Notes:

- **Resident Connections:** RS232 Ports are *not* allowed to initiate a Resident Connection to the Network Port.
- **Third Party Connections:** RS232 Ports are not allowed to connect another port to the network port. For example, Port 1 is not allowed to connect Port 3 to the Network Port.

When the /C command specifies the port name, it is only necessary to enter enough letters to differentiate the desired port from other ports. Type an asterisk (\*) to represent the remaining characters in the port name. For example, to connect your resident port to a port named "SALES", the connect command can be invoked as `/C S*`, providing no other port names begin with the letter "S".

### 7.1.1.2. Disconnecting Ports

There are three different methods for disconnecting ports, the Resident Disconnect, the Third Party Disconnect, and the No Activity Timeout. Providing the Timeout feature is enabled, a No Activity Timeout will disconnect resident ports or third party ports.

**Note:** The "DTR Output" option in the Port Parameters menu determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed and then held high.

1. **Resident Disconnect:** Disconnects your resident port from another port. For example, if you are communicating via Port 3, and Port 3 is connected to Port 4, a Resident Disconnect is used to disassociate the two ports. The SCM offers two different disconnect command formats; the One Character Format and the Three Character Format (for more information, please refer to Section 5.7.2.):

**Note:** The Resident Disconnect methods discussed here *cannot* be used to terminate a Telnet Direct Connection. For more information, please refer to Section 8.3.4.

- a) **One Character (Default):** Enter the logoff character once (Default = [Ctrl] plus [X]). It is not necessary to enter a carriage return before or after the logoff character.
  - b) **Three Characters:** Uses the "[Enter]LLL[Enter]" format, where **L** is the logoff character. For example, if the logoff character is "+", then the disconnect sequence is [Enter]+++[Enter].
  - c) If the default disconnect command is not compatible with your application, both the command format and logoff character can be redefined via the Port Configuration menus, as described in Section 5.7.2.
2. **Third Party Disconnect:** (Supervisors Only) The /D command is issued from your resident port to disconnect two other ports. For example, if your Resident Port is Port 1, a Third Party Disconnect is used to disconnect Ports 3 and 4.

**Note:** The Third Party Disconnect method can be used to terminate a Telnet Direct Connection. For more information, please refer to Section 8.3.4.

- a) The /D command uses the format: /D **xx** **xx** [Enter], where **xx** and **xx** are the numbers of the ports you wish to disconnect.

- b) The /D (Disconnect) command can only be invoked by accounts and ports that permit Supervisor commands.
- c) The /D command can specify both connected ports, or either of the two ports. For example, if Port 1 is your resident port, any of the following commands can be used to disconnect Port 3 from Port 4:

/D 3 4 [Enter]

or

/D 3 [Enter]

or

/D 4 [Enter]

- d) The /D command can also disconnect a remote user from the Network Port. This is useful in cases where a user has unsuccessfully disconnected via Telnet, and you can't wait for the SCM to timeout in order to free up the TCP port. To disconnect a TCP port, type /D **Nn** and then press [Enter]. Where **Nn** is one of the SCM's logical TCP ports (e.g. /D **N2** [Enter]).

3. **No Activity Timeout:** Providing the Timeout feature is enabled at either connected port, the No Activity Timeout can disconnect Resident Ports, or Third Party Ports.

**Note:** The No Activity Timeout also applies to Telnet Direct Connections. For more information, please refer to Section 8.3.

- a) **RS232 Ports:** To select the timeout period for RS232 Ports, access the Port Configuration Menu for the desired port as described in Section 5.7.2.
- b) **Network Port:** To select the timeout period for the Network Port, access the Network Port Configuration Menu as described in Section 5.7.3.
- c) When the Timeout Feature is enabled, the port will automatically disconnect if no data is received during the defined Timeout Period.

#### **Notes:**

- When two connected ports time out, both ports will exit command mode after disconnecting.
- The Timeout value also applies to unconnected ports that are left in command mode. When an unconnected port is left in command mode, and no additional activity is detected, the port will automatically exit command mode when its timeout value elapses.



### 7.1.2. Defining Hunt Groups

A Hunt Group creates a situation where the SCM will scan a group of similarly named ports and connect to the first available port in the group. Hunt Groups are created by assigning identical or similar names to two or more ports. Hunt Groups can be defined using Any-to-Any, Passive, Buffer, or Modem Mode Ports. Note that the Network Port *cannot* be included in Hunt Groups.

1. Access command mode using a port and account that permit Supervisor commands.
2. Access the Port Configuration Menu for the desired Port(s) as described in Section 5.7.2.
3. From the Port Configuration Menu, define the Port Name.
4. Repeat steps 2 and 3 to assign identical names to the other ports in the Hunt Group. For example, a series of ports in a group could all be named "SERVER".
5. To connect to the next available port in the hunt group, invoke the /C command using the port name to specify the desired group. For example, /C **SERVER** [Enter].
6. Your port will be connected to the first available port in the group. If all ports are presently connected, the SCM will respond with the "BUSY" message.
7. It is only necessary to enter enough letters of the port name to differentiate Hunt Group ports from other ports. Type an asterisk (\*) to represent the remaining characters in the name. For example, to connect to the first available port in a group of ports named "SALES1", "SALES2", and "SALES3", the connect command can be invoked as /C **S\*** [Enter], providing no other port names begin with the letter "S".

#### Notes:

- If the Hunt Group method is used by a port or account that does not permit Supervisor commands, the /C command will only connect to the ports allowed by that user account.
- Hunt Group port names must be unique. Otherwise, ports with similar names will also be included in the Hunt Group.

### **Hunt Group Example 1:**

1. Ports 1 and 2 are Modem Mode ports, and modems are installed at both ports. Port 1 is named "MODEM1" and Port 2 is named "MODEM2".
2. Your resident port is Port 4. To connect to the first available Modem, type **/C MODEM\* [Enter]**.

### **Hunt Group Example 2:**

1. Ports 3, 4, and 5 are Any-to-Any Mode ports. All three ports are named "SERVER".
2. Your resident port is Port 1. If you want to connect Port 2 to the first available server, type **/C 2 SERVER [Enter]**.

## **7.2. Passive Mode**

---

Passive Mode Ports function the same as Any-to-Any Mode Ports, but do not allow access to command mode. A Passive Mode Port can communicate with other ports, but cannot enter command mode, and therefore cannot redefine parameters, display status, or connect or disconnect ports. The Passive Mode is the default at Ports 2 through 16.

Passive Mode Ports can be connected by accessing command mode from a free Any-to-Any or Modem Mode Port, and invoking the Third Party Connect or Resident Connect Command as described in Section 7.1.1. Passive Mode ports will not buffer data, except during baud rate conversion.

**Note:** In order to ensure Supervisor access to important command functions, the Passive Mode is not available to Port 1 (the SetUp Port.)

---

## 7.3. Buffer Mode

---

The Buffer Mode allows collection of data from various devices without the requirement that all devices use the same communication parameters (e.g. baud rate, parity, etc.). In addition, Buffer Mode ports can also be configured to support the SYSLOG and SNMP Trap functions, as described in Sections 9 and 10.

### Notes:

- Buffer Mode Ports cannot access command mode.
- Buffer Mode is not available to Port 1 (the SetUp Port) or the Network Port.

### 7.3.1. Reading Data from Buffer Mode Ports

To check port buffers for stored data, access command mode via the text interface, using an account and port that permit Supervisor commands, and type **/S [Enter]** to display the Port Status Screen. The "Buffer Count" column in the Port Status Screen indicates how much data is currently being stored for each port.

To retrieve data from buffer memory, go to a free Any-to-Any or Modem Mode Port, then issue the **/R** command using the following format:  
**/R xx [Enter]**. Where **xx** is the number of the port buffer to be read.

### Notes:

- In order to read data from a given port, your account must allow access to that port.
- When the **/R** command is invoked, the counter for the SNMP Trap function will also be reset.

If the buffer contains data, the SCM will display a prompt that offers the following options:

- **Display One Screen:** To send data one screen at a time, press **[Enter]**. Each time **[Enter]** is pressed, the next screen is sent.
- **Display All Data:** To send all data currently stored in the buffer, type **1** and press **[Enter]**.
- **Erase Data on Screen:** To erase the data currently displayed on-screen, type **2** and press **[Enter]**.
- **Erase all Data:** (Supervisor Only) To erase all data currently stored in the buffer, type **3** and press **[Enter]**.
- **Exit:** To exit from Read Buffer mode, press **[Esc]**.

**Note:** Only one user can read from a port buffer at a time. If a second user attempts to read from a port that is already being read, an error message will be sent.

To clear data from any port buffer (with or without reading it first), access command mode via the text interface, using an account and port that permit Supervisor commands, then issue the /E (Erase Buffer) command using the following format:

**/E xx [Enter]**

Where **xx** is the number of the port buffer to be cleared.

**Note:** The /E command cannot erase data from a port buffer that is currently being read by another port.

### **7.3.2. Port Buffers**

The Status Screen lists the amount of Buffer Memory currently used by each port. The SCM uses buffer memory in two different ways, depending on the user-selected port mode.

- **Any-to-Any, Passive, and Modem Mode Ports:** When two ports are communicating at dissimilar baud rates, the buffer memory prevents data overflow at the slower port.
- **Buffer Mode Ports:** Stores data received from connected devices. The user issues a Read Buffer command (/R) from an Any-to-Any or Modem Mode port to retrieve data.

If the Status Screen indicates an accumulation of data, the /E (Erase Buffer) command can be invoked to clear the buffer.

**Note:** When a Buffer Mode port is reconfigured as an Any-to-Any, Passive, or Modem Mode port, any data stored in the buffer prior to changing the port mode will be lost.

---

## 7.4. Modem Mode

---

The Modem Mode provides features specifically related to modem communication. A Modem Mode Port can perform all functions normally available in Any-to-Any Mode. The Modem Mode is available to all SCM ports except the Network Port.

When Modem Mode is selected, the Port Configuration menu will display three additional prompts, which allow you to re-define the modem reset string, initialization string, and hang-up string.

When a call is received, the unit will prompt the caller to enter a username and password. The SCM allows three attempts to enter a valid username and password. If a valid username and password is not entered within three attempts, or if the user does not respond to the login prompt within 30 seconds, the modem will disconnect.

### Notes:

- When a Modem Mode port exits command mode, or the DCD line is lost while command mode is active, the SCM will pulse DTR to the modem. The unit will then send the user-defined modem command strings to make certain the modem is properly disconnected and reinitialized.
- When an external modem is installed at an SCM port, other ports can use the modem for calling out. To call out, invoke the /C command to connect to the port, then access the modem as you normally would.
- If desired, the Invalid Access Lockout feature can provide additional security for Modem Mode ports. When properly configured, the Invalid Access Lockout will automatically shut down a port whenever that port exceeds the user defined number of invalid access attempts. For more information, please refer to Section 5.4.1.



## 8. Telnet & SSH Functions

---

### 8.1. Network Port Numbers

---

Whenever an inbound Telnet or SSH session connects to an SCM RS232 Port, the Port Status Screen and Port Diagnostics Screen will indicate that the RS232 port is presently connected to Port "**Nn**" (where "**N**" indicates a network connection, and "**n**" is a number that lists the logical Network Port being used; for example, "**N7**".) This "**Nn**" number is referred to as the logical Network Port Number.

### 8.2. SSH Encryption

---

In addition to standard Telnet protocol, the SCM also supports SSH connections, which provide secure, encrypted access via network. In order to communicate with the SCM using SSH protocol, your network node must include an appropriate SSH client.

Note that when the /K (Get Key) command is invoked, the SCM can also provide you with a public SSH key, which can be used to streamline connection to the SCM when using SSH protocol.

Although you can easily establish an SSH connection to the unit *without* the public key, the public key provides validation for the SCM, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the SCM is not a recognized user when the client attempts to establish a connection.

The /K command uses the following format:

**/K <k> [Enter]**

Where **k** is an argument that determines which type of public key will be displayed, and the **k** argument offers the following options:

1. SSH1
2. SSH2 RSA
3. SSH2 DSA

For example, to obtain the public SSH key for an SSH2 RSA client, type **/K 2** and then press **[Enter]**.

**Note:** Although the SCM does not support SSH1, the /K 1 command will still return a key for SSH1.

## 8.3. The Direct Connect Feature

---

The Direct Connect feature allows you to initiate a Telnet session with the SCM and make an immediate connection to a specific RS232 Port of your choice, without first being presented with the command interface. This allows you to connect to a TCP port that is mapped directly to one of the SCM RS232 Ports.

Direct Connect employs unique, pre-assigned TCP port numbers for each RS232 Port. The user connects to the port of choice by including the associated TCP port number in the Telnet or SSH connect command line.

The Direct Connect feature can be individually configured at each RS232 Port and can be used to connect to Any-to-Any, Passive, Buffer, or Modem Mode ports.

### 8.3.1. Standard Telnet Protocol and SSH

The Direct Connect feature allows communication using either Standard Telnet Protocol or SSH encryption; the TCP Port number included in the Telnet connect command determines which protocol is used. When Standard Telnet Protocol is used, the SCM will respond to all IACs.

When configuring a port to allow Direct Connections using SSH protocol, note that the Direct Connect option (Port Configuration Menu, Item 13), must be set to "On - Password" as described in Section 8.3.2.

### 8.3.2. Configuration

The Direct Connect Function is configured on a per port basis using the Port Configuration Menus (/P nn), item 13, "Direct Connect". The following options are available:

1. **Direct Connect OFF:** Direct Connect disabled at this port. (Default)
2. **Direct Connect ON - NO PASSWORD:** The Direct Connect feature is enabled at this port, but no password is required in order to connect to the port.
  - a) When the Telnet connection is established, the user is immediately connected directly to the specified port, and the client is notified at the TCP level.
  - b) This option is intended for situations where security is provided by the attached device.



3. **Direct Connect ON - PASSWORD:** The Direct Connect feature is enabled at this port, but a password must be entered before a Direct Connection is established.
  - a) Upon login, the SCM will prompt for a username and password. If a valid username/password is entered, the SCM will return a message which confirms the connection and lists the name and number of the port (providing the user account allows access to the target port.)
  - b) If a valid username / password is not entered in 30 seconds or three attempts, the port will timeout and disconnect.

**Notes:**

- If you intend to use SSH to establish direct connections to the SCM, the "Direct Connect ON - PASSWORD" option must be selected.
- If Supervisor commands are disabled at the Network Port, then accounts that permit Supervisor commands will not be able to initiate a Direct Connection.
- If Supervisor commands are enabled at the Network Port, then accounts with Supervisor access and accounts *without* Supervisor access will both be allowed to establish Direct Connections.
- If your user account does not permit access to the target port, the connection will be refused.

### **8.3.3. Connecting to an RS232 Port using Direct Connect**

Direct Connect TCP port numbers are as follows:

1. **Standard Telnet Direct Connection (with Password):** TCP port numbers 2101 through 2116 correspond to RS232 Ports 1 through 16 respectively.
2. **Standard Telnet Direct Connection (without Password):** TCP port numbers 2301 through 2316 correspond to RS232 Ports 1 through 16 respectively.
3. **SSH Direct Connection:** TCP port numbers 2201 through 2216 correspond to RS232 Ports 1 through 16 respectively.

When establishing a Direct Connection, the correct TCP port number must be used. If conditions are acceptable (e.g. Target Port must be free and properly configured), an immediate connection will be made, with one possible exception; password entry may first be required depending on configuration settings.

**Note:** When a Direct Connect attempt fails because the Port is busy, the call is rejected at the TCP level.

### Connection Example

1. Assume that Port 8 is configured as described in Section 8.3.2. If the SCM's IP address is "1.2.3.4", and you wish to establish a standard Telnet protocol connection with port 8 (TCP Port Number 2108), then on a UNIX system, the connect command would be invoked as follows:

```
$ telnet 1.2.3.4 2108 [Enter]
```

2. The SCM will first send the site ID, Port Number, Port Name, and Telnet Port number, and then once a connection is established, the "Connected" message will be sent.

### 8.3.4. Terminating a Direct Connect Session

To terminate a Direct Connect session, use the client program's "disconnect" feature. The following will occur immediately upon a client initiated disconnect:

1. The Network port is disconnected from the RS232 Port.
2. The Network session is terminated.
3. The RS232 Port is put to sleep.

#### Notes:

- The Sequence Disconnect Command, which is defined via the Port Configuration menus, *cannot* be used to terminate a Direct Connection.
- Any SCM port that allows Supervisor commands *can* terminate a direct connection at another port by issuing the /D command as described in Section 7.1.1.
- Acknowledgment of data received by the SCM network port does not automatically indicate that the data has been completely sent out the serial port. Data may still be queued in SCM buffers. Any data queued at the time of a client initiated disconnect is discarded, and is not passed to the attached device.

## 9. The Syslog Feature

---

The Syslog feature can create time-stamped log records of each buffer event. As these event records are created, they are sent to a Syslog Daemon, located at an IP address defined via the Network Parameters menu.

### **Note:**

- The Syslog Function is only available to Buffer Mode ports.
- This option is not available to RS232 Port 1, which is reserved as a System SetUp Port, and therefore cannot be configured as a Buffer Mode Port.

### 9.1. Configuration

---

The Syslog function is individually configured for each SCM RS232 Port. If you wish to employ this feature, it must be enabled at each desired port using the Port Parameters menus. You must also set the real-time clock and calendar via the System Parameters Menu, and define the IP address for the Syslog Daemon via the Network Port Configuration menu.

To configure the Syslog function, please proceed as follows:

1. Access command mode. Note that the following configuration menus are only available to accounts and ports that permit Supervisor commands.
2. **System Parameters Menu:** Type **/F [Enter]** to access the System Parameters Menu. Set the following parameters:
  - a) **Set Clock and Calendar:** Use the Systems Parameters menu to set the Real Time Clock and Calendar and/or configure and enable the NTP server feature. If desired, the SCM can time stamp each Syslog message that is sent, as described in Step 4 below.

3. **Port Parameters Menu:** Access the Port Parameters Menu for the desired port as described in Section 5.7.2, and then set the following parameters:
  - a) **Port Mode:** Set the Port Mode to "Buffer."
  - b) **Syslog Function:** Enable the Syslog Function. The Syslog Function allows you to select either "On - Not Connected" (messages are only sent when a user is *not* connected to the Buffer port) or "On - Always" (all captured data is sent, whether a user is connected to the Buffer port or not.)
  - c) **Syslog Facility and Level:** If desired, set the Facility and Level (priority) for messages sent by this port.
4. **Network Parameters Menu:** Access the Network Parameters Menu as described in Section 5.7.3, then set the following parameters:
  - a) **Syslog IP Address:** Determine the IP address for the device that will run the Syslog Daemon, then use the Network Port Configuration menu to define the IP Address for the Syslog Daemon.
  - b) **Syslog Date-Time:** If desired, you may wish to enable automatic time/date stamping of all Syslog messages generated by the SCM. This is often useful if your Syslog Daemon does not perform time/date stamping itself.
5. **Syslog Daemon:** In order to capture messages sent by the SCM, a computer must be running a Syslog Daemon (set to UDP Port 514) at the IP address specified in Step 4 above.

---

## 9.2. Criteria for Generating a Syslog Message

---

Once the SCM is properly configured, Syslog messages will be generated as follows:

1. **Data Terminated by NULL Character:** Syslog will generate a message whenever a properly configured Buffer Mode Port receives data or text terminated by a NULL character (0x00). The message sent to the Syslog Daemon will contain header information and the event (buffered data or text) captured by the SCM. Note that the event written to the buffer port will also be retained.

If a Buffer Mode Port receives data or text that is *not* terminated by a NULL character, it will *not* be sent out as a Syslog message, but will be retained by the buffer, providing the maximum Syslog message size (described in item 2 below) is not exceeded. This prevents the SCM from sending spurious characters that do not represent actual text or data.

2. **Maximum Syslog Message Size Reached:** Syslog messages are limited to 1024 bytes (including the header). Therefore, if data or text in the buffer exceeds this limit, the queued message will be sent immediately, and the rest of the data will be accumulated and forwarded in another, subsequent message; either when a NULL is detected, or when the accumulated data (plus header) again reaches 1024 bytes.
3. **Audit Log:** If the System Parameters menu has been used to set the Audit Log feature for the "On - with Syslog" option, then a Syslog message will be sent each time that an Audit Log record is generated. Audit Log records will be generated whenever a user connects or disconnects from a port, whenever a user enters or exits from command mode, and whenever a user session is disconnected due to a time out.
4. The Port Parameters Menus are used to enable/disable the Syslog feature at each port, and also to determine whether or not messages will be sent while a user is connected to the port. As described in Section 5.7.2, the Syslog feature can be set to either send all information captured by the port, or to stop sending messages when a user is connected to that port.

### 9.3. Testing Syslog Configuration

---

After you have configured the SCM as described in Section 9.1, the /TEST command can be used to make certain that the function is properly set up. To test the Syslog function, type **/TEST**, press **[Enter]**, then follow the instructions in the resulting submenu.

The SCM will attempt to send a test Syslog message, using the current Syslog configuration. If the test message is not received by your Syslog Daemon, review the procedure outlined in Section 9.1 to make certain the SCM and the Syslog Daemon are properly configured.

## 10. SNMP Traps

---

SNMP is an acronym for "Simple Network Management Protocol". The SNMP Trap function allows Buffer Mode Ports to send a message to two different SNMP Managers, indicating the amount of data currently stored in buffer memory.

### Note:

- The SNMP Trap function is only available to Buffer Mode Ports.
- This option is not available to RS232 Port 1, which is reserved as a "System SetUp Port", and therefore, cannot be configured as a Buffer Mode Port.
- The SNMP feature cannot be configured via the SNMP Manager.
- SNMP reading ability is limited to the System Group.
- The SNMP feature includes the ability to be polled by an SNMP Manager.
- When the /R command is invoked, the counter for the SNMP Trap function will automatically be reset.

### 10.1. Configuration:

---

The SNMP Trap function is individually configurable for RS232 Ports 2 through 16. If you wish to employ this feature it must be enabled at each desired port. To configure the SNMP Trap function, proceed as follows:

1. Access command mode using an account and port that permit Supervisor commands.
2. **Port Parameters Menu:** Access the Port Parameters Menu for the desired port as described in Section 5.7.2, and then set the following parameters:
  - a) **Port Mode:** Set the Port Mode to "Buffer".
  - b) **SNMP Trap Level:** Enable the SNMP Trap function and select the byte level. The byte level determines the number of bytes the buffer must contain in order to cause an SNMP trap to be sent. Note that when the byte level is set to "0" (zero), the SNMP Trap function is disabled.

3. **Network Parameters Menu:** Access the Network Parameters Menu as described in Section 5.7.3. Set the following:
  - a) **SNMP Managers 1 and 2:** Consult your network administrator to determine the IP address(es) for the SNMP Manager(s), then use the Network Parameters menu to set the IP address for each SNMP Manager. Note that it is not necessary to define both SNMP Managers.
  - b) **SNMP Community:** Consult your network administrator, and then use the Network Parameters menu to set the SNMP Community.
  - c) **SNMP Contact:** (Optional.)
  - d) **SNMP Location:** (Optional.)

## 10.2. SNMP Trap Message

---

The trap messages which are sent to the SNMP Managers will appear as follows:

**SCM Port Buffer. SCM Site ID:** *[site id]*, **Port:** *[port number]*, *[byte level]* **byte trigger level reached.**

## 10.3. How and When SNMP Traps are Sent:

---

1. When the buffer port reaches the trigger level, SNMP Traps are immediately sent to each defined SNMP manager. SNMP uses the UDP protocol (an "unreliable" protocol). Successful manager receipt of traps are assisted by the following:
  - a) The SCM verifies that the ARP table is updated completely before sending a trap to each manager defined.
  - b) The user may choose to use the 2nd manager as a "backup" in the event that the 1st manager fails.
2. When an SNMP trap is sent to a manager for a particular port, the SCM also sets a one hour timer for that port:
  - a) If, during the hour, the buffer *never* drops below the trap level, then SNMP Traps are resent and the timer is reset.
  - b) If, during the hour, the buffer *does* drop below the trap level, the timer is immediately cleared. No more traps will be sent unless the buffer level once again exceeds the trap trigger level.



## **10.4. Testing the SNMP Trap Function**

---

After you have finished setting up the SNMP Trap function, it is recommended to test the configuration to ensure that it is working correctly. To test configuration of the SNMP Trap function, proceed as follows:

1. Configure the SNMP Trap function as described in Section 10.1.
2. Access the Text Interface command mode using an account and port that permit Supervisor commands, then invoke the `/TEST` command at the SCM command prompt. Note that the `/TEST` Command is only available in Supervisor Mode.
3. Select Item 1 or 2 to send an SNMP test trap to Manager 1 or 2, respectively. It is possible that the ARP table will not be properly setup. If this occurs a message to that effect is displayed and the SCM immediately refreshes the ARP table. Repeat steps 2 and 3 to try again.



## 11. Saving and Restoring Configuration Parameters

---

Once the SCM is properly configured, parameters can be downloaded and saved as an ASCII text file. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to automatically reconfigure the unit without the need to manually assign each parameter.

Saved parameters can also be uploaded to other SCM units, allowing rapid set-up when several units will be configured with the same parameters.

The "Save Parameters" procedure can be performed from any terminal emulation program (e.g. HyperTerminal, TeraTerm, etc.), that allows downloading of ASCII files.

**Note:** The Save and Restore features described in this section are only available via the Text Interface.

### 11.1. Sending Parameters to a File

---

1. Start your terminal emulation program (e.g. HyperTerminal) and access the Text Interface command mode using an account and port that permit Supervisor commands.
2. When the command prompt appears, type **/U** and press **[Enter]**. The SCM will prompt you to configure your terminal emulation program to receive an ASCII download.
  - a) Set your terminal emulation program to receive an ASCII download, and then specify a name for a file that will receive the saved parameters (e.g. SCM.PAR).
  - b) Disable the Line Wrap function for your terminal emulation program. This will prevent command lines from being broken in two during transmission.
3. When the terminal emulation program is ready to receive the file, return to the SCM's Save Parameter File menu, and press **[Enter]** to proceed. SCM parameters will be saved on your hard drive in the file specified in Step 2 above.

4. The SCM will send a series of ASCII command lines which specify currently selected parameters. The last line of the file should end with a `"/G-00"` command. When the download is complete, press **[Enter]** to return to the command prompt.

## 11.2. Restoring Saved Parameters

---

This section describes the procedure for using your terminal emulation program to send saved parameters to the SCM.

1. Start your terminal emulation program and access the SCM's Text Interface command mode using an account and port that permit Supervisor commands.
2. Configure your terminal emulation program to upload an ASCII text file.
3. Upload the ASCII text file with the saved SCM parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the SCM. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

**Note:** If the SCM detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.

5. If the parameter upload is successful, the SCM will send a confirmation message, and then return to the command prompt. Type `/S` and press **[Enter]**, the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

## 12. Upgrading SCM Firmware

---

When new, improved versions of the SCM firmware become available, the "Upgrade Firmware" function can be used to update the unit. Updates can be uploaded via Setup Port One, or via the Network Port.

### Notes:

- The upgrade procedure can only be performed via the Text Interface.
  - All other ports will be disabled during the firmware upgrade procedure.
  - If the upgrade includes new parameters or features not included in the previous firmware version, these new parameters will be set to their default values.
1. Obtain the update file. Firmware modifications can either be mailed to the customer on a CDR, or downloaded from WTI. Place the upgrade CDR in your disk drive or copy the file to your hard drive.
  2. Access Text Interface command mode using an account and port that permit Supervisor commands.
  3. When the command prompt appears, type **/UF** and then press **[Enter]**. The SCM will display a screen which offers the following options:
    - a) **Continue Upload and Save Parameters:** To proceed with the upgrade, while retaining user-defined parameters, type **1** and press **[Enter]**. All existing parameter settings will be restored when the upgrade is complete.
    - b) **Continue Upload and Default:** To proceed with the upgrade, and reset parameters to default settings, type **2** and press **[Enter]**. When the upgrade is complete, all parameters will be set to default values.
    - c) **Abort Upload:** To cancel the upgrade and return to the command prompt, type **3** and press **[Enter]**.

4. Set your communication program for Binary Mode, then use the program's "Send File" function to transfer the upgrade file to the SCM. Select Binary format, then specify the filename and directory location where the firmware upgrade file resides.

**Note:** Due to performance issues, WTI recommends using either TeraTerm or Hyperterminal to send the upgrade file to the SCM.

5. If the upload is successful, the SCM will load the upgrade firmware into RAM memory, and then reboot itself and break all connections.

**Note:** If you are performing the upgrade procedure via the Network Port, the SCM will break the network connection when the system is reinitialized.

- If you have selected "Continue Upload and Save Parameters", you may then reestablish a connection with the SCM using your former IP address.
  - If you have selected "Continue Upload and Default", you must then login using the SCM's default IP address (Default = 192.168.168.168.)
6. **Incomplete Upload:** If the upload is interrupted, times-out, or if the file is corrupted during transfer, the SCM will display a screen which asks for confirmation before proceeding. To proceed, type **1** and press **[Enter]**, then return to Step 4 above.
  7. **Emergency Recovery:** In the rare event that the SCM operating system becomes corrupted during installation, front panel indicators will blink, and the unit will automatically switch to Emergency Recovery Mode. Please contact WTI Customer Service for further instructions.

When firmware upgrades are available, WTI will provide the necessary files via download or mailed CDR. At that time, an updated Users Guide or addendum will also be available.

## 13. Command Reference Guide

---

### 13.1. Command Conventions

---

Most commands described in this section conform to the following conventions:

- **Text Interface:** Commands discussed in this section, can only be invoked via the Text Interface. These commands *cannot* be invoked via the Web Browser Interface.
- **Slash Character:** Most SCM commands begin with the Slash Character (/).
- **Apply Command to All Ports:** When an asterisk is entered as the argument of the /D (Disconnect) or /E commands (Erase Buffer) the command will be applied to all ports. For example, to erase all port buffers, type /E \* [Enter].
- **Port Name Wild Card:** It is not always necessary to enter the entire port name. Port names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (\*). For example, a port named "SERVER" can be specified as "S\*". Note however, that this command would also be applied to any other port name that begins with an "S".
- **Suppress "Sure?" Prompt:** When the /D (Disconnect), /E (Erase Buffer), or /I (Default) commands are invoked, the /Y option can be included in the command line to override the "Sure?" prompt. For example, to disconnect Port 8 without displaying the Sure prompt, type /D/Y 8 [Enter].
- **Enter Key:** Most commands are invoked by pressing [Enter].
- **Connected Ports:** When two ports are connected, most SCM commands will not be recognized by either of the connected ports. The only exceptions are the Resident Disconnect Sequence (Default = ^X ([Ctrl] plus [X])) and the Send Break command (^\\ ([Ctrl] plus [\\])).
- **Configuration Menus:** To exit from a configuration menu, press [Esc]. The only exception to this rule is the Copy Parameters Menu (/CP), and in that case the [Esc] key is used to confirm the copy operation.

13.2. Command Summary

| Function                      | Command Syntax                                                 | Command Availability |            |
|-------------------------------|----------------------------------------------------------------|----------------------|------------|
|                               |                                                                | Supervisor           | Non-Super. |
| Exit Command Mode             | /X [Enter]                                                     | X                    | X          |
| Help Menu                     | /H [Enter]                                                     | X                    | X          |
| Display Site ID               | /J [Enter]                                                     | X                    | X          |
| Display Port Status           | /S [Enter]                                                     | X❶❷                  | X❶         |
| Display Port Diagnostics      | /SD [Enter]                                                    | X❶                   | X❶         |
| Display Network Status        | /SN [Enter]                                                    | X❸                   |            |
| Display Port Parameters (Who) | /W [n] [Enter]                                                 | X                    | X❹         |
| Display Audit Log             | /A [search text] [Enter]                                       | X                    |            |
| Set System Parameters         | /F [Enter]                                                     | X                    |            |
| Set Network Port Parameters   | /N [Enter]                                                     | X                    |            |
| Set RS232 Port Parameters     | /P <x> [Enter]                                                 | X                    |            |
| Set User Account Password❺    | /PW [Enter]                                                    | X                    | X          |
| Copy RS232 Port Parameters    | /CP [Enter]<br>/CP [x,y,z] [Enter]<br>/CP [x-z] [Enter]        | X                    |            |
| Connect                       | /C <x> [x] [Enter]                                             | X                    | X❻         |
| Resident Disconnect❷          | ^X                                                             | X                    | X          |
| Third Party Disconnect❸       | /D [/Y] <x> [x] [Enter]<br>/D [/Y] * [Enter]<br>/D Nn [Enter]❹ | X                    |            |
| Erase Buffer                  | /E [/Y] <x> [x] [Enter]<br>/E [/Y] * [Enter]                   | X                    |            |
| Default                       | /I [/Y] [Enter]                                                | X                    |            |
| Send Parameter File           | /U [Enter]                                                     | X                    |            |
| Send SSH Keys                 | /K <k> [Enter]                                                 | X                    |            |
| Upgrade Firmware              | /UF [Enter]                                                    | X                    |            |
| Test Net Parameters           | /TEST [Enter]                                                  | X                    |            |
| Unlock Port                   | /UL [Enter]                                                    | X                    |            |
| Send Break                    | ^\                                                             | X                    | X          |

- ❶ Supervisor Mode displays parameters for all ports; User Mode only displays parameters for ports allowed by the Port Password.
- ❷ To display Port Passwords, include the "P" Option. (Supervisor Only).
- ❸ For the /SN command only, the "P" Option will display the passwords that were used to login to the SCM Network Port.
- ❹ A port or account that does not permit Supervisor commands cannot view parameters for other ports.
- ❺ If desired, The /PW can be disabled via the System Parameters Menu.
- ❻ A User Port cannot perform a Third Party Connect.
- ❼ Resident Disconnect: Disconnects your resident port from another port. The disconnect sequence can be redefined via the Port Configuration Menus.
- ❽ Third Party Disconnect: Disconnects two or more nonresident ports. Must be issued from a third port with Supervisor command capability.
- ❾ Disconnects a TCP Port, where Nn is the desired SCM TCP Port.



---

### 13.3. Command Set

---

This Section provides information on all Text Interface commands, sorted alphabetically by command.

#### **[Enter] Enter Command Mode (Local)**

---

When command mode is inactive (port asleep), the port will only respond after [Enter] has been pressed.

**Availability:** Supervisor / Non-Supervisor

**Format:** [Enter]

**Response:** Port Status Screen, followed by command prompt.

#### **^\ Send Break**

---

To send a break while connected via Telnet to an RS232 port, press the [Ctrl] key and backslash key ([\]) at the same time (^\  
). This command will only function when you have established a Telnet connection to an SCM RS232 port, and will have no effect if issued at the command prompt. In order for the Send Break command to function, the Accept Break option must be enabled at the target port as described in Section 5.7.2.

**Availability:** N/A (Issued at connected port, outside of command mode.)

**Format:** ^\  
 ([Ctrl] plus [\\])

**Response:** Sends Break.

#### **^X Resident Disconnect Sequence**

---

The Resident Disconnect Sequence is used to disconnect your resident port from another port as described in Section 5.7. Although the default Resident Disconnect Sequence is ^x ([Ctrl] plus [X]), the command can be redefined via the Port Configuration Menus as described in Section 5.7.2.

**Note:** The Resident Disconnect Sequence cannot terminate a Direct Connection. For more information, please refer to Section 8.

**Availability:** Supervisor / Non-Supervisor

**Format (Default):** ^x

**Response:**

**Verbose:** The SCM will send the "Disconnected" message, followed by the Port Status Screen.

**Terse:** 3

## **/A Audit Log**

---

Reads the contents of the Audit Log, and displays them on a screen which includes command options that can be used to erase the Audit Log. The Audit log provides a record of command activity at all SCM ports. For more information, please refer to Section 5.4.2.

**Availability:** Supervisor Only

**Format:** **/A [search] [Enter]**

Where the **search** option defines a text string. When the search option is included, the /A command will display all Audit Log Records that contain the specified text.

**Note:** The Audit Log's Delete function will delete *all* stored records; the Delete operation will not be limited to only the records displayed by the search option.

**Response:** Displays the Audit Log screen.

## **/C Connect**

---

Establishes a bidirectional connection between two ports. For more information, see Section 7.1. There are two types of connections:

- **Resident Connect:** If the /C command specifies only one port, your resident port will be connected to the specified port.
- **Third Party Connect:** If the /C command specifies two ports, the unit will connect the two ports indicated. Third Party Connections can only be initiated by ports and accounts that permit Supervisor commands.

### **Notes:**

- If your user account does not permit Supervisor commands, you will only be allowed to connect to ports specifically allowed by that account.
- If the user account permits Supervisor commands, you are allowed to connect to any port.
- RS232 Ports are not allowed to create a Third Party connection to the Network Port. For example, Port 1 cannot connect Port 3 to the Network Port.

**Availability:** Supervisor / Non-Supervisor

**Format:** **/C <x> [x] [Enter]**

Where **x** is the number or name of the port(s) to be connected.

**Response:**

**Verbose:** "Connected xx." When a Resident Connection is initiated, the SCM will also display the Resident Disconnect Sequence.

**Terse:** 1

**/CP Copy RS232 Port Parameters**

---

Allows quick set-up when several RS232 ports will be configured with similar parameters. When the /CP command is invoked, the SCM will display a menu that can be used to copy parameters to RS232 ports. For more information and other command options, please refer to Section 5.8.

**Availability:** Supervisor Only

**Format:** /CP [Enter]

**Response:** Displays Copy Parameters Menu.

**/D Third Party Disconnect**

---

Invoke the /D command at your resident port to disconnect two other ports. Note that the /D command cannot disconnect your resident port.

**Availability:** Supervisor Only

**Format:** /D [/Y] <x> [x] [Enter]

Where:

**/Y** (Optional) suppresses the "Sure?" prompt.

**x** Is the number or name of the port(s) to be disconnected.

To disconnect all ports, enter an asterisk. To disconnect a Telnet session, enter the "nn" format Network Port Number.

**Response:**

**Verbose:** "Are you Sure (y/n)?", if Y, unit will respond with "Disconnected".

**Terse:** 5, if Y, unit will respond with 3.

**Example:** To disconnect Port 2 from Port 3 without the "Sure?" prompt, access the Command Mode from a third port with Supervisor Level command capability and type:

**/D/Y 2 [Enter] or /D/Y 3 [Enter]**

## **/E Erase Buffer**

---

Erases data from the buffer for a specified port(s). Note that erased data cannot be recovered.

**Availability:** Supervisor / Non-Supervisor

**Format:** **/E** [/Y] <x> [x] [Enter]

Where:

**x** Is the number or name of the port buffer(s) to be cleared.  
To erase buffers for all ports, enter an asterisk.

**/Y** (Optional) Suppresses the "SURE? (Y/N)" prompt.

**Response:**

**Verbose:** "Are You Sure (y/n)?", if Y, unit responds with "OK".

**Terse:** 5, if Y, the unit will respond with 0.

**Example:** To clear the buffer for Port 3, access the Command Mode from a port and account that permit Supervisor commands, and type **/E 3 [Enter]**.

## **/F Set System Parameters**

---

Displays a menu which is used to define the Site ID message, create user accounts, set the system clock, and configure and enable the Invalid Access Lockout feature. Note that all functions provided by the /F command are also available via the Web Browser Interface in the "System Properties" menu. For more information, refer to Section 5.4.

**Availability:** Supervisor Only

**Format:** **/F [Enter]**

**Response:** Displays System Parameters Menu.

## **/H Help**

---

Displays a Help Screen, which lists all available Text Interface commands along with a brief description of each command.

**Availability:** Supervisor / Non-Supervisor

**Format:** **/H [Enter]**

**Response:** Displays Help Screen.

---

**/I Default**

---

Initializes the unit with the default parameters.

**CAUTION:** When /I is invoked, the SCM will revert to default parameters. All user selected parameters will be reset to defaults.

**Availability:** Supervisor Only

**Format:** /I [/Y] [Enter]

Where /Y is the option to suppress the "Sure?" prompt.

**Response:**

**Verbose:** "Are You Sure (y/n)?", if Y, initialization begins.

**Terse:** 5, if Y, initialization begins.

---

**/J Display Site ID**

---

Displays the Site I.D. message.

**Availability:** Supervisor / Non-Supervisor

**Format:** /J [Enter]

**Response:** Displays Site I.D. Message.

---

**/K Send SSH Key**

---

Instructs the SCM to provide you with a public SSH key for validation purposes. This public key can then be provided to your SSH client, in order to prevent the SSH client from warning you that the user is not recognized when you attempt to create an SSH connection. For more information, please refer to Section 8.2.

**Availability:** Supervisor Only

**Format:** /K k [Enter]

Where k is a required argument, which indicates the key type. The k argument provides the following options: 1 (SSH1), 2 (SSH2 RSA), 3 (SSH2 DSA.)

**Response:** Sends public key.

## **/N Set Network Port Parameters**

---

Displays a menu which is used to select parameters for the Network Port. Also allows access to the IP Security function, which can restrict network access by unauthorized IP addresses. Note that all of the functions provided by the /N command are also available via the Web Browser Interface in the "Network Configuration" menu. For more information, please refer to Section 5.7.3.

**Availability:** Supervisor Only

**Format:** /N [Enter]

**Response:** Displays Network Parameters Menu.

## **/P Set RS232 Port Parameters**

---

Displays a series of menus used to select options and parameters for the RS232 ports. Note that all functions provided by the /P command are also available via the Web Browser Interface in the "Serial Port" menu. Section 5.7.2 describes the procedure for defining port parameters.

**Availability:** Supervisor Only

**Format:** /P [x] [Enter]

Where x is the number or name of the port to be configured. If the port number/name is not specified, the SCM will display the configuration menu for your resident port.

**Response:** The Port Parameters Menu is displayed.

## **/PW Change Password**

---

When enabled, the /PW command can be invoked by a user/account in order to change their own password. Note that the /PW command can be enabled/disabled via the System Parameters command as described in Section 5.4, and that once a given password has been changed, accounts with Supervisor Level access can still employ the "Modify User" function to change the password.

**Availability:** Supervisor / Non-Supervisor

**Format:** /PW [Enter]

**Response:** Displays the Change Password Menu.

**/R Read Buffer**

---

Reads from Buffer Mode ports as described in Section 7.3.1. Note that when the /R command is invoked, the counter for the SNMP Traps function will also be reset.

**Availability:** Supervisor / Non-Supervisor

**Format:** /R <n> [Enter]

Where **n** is the number or name of the port buffer to be read.

**Response:** The Read Buffer Menu is displayed.

**/S Display Port Status**

---

Displays the Port Status Screen (Figure 6.1), which summarizes conditions and parameters for all ports. For more information, please refer to Section 6.1.

**Availability:** Supervisor / Non-Supervisor

**Format:** /S [Enter]

**Response:** Displays Port Status Screen.

**/SD Display Port Diagnostics**

---

Provides detailed information regarding the status of each port. When this command is issued by an account that does not permit Supervisor commands, the resulting screen will only display parameters for the ports allowed by the account. For more information, please refer to Section 6.2.

**Availability:** Supervisor / Non-Supervisor

**Format:** /SD [Enter]

**Response:** Displays Port Diagnostics Screen.

**/SN Display Network Status**

---

Displays the Network Status Screen, which lists current conditions and parameters for the Network Port. For more information, please refer to Section 6.3.

**Availability:** Supervisor Only

**Format:** /SN [Enter]

**Response:** Displays Network Status Screen

## **/TEST      Test Network Parameters**

---

Displays a menu which is used to test configuration of the Syslog and SNMP Trap functions. For more information, please refer to Sections 9 and 10.

**Availability:** Supervisor Only.

**Format:** **/TEST [Enter]**

**Response:** Displays Syslog / SNMP Trap Test Menu.

## **/U      Save Parameters**

---

Sends SCM configuration parameters to an ASCII text file as described in Section 11.

**Availability:** Supervisor Only

**Format:** **/U [Enter]**

**Response:** The SCM will send a series of command lines.

## **/UF      Upgrade Firmware**

---

When new versions of the SCM firmware become available, this command is used to update existing firmware as described in Section 12. This command will only function at the Network Port and at Port One (the Setup Port.)

**Availability:** Supervisor Only

**Format:** **/UF [Enter]**

**Response:** The SCM will display a menu which offers the options to retain existing parameters, default parameters, or abort.

## **/UL      Unlock Port (Invalid Access Lockout)**

---

Manually overrides the SCM's Invalid Access Lockout feature. Normally, when a user-defined number of unsuccessful password attempts are detected at a given port, the Invalid Access Lockout feature will shut down that port for a user specified time period in order to prevent further access attempts. When the /UL command is invoked, the SCM will immediately unlock all ports that are currently in the locked state.

**Availability:** Supervisor Only.

**Format:** **/UL [Enter]**

**Response:** The SCM will unlock all SCM RS232 Ports.



**/W Display Port Parameters (Who)**

---

Displays configuration information for an individual port, but does not allow the user to change parameters. Accounts that do not permit Supervisor commands can only display parameters for their resident port. For more information, please refer to Section 6.4.

**Availability:** Supervisor / Non-Supervisor

**Format:** **/w [x] [Enter]**

Where **x** is the port number or name. To display parameters for the Network Port, enter an **"N"**. If the **"x"** argument is omitted, parameters for your resident port will be displayed.

**Response:** Displays port parameters.

**Example:** To display parameters for a port named "SERVER", access the Command Mode from a port and account that permits Supervisor commands, and type **/w SERVER [Enter]**.

**/X Exit Command Mode**

---

Exits command mode. When issued at the Net Port, also ends the Telnet session. Note that exiting from command mode will not terminate port connections.

- **Any-to-Any Mode:** Exits command mode.
- **Modem Mode:** Disconnects and resets modem, hang-up message is sent, hardware line to modem drops for 500 ms, and reset message is sent.

**Availability:** Supervisor / Non-Supervisor

**Format:** **/x [Enter]**

**Response:** Disconnected.



## A. RS232 Port Interface

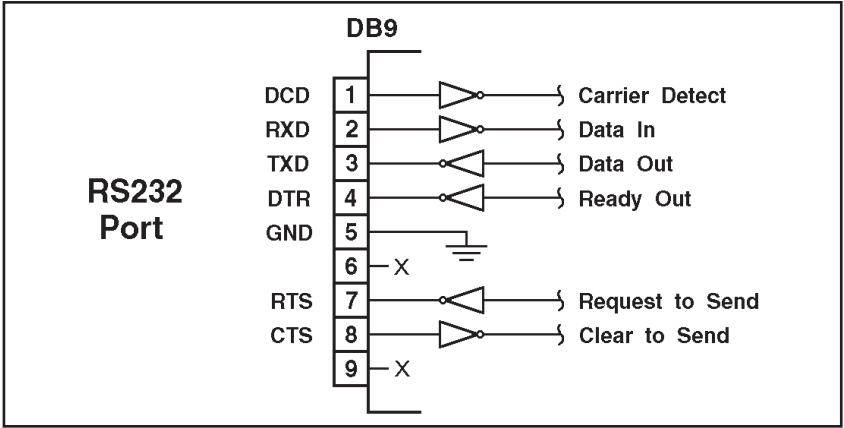


Figure A.1: RS232 Port Interface

DCD and DTR hardware lines function as follows:

1. **When connected:**

- If either port is set for Modem Mode, the DTR output at either port reflects the DCD input at the other end.
- If *neither* port is set for Modem Mode, DTR output is held high (active).

2. **When not connected:**

- If the port is set for Modem Mode, upon disconnect DTR output is pulsed for 0.5 seconds and then held high.
- If the port is *not* set for Modem Mode, DTR output is controlled by the DTR Output option (Parameters Menu, Option 64). Upon disconnect, Option 64 allows DTR output to be held low, held high, or pulsed for 0.5 seconds and then held high.

## B. Specifications

---

**Network Interface:** 10/100Base-T Ethernet, RJ45, multi-session Telnet.

**RS232 Port Interface:**

**Connectors:** Sixteen (16) DB9 connectors (DTE pinout.)

**Coding:** 7/8 bits, Even, Odd, No Parity, 1, 2 Stop Bits.

**Flow Control:** XON/XOFF, RTS/CTS, Both, or None.

**Data Rate:** 300 to 115.2K bps (all standard rates).

**Inactivity Timeout:** No activity timeout disconnects port/modem sessions.  
None, 1, 5, 10, 15, 30 seconds, 1, 5, 15, 30, 90 minutes.

**Memory:** Stores Parameters and captured data. 64K per port.

**Break:** Send Break or Inhibit Break

**Site ID:** 32 Characters.

**Port Name:** 16 Characters per port.

**Username & Passwords:** 16 characters each (case sensitive.) Up to 128 pairs, definable port and system access.

**LEDs:** Power On, Ready, Data Activity for Ports 1-16.

**Physical / Environmental:**

**Power:**

**AC Version:** IEC-320 Inlet, 100 to 240 VAC, 50/60 Hz, 5 Watts

**DC Version:** Terminal Strip (#6-32), -48 VDC, 0.2 Amp Max.

**Size:**

**Height:** 1.75" (4.4 cm), 1 Rack Unit.

**Width:** 19.00" (48.3 cm)

**Depth:** 6.50" (16.5 cm) Rack Mounts Included.

**Shipping Weight:** 6 lbs. (2.7 Kg.)

**Operating Temperature:** 32°F to 122°F (0°C to 50°C)

**Storage Temperature:** -4°F to 128°F (-20°C to 70°C)

**Humidity:** 10 to 90% RH, Non-Condensing

**Venting:** Side vents are used to dissipate heat generated within the unit.  
When mounting the unit in an equipment rack, make certain to allow adequate clearance for venting.

## **C. Customer Service**

---

Customer Service hours are from 8:00 AM to 5:00 PM, PST, Monday through Friday. When calling, please be prepared to give the name and make of the unit, its serial number and a description of its symptoms. If the unit should need to be returned for factory repair it must be accompanied by a Return Authorization number from Customer Service.

WTI Customer Service  
5 Sterling  
Irvine, California 92618

Local Phone: (949) 586-9950  
Toll Free Service Line: 1-888-280-7227  
Service Fax: (949) 457-8138

Email: [service@wti.com](mailto:service@wti.com)

## **Trademark and Copyright Information**

---

WTI and Western Telematic are trademarks of Western Telematic Inc.. All other product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

Information and descriptions contained herein are the property of Western Telematic Inc.. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Western Telematic Inc..

© Copyright Western Telematic Inc. 2007.  
Printed in the United States of America.

March, 2007  
Part Number: 13304, Revision: E

### **Trademarks Used in this Manual**

HyperTerminal is a registered trademark of Hilgraeve, Inc.  
ProComm and ProComm Plus are registered trademarks of  
Datastorm Technologies, Inc.

# Index

|                           |                   |  |
|---------------------------|-------------------|--|
| <b>#</b>                  |                   |  |
| 100BaseT Networks         | 2-2, 4-2          |  |
| <b>A</b>                  |                   |  |
| Accept Break              |                   |  |
| Network Port              | 5-35              |  |
| Serial Port               | 5-26              |  |
| ACTIVITY LEDs             | 2-1               |  |
| AC Powered Units          | 4-1               |  |
| Add User                  | 5-19              |  |
| Any-to-Any Mode           | 7-1 to 7-5        |  |
| Audit Log                 | 5-8, 5-12, 13-4   |  |
| Authentication Port       |                   |  |
| RADIUS                    | 5-39              |  |
| TACACS                    | 5-38              |  |
| <b>B</b>                  |                   |  |
| Baud Rate                 | 5-24              |  |
| Bits and Parity           | 5-24              |  |
| Buffer Connect            | 5-27              |  |
| Buffer Date/Time          | 5-27              |  |
| Buffer Mode               | 7-7 to 7-8        |  |
| Port Buffers              | 7-8               |  |
| Reading Data              | 7-7               |  |
| <b>C</b>                  |                   |  |
| Callback                  | 5-13 to 5-14      |  |
| Callback Attempts         | 5-14              |  |
| Callback Delay            | 5-14              |  |
| Callback Number           | 5-19              |  |
| Callback Security         | 5-8, 5-13 to 5-14 |  |
| Callback Attempts         | 5-14              |  |
| Callback Delay            | 5-14              |  |
| Cautions                  | i to ii           |  |
| Change Password           | 5-8, 13-8         |  |
| CLEAR Button              | 2-1               |  |
| Clock and Calendar        | 5-7, 5-8 to 5-9   |  |
| Command Conventions       | 13-1              |  |
| Command Echo              |                   |  |
| Network Port              | 5-35              |  |
| Serial Port               | 5-26              |  |
| Command Mode              | 13-3 to 13-11     |  |
| Access                    | 5-1 to 5-4        |  |
| Exit                      | 13-11             |  |
| Command Set               | 13-3 to 13-11     |  |
| Configuration             | 5-1 to 5-48       |  |
| Restoring                 | 11-2              |  |
| Saving                    | 11-1              |  |
| Confirmation Prompt       | 13-1              |  |
| Connecting Devices        | 4-2               |  |
| Connecting Ports          | 7-1 to 7-2, 13-4  |  |
| Resident Connections      | 7-1               |  |
| Third Party Connections   | 7-1               |  |
| Copy Parameters           | 13-5              |  |
| RS232 Ports               | 5-45              |  |
| Customer Service          | Apx-3             |  |
| <b>D</b>                  |                   |  |
| Date                      | 5-8               |  |
| DC Powered Units          | 4-1               |  |
| Default Parameters        | 13-7              |  |
| Delete User               | 5-21              |  |
| Dialback Number           | 5-19              |  |
| Dialback Security         | 5-8, 5-13 to 5-14 |  |
| Dialback Attempts         | 5-14              |  |
| Dialback Delay            | 5-14              |  |
| Direct Connect            | 5-28              |  |
| Port Numbers              | 5-28              |  |
| Direct Connect Feature    | 8-2 to 8-4        |  |
| Configuration             | 8-2 to 8-3        |  |
| Connecting                | 8-3               |  |
| Disconnecting             | 8-4               |  |
| Disconnecting Ports       | 7-3 to 7-4        |  |
| No Activity Timeout       | 7-4               |  |
| Resident Disconnection    | 7-3               |  |
| Third Party Disconnection | 7-3               |  |
| DTR Output                | 5-27              |  |
| Duplex Mode               |                   |  |
| Serial Port               | 5-26              |  |
| <b>E</b>                  |                   |  |
| Edit User                 | 5-20              |  |
| Encryption Key            |                   |  |
| SSH                       | 8-1               |  |
| Erase Buffer              | 13-6              |  |
| Exit Command Mode         | 13-11             |  |
| External Modem            | 4-2, 7-9          |  |
| <b>F</b>                  |                   |  |
| Facility                  | 5-29              |  |
| Fallback Local            |                   |  |
| RADIUS                    | 5-39              |  |
| TACACS                    | 5-38              |  |
| Fallback Timer            |                   |  |
| RADIUS                    | 5-39              |  |
| Firmware Upgrade          | 12-1 to 12-2      |  |
| Flow Control              | 5-24              |  |
| <b>G</b>                  |                   |  |
| Gateway Address           | 5-32              |  |
| General Parameters        | 5-7 to 5-9        |  |

|                        |                    |                                   |                              |
|------------------------|--------------------|-----------------------------------|------------------------------|
| <b>H</b>               |                    | Network Port ( <i>continued</i> ) |                              |
| Handshake Mode         | 5-24               | SSH Access                        | 5-33                         |
| Hang-Up String         | 5-27               | Static Route                      | 5-36                         |
| Hardware Installation  | 4-1 to 4-2         | Subnet Mask                       | 5-32                         |
| Help Screen            | 13-6               | Supervisor Mode                   | 5-34                         |
| Hunt Groups            | 7-5                | SYSLOG IP Address                 | 5-33                         |
| <b>I</b>               |                    | Telnet Access                     | 5-33                         |
| Inactivity Timeout     |                    | Timeout Disconnect                | 5-35                         |
| Serial Port            | 5-26               | Web Access                        | 5-33                         |
| Initialization         | 2-1                | Network Status Screen             | 6-2                          |
| Initialization String  | 5-27               | No Activity Timeout               | 7-4                          |
| Invalid Access Lockout | 5-7, 5-10, 13-10   | NTP Address                       | 5-10                         |
| IP Address             | 5-32               | NTP Server                        | 5-10                         |
| Default                | 4-2, 5-2           | NTP Timeout                       | 5-10                         |
| RADIUS                 | 5-39               | <b>O</b>                          |                              |
| TACACS                 | 5-38               | ON Indicator                      | 2-1                          |
| IP Security            | 5-36, 5-40 to 5-44 | Operation                         | 7-1 to 7-10                  |
| Adding IP Addresses    | 5-42               | Overview                          | 3-1 to 3-6                   |
| Linux Operators        | 5-43               | <b>P</b>                          |                              |
| Net/Mask Pairs         | 5-43               | Parity                            | 5-24                         |
| Wild Cards             | 5-43               | Passive Mode                      | 7-6                          |
| <b>L</b>               |                    | Password                          | 5-19                         |
| Level                  |                    | Change                            | 13-8                         |
| Syslog                 | 5-29               | Default                           | 5-3                          |
| Linux Routing Commands | 5-36               | Password on Dialback              | 5-13                         |
| Lockout Attempts       | 5-11               | Periodic Reset Value              | 5-27                         |
| Lockout Duration       | 5-11               | Port Access                       | 5-15, 5-19                   |
| Logoff Character       |                    | Port Buffers                      | 7-8                          |
| Network Port           | 5-34               | Port Configuration                | 5-22 to 5-44                 |
| Serial Port            | 5-25               | Port Diagnostic Screen            | 6-2                          |
| <b>M</b>               |                    | Port Mode                         | 5-22, 5-26, 5-27, 7-1 to 7-9 |
| Modem Mode             | 7-9                | Any-to-Any Mode                   | 7-1 to 7-5                   |
| Hang-Up String         | 5-27               | Buffer Mode                       | 7-7 to 7-8                   |
| Initialization String  | 5-27               | Modem Mode                        | 7-9                          |
| Periodic Reset Value   | 5-27               | Passive Mode                      | 7-6                          |
| Reset String           | 5-27               | Port Name                         | 5-24                         |
| Modify User            | 5-20               | Port Status Screen                | 6-1                          |
| <b>N</b>               |                    | Power Cable Receptacle            | 2-2                          |
| Network Cable          | 4-2                | Power Connection                  | 4-1                          |
| Network Port           | 2-2, 13-8          | Power Switch                      | 2-2                          |
| Accept Break           | 5-35               | PW Command                        | 5-8                          |
| Command Echo           | 5-35               | <b>Q</b>                          |                              |
| Configuration          | 5-30 to 5-44       | Quick Start Procedure             | 3-1 to 3-6                   |
| Gateway Address        | 5-32               | <b>R</b>                          |                              |
| IP Address             | 5-32               | Racking                           | i                            |
| IP Security            | 5-36               | RADIUS                            | 5-39                         |
| Logoff Character       | 5-34               | Authentication Port               | 5-39                         |
| Sequence Disconnect    | 5-35               | Enable                            | 5-39                         |
| SNMP Access            | 5-37               | Fallback Local                    | 5-39                         |
| SNMP Community         | 5-37               | Fallback Timer                    | 5-39                         |
| SNMP Location          | 5-37               | IP Address                        | 5-39                         |
| SNMP Manager           | 5-37               | Secret Word                       | 5-39                         |





|                                |                   |                       |          |         |
|--------------------------------|-------------------|-----------------------|----------|---------|
| Third Party Connections        | 7-1               |                       | <b>V</b> |         |
| Third Party Disconnection Time | 7-3, 13-5<br>5-8  | View Users            |          | 5-17    |
| Timeout Disconnect             |                   |                       | <b>W</b> |         |
| Network Port                   | 5-35              | Warnings and Cautions |          | i to ii |
| Time Zone                      | 5-9               | Web Access            |          |         |
|                                |                   | Enable                |          | 5-33    |
|                                |                   | Web Browser Interface |          | 5-4     |
|                                |                   | Who Command           |          | 6-6     |
| <b>U</b>                       |                   |                       |          |         |
| Unlocking Ports                | 5-11              |                       |          |         |
| Unlock Port                    | 13-10             |                       |          |         |
| Username                       | 5-19              |                       |          |         |
| User Directory                 | 5-7, 5-14 to 5-21 |                       |          |         |
| Add User                       | 5-19              |                       |          |         |
| Delete User                    | 5-21              |                       |          |         |
| Edit User                      | 5-20              |                       |          |         |
| View Users                     | 5-17              |                       |          |         |





---

**5 Sterling • Irvine • California 92618**  
**(949) 586-9950 • Toll Free: 1-800-854-7226**  
**Fax: (949) 583-9514 • <http://www.wti.com>**