SCS Reference Manual

For the Lantronix Family of Secure Console Servers

Part Number 900-235
Revision D December 2003

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors which may appear in this guide.

The revision date for this manual is December 2003.

Part Number: 900-235

Revision D

WARNING

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

Contents

1: Introduction

The Lantronix SCS family of Secure Console Servers provides secure communication for remote users to access local network resources. Our Servers enable IT professionals to configure and administer servers, routers, switches, telephone equipment, or any device with a serial port.

In addition to remote networking capabilities, the SCS includes traditional terminal server functionality such as security features and modem control. The security features include dialback, passwords, database authentication, and menu mode. The SCS also allows automatic modem configuration and control.

This reference manual provides instructions for advanced configuration as well as the complete command set for all products in the SCS family. Many of these features can also be setup using EZWebCon and the web browser interface, and are noted as such.

Before reading this manual, follow the installation procedure described in your *Installation Guide*. Basic configuration for your SCS is also described in your *Installation Guide*.

1.1 What Is New

This manual now includes instructions for the SCS100 and SCS400, the newest members of the Lantronix family of Secure Console Servers, in addition to instructions for the SCS200, SCS1600, and SCS3200.

1.2 How To Use This Manual

The rest of this reference manual is divided as follows:

- Chapter 2, *Getting Started*, provides information on system passwords, rebooting, and basic time and date setup.
- Chapter 3, *Console Server Features*, discusses the console server features of the SCS.
- Chapter 4, *Basic Remote Networking*, contains instructions on configuring LAN to LAN and remote node networking.
- Chapter 5, *Additional Remote Networking*, describes how to optimize your remote networking connection and introduces basic security concepts.
- Chapter 6, *IP*, configures the Internet Protocol (IP) for your SCS.
- Chapter 7, *PPP*, contains conceptual information about the Point-to-Point Protocol (PPP).
- Chapter 8, *Ports*, describes how to configure the SCS's serial ports.
- Chapter 9, *Modems*, explains how to configure modems that are attached to the serial ports or, for certain SCS models, installed in the PC card slot.
- Chapter 10, *Modem Sharing*, describes how to configure the attached modems if they are to be shared.

- Chapter 11, *Security*, offers a comprehensive description of all security features.
- Chapter 12, *Command Reference*, is divided into sections for Navigation/Help, IP/Network, Port, Modem, Service, Server, Site, and Security commands.
- Appendix A, *Environment Strings*, discusses the environment strings that can be used with several of the commands described in Chapter 12.
- Appendix B, *Show 802.11 Errors*, defines the error bits that appear in the Show 80211 screen.
- Appendix C, covers the SNMP features supported by the SCS.
- Appendix D, *Supported RADIUS Attributes*, lists and explains the RADIUS attributes currently supported by the SCS.

2: Getting Started

This chapter covers basic configuration that should get you started using the SCS. Topics include methods for setting up the SCS and ongoing maintenance issues such as restoring factory default settings. You can perform almost all of these configurations using EZWebCon (the recommended method for initial configuration), the web browser interface (recommended for further configurations), or by issuing commands at the command line (Local> prompt).

This chapter assumes that you have completed the following steps, which are described in your *Installation Guide*:

- The SCS is running operational code (i.e. the unit has successfully booted).
- The SCS is connected to an Ethernet.
- The SCS has been assigned an IP address.

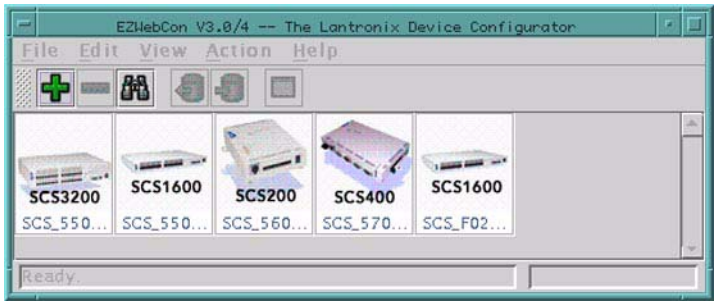
2.1 Configuration Methods

EZWebCon is the recommended method for initial configuration. However, the web browser interface and the command line offer options for advanced configuration.

2.1.1 EZWebCon

The EZWebCon utility is the easiest way to initially configure the unit. EZWebCon guides you through configuration using a graphical interface.

Figure 2-1: The EZWebCon Utility



EZWebCon is included on the CD-ROM that is shipped with each SCS unit. Instructions are listed in the Read Me file, also located on the CD-ROM. For assistance once EZWebCon is running, refer to the EZWebCon online help.

2.1.2 Web Browser Interface

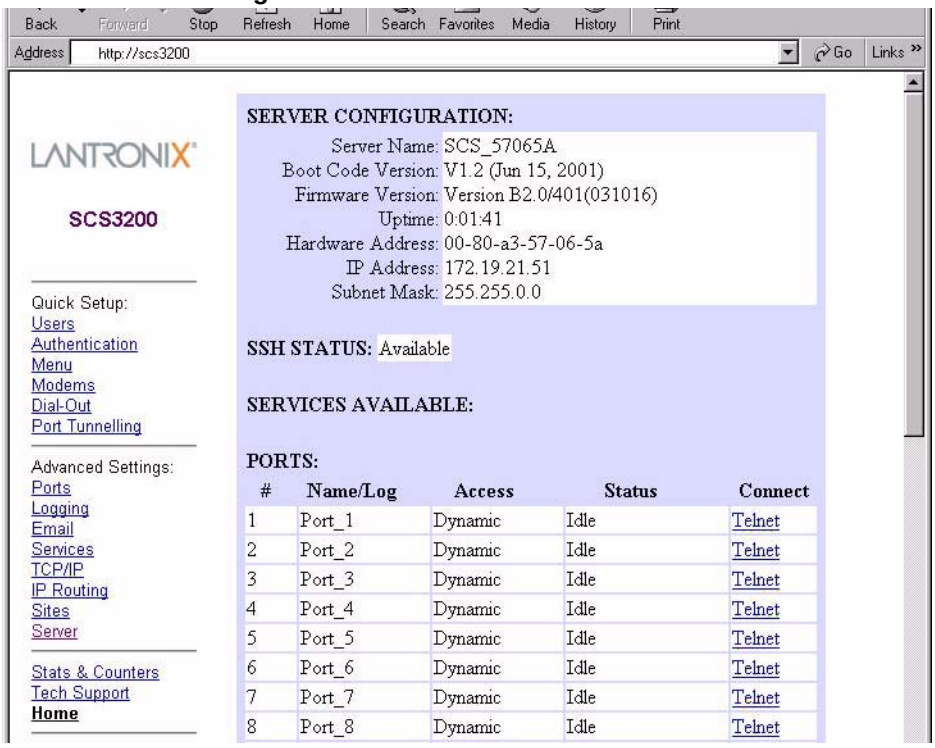
The web browser interface allows you to log into and configure your SCS using a standard web browser. To connect to your SCS using the web browser interface, do one of the following:

- From EZWebCon, select your device and choose **Manage** from the Actions menu.

  OR

- Type your SCS's IP address or resolvable text name into your web browser's URL/Location field.

Figure 2-2: The Web Browser Interface



Once you have connected and entered the login password (see *Login Password* on page 2-7), you can configure important settings, view statistics, and update other Server information. Many of the configurations discussed in this manual can be set using these web pages.

The on-board web browser can be disabled. See *Set/Define Protocol HTTP* on page 12-114 for more information.

2.1.3 Command Line

To configure the SCS without EZWebCon or the web browser interface, you must enter configuration commands at the command line. These commands should be entered when a port is in character mode, which is when the Local> prompt is displayed.

To display the Local> prompt, do one of the following:

- Connect a terminal to the serial console port and press the Return key until the prompt is displayed.

  Note: *The default serial port parameters are 9600 baud, 8 data bits, 1 stop bit, no parity, and XON/XOFF flow control.*

- Establish a Telnet, SSH, or Rlogin connection to the SCS from a TCP/IP host. See *Establishing Sessions* on page 6-8 for more information.

- In EZWebCon, select **Telnet To Device** from the Actions menu.

2.1.3.1 Entering Commands

In examples throughout the manual, SCS commands and keywords are displayed in upper case for clarity. They may be entered in upper, lower, or mixed case. **When entering a string, such as a username or filename, enclose the string in quotes; this will retain the case entered. If a string is not enclosed in quotes, it will be changed automatically to all uppercase characters.**

The *Command Reference* chapter (Chapter 12) displays the syntax of each command, including any restrictions, known errors, and references to related commands. Optional parameters are enclosed in brackets **[]**. Required parameters are enclosed in curly braces **{}**; one and only one of those parameters must be used. User-supplied parameters, such as a particular port number or host name, are shown in italics.

The SCS command completion feature will complete partially-typed commands for you. This feature can save time and reduce errors if you're entering a number of commands. To use command completion, type part of a command, then press the space bar. The SCS will automatically "type" the remainder of the command. If the partially-entered command is ambiguous (or if you are entering an optional string), the SCS will be unable to finish the command and the terminal will beep.

Note: *Command completion is disabled by default. To enable command completion, refer to Set/Define Ports Command Completion on page 12-65.*

All keys used for entering and editing commands are listed in Table 2-1.

Table 2-1: Command Editing Keys

Key	Purpose
Return	Executes the current command line
Delete	Deletes the current character before the cursor
Ctrl-A	Toggles insert mode (insert or overstrike). Overstrike is on by default.
Ctrl-D	Logs out of the server
Ctrl-E	Moves the cursor to the end of the line
Ctrl-H or Backspace	Moves the cursor to the beginning of the line
Ctrl-R	Redisplays the current command
Ctrl-U	Deletes the entire current line
Ctrl-Z	Logs out of the server
Left Arrow	Moves the cursor left
Right Arrow	Moves the cursor right
Up Arrow or Ctrl-P	Recalls the previous command
Down Arrow or Ctrl-N	Recalls the next command
!*text*	Recalls the last command starting with *text*
!!	Recalls the last command

2.1.3.2 Command Types

The following types of commands appear frequently throughout this manual. There are subtle differences between each group of commands.

The **Set** and **Define** commands make configuration changes to your SCS.

Set — Makes an immediate (but not permanent) change; the change will be lost when the SCS is rebooted. To make the change permanent, you must also enter the **Save** command (discussed on page 12-189).

Define — Makes a permanent change, but the change doesn't take effect until the SCS is rebooted.

Define Port and Define SLIP settings take effect after the current user logs out. Define Site takes effect when a site is started. Define Server, Define Telnet Host, and Define Service settings take effect when the SCS is rebooted.

The **Show**, **Monitor**, and **List** commands display information about the SCS.

Show — Displays the current settings. Current settings include those made using the Set command but not yet defined or saved as permanent changes.

Monitor — Displays current operating characteristics, which are updated every three seconds until a key is pressed. Monitor commands may only be used by the privileged user.

List — Displays settings that will take effect the next time the SCS is rebooted.

Clear and **Purge** alter previously configured SCS settings.

Clear — Removes a configured setting immediately, but does not make a permanent change.

Purge — Removes a configured setting permanently, but does not take effect until the unit is rebooted.

Note: *Purge Port will take effect as soon as the port is logged out, and Purge Site will take effect when a site starts.*

2.1.3.3 Restricted Commands

Some commands require privileged (superuser) status. To obtain privileged status, you must enter the privileged password. See *Privileged Password* on page 2-8 for instructions on entering and editing the privileged password.

By default, the SCS prompt changes from Local> to Local>> to reflect privileged user status.

2.1.3.4 Abbreviating Commands

When configuring the Server via the command line, you only need to enter as many characters as are needed to distinguish the keywords from one another. For example, the following two commands are equivalent:

Figure 2-3: Abbreviating a Command

```
Local>> DEFINE PORT 2 BROADCAST ENABLED AUTOCONNECT ENABLED PARITY EVEN SPEED 4800
Local>> DEF PO 2 BRO EN AUTOC EN PAR E SP 4800
```

An abbreviation must be unique to the desired command. For example, if **autoconnect** was abbreviated as auto, that auto could denote **autobaud**, **autostart**, or **autoconnect**. Be sure that any abbreviations are unambiguous, such as **autoc** in the example above.

2.2 Rebooting

There are four ways to reboot the SCS:

- From within EZWebCon, select **Reboot** from the Actions menu.
- From the Server section of the web browser interface, check the **Reboot Server** checkbox. Then, click the **Update Server Settings** button at the bottom of the page.
- At the Local> prompt, issue the **Initialize Server** command.
- Cycle power to the unit.

When the SCS is rebooted, any changes made using Set commands will be lost. To ensure that the changes will be saved, use Define commands, or use the Save command after the Set command.

Before rebooting the SCS, log out any current user sessions (if possible). Disconnecting sessions may prevent connection problems after the SCS is rebooted. If possible, warn users that the SCS will be going offline by sending a **Broadcast** message.

2.2.1 Sending a Broadcast Message

Broadcast messages are sent to local users, but not remote networking users. Broadcasts can be sent to all Server ports with the following command.

Figure 2-4: Broadcast Command

```
Local>> BROADCAST ALL "Server shutdown in 5 minutes."
```

2.2.2 Restoring Factory Defaults

Restoring factory default settings will erase all changes made since the SCS was shipped; the unit will function as if it just came out of the box. To restore factory defaults, enter the **Initialize Server Factory** command at the Local> prompt.

To perform a TFTP boot after restoring the factory defaults, you must enter the SCS IP and loadhost information. (If a BOOTP server will provide this information, this step is not required.) Refer to your *User Guide* for instructions.

When initialized, the SCS sets local authentication in the first precedence slot. For more information on authentication and precedence, see *Database Configuration* on page 11-9.

2.2.3 Reloading Operational Software

The SCS stores its software in Flash ROM. The software controls the initialization process, the operation of the SCS, and the processing of commands. The contents of Flash ROM can be updated by downloading a new version of the operational software.

For instructions on reloading Flash ROM, refer to your *Installation Guide*.

2.2.4 Editing Boot Parameters

If the information that the SCS uses at boot time changes, you will need to change the SCS boot parameters. Boot parameters include the following:

- Loadhost (TCP/IP). The loadhost is the host from which the SCS operational software is downloaded at boot time.
- Backup loadhost (optional). Software is downloaded from a backup loadhost when the primary loadhost is unavailable.
- Software filename
- RARP (may be enabled or disabled)
- BOOTP (may be enabled or disabled)

Boot parameters are edited using Set/Define Server commands such as **Set/Define Server Loadhost**. All available server commands are listed in *Server Commands* on page 12-111. Use the Define commands if you want any changes to be saved after reboot.

Figure 2-5: Editing the Loadhost Address

```
Local>> DEFINE SERVER LOADHOST 192.0.1.8
```

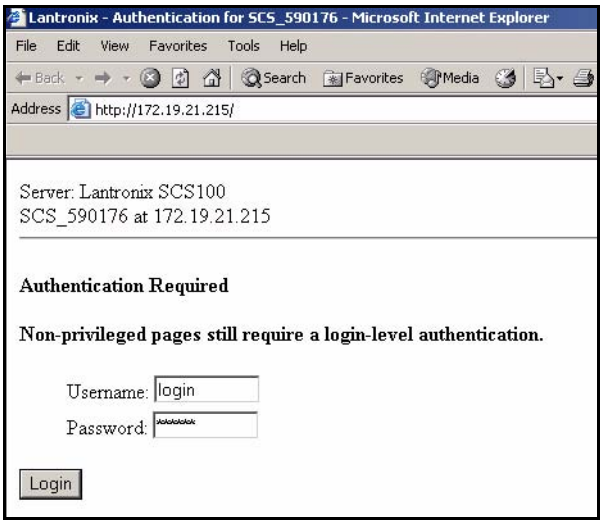
2.3 System Passwords

The SCS has both a login password and a privileged password. These passwords have default settings which should be changed as soon as possible. The following sections discuss each password in more detail.

2.3.1 Login Password

When you open the web browser interface for an SCS, you are prompted for the login username and password. To control this setting, use the Server Login Password Required checkbox on the Server page.

Figure 2-6: Web Browser Authentication



When a serial port has the login password enabled, users must enter the correct password to access that port's Local> prompt. The default login username is **login,** and the default login password is **access**.

To change the login password, use the **Set/Define Server Login Password** command.

Figure 2-7: Defining the Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
```

Note: *The login password is case-insensitive, so it does not need to be enclosed in quotes.*

To enable the use of the login password on a particular port, use the following command:

Figure 2-8: Enabling the Login Password

```
Local>> DEFINE PORT 3 PASSWORD ENABLED
```

Note: *To enable the password on virtual ports, which are used for incoming connections, use the Set/Define Server Incoming command.*

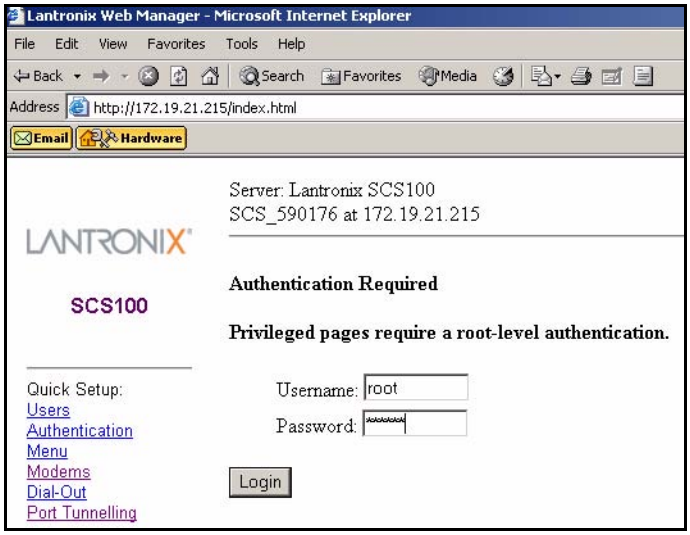
Login passwords are also discussed in *Character Mode Logins* on page 11-1.

2.3.2 Privileged Password

Changing any server, site, or port setting requires privileged user status. Use the default username, **root**, and the default privileged password, **system**.

When you click on a link in the left navigation column of the SCS web browser interface, you are prompted for the privileged username and password. Once you enter the password, you can access all of the configuration pages.

Figure 2-9: Root-Level Authentication



If you are at the command line, become the privileged user by entering the following command.

Figure 2-10: Set Privileged Command

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>>
```

Note: *The complete command syntax for Set Privileged is available on page 12-92.*

To change the privileged password, use the **Set/Define Server Privileged Password** command (discussed on page 12-123). Figure 2-11 displays an example of this command.

Figure 2-11: Changing the Privileged Password

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> DEFINE SERVER PRIVILEGED PASSWORD hippo
```

Note: *The privileged password is case-insensitive, so it does not need to be enclosed in quotes.*

2.4 Basic Configuration

The following sections discuss features that will identify and personalize each SCS.

2.4.1 Changing the Server Name

Each SCS is initially configured with a server name in the form of **SCS_xxxxxx**, where xxxxxx represents the last three segments of its hardware address. However, you can give the Server a custom name of up to 16 alphanumeric characters using the following command.

Figure 2-12: Changing the Server Name

```
Local>> DEFINE SERVER NAME "CommServer"
```

Note: *The server name must be enclosed in quotes to preserve case.*

2.4.2 Changing the Local Prompt

The prompt each user receives (usually a Local_*xx*> prompt, where *xx* is the port number) is configurable in a variety of ways. For a basic prompt, enter a string similar to the following.

Figure 2-13: Configuring the Server Prompt

```
Local> SET SERVER PROMPT "Server> "
Server>
```

For a customized prompt, optional key combinations can be added to the prompt string. See **Set/Define Server Prompt** on page 12-123 for more information. Placing a space after the end of the prompt is recommended to improve readability.

Figure 2-14 displays a few examples of commands used to change prompts. In the examples, the first command line results in the prompt used in the second command line, and so on.

Figure 2-14: Prompt Examples

```
Local> SET SERVER PROMPT "Port %n: "
Port 5: SET SERVER PROMPT "%D:%s: "
SCS:LabServ: SET SERVER PROMPT "%p%s_%n%P%% "
Port_5[NoSession]_5>%
```

2.4.3 Changing the Login Prompts

When a user logs into the SCS, he is prompted for a username, and sometimes a login password. By default, the prompts are **Username>** and **Password>**. The prompts can be changed to be more like UNIX prompts (**login:** and **Password:**) with the following command.

Figure 2-15: Enabling the Alternate Login Prompt

```
Local> SET SERVER ALTPROMPT ENABLED
```

2.4.4 Setting the Date and Time

The SCS can calculate and save the local time, coordinated Universal Time (UTC, also known as Greenwich Mean Time or GMT), standard and Daylight Savings timezones, and the corresponding number of hours difference between UTC and the set timezone.

2.4.4.1 Setting the Clock

Use the **Set/Define Server Clock** command at the Local> prompt. Time should be entered in hh:mm:ss "military format" as shown in the example below.

Figure 2-16: Setting the Clock

```
Local>> SET SERVER CLOCK 14:15:00 12/01/2000
```

2.4.4.2 Setting the Timezone

The SCS is configured to recognize a number of timezones. To display these timezones, use the **Show Timezone** command at the Local> prompt. Set the timezone by using the **Set/Define Server Timezone** command at the Local> prompt.

Figure 2-17: Setting the Timezone

```
Local> DEFINE SERVER TIMEZONE AMERICA/PACIFIC
```

If your timezone is not listed, you will need to set it manually. Use the following information to set the timezone:

- A three-letter timezone abbreviation; for example, PST
- The number of hours offset from UTC (Greenwich Mean Time); for example, -9:00
- The time, day, and amount of any time changes (for example, daylight savings time information)

Note: *Specifying time change information is optional.*

Figure 2-18 shows an example of how to set the timezone.

Figure 2-18: Manual Timezone Configuration

```
Local>> DEFINE SERVER TIMEZONE EST -3:00 EST 1 Mar Sun>=1 3:00 Oct lastSun 2:00
```

The first **EST** specifies that Eastern Standard Time will be used as the reference point. The second value of **-3:00** indicates that this timezone is 3 hours behind Eastern Standard Time. The third and fourth values, **EST** and **1**, specify that when a time change occurs the time will move forward one hour. The time change will occur in March, denoted by **Mar**. The date that the time change will occur will be the Sunday (**Sun**) greater than or equal to 1 (**>=1**), in other words, the first Sunday in the month. The **3:00** specifies that the time change will occur at 3 o'clock.

The final three values of the command string represent the day and time when the time will revert to the original time, in other words, when the time change will be reversed. The **Oct** and **lastSun** indicate that the time will revert on the last Sunday in October. The time change will occur at **2:00**.

2.4.4.3 Designating a Timeserver

The SCS regularly verifies and updates its setting with the designated timeserver. A timeserver is a host which provides time of day information for nodes on a network. The SCS can communicate with either Daytime or Network Timeserver Protocol (NTP) servers. For NTP, the SCS can periodically broadcast a message asking for time information and wait for an NTP timeserver to reply (the Broadcast parameter), periodically query a specific NTP timeserver (the IP *ipaddress* parameter), or just listen for NTP broadcasts on the network (the Passive parameter).

To specify a timeserver, use the **Set/Define IP Timeserver** command.

Figure 2-19: Defining Timeservers

```
Local>> DEFINE IP TIMESERVER DAYTIME 193.0.1.50
Local>> DEFINE IP TIMESERVER NTP PASSIVE
```

2.4.5 802.11 Configuration

This section applies only to the SCS200. Topics discussed in this section assume that you understand IEEE 802.11 wireless Ethernet concepts and architectures. If you do not, please refer to the IEEE 802.11 standard or the documentation that came with your PC card or Access Point (AP).

Note: *The SCS does not support PC card hot-swapping. Any time you insert a PC card into an SCS PC card slot, you must reboot the SCS.*

The following parameters should be configured only if you are using the SCS for 802.11 wireless Ethernet networking and plan to use a wireless LAN PC card in one of the PC card slots. Users in countries other than the United States must set the Region appropriately before using 802.11.

Not all configuration options will be available on all 802.11 cards. If you try to enter an option that is not supported by your card, you will receive an Error message.

Any time you enable or disable 802.11 networking, you must reboot the SCS before the change takes effect. Any other changes you request with the **Set/Define 80211** commands will not take place until you have entered the **Set 80211 Reset** command. You can enter the **Show IP Counters** command to see the current 802.11 settings.

To use the web browser interface to configure 802.11 settings, select the 802.11 link under the Advanced Settings section.

2.4.5.1 802.11 Terms

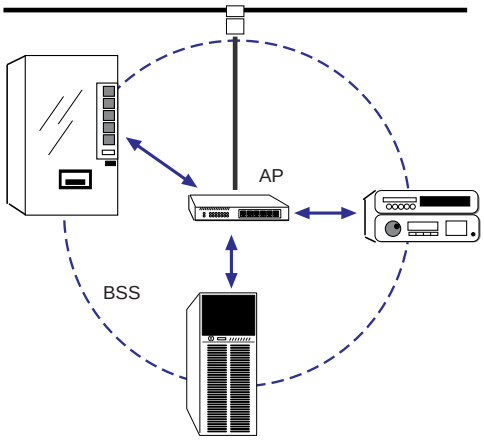
The following acronyms are used in this section:

AP Access Point, a device that relays communications between one or more wireless devices and possibly other devices on a network. APs are usually connected to a physical network.

Note: *If you are using an AP and WEP is not enabled, set the AP to accept Open System Authentication. If WEP is enabled, set the AP to Shared Key Authentication. For more information about WEP, see the definition below.*

BSS Basic Service Set (or Cell), a group of wireless devices that speak directly with each other. A BSS may consist of at most one AP.

Figure 2-20: Simple Wireless Network BSS



ESS Extended Service Set, a network consisting of one or more BSSs that share the same ESSID. An ESS can contain multiple APs.

IBSS Independent Basic Service Set, a BSS with no APs. Devices work in an ad-hoc networking mode.

WEP Wireless Equivalent Privacy, a form of encryption for wireless communication.

2.4.5.2 Enabling 802.11 Networking

The SCS has 802.11 networking enabled by default. This allows the SCS to check for a compatible wireless networking card at startup. If a compatible card is present, the SCS will use the wireless network and ignore any wired Ethernet settings. If no compatible PC card is present, the SCS will use the 10/100BASE-T Ethernet interface.

If you want the SCS to only look for a wired Ethernet connection, you must disable 802.11.

Figure 2-21: Disabling 802.11

```
Local>> DEFINE 80211 DISABLED
```

Note: *You must reboot the SCS after enabling or disabling 802.11 networking.*

2.4.5.3 802.11 Region

When using 802.11 networking, you **must** make sure the SCS is configured for the correct regulatory region. Configuring this option incorrectly may cause the SCS to broadcast on frequencies that are illegal in your area. The factory default setting is correct for the United States; users in other countries should change it to a value appropriate for their area before attempting 802.11 operation.

Other region settings are listed in **Set/Define 80211 Region** on page 12-30. In the following example, IC sets the region to Canada.

Figure 2-22: Setting the 802.11 Region

```
Local>> DEFINE 80211 REGION IC
Local>> SET 80211 RESET
```

2.4.5.4 MAC Address

A MAC address is a unique identifier that distinguishes different devices on the 802.11 network. It is the same as the unit's hardware address. The SCS can be configured to use either the PC card's MAC address or its own internal MAC address (the default) with the **Set/Define 80211 MAC Address** command. For seamless operation when switching between wired and wireless networking, use the SCS's MAC address.

Figure 2-23: Configuring the MAC Address

```
Local>> DEFINE 80211 MACADDRESS CARD
Local>> SET 80211 RESET
or
Local>> DEFINE 80211 MACADDRESS SCS
Local>> SET 80211 RESET
```

2.4.5.5 Extended Service Set ID (ESSID)

Whenever there is more than one ESS in a wireless LAN architecture, each device needs to be told which ESS it belongs to. The ESSID ensures that devices communicate with the right AP.

To tell the SCS which ESS it belongs to, enter the **Set/Define 80211 ESSID** command. The exact string you enter will be determined by the settings of the AP with which you want the SCS to communicate.

Figure 2-24: Configuring the ESS ID

```
Local>> SET 80211 ESSID "floor3"
Local>> SET 80211 RESET
```

Setting the ESSID to none (**Set/Define 80211 ESSID None**) allows the SCS to associate with any AP within range.

2.4.5.6 Network Mode

There are two types of 802.11 networks: ad-hoc and infrastructure. In an ad-hoc network, devices communicate directly with one another on a peer-to-peer basis. In an infrastructure network (the default), several devices communicate with one or more APs. The APs may or may not be connected to a physical Ethernet network. You must tell your SCS which type of network is present with the **Set/Define 80211 Network Mode** command.

Figure 2-25: Configuring the Network Mode

```
Local>> DEFINE 80211 NETWORKMODE ADHOC
Local>> SET 80211 RESET
or
Local>> DEFINE 80211 NETWORKMODE INFRASTRUCTURE
Local>> SET 80211 RESET
```

The network mode setting relates to the channel setting, explained next.

2.4.5.7 Channel

The frequency band allocated to 802.11 wireless communications is subdivided into different channels to allow subnetworking. Your SCS needs to know which channel it should use for communications—the channel will be the same as the one being used by the local AP. The default setting, **Any**, causes the SCS to use the same channel used by the strongest AP with the same ESSID.

For infrastructure network mode, you should set the channel to Any so that the SCS can synchronize with an AP. For Ad-Hoc network mode, you should set a specific channel number so that the SCS can start a new IBSS if needed. When the channel is set to Any, the SCS can only join an existing IBSS.

Figure 2-26: Configuring the 802.11 Channel

```
Local>> DEFINE 80211 CHANNEL 7
Local>> SET 80211 RESET
```

2.4.5.8 WEP

Some 802.11 cards can be set with a WEP key, which will encrypt any data you transmit through wireless communication. To enable WEP, enter the following command:

Figure 2-27: Enabling WEP

```
Local>> DEFINE 80211 WEP ENABLED
Local>> SET 80211 RESET
```

When WEP is enabled and a WEP key is set, the SCS will only connect to an AP (in infrastructure mode) or communicate with other ad-hoc peers (in ad-hoc mode) that have been programmed with the same WEP key as the SCS. For a key to match, both the key data and the index number must be identical.

Enter a WEP key if you have not previously done so. The key can be either 40-bits or 128-bits. Each key is also assigned an index number, which is an integer between 1 and 4.

Figure 2-28: Setting the WEP Key and Index Number

```
Local>> DEFINE 80211 WEP KEY 26-e4-97-db-1f
Local>> DEFINE 80211 WEP INDEX 3
Local>> SET 80211 RESET
```

The SCS will receive both encrypted and unencrypted traffic. You can disable the reception of unencrypted traffic and accept only frames encrypted with its WEP key by entering the following command:

Figure 2-29: Disabling WEP Unencrypted Traffic Reception

```
Local>> DEFINE 80211 WEP RECEIVE ENCRYPTED
Local>> SET 80211 RESET
```

2.5 Configuration Files

Once you have configured one SCS, you can create a **configuration file** from those settings and download that file to other devices. A configuration file is a series of commands used to automatically configure an SCS. By using a configuration file, you save time that would otherwise be spent manually entering commands. You can also update the configuration of many devices simultaneously, ensuring that each device is configured the same. You can download a file manually, or configure the SCS to automatically download a file each time it boots.

EZWebCon can automatically translate your current SCS configuration into a configuration file, which can then be downloaded through EZWebCon to other devices. Refer to EZWebCon's online help for more information.

The rest of this section describes how to create and use configuration files at the command line.

2.5.1 Creating a Configuration File

To create a configuration file without EZWebCon, you must manually enter each command in the file.

1. On your host, enter a series of SCS commands in a text file, one command per line. Privileged commands may be included; when the file is downloaded, the commands will be executed as if a privileged user was logged into the SCS.

   Capitalization of commands is optional. **If a string (such as a filename) is entered, it must be enclosed with quotes in order to preserve the case.** To include a comment in the file, preface the line with a pound (#) character. These lines will be ignored.

   If **Define Server** commands are included in the file, they will not take effect until the SCS is rebooted. **Define Port** commands will not take effect until the specified ports are logged out. **Define Site** commands will take effect when the specified site is started.

   The configuration file must not contain any initialization commands (such as **Initialize Server**). Because the file is read when the SCS boots, a "reboot" command in the file would cause the SCS to boot perpetually. You would then have to flush the NVR to correct the error.

2. Test the configuration file. To test the file, use the **Source** command, discussed on page 12-131.

An example of a configuration file is displayed below.

Figure 2-30: Configuration File

```
DEFINE PORT 2 SPEED 9600
DEFINE PORT 2 PARITY NONE
# The following commands set up the ports:
DEFINE PORT 2 ACCESS DYNAMIC
```

2.5.2 Using a Configuration File

A configuration file can be downloaded from a TCP/IP host (via TFTP). Ensure that TFTP downloading is enabled on your host and place the configuration file in a download directory.

To download a configuration file to the SCS using TFTP, use the **Source** command.

Figure 2-31: Downloading From a TFTP Host

```
Local>> SOURCE “labsun:start.com”
```

If the configuration file must be downloaded each time the SCS boots, specify the filename using the **Set/Define Server Startupfile** command. A TCP/IP filename must be specified in **host:filename** format, where host is an IP address.

Note: *If lower-case or non-alphabetical characters are used, the filename must be enclosed in quotes.*

For example, to download the file config.sys from TCP/IP host 192.0.1.110, use the following command:

Figure 2-32: Downloading From a TCP/IP Host

```
Local>> DEFINE SERVER STARTUP "192.0.1.110:config.sys"
```

Note: *The SCS is not usable during download attempts.*

If the SCS has a nameserver defined, a text name may be specified as a TCP/IP host name. The SCS will attempt to resolve the name at boot time; if it cannot resolve the name, the download will fail. To designate a nameserver, see **Set/Define IP Nameserver** on page 12-39.

During its boot sequence, the SCS will load its operational code first, then attempt to download the configuration file. If the attempt to download the configuration file is unsuccessful, the SCS may re-attempt the download. By default, the SCS will make a total of six attempts to download the file (one initial attempt and five re-attempts). To change this setting, use the **Set/Define Server Startupfile Retry** command.

Figure 2-33: Setting Number of Download Attempts

```
Local>> DEFINE SERVER STARTUPFILE "TROUT\SYS:\LOGIN\config.sys" RETRY 10
```

If Retry is set to zero, the SCS can no longer be used; it will wait indefinitely for the configuration file to download.

2.6 Disk Management

The SCS contains three filesystems:

/flash	Flash is rewriteable memory that allows you to customize your SCS. Any data that you want the SCS to save after it is rebooted should be stored on the Flash disk.
/ram	The RAM disk stores temporary information. The SCS will hold information stored on this disk until it is powered off or rebooted. At startup, the RAM disk will be empty. FTP connections to the SCS automatically use the RAM disk as the default working directory. The RAM disk size is 512 Kbytes.
/rom	The ROM disk is read-only and cannot be modified by users.

In addition to the onboard Flash disk, the PC card slots on the SCS200 and SCS400 can be used with ATA flash cards and hard-drive PC cards for portable storage of local files.

In some instances, you may need to edit a file on another machine and then FTP it to the SCS. Use your FTP client software to form a connection to the SCS (using the SCS's resolvable name or IP address). You can then transfer files to (put) and from (get) the /flash, /pccard, and /ram disks.

2.6.1 Flash Disk

The Flash disk (/flash), rewriteable memory, should be used to hold any data that you want the SCS to save after it is rebooted. Because power glitches can affect data integrity, important files on /flash should be backed up on an ATA flash card or on another server.

The **Disk** commands can be used to manage files on the Flash disk. For example, the following command creates a new directory on the Flash disk that could be used for custom application files:

Figure 2-34: Creating a New Directory on the Flash Disk

```
Local>> DISK MKDIR /flash/customapps/
```

To view all of the files and directories currently on the Flash disk, enter **Disk ls** with or without flags. The following example will display all the files as well as the modification date, size, owner, and permissions:

Figure 2-35: Listing Directory Contents

```
Local>> DISK LS -l /flash
```

The complete syntax of the **Disk** command is available on page 12-182.

2.6.2 ATA Cards

Once an ATA flash disk or hard-drive PC card is formatted (using the **Disk Format /pccard** command), the card can be used the same as the on-board Flash disk. Files on the card can be references as "/pccard1/*directory*/*filename*."

Note: *The SCS does not support PC card hot-swapping. Any time you insert a PC card into an SCS PC card slot, you must reboot the SCS.*

The **Disk** commands described above and on page 12-182 can also be used for file management on the flash card. For example, to back up a Flash disk file (data.txt) to an ATA card, use the following commands to create a backups folder on the card and to copy the desired file into that folder:

Figure 2-36: Backing Up Files To a Flash Card

```
Local>> DISK MKDIR /pccard1/backups/
Local>> DISK CP /flash/customapps/data.txt /pccard1/backups
```

The maximum number of files and directories (total sum) that can fit on the card is a function of the size of the card: divide the size of the card by 5k (5120 bytes). This assumes that the average size of all the files that will fill up the card will be smaller than 5k.

Data can be corrupted if power is lost in the middle of a write (for example, if the cord is pulled). If the **Disk Sync** command is issued and power is removed after the command is completed, data will be stored correctly on the card. Likewise, there should be no problems with data integrity if the **Initialize Server Delay 0** command is used to reboot the unit.

3: Console Server Features

This chapter describes how to configure your SCS to serve as a console server. The SCS features both in-band management for access to connected devices over IP (e.g. through Telnet and SSH connections directly to the SCS), and out-of-band management for access through a connected modem.

This chapter is divided as follows:

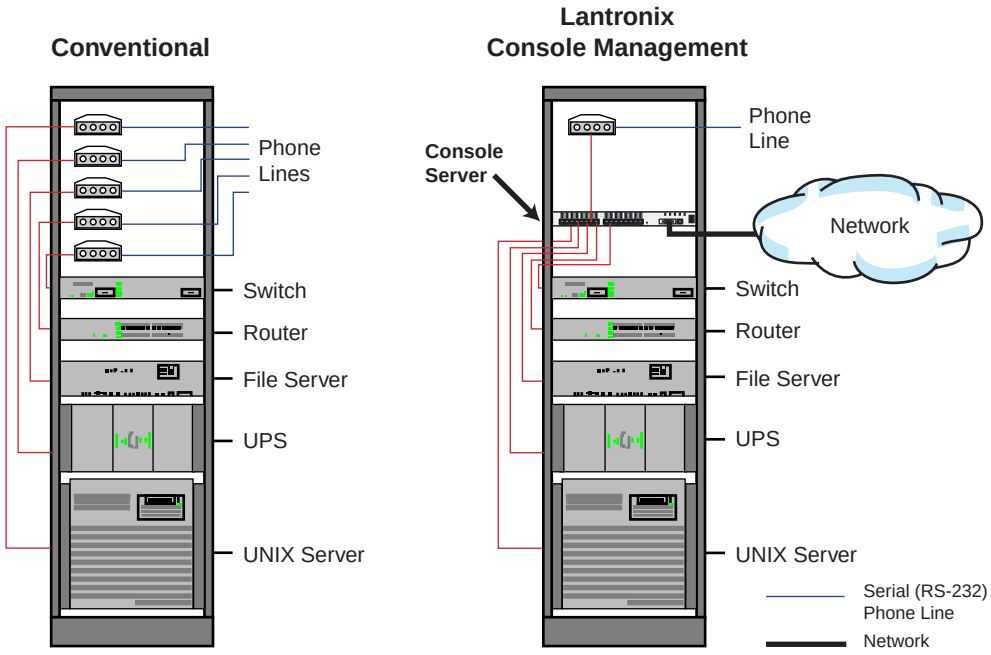
- *Overview of Console Servers* on page 3-1 introduces the functions of a console server.
- *Event Port Logging* on page 3-2 describes how to save idle serial data in an easily accessible log file
- *Email Alerts for Serial Events* on page 3-3 shows how to send the serial log via email.
- *Configuring Menu Mode* on page 3-4 discusses the options for configuring SCS menus.
- *Login Banner Pages* on page 3-8 covers in-band and out-of-band management options.
- *Serial Port Configurations* on page 3-14 describes optimal serial port settings.

Most of these features are discussed in more detail in the *IP*, *Ports*, and *Security* chapters.

3.1 Overview of Console Servers

The SCS can be connected to the serial console ports of a variety of devices. You can then manage these devices remotely either over an IP network or through a dial-up modem connection.

Figure 3-1: Console Server Setup



3.2 Event Port Logging

Port logging saves all idle data from an SCS serial port in a log file. This log file can be accessed by a system administrator after a system crash, and can provide valuable information about the cause of and solution for any problems with the attached serial device.

If email notification (discussed in *Email Alerts for Serial Events* on page 3-3) is enabled, the serial log can be sent via email to the system administrator.

3.2.1 Enabling Port Logging

Enable port logging with the **Set/Define Ports Serial Log** command. This command sets the file size for the log file, which can be up to 250 Kbytes. To disable the log file, enter a file size of 0.

Figure 3-2: Saving Serial Data to a Logfile

```
Local>> DEFINE PORT 2 SERIALLOG LIMIT 200
```

Note: *This command sets port access to Access Remote.*

The log file is stored on the SCS /ram disk in the form **/ram/Port_*xx*.log** where *xx* is the port number. When the file reaches its specified limit, it is truncated to half its current size and begins logging again. The oldest data is discarded.

When the SCS is rebooted, the data stored in the log file is lost.

3.2.2 Viewing the Port Log

This section describes three methods for retrieving port logs.

3.2.2.1 Telnet/Serial Login

To retrieve the port log using Telnet, SSH, or terminal login:

1. At a **Local_n** >prompt, type **disk ls** to see the files. The file is **Port_nn** by default, where nn is the port number.
2. To view the entire log, type **disk cat port_nn.log**.

Note: *You can use other Unix commands, such as **tail** and **top**.*

3.2.2.2 Web Interface

To retrieve the port log using the web browser interface:

1. Open the web browser interface and http to the IP address or hostname of the SCS. The SCS Home page displays. If logging is enabled, the port name is a link.
2. Click the link to open the file in the default text viewer.

3.2.2.3 FTP

To retrieve the port log using an FTP session:

1. FTP to the SCS.
2. Type **ls** to get a listing of log files.
3. "**Get**" or "**mget**" a copy of the log file (for example., **# mget Port_1.log**).

3.3 Email Alerts for Serial Events

Once a port is configured for port buffering (as described in *Event Port Logging* on page 3-2), you can enable email notification. This feature triggers an email if the connected device reboots or otherwise produces a burst of console output of 20 or more characters.

The port buffers incoming data for up to 25 seconds or until the log file reaches1500 bytes before sending the email, which contains the current contents of the log file. Any data that comes in after that 25 seconds will be saved in the file, but not included in that email. Email can not be sent from the same port more than once every 10 minutes.

The email sent by the SCS also includes a URL that refers to the serial log file directly, so you can open it in an email client or web browser. You will need to enter the system login password to access the file.

Note: *If the HTTP server has been disabled with the Set/Define Protocol HTTP command, you will not be able to use the URL to access the log file.*

Each port's email settings can be separately configured, or a default configuration can be created that will be used for all email notifications. An **emailsite** stores the information necessary for email notification. The only possible names for emailsites are **port*xx***, where *xx* is a serial port number, or **default**. Settings for the default emailsite will be used for any that are missing in the port-specific files.

Use the **Define Email** commands to configure each emailsite with features such as an email address for the email to be sent to, a from line, a subject line, an SMTP mailhost, and a reply-to address.

The following example configures an emailsite for the second serial port.

Figure 3-3: Configuring an Email Site

```
Local>> DEFINE EMAIL port2 TO "admin@strut.com"
Local>> DEFINE EMAIL port2 FROM "Conserv2"
Local>> DEFINE EMAIL port2 SUBJECT "System Crash"
Local>> DEFINE EMAIL port2 MAILHOST "mail.strut.com"
Local>> DEFINE EMAIL port2 REPLYTO "managers@strut.com"
```

Dynamic print variables can be used with all of these command strings. For a complete list of available variables, see **Define Email** on page 12-55.

To enable email notification for a port, use the **Define Ports Event Email Serialdata** command. This command also sets the port's access to Access Remote.

Note: *Email notification only works on ports that have port buffering enabled.*

Figure 3-4: Enabling Email Notification

```
Local>> DEFINE PORT 2 EVENT EMAIL SERIALDATA ENABLED
```

The **List Email** command can be used to show the emailsite configurations for one or more emailsites.

If network logging is enabled (**Set/Define Logging Network Enabled**), any errors that occur during email notification are stored in the system log. System logging is discussed in Chapter 11, *Security*.

3.4 Configuring Menu Mode

When a port is in menu mode, users who log into the port will be presented with a list of menu options. Their choices are limited to those displayed in the menu, as they will not be permitted to enter text commands.

Figure 3-5: Sample Menu

```
Lantronix Console Server

1) Cisco Router                 4) Local> Prompt
2) Sun Server                   5) Logout
3) Linux Server                 6)

Enter Selection:
```

Menus can be configured one of two ways: by entering title and item entries individually with the web browser interface or at the command line, or by creating a menu configuration file.

To enable menu mode on a particular port, use the **Set/Define Ports Menu** command.

Figure 3-6: Enabling Menu Mode on a Port

```
Local>> DEFINE PORT 2 MENU ENABLED
```

To display the current menu, use the **Show/Monitor/List Menu** command. If you are using a menu configuration file, this command will not work—you must view that file to see the menus.

3.4.1 Menu Configuration at the Command Line

Use the **Set/Define Menu** command to create entries for your menu. For each menu entry, specify the option's numbered position in the table, the entry description that will be displayed in the menu, and the actual command invoked when the user chooses that option. **Enclose option and command names in quotes.**

Figure 3-7: Adding a Command Entry

```
Local>> DEFINE MENU 2 "Sun Server" "CONNECT LOCAL PORT_2"
```

It is a good idea to add a command to the menu that allows the user to log out of the server. The **Exit** command only works in menu mode. It allows users to return to the Local> prompt on the SCS on which the menu was configured. It is helpful to include this command in your menus until you have fully tested them—otherwise there is no way for users on menu mode ports to return to the Local> prompt.

Figure 3-8: Adding a Logout Command

```
Local>> DEFINE MENU 5 "Exit" "Logout"
```

3.4.2 Menu Configuration Files

If you need to configure menus for multiple sets of users, you should create a menu configuration file. These files provide more flexibility than the command line options and are easier to use when setting up larger menus. The file is typically stored on the SCS flash disk (/flash).

Each menu in a configuration file is associated with a group. Each group consists of one or more users. One group can include a user **default**, meaning that menu will be used for any users not explicitly in an other group. Only one group can include the default user.

Follow the steps below to create a menu configuration file:

1. Start a new text file on a host other than the SCS. Once the file is complete, you will FTP it to the SCS's /flash disk. The /flash disk and the **Disk** commands are discussed in detail on page 2-18.

2. Define up to 10 groups of users. Each group, listed on separate lines, will later be assigned a specific menu. Do not leave any whitespace between each name—the names should be separated by commas.

```
GROUP austin = sandy,dave,bob,kathy,default
GROUP admin = admin
```

Note: *A space must be included on both sides of the = when defining the groups, as shown in the example above. Also, remove any extra spaces from the end of each line, as they will cause the menu parsing to fail.*

*If desired, you can use wildcards in usernames. To match a single character, use a question mark (**?**), and to match any number of characters, use an asterisk (*****).*

3. Begin defining the menus. Start by assigning a menu to a specific group.

```
MENU austin
```

Then, assign the menu a title (up to five lines). This string will appear at the top of the menu. You can use dynamic print variables in the title, which will appear appropriately when the menu is viewed. You can include up to 5 lines of title information per menu.

```
TITLE "Lantronix Console Server"
```

Note: *For a list of dynamic print variables, see Set/Define Menu on page 12-112.*

4. Define the items that will appear in the menu. The items will be numbered in the order entered. Up to 36 items can be defined in one menu.

```
ITEM "Cisco Router"  "telnet 192.0.1.250"
ITEM "Sun Server" "telnet 192.0.1.251"
ITEM "Linux Server" "connect local port_4"
ITEM "Exit" "Logout"
ENDMENU
```

End the Menu with the line ENDMENU.

5 After ENDMENU, you can go on to define more menus for other groups of users.

```
MENU admin
TITLE “Lantronix Console Server”
ITEM “Cisco Router” “telnet 192.0.1.250"
ITEM “Exit” “Logout”
ENDMENU
```

Figure 3-9 shows what the above entries would look like in the completed menu configuration file:

Figure 3-9: Completed Menu Configuration File

```
GROUP austin = sandy,dave,bob,kathy,default
GROUP admin = admin

MENU austin
TITLE “Lantronix Console Server”
ITEM "Cisco Router"  "telnet 192.0.1.250"
ITEM "Sun Server" "telnet 192.0.1.251"
ITEM “Linux Server” “connect local port_4”
ITEM “Exit” “Logout”
ENDMENU

MENU admin
TITLE “Lantronix Console Server”
ITEM “Cisco Router” “telnet 192.0.1.250"
ITEM “Exit” “Logout”
ENDMENU
```

6 FTP the file to the SCS /flash disk.

To use the menu configuration file, enter the following command:

Figure 3-10: Using a Configuration File

```
Local>> SET MENU FILE /flash/menu.txt
```

Using Set with the above command will automatically parse the file for correctness. You can then permanently set the file with the Define Menu File command. For more information on this command, see **Set/Define Menu** on page 12-112.

Once the file is set and stored on the /flash disk, a user logging into the SCS will be presented with the appropriate menu. The menu configured above, for one of the defined users (sandy, dave bob, kathy, default), would look like the one shown below:

Figure 3-11: Menu Example

```
Lantronix Console Server

 1) Cisco Router          3) Linux Server
 2) Sun Server            4) Exit

Enter Selection:
```

3.4.3 Nested Menus

Nested menus are file-based menus that allow you to nest submenus within a menu file. Submenus have to appear in the file before the menu that references them.

To use submenus, specify **SUBMENU** instead of **MENU** for the start of a new menu block. Then from a different menu, include an action of **GOTOMENU** to jump to the submenu. One or more of the submenu items can include an action of **RETURNMENU** to return to the top-level menu for the current user. After Selecting an Action from the submenu, the user is returned to the top-level menu.

Following is an example of how to nest a menu.

Figure 3-12: Nested Menu Example

```
SUBMENU consoles
TITLE “This is the console submenu”
ITEM ...
ITEM “Return to Main Menu” “RETURNMENU”
ENDMENU


MENU main
TITLE “Welcome to Menuing”
ITEM ...
ITEM “Select a console connection” “GOTOMENU consoles”
ENDMENU
```

3.5 Login Banner Pages

Banner pages allow you to display text messages to users before and after authentication. Banner text information is taken from two files named **prelogin.txt** and **postlogin.txt** stored in the **/ram** or **/flash** directory on the SCS. The SCS does not store or display files stored in the **/ram** directory after rebooting.

To implement login and logout banner text:

1. Create text files with the desired text name **prelogin.txt** and/or **postlogin.txt**.
2. FTP to the IP address of the SCS.
3. Log in with the username **root** and enter the privileged password (**system** by default.)
4. Change directories to **/flash** or **/ram**.
5. "**Put**" the text files into the desired directory.
6. Reboot the SCS.

Subsequent users logging in or out of the SCS see the text in the **prelogin.txt** and **postlogin.txt** files, respectively. The standard company/product/version banner displays if either of these two files is not present in the SCS.

3.6 Managing the Attached Devices

You can manage the SCS's connected serial devices over a network connection or through a modem connection. Both of these methods ensure that the SCS and its attached serial devices are always accessible and manageable, even in critical situations.

3.6.1 In-Band Management

The SCS provides TCP/IP socket connections to its serial ports. A TCP session to port 30*xx*, where *xx* is the serial port number, will form a raw TCP/IP connection to that serial port. A connection to port 20xx provides Telnet IAC interpretation.

Figure 3-13: Telnet IAC Connection to the Second Serial Port

```
% telnet 192.0.1.66 2002
```

To connect to a specific SCS port using SSH, use socket number 22*xx*, where *xx* is the port number. The syntax for an SSH connection depends on your client software. SSH is discussed in *SSH Sessions* on page 6-10.

Figure 3-14: Example of an SSH Connection to the Second Serial Port

```
% ssh -p2202 192.0.1.66
```

3.6.2 Out of Band Management

To ensure that you can manage attached equipment even if there are network problems, the SCS provides an out-of-band management feature. If you have a modem connected to one of the SCS serial ports, you can access and manage the SCS via a dial-in modem connection.

Instructions on modem configuration are available in Chapter 9, *Modems*.

To dial-in to the SCS,

1. Open a terminal emulator such as Hyperterminal
2. Dial the phone number for the modem attached to the SCS.
3. When the connection is complete, press <CR>.

   The username and password prompt appear.
4. Enter your username and password.

   You are now logged in to the SCS serial port.

For instructions on dialing in with PPP, read Chapter 4, *Basic Remote Networking*. Instructions on attaching modems are included in Chapter 9, *Modems*.

3.6.3 Connecting from the Local> Prompt

Before you connect to a serial port, make sure that you have a way to exit the connection. If your keyboard does not have a break key, specify an equivalent using the **Set/Define Ports Local Switch** command.

Figure 3-15: Specifying Local Switch

```
Local>> DEFINE PORT 2 LOCAL SWITCH ’
```

Then, use the **Set/Define Ports Break** command to instruct the break key to bring you back to Local> prompt when pressed during a session.

Figure 3-16: Configuring Break Key Processing

```
Local>> DEFINE PORT 2 BREAK LOCAL
```

To connect to a serial port from the SCS Local> prompt, use the **Connect Local** command.

Figure 3-17: Connect Local Command

```
Local> CONNECT LOCAL PORT_2
```

Once within the session, you can exit by pressing the break key. This returns you to the Local> prompt. For more information on available session options, see *Port-Specific Session Configuration* on page 8-4.

3.6.4 Serial Break Handling

This section describes how to specify serial breaks and alternate break (AltBreak) sequences.

3.6.4.1 Serial Breaks

Break conditions originating from serial connections are controlled on a per port basis. Break conditions originating from incoming Telnet and SSH connections are based on the settings for port 0, the network (template) port.

To define where the break condition will be processed, use the Set/Define Ports Break **[local | Remote]** command for each serial port and port 0.

The default break sequence for port 0 is <Ctrl+Y>. There is no default break sequence for the serial ports.

3.6.4.2 Alternate Break Sequences

You can specify an alternate break (AltBreak) character for use with terminals that cannot natively generate a break condition and for Telnet or SSH clients that cannot generate break IAC sequences. The syntax for specifying an AltBreak sequence is Set/Define Ports Break**[<char> | None]**, where **<char>** is a single character enclosed in **quotes**. You can specify non-printable characters using the notation **\xx**, where xx is the hexadecimal representation for the desired character. The Show/Monitor/List Ports command displays the current setting.

The table below shows some examples to help you understand how the SCS handles breaks.

Table 3-1: Examples of Alternate Break Sequences

If	And	Then
The user Telnets to a remote network host from a local (SCS) serial port	The serial port has **Break = Local**	The AltBreak sequence returns the user to a local (SCS) command prompt.
	The serial port has **Break = Remote**	The AltBreak sequence causes the SCS to transmit a Telnet Break IAC sequence to the remote host.
The user issues a **Connect Local** command to another serial port from a local (SCS) serial port	The user's serial port has **Break = Local**	The AltBreak sequence returns the user to a local (SCS) command prompt.
	The user's serial port has **Break = Remote**	The AltBreak sequence generates a break condition to the target port. (The target port's break settings do not apply or affect this situation.)
The user Telnets to the SCS **Local>** prompt and issues a **Connect Local** command to a serial port	Template port has **Break = Remote**	The AltBreak sequence returns the user to a local (SCS) command prompt.
	Template port 0 has **Break = Local**	The AltBreak sequence generates a break condition to the target port. (The target port's break settings do not apply or affect this situation.)
The user on an SCS serial port makes an SSH connection to a network host	The serial port has **Break = Local**	The AltBreak sequence returns the user to a local (SCS) command prompt.
	The serial port has **Break = Remote**	Nothing happens as there is no way to propagate a break across an SSH connection.
At the **Local>** prompt, the user Telnets to the SCS and receives the default AltBreak character from template port 0	Template port 0 has **Break = Local**	The AltBreak sequence does nothing because breaks are ignored at the **Local>** prompt.
	Template port 0 has **Break = Remote**	

Table 3-1: Examples of Alternate Break Sequences

If	And	Then
The user forms a Telnet or SSH connection to the SCS and Issues a **Connect Local** command to connect to port 7 (Note that port 7's break settings are not applicable.) and receives a default AltBreak character from port 0	The template port (port 0) has **Break = Local**	The AltBreak sequence returns the user to a local (SCS) command prompt.
	The template port has **Break = Remote**	A break condition is generated on port 7.
The user forms a Telnet connection from a host to port 7 on the SCS using socket 2007 and the AltBreak character has been defined on port 7 and the AltBreak character is detected in the data stream from the host (Note that the 20xx range of sockets performs Telnet IAC interpretation.)	Port 7 has **Break = Remote**	A serial break condition is generated on the port.
	Port 7 has **Break= Local**	Nothing happens.
The user forms a Telnet connection from a host to port 7 on the SCS using socket 2007 and the AltBreak character has been defined on port 7 and the a break condition is detected on the serial port (Note that the 20xx range of sockets performs Telnet IAC interpretation.)	Port 7 has **Break = Remote**	A Telnet Break IAC is sent on the network connection.
	Port 7 has **Break = Local**	Nothing happens.

Table 3-1: Examples of Alternate Break Sequences

If	And	Then
The user forms a TCP connection from a host to port 7 on the SCS using socket 3007 and The AltBreak character has been defined on port 7 and The AltBreak character is detected in the datastream from the host (Note that the 30xx range of sockets is 8-bit clean.)	Port 7 has **Break = Remote**	A serial break condition is generated on the port.
	Port 7 is set to **Break = Local**	Nothing happens.
The user forms a TCP connection from a host to port 7 on the SCS using socket 3007 and The AltBreak character has been defined on port 7 and A break condition is detected on the serial port (Note that the 30xx range of sockets is 8-bit clean.)	Port 7 has **Break = Remote** or Port 7 has **Break = Local**	Nothing happens because there is no way to propogate a break across an 8-bit clean connection.

3.7 Serial Port Configurations

This section describes several available configuration and management options for the SCS serial ports. These configurations help ensure easy management of the attached devices.

3.7.1 Enabling the Incoming Password

The **Set/Define Ports Password Incoming Enabled** command requires users who Telnet or SSH directly to the target serial port to provide their username and password pair, which will be checked against the configured authentication databases, before gaining access to the serial port.

Figure 3-18: Enabling the Incoming Password

```
Local> DEFINE PORT 2 PASSWORD INCOMING ENABLED
```

The login password is discussed in *System Passwords* on page 2-7.

3.7.2 Setting the Port Access Mode

A port's access may be set to one of the following: dynamic, local, remote, or none. **Dynamic** (the default) permits both local and remote logins, **local** allows only local logins, and **remote** permits only remote logins. **None** prevents all incoming and outgoing connections, rendering the port unusable.

When using the SCS as a console server, you will want to set most ports to Remote access so any serial data from the attached device will not accidentally cause the SCS to create a local connection and make that port unavailable.

Note: *When port buffering is enabled, the port access is automatically changed to Remote access.*

To configure access to a port, use the **Set/Define Ports Access** command.

Figure 3-19: Setting Remote Access for a Serial Port

```
Local>> DEFINE PORT 2 ACCESS REMOTE
```

3.7.3 Displaying Port Status

Use the **Show Ports Counters** and the **Show Ports Status** commands to display current serial port information. Counters displays the port's local and remote accesses as well as any communication errors. The Status parameter shows information regarding the port's serial connections, including the current flow control state and the state of the DSR and DTR signals.

3.7.3.1 SNMP Queries

You can also check a port's status by sending an SMNP query. Parts of the MIB-II, RS-232 MIB, and Character MIB cover individual serial port status. Use an SNMP management application to query the SCS for the port status.

For more information on SNMP, see , .

4: Basic Remote Networking

The SCS allows remote users to securely connect to local network resources, or two Local Area Networks (LANs) to connect to each other. This chapter describes how to initialize, maintain, and disconnect individual remote user dial-ins and LAN to LAN remote connections.

After completing this chapter, you should be able to configure the SCS to support the following types of connections:

- Incoming remote user dial-in
- Incoming character, PPP, and SLIP modes
- Basic outgoing LAN to LAN using PPP

The functionality described in this chapter may not meet all of your performance or network security needs. If your network requires more complex configuration, or if you are not using modems, refer to Chapter 5, *Additional Remote Networking*, for additional configuration instructions.

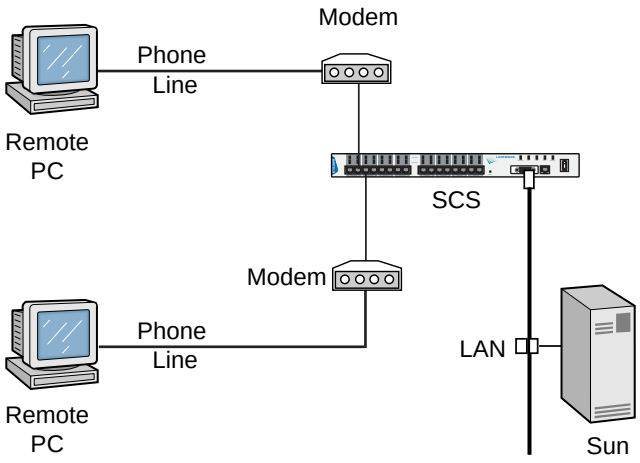
4.1 Remote Connection Types

The SCS is capable of two types of remote networking connections: LAN to LAN and remote node.

4.1.1 Remote Dial-in

A remote user, or **remote node,** connection allows remote dial-in users to securely access network resources. Users can access network file servers, send or receive email, use the Internet, or remotely administer equipment. For example, a laptop user on a business trip may wish to access files from a network's file server. Using a modem, the laptop could dial the SCS, form a connection, and download the files as if the laptop were directly connected to that network.

Figure 4-1: Remote Dial-In Example

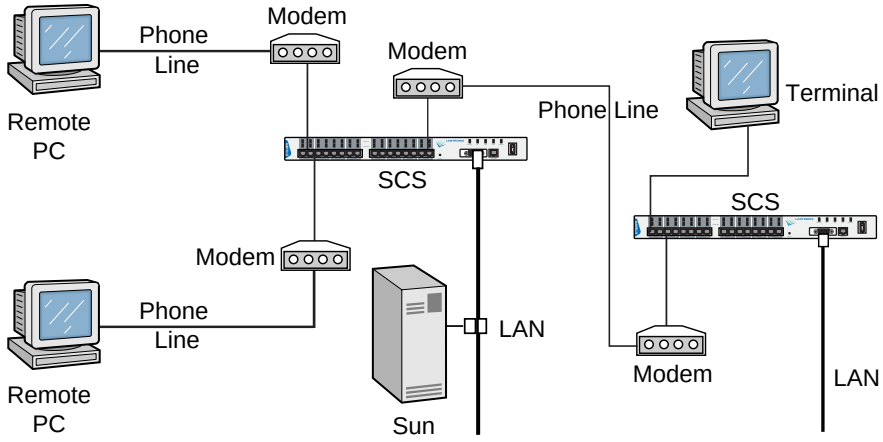


The SCS cannot initiate connections to remote nodes. Remote nodes must call the SCS when they wish to communicate with the network.

4.1.2 LAN to LAN

In **LAN to LAN** connections, the SCS provides a link between two networks. The SCS will communicate with a remote router, which may be another access server, a UNIX machine capable of PPP routing, or another SCS. The SCS may be connected to the remote router with temporary "dial on demand" connections such as ordinary dialup modems. The SCS may also be permanently connected to the remote router with leased lines, a statistical multiplexor, or a direct serial connection.

Figure 4-2: LAN to LAN Example



LAN to LAN connections are often used to connect two locations that do not always need to be connected. For example, a small remote office with only a few nodes and a central office might need to be connected occasionally, however, the amount of traffic wouldn't warrant using a leased line for the connection. Using an SCS and dialup modems, the connection would come up and go down when required, simulating a permanent connection between the two locations.

4.2 Managing Connections With Sites

Every incoming and outgoing network connection is associated with a site. A **site** represents a remote physical location, such as a remote router or a remote node. Sites are referenced by a name, such as **seattle**. The site's name should indicate the physical location of the remote device, a group of remote node users, or a particular remote node user.

Note: *Using sites for connections enables each connection to have different characteristics; connections aren't limited solely to the characteristics of the ports used.*

Sites serve four purposes:

1. To configure the SCS and the remote router appropriately for a connection. For example, particular SCS ports may be assigned for use with the connection.

2. To enforce specific network requirements. For example, compression may be required for all connections.

3 To manage a connection once it is in place. For example, it may be desirable to control the amount of bandwidth used for a connection.

4 To enable a system administrator to monitor a single connection. For example, a system administrator may wish to restrict remote node users to a particular range of IP addresses.

The type of authentication used determines which sites will be used. For more information, see *Incoming Connections* on page 4-11 and *Outgoing Connections* on page 4-16.

The **Define Site** commands are used to create new sites and edit existing sites. The **Show/Monitor/List Sites** commands are used to get information about existing sites. These commands require privileged access, which is denoted in the following examples with the Local>> prompt. For information on obtaining privileged access, see *Privileged Password* on page 2-8.

4.2.1 Creating a New Site

To create a new site, assign a name using the following command.

Figure 4-3: Creating a New Site

```
Local>> DEFINE SITE IRVINE
```

The site you just created will use the **default site** configuration (see Table 4-1 on page 4-3). Those settings can be changed to meet your needs.

4.2.1.1 Default Site Configuration

The default site configuration is used for all temporary sites and is automatically assigned to any new site created with the **Define Sit**e commands. To display the default configuration, use the following command:

Figure 4-4: Displaying Default Sites

```
Local>> LIST SITE DEFAULT
```

The following table lists the default site configuration.

Table 4-1: Default Site Configuration

Characteristic	Configuration in Default Site
CHAP authentication on outgoing calls	Disabled
PAP authentication on outgoing calls	Disabled
Remote password	None configured
Local password	None configured
Username	None configured
Chat script entries	None
IP compression	Enabled
IP packet forwarding	Enabled
Maximum idle time	10:00 (10 minutes)

Table 4-1: Default Site Configuration

Characteristic	Configuration in Default Site
Remote host's IP configuration	Undefined
IP compression slots	16
Maximum packet size (MTU): PPP	1522
Ports defined	None
PPP	Enabled
SLIP	Disabled
Telephone number of remote site	None defined
Outgoing packet filter	None defined
Incoming packet filter	None defined
Idle time filter	None defined
Startup filter	None defined
Maximum packet size (MTU): SLIP	1500
Maximum session time	Disabled

4.2.2 Displaying Existing Sites

To display all defined sites, use the **List Site** command. To display currently active sites, use the **Show Site** command.

To display specific information about sites, the following parameters may be used in conjunction with **Show Site** and **List Site**: IP, Ports, Counters, and Status. For example, to display the IP configuration of site **irvine**, use the following command:

Figure 4-5: Displaying a Site's IP Configuration

```
Local>> LIST SITE IRVINE IP
```

Note: *The List Site command is used in Figure 4-5 because site irvine isn't currently running.*

4.2.3 Editing Sites

All site characteristics can be edited with the **Define Site** commands. For example, a site's authentication can be edited with the command below.

Figure 4-6: Editing Site Characteristics

```
Local>> DEFINE SITE irvine AUTHENTICATION PAP DISABLED
```

Note: *Site Commands are discussed on page 12-132.*

Currently active sites can be edited, but changes will not take effect until the site is logged out.

4.2.4 Testing Sites

The **Test Site** command causes a site to start as if outgoing traffic for the site had come into the SCS. It allows users to test sites without having to generate packet traffic. To test a site, enter a command similar to the following.

Figure 4-7: Testing a Site

```
Local>> TEST SITE irvine
```

The terminal will display a message that the specified site has started. To stop the test, enter the **Logout Site** command followed by the site name.

In the event that there is a problem with the site, or if the Test Site command does not work, use the SCS site logging feature to troubleshoot the problem. See **Set/Define Logging Site** on page 12-172 and **Show/ Monitor/List Logging Site** on page 12-179 for more information.

4.2.5 Deleting Sites

To delete a site, use the **Purge Site** command.

Figure 4-8: Deleting a Site

```
Local>> PURGE SITE irvine
```

When the Purge command is used with the default site, the site's default configuration will be restored. Any editing changes you've made to the default site will be removed.

Figure 4-9: Restoring Default Site Configuration

```
Local>> PURGE SITE DEFAULT
```

4.2.6 Using Sites for Incoming Connections

Incoming connections, both remote node and LAN to LAN, can use either custom sites or temporary sites which use the default site's configuration.

Custom sites allow the most flexibility in the control and configuration of incoming connections. They are used when a specific configuration is required for the incoming router or remote node, and should be named for the location or user that is calling the SCS. Custom sites are required for Dialback and are recommended for incoming LAN to LAN connections.

If a group of incoming connections can use the same configuration, they can be allocated temporary sites used only for that session to save time and system resources. Each temporary site takes its configuration from the SCS default site. The default site may be customized in the same manner as custom (named) sites; this customized configuration can then be shared with many remote routers and remote nodes.

Note: *The default site configuration is listed in Table 4-1 on page 4-3.*

When an incoming caller is allocated a temporary site, the name of the site is based on the port receiving the call. For example, an incoming call to port 3 may be allocated a temporary site named **Port3**.

4.2.7 Using Sites for Outgoing Connections

Note: *The SCS does not support outgoing remote node connections.*

A site must be configured for each outgoing LAN to LAN connection. This site controls when and how the SCS will call the remote location, what protocols to use, and when to terminate the connection.

Outgoing sites are typically named for the remote router that the SCS will call; for example, if a site is used for outgoing connections to a remote router in Dallas, the site used for the connection might be named **dallas**. This site could also be used for incoming calls; if the router in Dallas needed to call the first SCS, it could use dallas to make the connection.

4.2.8 ISP Site Connections with NAT

Network Address Translation (NAT) functionality allows a private network to share a single public (Internet) IP address to access the Internet. This connection is normally made by dialing an ISP dialup account. Note that the ISP must support PPP dialers. ISPs that use proprietary dialers (for example, ones that do not work with Windows Dialup Networking) will not work with the SCS's ISP connection.

To set up NAT, the systems administrator must select a private network range for the local devices and assign a single valid non-private IP address for the SCS. Valid private IP address ranges are:

Table 4-2: Valid Private IP Address Ranges

Class	Address Range	Subnet Mask
Class A	10.n.n.n	255.0.0.0
Class B	172.16.n.n through 172.20.n.n	255.255.0.0
Class C	192.168.n.n	255.255.255.0

To configure NAT support:

1. Create the SCS's IP address to an address on a private subnet, for example:

Figure 4-10: Configuring the SCS's IP Address

```
DEFINE PROTO IP IPADDR 192.168.13.1
```

2. Create the site that will dial up the ISP. Your ISP will provide most of the information:

Table 4-3: Creating the Site

Command	Description
DEFINE PORT n MODEM TYPE y	n = port or ports; y = modem type # (Use command SHOW MODEM to see list of modem types.)
DEFINE SITE OUTGOING PORT n	n = port(s) with modem attached
DEFINE SITE OUTGOING AUTH USER n	n = username provided by the ISP

Table 4-3: Creating the Site

Command	Description
DEFINE SITE OUTGOING AUTH REMOTE n	n = password from ISP (place in quotes if lower case)
DEFINE SITE OUTGOING TELEPHONE n	n = ISP dial-up POP phone number
DEFINE SITE OUTGOING AUTH PAP ENABLE	Support for PAP authentication
DEFINE SITE OUTGOING AUTH CHAP ENABLE	Support for CHAP authentication
DEFINE IP NAMESERVER n	n = DNS provided by ISP
DEFINE IP SEC NAMESERVER n	n = back-up DNS provided by ISP
DEFINE IP ROUTE DEFAULT SITE OUTGOING	Routes non-private traffic to Internet

3 Set the IP address of the site to the single non-private (Internet) address for your network.

If your ISP provides a static IP address, the command would look like this:

Figure 4-11: Configuring a Static Public IP Address

```
DEFINE SITE OUTGOING IP ADDRESS 201.73.220.92
```

or, if your ISP provides an IP address dynamically, the command is:

Figure 4-12: Configuring a Dynamically Assigned IP Address

```
DEFINE SITE OUTGOING IP ADDRESS DYNAMIC
```

Note: *This command will turn the site interface into a **numbered** interface.*

4 Enable NAT on the SCS, using the **DEFINE IP NAT ENABLED** command.

5 Configure the NAT parameters if needed.The default parameters are sufficient for most situations.To view the settings, use the **LIST IP NAT** command.

6 Configure the SCS as the gateway on the machines on the private network (e.g., 192.168.13.2,.3, etc.). Where possible, set the default route and gateways for machines in the private network to the SCS's IP address.

4.3 IP Address Negotiation

By default, sites use "unnumbered" interfaces for IP. The IP address of the Ethernet connected to the SCS will be used as the IP address on all SCS serial ports. This reduces the amount of configuration and eliminates the need to allocate a separate IP network for each port.

When the SCS receives an incoming connection request (remote node or LAN to LAN), an IP address is negotiated for the caller. The address agreed upon depends on the caller's requirements; some don't have a specific address requirement, while others must use the same IP address each time they log into the SCS.

Note: *PPP negotiation is covered in Chapter 7, PPP.*

The SCS can also be used to connect to a dialup network such as Earthlink, where the network will then assign you a nameserver and an IP address. For this functionality, the nameserver of the SCS should be set to 0.0.0.0 (with the **Set/Define IP Nameserver** command) and the SCS should be set to accept dynamic IP addresses (with the **Define Site IP Address Dynamic** command).

For a complete discussion of IP address assignment (including configuration instructions), see *IP Addresses* on page 6-1.

4.4 IP Routing

The following sections discuss IP routing issues as they pertain to remote networking. For a complete discussion of IP routing, refer to Chapter 6, *IP*.

When a packet is received from or generated for a remote network, the SCS will check its routing table to determine the most efficient route to the destination. If the SCS does not have a route to a remote network, it cannot send the packet to the destination.

The entries in the routing table are one of three types:

Local routes — The network that is directly attached. This route is automatically determined from the SCS IP address and network mask, and is never deleted.

Static routes — Routes that were manually entered in the routing table by a system administrator. These routes are used when the dynamic routes cannot be.

Dynamic routes — Routes learned through the receipt of RIP (Routing Information Protocol) packets. RIP is discussed in more detail on page 4-10.

Each routing entry can point to another router on the Ethernet or to a site configured for LAN to LAN connections.

4.4.1 Routes for Outgoing LAN to LAN

Generally, the SCS has static routes configured for each remote LAN that it will connect to. These routes point to sites that are configured for outgoing LAN to LAN connections. The first time that the SCS needs to send a packet destined for a network on a remote LAN, the site will be activated and the SCS will attempt to call the remote router. Once the connection has been formed, subsequent packets for the remote LAN will be forwarded over that link.

While the SCS is connected to the remote router, it may learn additional dynamic routes from that remote router. Once these additional routes are entered into the routing table, packets may be routed to these new networks as well. Once the connection is dropped, the SCS can be configured to maintain these routes. Subsequent traffic to these dynamically learned networks or to the pre-existing static route networks will cause the site to form a new connection.

If the SCS is a **stub router** (or you're using the SCS to connect to the Internet), default routes can be used to reduce configuration time. A stub router connects a LAN without any routers to a larger LAN. For example, in a remote office with no other outside connections, an SCS that connects to exactly one other (larger) location is a stub router. All traffic generated on the remote office's LAN that is destined for the remote location must pass through the SCS. A default route pointing to the larger site may be entered on the SCS.

Note: *Default routes should be used with caution. See Chapter 6, IP for complete details.*

4.4.2 Routes for Incoming LAN to LAN

If RIP (Routing Information Protocol) is being used, no static routing entries need to be configured on the SCS. Routes to networks on the remote LAN will be learned automatically. For more information on RIP, see *Configuring RIP for Sites* on page 4-10.

Note: *RIP is enabled by default.*

If RIP is not being used, the SCS must have a specific site configured for this incoming connection. The remote router must use this site when it connects to the SCS. The site may be started in one of two ways: through the authentication sequence (which requires that authentication be appropriately configured), or with the **Set PPP *sitename*** command. Static routes pointing to the site must be configured for each of the incoming caller's IP networks.

Note: *To configure authentication, see Configuring Incoming Connections on page 4-14 or Chapter 11, Security.*

4.4.3 Routes for Remote User Dial-ins

The SCS automatically generates routes for remote nodes when the node connects. These routes are deleted when the connection is terminated.

If the remote node receives a dynamic address from the SCS's IP address pool, a host route is entered for that address. If proxy ARPing is enabled (see *Proxy ARP* on page 6-22), the SCS will proxy-ARP for the address. See *Types of Routes* on page 6-19 for more information.

If a remote node uses an IP address that is not on the Ethernet's IP network, then the SCS will enter a network route for that node. For example, if the SCS's Ethernet IP address is 192.0.1.4, and a node selects the address 192.0.2.6, the SCS will enter a route to 192.0.2.0 in its routing table.

Remote nodes do not have to make routing decisions, as they can only send network packets to the SCS. Therefore, most remote nodes do not need to receive RIP packets. Sites that only support remote nodes may turn off RIP to reduce traffic on the connection.

Figure 4-13: Disabling RIP Packets

```
Local>> DEFINE SITE IP RIP DISABLED
```

Note: *For more information about disabling RIP, see Define Site IP on page 12-140.*

4.4.4 Configuring RIP for Sites

RIP (Routing Information Protocol) packets enable the SCS to broadcast its known routes and receive routing information from other routers. Each site may configure RIP in a number of ways.

4.4.4.1 Disabling RIP

By default, SCS sites will both listen for and send RIP packets. However, in some situations, RIP should be disabled. For example, if the routers on both sides of a link have been pre-configured with all necessary routing information (with static routes)

Figure 4-14: Disabling RIP

```
Local>> DEFINE SITE irvine IP RIP DISABLED
```

If you want the SCS to either listen for or send RIP packets, but not both, you can selectively disable one or the other. The following example turns off listening for RIP packets.

Figure 4-15: Disabling RIP Listen

```
Local>> DEFINE SITE irvine IP RIP LISTEN DISABLED
```

4.4.4.2 Interval Between RIP Updates

When RIP sending is enabled, the SCS sends RIP updates every thirty seconds. This number can be adjusted; for example, the update interval may be raised so that RIP updates are sent every minute to reduce network traffic.

To configure the update interval, use the **Define Site IP RIP Update** command. The interval must be specified in seconds; intervals between 10 and 255 seconds are permitted.

Figure 4-16: Adjusting RIP Update Intervals

```
Local>> DEFINE SITE irvine IP UPDATE 60
```

4.4.4.3 Configuring the Metric

Each RIP packet lists known routes and the “cost” associated with each of these routes. Each SCS site may configure the cost of its interface; all routes learned through the site will be associated with that cost.

When a router determines a route to a particular destination, a route with a lower cost is more likely to be included in the route. Configuring a higher RIP cost on a particular site makes the interface a less desirable route to other destinations.

To set a site's IP RIP metric, use the **Define Site IP RIP Metric** command.

Figure 4-17: Configuring a Site's RIP Metric

```
Local>> DEFINE SITE irvine IP RIP METRIC 4
```

In the example above, all routes learned through site **irvine** will be associated with cost 4. The higher the cost number, the less desirable the route.

Note: *If IP RIP sending is disabled on a site, the Update and Metric values will be ignored.*

4.5 Incoming Connections

This section describes how the SCS deals with incoming connections. When a remote device or network tries to connect, the SCS forms a serial connection using its asynchronous serial lines. A protocol is then run on this serial connection to allow network packets to be sent.

The SCS supports the use of PPP and SLIP to send network packets.

PPP The Point to Point protocol (PPP) is recommended whenever possible. PPP enables devices to simultaneously transport IP packets, negotiate certain options, authenticate users, and use checksums with virtually no performance loss.

SLIP The Serial Line Internet Protocol (SLIP) is supported primarily for backwards compatibility with equipment that does not support PPP. SLIP can only transport IP packets—it does not support negotiation of IP address or other options, nor does it provide any diagnostic facilities.

PPP is enabled by default, while SLIP is disabled by default. To change these settings, use the **Define Ports PPP** and **Define Ports SLIP** commands. For more information on these commands, see *Port Modes* on page 8-3.

Figure 4-18: PPP and SLIP

```
Local>> DEFINE PORT 2 PPP DISABLED
Local>> DEFINE PORT 2 SLIP ENABLED
```

4.5.1 Starting PPP/Slip for Incoming Connections

When you initiate an incoming LAN to LAN or remote node connection, you can start PPP or SLIP one of several ways:

- The caller may be presented with a Local> prompt (the port will be in character mode), requiring him to enter commands in order to run PPP or SLIP.

Note: *For a description of the port modes, see Port Modes on page 8-3.*

- The port may detect when a PPP or SLIP packet is received and automatically run the appropriate protocol.
- The port may be dedicated to PPP or SLIP; the protocol will automatically run when any character is received.

A port may be configured to offer a combination of these methods, giving the incoming remote node or router flexibility in how the connection is started.

To configure the SCS for incoming LAN to LAN and remote node connections, see *Configuring Incoming Connections* on page 4-14.

4.5.1.1 Starting PPP or SLIP from the Local> Prompt

You can enter the **Set PPP** and **Set SLIP** commands at the Local> prompt. The remote router or node must then pass through the authentication procedures, if enabled, on the port in character mode. The remote device must support chat scripts or must rely on a user to enter the required information and type **Set PPP** or **Set SLIP** at the Local> prompt.

> **Note:** *For a complete description of authentication, refer to Chapter 11, Security. For information on chat scripts, see Chat Scripts on page 5-3.*

If no site name is given in the **Set PPP** or **Set SLIP** command, a temporary copy of the default site will be started. If a custom site is to be started, it can be specified as a string: **Set PPP *sitename***.

> **Note:** *To prevent users from starting inappropriate sites, users can be prompted for the site's local password.*

To use the **Set PPP** and **Set SLIP** commands, enable PPP and/or SLIP on the port used for the connection. See *Incoming Connections* on page 4-11.

4.5.1.2 Starting PPP or SLIP Using Automatic Protocol Detection

You can configure an SCS port to automatically detect a PPP or SLIP packet and, if PPP or SLIP is enabled on the port, run the appropriate protocol when the packet is received. This eliminates the need for callers to explicitly start PPP or SLIP.

Enable the PPP autodetection feature with the **Define Ports PPPdetect** command. This starts PPP with a temporary copy of the default site. To enable SLIP autodetection, use **Set/Define Ports SLIPdetect**.

Figure 4-19: Enabling Automatic Protocol Detection

```
Local>> DEFINE PORT 2 PPPDETECT ENABLED
Local>> DEFINE PORT 3 SLIPDETECT ENABLED
```

To run a custom site, enable PPP authentication on the port (see Chapter 11, *Security*, for more information on PPP authentication). If the remote device sends a valid username and password, and the username matches a site name, that site will start running on the port. All further configuration of the connection will be from this new site.

Be aware that in some cases automatic protocol detection should be disabled for security purposes. For more information, see *Automatic Protocol Detection* on page 8-4.

4.5.1.3 Starting PPP or SLIP on a Dedicated Port

You can dedicate an SCS serial port so it automatically runs PPP or SLIP when that port is started. No other protocol can be run on the port; it will continue to run PPP or SLIP until the port is logged out. Whenever the port receives a character, it starts up a temporary copy of the default site using the appropriate link layer. A dedicated port cannot be used for character mode connections and the Local> prompt cannot be reached.

To dedicate a port to PPP or SLIP, use the following command:

Figure 4-20: Dedicating a Port to PPP/SLIP

```
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 3 SLIP DEDICATED
```

Once PPP or SLIP is running, the behavior of a dedicated port is the same as a port with automatic protocol detection enabled. A dedicated port also has the same security issues as a port with automatic protocol detection enabled, so you should setup some form of PPP authentication if you wish to avoid potential abuses. Dedicated ports only provide access to the temporary site; if you wish to use a custom site, you should instead enter the **Set PPP**/**Set SLIP** commands at the Local> prompt.

When a port is dedicated, the local prompt cannot be accessed, therefore, commands can't be entered to disable the Dedicated characteristic. Take caution when dedicating ports; if you're going to dedicate all SCS ports, be sure that you have another way to log into the server (such as a Telnet login).

Note: *If you cannot log into the SCS, you'll need to restore the server to its factory default settings. See Initialize Server on page 12-111.*

4.5.2 Incoming Connection Sequence

The following steps detail the events that occur when the SCS receives an incoming call.

4.5.2.1 Ports Using Automatic Protocol Detection

If the port receiving the call is using automatic protocol detection, or is dedicated to SLIP or PPP, the following sequence of events take place:

1. If automatic protocol detection (for PPP, SLIP, or both) is enabled, the link layer starts up when a PPP or SLIP character is received from the incoming call.

   If the port is dedicated, the link layer starts upon the receipt of any character.

2. The caller is attached to a temporary site. The name of this site is based on the port number used. For example, an incoming call to port number 6 will generate a temporary site named **Port6**.

3. If using SLIP, callers continue to use the temporary site for the remainder of the connection.

   If using PPP, the following steps occur:

   A. If the SCS port receiving the call has been configured to authenticate remote hosts using CHAP or PAP, CHAP/PAP requests a username and password from the remote host.

      If the remote host has been configured to send a username and password, it sends the pair to the SCS.

B The username and password are compared to existing site names. One of the following occurs:

1 If the username matches the name of a site, the site will be checked to see if it has a local password. If it does, this will be compared to the password entered by the caller. If the passwords match, the user will begin using the custom site; the temporary site will stop running.

2 If a site isn't configured with a password, or the password entered by the caller doesn't match the site password, the username/password pair are compared to any authentication databases.

One of two outcomes is possible.

- If a match is found, the connection is successfully authenticated. The caller continues using the temporary site for the remainder of the connection.

- If a match is not found, the connection attempt fails.

4.5.2.2 Ports Not Using Automatic Protocol Detection

If an incoming call is received on an SCS port that's not configured to automatically run PPP or SLIP, the following login sequence occurs.

1 The caller sends a carriage return.

2 If the port is configured to prompt for a login password, the caller must enter the correct login password to continue.

If the port is configured to prompt for a username, the caller must enter a username.

If the port is configured for authentication, the caller must enter a valid password for the username.

3 To start the link layer, the caller has to enter commands to start PPP or SLIP (**Set PPP** or **Set SLIP**).

One of two scenarios occurs:

A If the caller specifies a site to be started when PPP or SLIP is started, the user is attached to that site. If the site is configured to prompt for its local password, the user must enter the site's local password.

At this point, the caller is unable to run another site.

B If a site isn't specified, the user is attached to a temporary site. The name of this site is based on the port number used. For example, an incoming call to port number 6 generates a temporary site named **Port6**. This site is then used for the remainder of the call.

Note: *Incoming LAN to LAN connections use chat scripts to enter any necessary commands. See Chat Scripts on page 5-3.*

4.5.3 Configuring Incoming Connections

Configuring the SCS for LAN to LAN and remote node networking involves the following steps.

1 Configure the Ports

To properly configure the serial ports, decide whether PPP or SLIP will be used, whether the ports will be dedicated to PPP or SLIP, whether autodetection of PPP or SLIP will be used, and, if a modem is attached it any of the ports, how it will be configured.

To configure a port's use of PPP or SLIP, see Chapter 8. To configure modems, see Chapter 9.

2 Create the Sites

See *Creating a New Site* on page 4-3 for instructions.

3 Configure Authentication

Two types of authentication can be configured: use of the server login password and username password pairs for individual users.

- Login Password

  In order to use a login password, a port must be in character mode. See Chapter 8, *Ports*, to configure a port's use of modes.

  Set the login password using the **Set/Define Server Login Password** command. Then, enable the use of the login password on the appropriate port(s) using the **Set/Define Ports Password** command.

Figure 4-21: Defining the Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
Local>> DEFINE PORT 3 PASSWORD ENABLED
```

Note: *Passwords are case-independent, even when enclosed in quotes.*

By default, incoming Telnet and Rlogin connections are not required to enter the login password. To require the login password, use the **Set/Define Server Incoming** command, described on page 12-119.

- Username/Password Authentication

  Enable authentication on the appropriate ports.

Figure 4-22: Enabling Authentication

```
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
```

If authentication should be performed before PPP or SLIP is running (while the port is still in character mode), ensure that autodetection of PPP and SLIP is disabled (see Figure 4-23). If the port automatically detects and runs PPP or SLIP, there will be no way to authenticate the user because the local prompt cannot be accessed.

Keep in mind that PPPdetect and SLIPdetect will only need to be disabled on ports that have PPP and/or SLIP enabled.

Figure 4-23: Disabling Autodetection of PPP and SLIP

```
Local>> DEFINE PORT 2 PPPDETECT DISABLED
Local>> DEFINE PORT 2 SLIPDETECT DISABLED
```

In order for SLIP users to perform authentication, SLIPdetect must be disabled. SLIP users will only be able to authenticate incoming connections while the port is in character mode; once the port is running SLIP (for example, if the port is dedicated to SLIP using the **Define Ports SLIP Dedicated** command), authentication cannot be performed.

If the port is configured to automatically run PPP and you'd like to use CHAP or PAP to obtain a username and password from the incoming caller, enable remote CHAP and/or PAP authentication on the desired port.

Figure 4-24: Enabling CHAP Authentication

```
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 PPP PAP REMOTE
```

Note: *CHAP and PAP may both be enabled on the same port.*

If incoming connections will be entering usernames to start a custom site, ensure that the site has a local password. Callers will be required to enter this password in order to start the site.

Figure 4-25: Configuring a Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION LOCAL "gorilla"
```

Configure any databases that will be used for authentication and add the appropriate usernames and passwords. See Chapter 11, *Security*, for configuration instructions.

4.6 Outgoing Connections

Note: *The SCS does not support outgoing remote node connections.*

When the SCS receives a packet, it consults its routing table to determine the best route to the packet's destination. If the specified route points to a site, a connection to the site may be initiated. The connection will be subject to any restrictions defined for the site, such as a startup filter or time of day restrictions.

When a connection to the remote router is initiated, a limited number of packets will be buffered until the connection is formed. When the connection is successful, the packets will be sent.

Note:*To restrict outgoing connections, see Chapter 11, Security.*

The SCS can form outgoing connections where it accepts an IP address and a nameserver from the remote PPP site. Enable this feature with the **Set/Define IP IPaddress Dynamic** command. Connections which require these settings include sites which dial up an ISP, where the ISP then assigns the SCS a nameserver and IP address. For more information, see *Dialing Out to an ISP* on page 6-5.

To configure the SCS for outgoing connections, you must set up sites. The following sections describe how the SCS handles these connections.

4.6.1 Ports for Outgoing Connections

Each site must specify which SCS ports may be used for outgoing connections. More than one port may be specified; for example, site **dallas** might specify that port 2 or port 3 could be used for outgoing connections.

When the SCS attempts to make a connection to a site, it attempts to use one of the specified ports. If the port is busy (in use with another connection), it attempts a connection using another specified port. The SCS uses the port priority setting to determine which ports to try and in what order. In the following example, site **dallas** will try port 2 first, then port 3.

Figure 4-26: Port Priority for Sites

```
Local>> DEFINE SITE dallas PORT 2 PRIORITY 1
Local>> DEFINE SITE dallas PORT 3 PRIORITY 2
```

If all ports are busy, the SCS will time out the site for a few minutes and then try again. The connection timeout between call attempts is user configurable. See **Define Site Time Failure** on page 12-146.

More than one site may specify a particular port. For example, site **dallas** and site **seattle** may specify that port 3 may be used for connections. If site dallas is using port 3 at a certain time and site seattle is started, seattle will attempt a connection using another specified port. If no other port is specified for site seattle, it will wait until port 3 becomes available.

Note: *To learn how incoming calls use ports and sites, see Starting PPP/Slip for Incoming Connections on page 4-11.*

4.6.2 Telephone Numbers

Each site may specify one port-independent telephone number and one or more port-specific telephone numbers. A port-independent telephone number is typically used if all ports are configured to call the same number; for example, if the ports are calling a telephone hunt group. Port-independent telephone numbers should be used whenever possible; this frees a site to dial the remote site's number from any of the ports the site is associated with.

Port-specific telephone numbers are used when a particular SCS port should call a specific number at the remote site. These numbers will override a port-independent telephone number. For example, in order to get the most efficient use out of connected modems, a site might specify that when port 2 (connected to a high speed modem) is used, another high speed modem should be dialed. When port 3 (connected to a slow speed modem) is used, the SCS should dial another slow speed modem.

If a site does not have a telephone number defined, the SCS assumes that either there's a direct connection between the SCS and the remote host, or that a chat script (see Chapter 5, *Additional Remote Networking*) will be used to communicate with the remote host.

4.6.3 Authentication

The remote site may require that the SCS authenticate itself by sending a username and password. The username that the SCS sends is (by default) the site name. To send a different username, use the **Define Site Authentication Username** command, described on page 12-132.

The password sent is a site-specific password called the **remote password**. The remote password is used only for outgoing connections, and must be sent via PPP. See *Configure Authentication* on page 4-19 for configuration instructions.

SLIP does not support authentication. To perform authentication, SLIP users must use **chat scripts**. See *Chat Scripts* on page 5-3 for more information.

4.6.4 Configuring Outgoing Connections

To configure the SCS for outgoing connections, complete the steps in the following sections.

4.6.4.1 Configure Ports

All ports that will support outgoing connections must be configured for dynamic connections. Use the following command.

Figure 4-27: Permitting Outgoing Connections

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

Note: *For more information on port configuration, see Chapter 8, Ports.*

4.6.4.2 Configure Modems

Enable modem operation on the port(s) used for outgoing calls. Then, assign a **modem profile** to the port using the **Define Ports Modem Type** command.

Figure 4-28: Enabling Modem Operation

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 5
```

Note: *A modem profile automatically sets up a port for a specific type of modem. Define Ports Modem Type is listed on page 12-16. Modem profiles and complete modem configuration instructions are discussed in Chapter 9, Modems.*

4.6.4.3 Create a Site

Every outgoing connection must use a site. Each site is initially created with a default set of configurations. See *Creating a New Site* on page 4-3 for details on how to create a site.

To display the current configuration, use the **List Site** command.

Figure 4-29: Listing a Site's Configuration

```
Local>> LIST SITE irvine PORTS
```

List Site can be used with a number of parameters, which display different aspects of a site's configuration. For example, **List Site Ports** will display all ports associated with the site.

4.6.4.4 Select Ports to Use for Dialing Out

Once a site is created, the ports that it will use to dial the remote location must be defined. Each site must be associated with at least one port. Use the following command:

Figure 4-30: Associating a Site With a Port

```
Local>> DEFINE SITE irvine PORT 2
```

4.6.4.5 Assign a Telephone Number to the Port or Site

If the site will be used with modems, at least one telephone number must be specified so that the site can dial a remote host. The number may be assigned specifically for use with a particular port, or for use with any port. To assign a port-specific telephone number, use the **Define Site Port Telephone** command.

Figure 4-31: Assigning a Port Telephone Number

```
Local>> DEFINE SITE irvine PORT 2 TELEPHONE 547-9549
```

To assign a telephone number to the site that may be used with any port, use the **Define Site Telephone** command.

Figure 4-32: Assigning a Site Telephone Number

```
Local>> DEFINE SITE irvine TELEPHONE 867-5309
```

A port-specific telephone number will override a site telephone number. For example, site irvine may be configured to use the number 635-9202 on any port it's using, but only the number 845-7000 when it's using port 3.

4.6.4.6 Configure Authentication

When an outgoing connection is attempted, the remote router may or may not require the SCS to authenticate itself. One of the following scenarios will generally apply:

- The remote router uses CHAP or PAP to prompt the SCS to authenticate itself

  This scenario is the most common; the configuration instructions in this section assume that CHAP or PAP will be used.

- The remote router requires a login password

  In this case, the SCS will need to use a chat script to communicate the password to the remote router. See Chapter 5, *Additional Remote Networking*, for instructions.

- The remote router does not require authentication

The instructions in this section will not be necessary. Continue to *Configure Routing* on page 4-20.

Before configuring authentication, ensure that you have the username and password required to log into the remote router. In addition, determine whether the remote router will use PAP or CHAP to transmit the username and password.

Configure the username and remote password to be transmitted.

Figure 4-33: Defining Local Username and Password

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME "doc_server"
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE "giraffe"
```

If CHAP will be used, enable CHAP on the site. To use PAP to transmit the username and password, enable PAP on the site.

Figure 4-34: Enabling CHAP/PAP Authentication

```
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE irvine AUTHENTICATION PAP ENABLED
```

4.6.4.7 Configure Routing

Static routes to the site must be entered in the IP routing tables. To configure IP routing, see Chapter 6, *IP*.

4.7 Monitoring Networking Activity

To monitor current remote networking activity, use the **Show Site** or **Monitor Site** command. Show Site displays the activity associated with a particular site, including the number of packets received and transferred, idle time, current state of the site's ports, and configuration of its associated protocols (for example, IP). Monitor Site will update and redisplay this information at three-second intervals.

Table 4-4: Show/Monitor Site Commands

Commands	Description
Show/Monitor Sites	Lists currently running sites.
Show/Monitor Site <sitename>	Displays the site's configuration.
Show/Monitor Site <sitename> Counters	Displays the site's current performance.
Show/Monitor Site <sitename> Status	Shows all sites that have attempted or completed connections.
Show/Monitor Site <sitename> All	Shows cumulative statistics for this site. Statistics are reset upon boot.

During active connections, **Show/Monitor Site** commands will display the current state of the site or of its assigned ports. The state of the port or site depends on the activity taking place. For example, a port may be in an idle state, then transition to an on-line state when it begins transferring packets. The possible site states are listed in Table 4-5.

Table 4-5: Site States

Site State	Activity During State
Idle	The site is idle.
Startup	A user, PPP or SLIP, requested that the site start running.
Waiting	The site is waiting for a port to connect.
Connect	The site is connected and passing packet traffic.
Logout	The site was instructed to shut down.
Closing	The site is shutting down PPP or SLIP.
Freeing	The site is removing itself from memory.
NVR	A List Site command was used to display site information. The site's configuration is displayed, not its current activity.

The possible port states of ports assigned to the sites are listed in Table 4-6

Table 4-6: State of Ports Assigned to a Site

Port State	Activity During State
Idle	The site is not currently using this port. The port may be in use by other sites.
Dial	The remote modem is being dialed.
Chat	The chat script defined in the site is being executed. See Chapter 5, *Additional Remote Networking*, for a definition of chat scripts.
Link	PPP is being negotiated with the remote router or remote node. (This state does not apply to SLIP users.)
Ready	PPP negotiation has been completed. (This state does not apply to SLIP users).
Online	Traffic is being forwarded to the remote site.

4.8 Examples

4.8.1 LAN to LAN—Calling One Direction Only

An SCS in a remote office in Dallas must call an SCS at the company headquarters in Seattle. This LAN to LAN connection must meet the following criteria:

- IP users in a remote office in Dallas must connect to IP network 192.0.1.0, which is located at the company headquarters in Seattle.
- The SCS in Seattle never calls Dallas.
- The SCS in Seattle must support character mode users as well as the SCS in Dallas.
- After 60 seconds of idle time, the connection between Dallas and Seattle should be timed out.

The SCS in Dallas must be configured for outgoing LAN to LAN connections.

Figure 4-35: Dallas SCS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>>
Local>> DEFINE SITE SEATTLE AUTHENTICATION USERNAME “dallas”
Local>> DEFINE SITE SEATTLE AUTHENTICATION REMOTE “xyz”
Local>> DEFINE SITE SEATTLE AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE SEATTLE IDLE 60
Local>> DEFINE SITE SEATTLE PORT 2
Local>> DEFINE SITE SEATTLE TELEPHONE 2065551234
Local>>
Local>> DEFINE IP ROUTE 192.0.1.0 SITE SEATTLE 2
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

The **Initialize Server Delay 0** command will reboot the SCS; when the unit has rebooted, changes made with the Define commands will be in effect.

The SCS in Seattle must then be configured using the following commands:

Figure 4-36: Seattle SCS Configuration

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 PPPDETECT ENABLED
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>> LOGOUT PORT 2
Local>>
Local>> DEFINE SITE dallas AUTHENTICATION LOCAL “xyz”
Local>> DEFINE IP ROUTING ENABLED
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

4.8.2 LAN to LAN—Bidirectional (Symmetric) Calling

An SCS in a remote office in Dallas must be able to call an SCS at the company headquarters in Seattle. This LAN to LAN connection must meet the following criteria:

- The SCS in Seattle must also be able to call Dallas.
- IP traffic must be transferred between Seattle and Dallas.
- IP users in Dallas must connect to IP network 192.0.1.0 in Seattle. IP users in Seattle must connect to IP network 192.0.2.0 in Dallas.
- Both servers are to be dedicated to this purpose. No other applications are supported.
- After 60 seconds of idle time, the connection between Dallas and Seattle should be timed out.
- The SCS in Seattle expects the username **dallas** and the password **xyz**. The SCS in Dallas expects the username **seattle** and the password **abc**.

This SCS must be configured for incoming and outgoing LAN to LAN connections:

Figure 4-37: Dallas SCS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>>
Local>> DEFINE SITE SEATTLE AUTHENTICATION USERNAME “dallas”
Local>> DEFINE SITE SEATTLE AUTHENTICATION LOCAL “abc”
Local>> DEFINE SITE SEATTLE AUTHENTICATION REMOTE “xyz”
Local>> DEFINE SITE SEATTLE AUTHENTICATION CHAP
Local>> DEFINE SITE SEATTLE IDLE 60
Local>> DEFINE SITE SEATTLE PORT 2
Local>> DEFINE SITE SEATTLE TELEPHONE 2065551234
Local>>
Local>> DEFINE IP ROUTE 192.0.1.0 SITE SEATTLE 2
Local>> DEFINE IP ROUTING ENABLED
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

The **Initialize Server Delay 0** command will reboot the SCS; when the unit has rebooted, changes made with the Define commands will be in effect.

The Seattle SCS will have different authentication, telephone, site and router information than the SCS in Dallas. In all other respects, it is configured identically to the Dallas SCS.

Figure 4-38: Seattle SCS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 SPEAKER DISABLED
Local>>
Local>> DEFINE SITE DALLAS AUTHENTICATION USERNAME “seattle”
Local>> DEFINE SITE DALLAS AUTHENTICATION LOCAL “xyz”
Local>> DEFINE SITE DALLAS AUTHENTICATION REMOTE “abc”
Local>> DEFINE SITE DALLAS AUTHENTICATION CHAP
Local>> DEFINE SITE DALLAS IDLE 60
Local>> DEFINE SITE DALLAS PORT 2
Local>> DEFINE SITE DALLAS TELEPHONE 2145556789
Local>>
Local>> DEFINE IP ROUTE 192.0.2.0 SITE DALLAS 2
Local>> DEFINE IP ROUTING ENABLED
Local>>
Local>> INITIALIZE DELAY 0
```

4.8.3 Remote Dial-in User Example

This example sets up ports 2 and 3 to support remote node users via PPP. All users will use temporary copies of the default site and may authenticate with CHAP, PAP, or chat scripts. Modems on port 2 and 3 will be automatically configured.

IP users will be forced to use either IP address 192.0.1.7 or 192.0.1.8. One IP user **wwwserver**, must have the same address (192.0.2.6) each time it logs in.

4.8.3.1 Configure the Ports & Modems

First, you need to configure ports 2 and 3. When the connection is initiated by the remote caller, the SCS will detect when a PPP packet is received and automatically run PPP. To provide a layer of security, PPP authentication (CHAP and PAP) will be enabled on the ports, requiring the remote user to authenticate itself before a true connection is established.

Figure 4-39: Configuring the Port

```
Local>> DEFINE PORT 2-3 PPPDETECT ENABLED
Local>> DEFINE PORT 2-3 PPP ENABLED
Local>> DEFINE PORT 2-3 PPP CHAP REMOTE
Local>> DEFINE PORT 2-3 PPP PAP REMOTE
Local>> DEFINE PORT 2-3 AUTHENTICATE ENABLED
```

Because both ports are attached to modems, you must enable modem control for each port. The SCS will interact with the modem by sending commands to and expecting responses from the modem. To properly communicate with the modem, the SCS uses a modem profile, which is configured for particular modem types.

To display a list of modem profiles, enter the **List Modem** command. Once you identify the appropriate profile for the attached modems, assign it to the port using the **Define Port Modem Type** command.

Figure 4-40: Configuring the Modems

```
Local>> DEFINE PORT 2-3 MODEM CONTROL ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 3 MODEM TYPE 2
```

4.8.3.2 Define the IP Address Pool

For this example, remote users will be assigned one of two IP addresses: 192.0.1.7 or 192.0.1.8. By enabling proxy-ARPing, the SCS will respond to ARP requests for these addresses, even if they're not currently assigned to a caller.

Figure 4-41: Configuring IP

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.7 192.0.1.8
Local>> DEFINE IP ETHERNET PROXY-ARP ENABLED
```

4.8.3.3 Configure the Default Site

Once the connection is authenticated, the SCS will start with a temporary copy of the default site. For this example, you need to configure a range of IP addresses for default site users that corresponds to the IP addresses defined for the IP address pool.

Figure 4-42: Configuring Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.7 192.0.1.8
```

Configure a static IP address site.

Figure 4-43: Configuring Static IP Address

```
Local>> DEFINE SITE wwwserver IP REMOTEADDRESS 192.0.2.6
Local>> DEFINE SITE wwwserver AUTHENTICATION LOCAL "monkey"
```

5: Additional Remote Networking

This chapter discusses how to “fine-tune” remote networking and related features on your SCS. Performance and cost issues are covered, as well as how to manage bandwidth on demand, use direct connections and leased lines, and restrict access to the SCS.

Topics discussed in this chapter include:

- *Basic Security*, page 5-1, describes how to set up basic authentication and filter lists.
- *Chat Scripts*, page 5-3, details how to define chat scripts.
- *Bandwidth On Demand*, page 5-4, explains bandwidth management for LAN to LAN connections.
- *Increasing Performance*, page 5-8, and *Reducing Cost*, page 5-10, describe how to maximize your SCS while minimizing your related costs.
- *Using the SCS Without Dialup Modems*, page 5-13, illustrates alternate configuration methods.
- *Examples*, page 5-16, show the features described in this chapter put to the test in real-life situations.

5.1 Basic Security

For a complete discussion of security issues, including instructions on restricting incoming and authenticated logins, see Chapter 11, *Security*. PPP authentication is discussed in Chapter 7, *PPP*.

5.1.1 Port Authentication

Authentication may be used to restrict users to a particular configuration when they log into a port. When a username is entered in the local authentication database, a series of commands may be associated with that user. These commands (including starting a site) will be executed when the user is successfully authenticated.

To execute commands when a user logs into the SCS, complete the following steps:

1. Ensure that the authentication databases have been configured using the **Set/Define Authentication** commands.
2. Associate commands with a username by entering the **Set/Define Authentication User** command. When the user is successfully authenticated, these associated commands will be executed.

Figure 5-1: Restricting a User to a Particular Site

```
Local>> DEFINE AUTHENTICATION USER “bob” COMMAND “set ppp dialin_users”
```

In the example above, when user **bob** logs into the SCS, he will automatically run site **dialin_users**.

3 Enable authentication on each port that will be used for incoming logins.

Figure 5-2: Enabling Port Authentication

```
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
```

5.1.2 Filter Lists

Filters enable the SCS to restrict packet traffic. Each filter specifies a particular rule, for example, only IP packets are permitted passage. Packets that pass the filter are forwarded; all others are discarded.

Filters are organized into ordered filter lists, referenced by name. For example, a filter named **firewall** may permit forwarding of packets that match a particular IP rule, but deny passage to packets that match a generic rule.

Filter lists are associated with sites. Table 5-1 describes the available filter lists and how they are used.

Table 5-1: Types of Filter Lists

Type of Filter List	Purpose
Idle	Determines whether the site will remain active. Packets that pass the filter will reset the site's idle timer, preventing the site from being timed out.
Incoming	Determines whether to forward incoming packets received from a remote site. Packets that pass the filter will be forwarded.
Outgoing	Determines whether to forward outgoing packets to a remote site. Packets that pass the filter will be forwarded.
Startup	Determines whether a site will initiate a connection to a remote site. When a packet passes the filter, the SCS will initiate an outgoing connection. (If an outgoing connection currently exists, this filter will be ignored.)

When a site with an associated filter list receives a packet, the SCS compares the packet against each filter starting with the first filter on the list. If the packet matches any of the filters, the packet is forwarded or discarded according to the filter's specification. If the packet does not match any of the filters in the list, that packet is not forwarded.

The order filters appear in a list is very important. For example, consider the following filter list.

1 Allow any packet

2 Deny all IP traffic matching a particular rule

When this filter list is associated with a site, all packets are forwarded. Packets are compared to filters in the order in which the filters appear in the list. Because all packets match the specification of "any packets," all packets are forwarded without being compared to the second filter.

Switching the order of the filters has a significant effect. Examine the filter list below, where the order of the above two filters is reversed.

1 Deny all IP traffic matching a particular rule

2 Allow any packet

When this filter list is used, all IP traffic matching the specified rule is discarded. Therefore, some IP packets are discarded without being compared to the second filter.

To prevent all packet traffic from the IP protocol, use the **Define Site IP Disabled** command instead of a filter list.

Figure 5-3: Preventing IP Packet Traffic

```
Local>> DEFINE SITE irvine IP DISABLED
```

Configuring filter lists involves two primary steps: creating the filter list and associating the list with a particular site. See *Setting Up a Filter List* on page 11-24 for complete configuration instructions.

5.2 Chat Scripts

Chat scripts enable the SCS to communicate with virtually any type of equipment at the remote site. They are typically configured to send a string of characters, then wait to receive a particular string in return.

For example, the SCS might log into a remote site that has a login program. Using a chat script defined for the site, the SCS could send carriage returns until the login prompt is returned, send a username, wait for the password prompt, and send a password.

5.2.1 Creating a Chat Script

Chat scripts are defined one line at a time following a given syntax. A chat script to be used for outgoing connections from a particular site can be created with the **Define Site Chat** commands. These commands enable you to do the following: send a particular string, replace, add, or delete existing lines in the script, expect a particular string, and configure timeout periods.

For example, to configure the script to send or expect strings, use the following command.

Figure 5-4: Sending and Expecting Strings

```
Local>> DEFINE SITE irvine CHAT SEND "hello?"
Local>> DEFINE SITE irvine CHAT EXPECT "login:"
```

Note: *Chat script expect strings are case-sensitive.*

5.2.2 Editing and Adding Entries

To replace, delete, or insert entries, specify the line numbers. Figure 5-5 displays a few examples.

Figure 5-5: Editing Script Entries

```
Local>> DEFINE SITE irvine CHAT REPLACE 1 EXPECT "login:"
Local>> DEFINE SITE irvine CHAT DELETE 4
Local>> DEFINE SITE irvine CHAT AFTER 3 EXPECT "login:"
Local>> DEFINE SITE irvine CHAT BEFORE 3 EXPECT "login:"
```

To determine the number of a particular line, display the script using the **List Site Chat** command. All chat script entries for that site will be displayed.

5.2.3 Configuring Timeouts

The **Define Site Chat Timeout** command enables you to configure the timeout after an Expect command, or a delay before a Send command is executed. Figure 5-6 displays some examples.

Figure 5-6: Setting Timeouts and Delays

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT "login:"
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 SEND "hello?"
```

The first command in Figure 5-6 will cause the SCS to wait two seconds for a response from the remote host after sending an Expect command. If no response is received after two seconds, the chat script will fail or return to the previous fail marker. The second command will send the “hello?” string after a 4-second delay.

The default Send timeout (delay before a Send command is executed) is 0; in other words, strings will be sent right away. The default timeout for Expect commands is 30 seconds.

5.2.4 Setting Markers

The **Fail** parameter sets a marker in a chat script for a Timeout command. When the Timeout associated with an Expect command expires (the expected string is not received within the specified number of seconds), the SCS will return to the last command containing the Fail parameter. The script will be executed from that point, continuously looping if the Expect command repeatedly fails.

Figure 5-7: Expect/Fail Scripts

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL
Local>> DEFINE SITE irvine CHAT SEND "\r"
Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT "login:"
```

The script in Figure 5-7 will send a carriage return, then wait for two seconds while a “login:” string is expected. If the “login:” string is not received within two seconds, the chat script will loop back to the Fail command and continue running from that point. Each time the Expect command fails (i.e. the “login:” string is not received within two seconds), the Fail counter is decremented one value. When the Expect command has failed four times (i.e. the “login:” string is never received), the looping will stop and the chat script will exit.

5.3 Bandwidth On Demand

Note: *Remote Node sites have a fixed bandwidth. The SCS cannot add or remote bandwidth for Remote Node connections. This section discusses bandwidth for LAN to LAN connections only.*

The following sections outline the basic configuration needed to utilize SCS bandwidth on demand functionality for LAN to LAN connections. For more detailed instructions on setting up both sides of a bandwidth on demand connection, refer to *Multilink PPP* on page 7-4.

By default, sites will only attempt to bring up one port to a remote site in a LAN to LAN connection. If the amount of incoming data on the Ethernet exceeds the current bandwidth of the serial port (and the SCS is configured not to dial up additional bandwidth), congestion occurs and the extra data is discarded.

To avoid congestion, the SCS enables you to customize a site's use of bandwidth. As it is needed, additional bandwidth will be added. The SCS will assign more ports to the site until it has enough bandwidth or reaches a certain threshold. When it is no longer needed, the extra bandwidth will be removed.

5.3.1 How Bandwidth is Controlled

A site's use of bandwidth is controlled by the following factors:

- The initial and maximum bandwidth allotted to the site. These are static values.
- The threshold at which additional bandwidth should be added. This threshold is a percentage of the currently-dialed bandwidth.
- The threshold at which unnecessary (unused) bandwidth should be removed. This threshold is a percentage of the currently-dialed bandwidth.
- The period of time during which the current bandwidth usage is measured.
- The delay between bandwidth adjustments.

By default, additional bandwidth will not be added to a connection. In order for a connection to have flexible bandwidth (bandwidth that is added and removed as necessary), the site's maximum bandwidth must be configured, as well as the thresholds at which bandwidth is added and removed.

Note: *The initial bandwidth allotted to the site may also be configured. This is optional.*

The threshold at which bandwidth is added and removed should have some room between them to regulate how often bandwidth is added and removed. The "add bandwidth" threshold should be set to a percentage between 80 and 100 percent; the "remove bandwidth" threshold should generally be set to less than 50%. If the threshold values are set too close to one another, the connections will **thrash**; in other words, bandwidth will be continuously added and dropped.

The order in which ports are selected to be added and removed is controlled by a priority setting; when SCS bandwidth needs change, ports with the highest priority are the first to be added and the last to be removed.

Bandwidth is controlled by the host that initiates the call. If the SCS initiates a call, it controls the bandwidth for each site. If the SCS receives an incoming call, the bandwidth is controlled by the remote host.

The SCS will always use at least one port for a connection, even if the traffic is below the "remove bandwidth" threshold. If this is not desired behavior, the last connection can be controlled by the idle timer.

Note: *To configure the idle timer, see Set/Define Server Inactivity on page 12-118.*

5.3.2 Disadvantages of Additional Bandwidth

Increasing bandwidth by bringing up additional links has two disadvantages: increased cost and reduced resources. Phone rates will go up as more phone lines are used, and fewer ports will be available for other purposes. Assess your needs carefully before increasing bandwidth.

5.3.3 Configuring Bandwidth Allocated to Sites

To configure bandwidth, follow the instructions in the following sections.

5.3.3.1 Estimate Each Port's Bandwidth

Before sites can be configured to use particular bandwidths, the bandwidth of each SCS port must be estimated in bytes per second. This estimate should be made based upon two factors: the amount of compression expected for typical data on this site, and the fastest data transfer rate that the local and remote modems can support.

The SCS will truncate the bandwidth setting to the nearest 100 bytes per second. For example, a setting of 5790 will be truncated to 5700.

Consider the following example. Site **irvine** may use SCS port 2 and port 3 (if needed) for connections. A V.34 modem with a baud rate of 28800 bits per second is attached to each port. The remote modems are also V.34 modems with the same baud rate. Compression is enabled and a 2:1 compression rate is expected, which will increase the data transfer between the modems to 57600 bits per second.

The bandwidth for ports 2 and 3 should be estimated as follows:

Figure 5-8: Estimating a Port's Bandwidth

```
Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 5800
Local>> DEFINE SITE irvine PORT 3 BANDWIDTH 5800
```

Note: *If you are using 8 bits, no parity, and 1 stop bit, the modem will actually transmit ten bits for each byte.*

If the modems attached to a series of SCS ports are going to be calling similar remote modems, these ports should be set to the same bandwidth estimates. In addition, if several ports have compression enabled, you should assume that the compression rate on each port will be the same (for example, a 2:1 compression rate). Avoid using small variations in bandwidth estimates.

It is important to correctly estimate bandwidth. The SCS will attempt to reduce the total number of ports in use by using higher bandwidth ports (of the same priority) first until the bandwidth goal is met.

5.3.3.2 Assign Port Priority Numbers

Priority numbers enable a site to determine which of its assigned ports it should use first for outgoing calls. The highest priority ports, those with higher priority numbers, will be used first. As additional bandwidth is needed, lower priority ports will be used in descending order of priority.

To assign priority numbers to a site's ports, use the following command:

Figure 5-9: Assigning Port Priority Numbers

```
Local>> DEFINE SITE irvine PORT 2 PRIORITY 2
```

Note: *By default, all ports are assigned a priority of 1.*

5.3.3.3 Specify the Bandwidth Measurement Period

A period must be specified (in seconds) during which the SCS will measure a site's use of bandwidth. The measurement taken during this period will be compared to the Add and Remove values (see below) to determine if bandwidth should be added or removed. Short periods may lead to "thrashing."

Figure 5-10: Specifying the Bandwidth Measurement Period

```
Local>> DEFINE SITE irvine BANDWIDTH PERIOD 60
```

5.3.3.4 Specify When Bandwidth is Added or Removed

Determine when bandwidth will be added or removed from a site. This is specified in terms of a percentage; when a site's bandwidth use on its currently-dialed out ports reaches or falls below this percentage, bandwidth will be added or removed as appropriate.

Figure 5-11: Determining When Bandwidth Will Be Added/Removed

```
Local>> DEFINE SITE irvine BANDWIDTH ADD 90
Local>> DEFINE SITE irvine BANDWIDTH REMOVE 40
```

5.3.3.5 Configure the Delay Between Bandwidth Adjustments

Determine the minimum period of time between one adjustment in bandwidth (addition or removal) and a following adjustment. Configure this delay using the **Define Site Bandwidth Holddown** command; by default, this timer is set to 60 seconds.

Figure 5-12: Configuring the Holddown Timer

```
Local>> DEFINE SITE irvine BANDWIDTH HOLDDOWN 30
```

The holddown timer helps to limit the "thrashing" caused by rapid adjustments in bandwidth. When the holddown timer is used in conjunction with a short bandwidth measurement period, the site will respond quickly to initial changes in packet traffic without thrashing.

In the example above, the holddown timer is set to 30 seconds. When bandwidth is added to site **irvine**, additional bandwidth cannot be added until 30 seconds have passed. Bandwidth changes in the opposite direction (addition or subtraction) require a delay of double the holddown timer; for example, when bandwidth is removed from irvine, it cannot be added for 60 seconds.

5.3.4 Displaying Current Bandwidth Settings

To display a site's current bandwidth settings, use the **List Site Bandwidth** command.

Figure 5-13: Current Bandwidth Settings

```
Local>> LIST SITE irvine BANDWIDTH
SCS Version 1.1/101                                  Name:              SCS_0C0021
    Hardware Addr:      00-80-a3-0c-00-21 Uptime:                       1 Day 02:56
    Site Name:          irvine                       Period:            60
    Add @ Utilization:  Disabled                     Remove @           Disabled
    Maximum Bandwidth:  100                          Initial Bandwidth: 100
    Multilink:          Disabled                     Hold Down Timer:   01:00
    Input Utilization:  0%                           Output Utilization: 0%
    Next Adjust Up:     Any Time                     Next Adjust Down:  Any Time
    Target Bandwidth:   0                            Waiting Bandwidth: 0
    On-line Bandwidth:  0

                        Average Period   -- Input --   -- Output --   - Dropped -
                        (in seconds)     Bytes/Second  Bytes/Second  Bytes/Second
    Size Total:         4                0             0             0
    Size Total:         60               0             0             0
```

To display how the SCS is currently managing a particular site's use of bandwidth, use the **Show Site Bandwidth** command.

5.3.5 Restoring Default Bandwidth Settings

To return a site's bandwidth parameters to their default values, use the following command:

Figure 5-14: Restoring Default Bandwidth Values

```
Local>> DEFINE SITE irvine BANDWIDTH DEFAULT
```

5.3.6 Monitoring Bandwidth Utilization

The **Show/Monitor Site** command is particularly useful when allotting bandwidth to a site. Periodically monitoring a site's use of bandwidth will enable you to determine if the bandwidth configuration is appropriate and to make adjustments when necessary.

Figure 5-15: Displaying Bandwidth Utilization

```
Local>> SHOW SITE irvine BANDWIDTH
```

Note: *For information on port and site states, see Table 4-5 on page 4-21.*

5.4 Increasing Performance

5.4.1 Filtering Unwanted Data

To reduce the use of bandwidth for unwanted packet traffic, each site may configure an incoming and an outgoing filter list. Packets will be compared to these filter lists as they are received or generated. If they do not pass the filter, they will be discarded. See *Filter Lists* on page 5-2 for more details.

5.4.2 Compressing Data and Correcting Errors

The amount of data that can be transmitted at once (throughput) can be increased by using data compression. Data compression enables a device such as a modem to transfer a larger amount of data at once. When compression is used, uncompressed data arrives on the modem's serial port and the modem compresses the data before sending it over the phone line.

The disadvantage of compression is increased latency, the time required to transfer data from one place to another. Compression increases latency due to the time required to compress the data before it is sent. Error correction can also increase latency, as the data must be checked for integrity after it is received.

In situations where the delay is undesirable (for example, during interactive use over a long distance line), compression and error correction should not be used. These options are enabled by default on the SCS; to disable them, use the following commands:

Figure 5-16: Disabling Error Correction and Compression

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION DISABLED
Local>> DEFINE PORT 2 MODEM COMPRESSION DISABLED
```

Note: *For a complete discussion of compression and error correction, see Chapter 9, Modems.*

5.4.3 Adding Bandwidth

Like compression, adding bandwidth can increase throughput. Sites can be configured to automatically bring up additional connections when more bandwidth is needed, for example, when the amount of data to be transmitted exceeds the bandwidth of the port.

How "aggressively" a site will add bandwidth can be controlled with two factors: the period during which the use of bandwidth is measured, and the percentage at which bandwidth is added.

For example, to increase bandwidth for small or periodic increases in traffic, reduce the measurement time period. A similar effect could be obtained by reducing the percentage utilization at which bandwidth is increased. To require a sustained increase in traffic to increase bandwidth, the measurement time period and the utilization percentage should be increased. See *Bandwidth On Demand* on page 5-4 for more information.

5.4.4 IP Header Compression

Each site may be configured to compress the header information on IP (TCP only) packets before they are forwarded. When a site is created, IP header compression will be enabled by default.

Header compression is most useful for interactive traffic such as Telnet sessions. Compressing the header information for interactive traffic decreases the delay before data is transferred. In other words, if a key is pressed during a Telnet session, the time required to echo that character back to the user's terminal will be reduced.

For more information on IP header compression, see *Header Compression* on page 6-8.

5.5 Reducing Cost

5.5.1 Inactivity Logouts

The SCS can be configured to log out a particular site after a certain period of inactivity (referred to as idle time). To configure an inactivity timeout, the site must be allocated a maximum idle time in seconds using the **Define Site Idle** command.

Figure 5-17: Setting Site Idle Time

```
Local>> DEFINE SITE irvine IDLE 600
```

The site may then be associated with an idle time filter list. When a site receives packets, it compares them to this list. Packets that "pass" the filter list will reset the idle timer to zero. If no packets pass the list or traffic is not received within the idle time, the site will be timed out. If an idle time filter is not used, any packet traffic sent by the site will reset the idle timer.

Note: *Incoming packet traffic does not reset the idle timer if there is no idle time filter.*

Idle time filter lists enable the SCS to keep a site active for specific types of traffic, disconnecting the site if this traffic isn't sent. For example, imagine that a particular site was intended for interactive traffic. Using an idle filter list, the site could ensure that other traffic (such as email) wouldn't keep the connection active.

Note: *To configure an idle time filter, see Filter Lists on page 5-2.*

5.5.2 Restricting Packets with Startup Filters

To prevent unwanted packets from initiating a connection, each site may be associated with a startup filter list. Packets destined for a remote site are compared to this list; if they do not pass the filter, they are discarded.

Startup filter lists are only intended to prevent unwanted connections. If a connection is already in place, the list is ignored. To configure a startup filter, see *Filter Lists* on page 5-2.

5.5.3 Reducing the Number of Ports Used

When additional links are brought up to increase bandwidth, phone charges will increase. Reducing the number of ports or reducing the site's maximum bandwidth can reduce total cost; see **Purge Site** on page 12-148 and **Define Site Bandwidth** on page 12-134 for details.

5.5.4 Using Higher Speed Modems

The time used to transfer data can be reduced by using the highest speed modems available. To ensure that high speed modems are used before low speed modems, priority numbers may be assigned to each site's ports. If high speed modems are attached to ports with high priority numbers, they will be dialed before other modems.

5.5.5 Restricting Connections to Particular Times

Sites can be configured to permit outgoing connections only within particular time ranges on particular days. For example, outgoing connections can be restricted to Monday through Friday, between 9 a.m. and 5 p.m.

5.5.5.1 Determining if Site Restrictions are Appropriate

Sites don't need to be configured to restrict connections; applications can be restricted to run only at particular times. Before configuring a site, it is important to consider whether it's appropriate for a remote application or an SCS site to control the access restriction.

5.5.5.2 Setting Up Site Restrictions

To configure a time range, use the **Define Site Time Add** command. The time range may be within one day, or may span from one day to another day. (If a second day isn't specified, the time period is assumed to take place entirely on the first day specified.) The beginning and end times of the range must be specified in 24-hour format. Some examples are displayed below.

Figure 5-18: Adding Time Ranges

```
Local>> DEFINE SITE irvine TIME ADD MON 8:00 17:00
Local>> DEFINE SITE irvine TIME ADD TUES 23:00 WED 6:00
Local>> DEFINE SITE irvine TIME ADD WED 8:00 THURS 8:00
```

Note: *Up to ten time ranges may be specified.*

Next, specify whether connections will be permitted or prevented during these times using the **Define Site Time Default** command. **Enabled** permits outgoing connections, except during the time ranges stated. **Disabled** prevents outgoing connections, except during the time ranges stated.

Figure 5-19: Enabling Connections During Time Ranges

```
Local>> DEFINE SITE irvine TIME DEFAULT ENABLED
```

Configurable time ranges are based on a Sunday-to-Saturday week. To configure access that spans weekend hours, see *Controlling Access During Weekend Hours* on page 5-16.

5.5.5.3 Getting Timesetting Information

In order to restrict packet traffic during the specified times, the SCS must get accurate time information from one of two sources: an IP timeserver or from the SCS' internal clock.

To configure an IP timeserver, see **Set/Define IP Timeserver** on page 12-46. To set the SCS internal clock, see **Set/Define Server Clock** on page 12-117. To configure the SCS timezone, see **Set/Define Server Timezone** on page 12-128.

To display the site restrictions you've configured, use the **List Site Time** command.

Figure 5-20: Displaying Site Restrictions

```
Local>> LIST SITE irvine TIME
SCS Version B1.1/102int(951128) Name: DOC_SERVER
Hardware Addr: 00-80-a3-0b-00-5b uptime: 3 Days 12:07
20:42:54
Access default: Enabled

01) Mon 08:00 - Mon 17:00 Disabled
02) Tue 23:00 - Wed 06:00 Disabled
03) Wed 08:00 - Thu 08:00 Disabled

Success Timeout: 0:01
Failure Timeout:0:30
```

5.5.6 Increasing Requirements for Adding Additional Bandwidth

The SCS will periodically measure how much bandwidth a particular port is using. The period of time during which this measurement is taken may be configured differently for each site. When the measurement period is short, a temporary increase in network traffic may cause the site to bring up additional connections to increase bandwidth, increasing cost. If a site's bandwidth utilization is measured (averaged) over a longer period of time, a temporary increase in network traffic will have less impact on whether or not additional bandwidth is added.

Another way to reduce cost is to increase the percentage utilization required to add additional connections. If a site is permitted to use up to 80% of the total currently-dialed bandwidth on a particular port (rather than, for example, 25%), the site will be less likely to require additional connections to increase bandwidth.

5.5.7 Controlling Frequency of Calls

The success and failure timers can be used to control how aggressive the SCS will be when attempting connections. Two commands control this behavior.

- **Define Site Time Success** sets the time lapse between attempts to connect to a remote site after a successful connection has been made.
- **Define Site Time Failure** sets the time lapse between attempts to connect to a remote site when a connection attempt fails.

If the last connection attempt succeeded and the success timer is set to a high value (for example, 20 minutes), the SCS will wait for a longer period of time before attempting a new connection. If the SCS was not able to connect for some reason, setting the failure timer to a low value (for example, 5 seconds) will cause the SCS to retry the connection at short intervals until it succeeds.

In Figure 5-20, the SCS is configured to allow a new connection attempt almost immediately upon completion of a successful connection. If the last attempt to connect to the site failed, the SCS will wait 30 seconds before attempting another connection. It will continue to retry the connection every 30 seconds until it succeeds.

5.6 Using the SCS Without Dialup Modems

The SCS may be configured to allow Remote Node and LAN to LAN functionality without using modems; dial-on demand features will be ignored.

5.6.1 Situations Where Dialup Modems Are Not Used

There are four primary situations in which the SCS may be used without modems:

Direct connections	Two SCS units are linked with a serial cable.
Statistical multiplexors	Multiplexors (stat-mux) allow multiple serial lines to run over a single leased line. The stat-mux must support asynchronous serial communication.
Synchronous leased line	Lines are leased from the telephone company and dedicated to synchronous serial communication between two fixed locations.
Analog leased lines	Analog lines are ordinary telephone lines leased from the telephone company and used in conjunction with standard modems. The modems must have leased line capabilities.

5.6.1.1 Direct Connections

Two buildings may be linked with a serial cable. Two SCS units may use the serial cable to connect two networks together.

5.6.1.2 Statistical Multiplexors

Two locations may have statistical multiplexors (commonly called stat-muxes) in place. These stat-muxes may be used to connect to SCS units. A series of commands may have to be sent to the stat-mux to connect to the remote SCS; chat scripts make sending these commands easy and relatively error-free.

Note: *See Chat Scripts on page 5-3 for more information.*

The SCS assumes an 8-bit data path. If you are using SLIP, all characters must be sent and received unchanged by the intervening communications equipment. PPP has a feature called ACCM which causes the SCS to avoid sending user-specified control characters. If the equipment connecting the SCS cannot send certain control characters, configure PPP and ACCM on the SCS port.

Note: *ACCM is discussed in detail in Character Escaping on page 7-1*

5.6.1.3 Synchronous Leased Lines

The SCS supports asynchronous serial connections. Many leased lines are synchronous. Devices which convert between synchronous and asynchronous serial signals exist, but they may result in some performance loss. The current SCS units are not always the best solution for synchronous leased line applications.

5.6.1.4 Analog Leased Lines

To use an SCS with analog leased lines, the modems on each end of the connection must support leased line mode and should use asynchronous serial communication.

Note: *See your modem's documentation to configure the modem for leased line mode.*

5.6.2 Configuring the Unit for Modemless Connections

The SCS should initiate the connection at boot time and should not time out the connection.

The following configuration is recommended:

- Idle timeouts are disabled.
- RTS/CTS flow control is used between the SCS and the communications equipment.
- If RTS/CTS flow control is not supported, XON/XOFF flow control may be used in conjunction with PPP. If flow control cannot be used, use PPP and monitor the port for checksum errors which may be the result of disabled flow control.
- The port is dedicated to PPP or SLIP.
- PPP or SLIP starts automatically.
- The port is configured to support incoming and outgoing connections.
- Modem control is disabled

In the following examples (both SLIP and PPP), the SCS has an IP address of 192.0.1.1, and must connect to another router with IP address 192.99.99.99.

5.6.2.1 PPP

Figure 5-21 displays the command required if PPP is used. Both sides of the leased line should be configured using these commands.

Figure 5-21: SCS Configuration Without Modems: PPP

```
Local>> DEFINE IP IPADDRESS 192.0.1.1
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 SPEED 19200
Local>> DEFINE PORT 2 FLOW CONTROL CTS
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE SITE port2 IDLE 0
```

If static routing is to be used on the line, routes pointing to the site **port2** will be required.

Figure 5-22: Configuring Static Routing

```
Local>> DEFINE SITE port2  IP RIP DISABLED
Local>> DEFINE SITE IP ROUTE 192.99.99.0 SITE port2 2
```

5.6.2.2 SLIP

Figure 5-23 displays the commands required if SLIP is used. Both sides of the leased line should be configured using these commands.

Figure 5-23: SCS Configuration Without Modems: SLIP

```
Local>> DEFINE IP IPADDRESS 192.0.1.1
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 SPEED 19200
Local>> DEFINE PORT 2 FLOW CONTROL CTS
Local>> DEFINE PORT 2 SLIP DEDICATED
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE SITE port2 PROTOCOL SLIP
Local>> DEFINE SITE port2 IDLE 0
Local>> DEFINE SITE port2 IP REMOTEADDRESS 192.99.99.99
```

If static routing is to be used on the line, routes pointing to the site **port2** will be required.

Figure 5-24: Configuring Static Routing

```
Local>> DEFINE SITE port2 IP RIP DISABLED
Local>> DEFINE IP ROUTE 192.99.99.0 SITE port2 2
```

5.7 Character Mode Sites

The SCS allows you to create a character mode site. A character mode site is treated as a normal site that does not run a serial protocol. The site still allows modems to be dialed and can execute a chat script, but once the site is up, it will not run PPP. The character mode site is normally used to associate an IP address with a particular serial port and to control an external device using a chat script.

To create a character mode site, use the **Set/Define Site <sitename> Protocol None** and **Set/Define Site <sitename> IP Remoteaddr <ip_address>** commands. Then create a host route that points to it with the Set/Define IP Route **<ip_address> Site <sitename>** command. This is only necessary if the IP address is going to be on a different IP subnet. To make a text mode connection to the serial port, Telnet to <ip_address>. To keep the site up all the time, first issue the command **Define Site <sitename> Idle 0**, and then use the **Define Site <sitename> Permanent Enable** command.

Character mode sites still obey time-of-day restrictions and idle time-outs. All site authentication options for the site are ignored, as are settings for MTO, bandwidth, and packet filters. Sites without protocols cannot be started by users logging in serially.

5.8 Examples

5.8.1 Creating a Chat Script

Figure 5-25 displays a sample chat script. This script will send a series of text strings to the remote host, and will expect particular strings in return. If an expected string is not received from the remote host, the script will loop up to four times before the entire script fails.

Figure 5-25: Creating a Chat Script

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL
Local>> DEFINE SITE irvine CHAT SEND ""
Local>> DEFINE SITE irvine CHAT EXPECT "login:"
Local>> DEFINE SITE irvine CHAT SEND "user"
Local>> DEFINE SITE irvine CHAT EXPECT "word:"
Local>> DEFINE SITE irvine CHAT SEND "password"
```

5.8.2 Creating a Simple Firewall

Firewalls are used to protect a network or networks from unauthorized access. To set up a firewall, a filter list is used; packet traffic is compared to the filters in the list to determine whether or not it will be forwarded. In general, firewalls prevent all packet traffic, with the exception of traffic to a particular service or services.

In this example, a network policy prevents all IP traffic, permitting only ICMP ping packets and email. Telnet connections are permitted to only one secure host (192.0.1.4) on the local network. The SCS is calling site **memphis**.

First, create a filter list for IP traffic. This list is called **mem**.

Figure 5-26: Creating IP Filter

```
Local>> DEFINE FILTER mem CREATE
Local>> DEFINE FILTER mem ALLOW IP ICMP
Local>> DEFINE FILTER mem ALLOW IP TCP DPORT EQ SMTP
Local>> DEFINE FILTER mem ALLOW IP DST 255.255.255.255 192.0.1.4 TCP DPORT EQ TELNET
Local>> DEFINE FILTER mem ADD DENY ANY
```

Finally, the **mem** filter list must be associated with site memphis as an incoming filter list.

Figure 5-27: Assigning mem Filter List to Site memphis

```
Local>> DEFINE SITE memphis FILTER INCOMING mem
```

Note: *For a more complex firewall example, see Creating a Firewall on page 11-30.*

5.8.3 Controlling Access During Weekend Hours

Configurable time ranges are based on a Sunday-to-Saturday week. If you want to allow or restrict access for a time period that spans Saturday and Sunday, you need to use multiple commands.

The following example restricts access during the weekend hours between 5:00 p.m. on Friday and 6:00 a.m. on Monday. Two commands are used to configure the necessary blocks of time: one that spans Friday evening to Saturday just before midnight, and one that spans midnight on Sunday to Monday morning.

Figure 5-28: Disabling Connections During the Weekend

```
Local>> DEFINE SITE irvine TIME ADD FRI 17 SAT 23:59
Local>> DEFINE SITE irvine TIME ADD SUN 0 MON 6
```

Note: *In the above example, it is assumed that the access default is "Enabled," in which case connections are restricted during the specified time periods.*

The following example achieves the same result by first adding a time range from Monday morning to Friday evening. The access default is then set to Disabled, which allows connections only during the specified time period.

Figure 5-29: Enabling Connections During Weekdays only

```
Local>> DEFINE SITE irvine TIME ADD MON 6 FRI 17
Local>> DEFINE SITE irvine TIME DEFAULT DISABLED
```

6: IP

This chapter explains some important concepts about IP addressing, configuration, and routing.

To configure IP for remote networking, see Chapter 4, *Basic Remote Networking*, and Chapter 5, *Additional Remote Networking*. For specific IP commands, see *IP/Network Commands* on page 12-18.

This chapter is divided as follows:

- *IP Addresses*, page 6-1, describes how the SCS handles IP address assignment.
- *Subnet Masks*, page 6-5, explains how the SCS works with subnetworks.
- *Name Resolving*, page 6-6 discusses name resolution.
- *Header Compression*, page 6-8, covers how to enable and disable IP header compression.
- *Establishing Sessions*, page 6-8, describes SSH, Telnet, and Rlogin sessions.
- *IP Security*, page 6-17, discusses how to configure the IP security table.
- *Displaying the IP Configuration*, page 6-23, explains the parameters of the **Show IP** command.
- *Examples*, page 6-25, shows examples of the SCS in various real-life situations.

6.1 IP Addresses

Each TCP/IP node on a network has a unique IP address. The IP address provides the information needed to forward packets on the local network and across multiple networks if necessary. IP addresses are specified as n.n.n.n, where each n is a number from 0 to 254; for example, 192.0.1.99.

You must assign the SCS a unique IP address. This IP address will also be used for each individual serial port on the SCS.

IP addresses contain three pieces of information: the **network**, the **subnet**, and the **host**. The **network** portion of the IP address is determined by the network type: Class A, B, or C.

Table 6-1: Network Portion of IP Address

Network Class	Network Portion of Address
Class A	First byte (2nd, 3rd, and 4th bytes are the host)
Class B	First 2 bytes (3rd and 4th bytes are the host)
Class C	First 3 bytes (4th byte is the host)

In most network examples, the host portion of the address is set to zero.

Table 6-2: Available IP Addresses

Class	Reserved	Available
A	0.0.0.0 127.0.0.0	1.0.0.0 to 126.0.0.0
B	128.0.0.0 191.255.0.0	128.1.0.0 to 191.254.0.0
C	192.0.0.0 223.255.255.0	192.0.1.0 to 223.255.254.0
D, E	224.0.0.0 to 255.255.255.254 255.255.255.255	None

Consider the IP address 36.1.3.4. This address is a class A address, therefore, the network portion of the address is 36.0.0.0 and the host portion is 1.3.4.

The **subnet** portion of the IP address represents which subnetwork the address is from. Subnetworks are formed when an IP network is broken down into smaller networks using a subnet mask.

Note: *Subnetworks and subnet masks are discussed on page 6-5.*

A **router** is required between all networks and subnetworks. Generally, hosts can send packets directly only to hosts on their own subnetwork. All packets destined for other subnets are sent to a router on the local network. The **host** portion of the IP address is a unique number assigned to identify the host.

For instructions on setting the IP address for your SCS, see your *Installation Guide*.

6.1.1 IP Addresses for Incoming Connections

When the SCS receives an incoming connection request (remote node or LAN to LAN), an IP address is negotiated for the caller. The address agreed upon depends on the caller's requirements; some don't have a specific address requirement, while others must use the same IP address each time they log into the SCS.

Note: *PPP negotiation is covered in Chapter 7, PPP.*

If an incoming caller does not require the same address for each login, a dynamic address can be assigned from an address pool. See *Defining an IP Address Pool* on page 6-3 for configuration instructions.

Some remote nodes or remote routers cannot be dynamically assigned an IP address. For example, a remote node may offer a service to other hosts on its network. If the other hosts are statically configured to use that IP address to contact the remote node, the node's IP address must not change. In this situation, two courses of action may be taken: the caller may be permitted to choose any address, or may be restricted to a specific address or range of addresses.

Permitting the caller to choose an address presents a number of risks. If the caller chooses an unacceptable IP address (for example, the address of a server), it could affect the accuracy of routing tables elsewhere on the network. In addition, the caller could choose an IP address intended for another host, compromising network security.

To avoid routing and security problems, the SCS should restrict incoming callers to a particular address or range of addresses. This restriction may be defined in each site to force each caller to use a unique IP address; see *Specifying a Site's IP Address Range* on page 6-3 for configuration instructions.

6.1.1.1 Defining an IP Address Pool

An **address pool** is a range of IP addresses that have been reserved for allocation to incoming callers. The range is defined for the entire server; in other words, an address pool cannot be defined for each site.

To define an address pool, use the **Set/Define IP Ethernet Pool** command. You must specify both the beginning and end of the address range.

Figure 6-1: Defining an IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

Note: *Set/Define IP All Pool is not a valid command. The Ethernet parameter must be used.*

Ensure that the address pool is at least as large as the number of serial ports that can accept incoming connections. If all addresses in the pool are in use, incoming callers will not be assigned an IP address.

The SCS will automatically add host routes to the routing table for all addresses in the pool. When an address from the pool is assigned to an incoming caller, the route to the address will be announced in RIP broadcasts.

Addresses in the pool are automatically added to the SCS ARP table. If proxy ARPing is enabled (see *Proxy ARP* on page 6-22), the SCS will respond to ARP requests for these addresses, even when they aren't currently assigned. This enables the SCS to defend the addresses in the pool; other hosts will not be able to use them.

6.1.1.2 Specifying a Site's IP Address Range

Each site may specify a particular **range** of acceptable IP addresses. When an incoming caller requests to use a specific address, it will be compared to this range. If the address falls within this range, the connection will be permitted; if not, the connection attempt will fail.

To specify the beginning and end of the range, use the **Define Site IP Remoteaddress** command. Two addresses must be specified: the beginning of the range and the end of the range.

Figure 6-2: Specifying a Range of Addresses

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.250
```

Callers will not be permitted to use IP addresses with the host part of the address set to zero or -1. These addresses are reserved to identify broadcast packets. If the range that you specify includes such an address (for example, 192.5.6.0 or 192.4.2.255) and a caller requests this address, the connection will not be permitted.

RADIUS can also be used to set the IP address range for a site. See *Framed-IP-Address* on page D-3 for more information.

6.1.1.3 Assigning a Specific IP Address for a Site

To require that incoming callers to a particular site use a specific IP address, use the **Define Site IP Remoteaddress** command.

Figure 6-3: Specifying a Specific IP Address

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108W
```

When an incoming caller requests an IP address, the requested address is compared to this address. If they match, the caller will use the address. If the addresses do not match, the SCS terminates the call.

6.1.2 IP Addresses For Outgoing Connections

By default, when a new site is defined, the SCS IP address on that interface will be the IP address assigned with the **Define Site IP Address** command.

Remote hosts may require that the SCS have a certain IP address on that interface. For example, a remote host may require that RIP updates be received from a particular IP address, or an address within a certain range. In these cases, a site-specific IP address may be configured for a particular interface. For example, site **irvine** may configure the SCS IP address on its interface as 193.20.339.2, and site **dallas** may configure the SCS address on its interface as 192.20.338.0.

To change the IP address for a particular site's interface, use the **Define Site IP Address** command.

Figure 6-4: Defining IP Address for a Site

```
Local>> DEFINE SITE irvine IP ADDRESS 192.0.1.220
```

6.1.2.1 SLIP

SLIP does not support negotiation of IP addresses. If a SLIP user requires the same IP address for each login, the user may enter the address using the **Set SLIP** command.

Figure 6-5: Specifying IP Address with Set SLIP Command

```
Local>> SET SLIP irvine 192.0.1.35
```

If the port receiving the incoming call is dedicated to SLIP, a specific IP address may be assigned via a custom site. To define the address for the site, use the **Define Site IP Remoteaddress** command.

Figure 6-6: Specifying IP Address for a Custom Site

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108
```

If the user does not require the same address for each login, an address may be dynamically assigned from the address pool. To configure the range of addresses in the pool, use the **Set/Define IP Ethernet Pool** command. You must specify both the beginning and end of the address range.

Figure 6-7: Defining IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

All incoming SLIP users that do not use a custom site will use the default site for the connection. To require that default site users use an IP address from the pool, use the **Define Site Default IP Remoteaddress** command.

Figure 6-8: Using the Address Pool for the Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.100 192.0.1.105
```

6.1.2.2 Dialing Out to an ISP

An SCS site can be configured to dial out to an ISP that uses PPP, such as Earthlink. Most ISPs will want to assign a nameserver and an IP address to the SCS. To accept this assignment, set the SCS IP address assignment to dynamic and set its nameserver to 0.0.0.0.

Figure 6-9: Using the SCS With an ISP

```
Local>> DEFINE SITE irvine IP IPADDRESS DYNAMIC
Local>> DEFINE SERVER NAMESERVER 0.0.0.0
```

These settings allow site irvine to accept an IP address and a nameserver setting from the ISP.

6.2 Subnet Masks

IP networks can be divided into several smaller networks by subnetting. When you request a connection, the SCS decides whether the desired TCP/IP host is on the local network segment with the help of the **subnet mask**. The mask identifies the network and node parts of the IP address, which is then applied to the addresses of both the SCS and the remote host. If the resulting addresses are identical, the connection is deemed local and the host is contacted directly. If not, the connection attempt and all subsequent messages to this host will be directed to the SCS's gateway host for forwarding. All hosts must agree on the subnet mask for a given network.

For example, IP address 128.1.150.35 is on a class B network. The network portion of this address is 128.1. This large network can be broken down into 254 networks using a subnet mask of 255.255.255.0, which makes the network portion 128.1.150.

It is not always necessary to divide a network into subnetworks. To determine whether subnetting is required, a number of factors should be considered, including the network size and whether or not network traffic needs to be isolated in a particular area.

When you configure the IP address for the first time, a default subnet mask will be configured automatically. This default subnet mask should work for most networks. If your network is divided into subnetworks, you will need to create a custom subnet mask. To override the default subnet masks, use the **Set/Define IP Subnet Mask** command.

Figure 6-10: Setting the Subnet Mask

```
Local>> DEFINE IP SUBNET MASK 255.255.0.0
```

It is also possible to learn a subnet mask from BOOTP, though not all BOOTP server implementations support sending subnet masks. Check your BOOTP server's documentation.

To display the subnet mask, use the **Show IP** command.

Figure 6-11: Show IP Output

```
Local>> SHOW IPSCS Version B1.1/102int(951128)     Name:          DOC_SERVER
        Hardware Addr: 00-80-a3-0b-00-5b           Uptime:        1 Day    22:49
        IP Address: 192.0.1.221                    Subnet Mask:   255.255.255.0
```

The SCS will not change the subnet mask once it is set. If the SCS IP address is changed to a different class, for example, from a class B to a class C address, the subnet mask will remain a class B address.

The SCS supports **CIDR** (classless routing). CIDR allows Internet Service Providers (ISPs) to group blocks of class C networks into larger networks. Your ISP will provide you with the appropriate subnet mask. If you enter a CIDR subnet mask with the **Set/Define IP Subnet** command, the SCS will display a reminder that classless routing is being used.

Figure 6-12: Using Classless Routing

```
Local>> DEFINE IP ADDRESS 192.0.1.1
Local>> DEFINE IP SUBNET 255.255.240.0
%Info: Supernet (CIDR) mask set.
```

6.2.1 Length of Subnet Masks

Variable length subnet masks divide networks into subnetworks of different sizes. For example, if network 128.1.0.0 used variable length subnet masks, the subnet 128.1.4.0 might have subnet mask 255.255.255.0, and subnet 129.1.224.0 might have subnet mask 255.255.255.240.

For the SCS to function properly, all subnetworks within a particular network must use the same subnet masks even if each network has a subnet mask of a different length.

6.3 Name Resolving

TCP/IP hosts generally have an alphanumeric host name, such as athena, as well as a numeric IP address, such as 192.0.1.35. As a text host name may be easier to remember than an IP address, users may use this name to refer to the host during a Telnet connection attempt.

Network hosts do not understand alphanumeric (text) host names. When a text name is used, the SCS must translate it into its corresponding IP address. The translation process is called **name resolution**.

To resolve a name, the SCS can use one of two resources: its local name table or the Domain Name Service (DNS). For example, suppose user Bob wishes to telnet to athena.com. The SCS first consults its local host table; if the name doesn't exist, the SCS attempts to resolve the name using the DNS. If the name cannot be resolved, Bob must enter the IP address in order to access the host.

Some host names and IP addresses are added to the local host table by rwho packets, periodically broadcasted by UNIX hosts that support the rwho protocol. If addresses are not learned from rwho packets and DNS is not available, hosts may be manually added to the table. See *Adding Hosts to the Host Table* on page 6-7 for instructions.

To use the DNS, the SCS must know the IP address of the DNS server.

6.3.1 Configuring the Domain Name Service (DNS)

To use the DNS for name resolution, use the **Set/Define IP Nameserver** command.

Figure 6-13: Setting the Domain Name Server

```
Local.>> DEFINE IP NAMESERVER 192.0.1.166
```

To specify a backup nameserver, use the **Set/Define IP Secondary Nameserver** command. If the first nameserver isn't available, the request will be sent to the secondary server.

6.3.2 Specifying a Default Domain Name

A default domain name may be configured using the **Set/Define IP Domain** command. This domain name will be automatically appended to any host name during name resolution.

Figure 6-14: Configuring a Default Domain Name

```
Local>> DEFINE IP DOMAIN ctcorp.com
```

In the example above, the default domain name is ctcorp.com. If user Bob typed **telnet athena**, the SCS would automatically append the domain suffix and attempt to resolve **athena.ctcorp.com**.

If a hostname is entered that ends with a period ("."), the SCS will not add the domain suffix to the hostname for resolution.

6.3.3 Adding Hosts to the Host Table

If DNS is not available on your network, hosts may be manually entered in the local host table using the **Set/Define Hosts** command.

Figure 6-15: Adding a Host to the Local Host Table

```
Local>> DEFINE HOST athena 192.0.1.15
```

To display the current entries in the host table, use the **Show Hosts** command.

Figure 6-16: Displaying Host Table Entries

```
Local>> SHOW HOSTS
IP Address                Host                TTL
192.0.1.15                ATHENA              8 min (Rwho)
192.0.1.123               MERCURY             8 min (Rwho)
```

To remove an entry from the host table, use the **Clear/Purge Hosts** command.

Figure 6-17: Deleting a Host From the Host Table

```
Local>> PURGE HOST mercury
```

6.4 Header Compression

Each site may enable or disable compression of IP header information. When a site is created, IP header compression will be enabled by default.

When IP headers are compressed, the SCS replaces the packet's header with a **slot number**. This number is assigned dynamically, and denotes that the packet originated from a particular connection (for example, a Telnet session). When the destination receives the packet, it will decompress the header, replacing the representative slot number with the complete header information.

To use header compression, configure the number of slots (connections) supported on the site. This number should be slightly higher than the anticipated number of connections; in the event that more connections are made than expected, additional slots will be available for those connections.

To disable IP header compression, use the following command.

Figure 6-18: Disabling IP Header Compression

```
Local>> DEFINE SITE irvine IP COMPRESS DISABLED
```

Note: *The SCS uses Van Jacobson TCP compression, discussed in RFC 1144.*

Note:

6.5 Establishing Sessions

When you log into an SCS port to connect to a network service, your connection is referred to as a **session**. A network service may be an interactive login to a TCP/IP host, a connection to a modem on the SCS, another server, etc.

Note: *The word "sessions" in this manual is used to describe interactive connections; PPP or SLIP connections are not referred to as sessions.*

The following section explains how to establish sessions and set up connection characteristics. Specific port configuration and other session characteristics are discussed in *Port-Specific Session Configuration* on page 8-4.

To display the current sessions, use the **Show Sessions** command. The port number and username will be displayed, along with the connection type and current number of sessions.

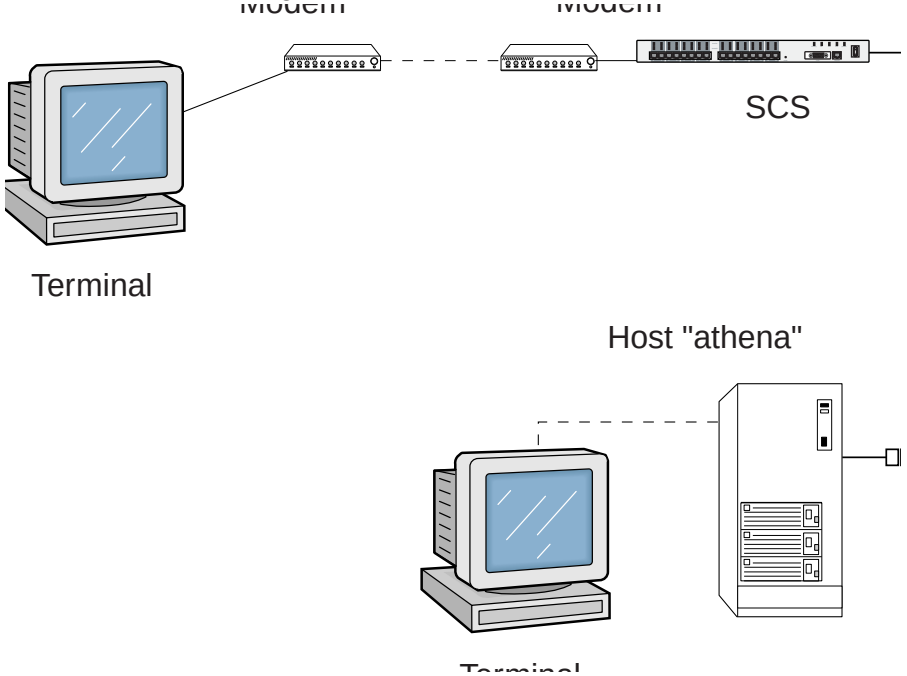
Figure 6-19: Displaying the Current Sessions

```
Local>> SHOW SESSIONS
Port 17:    bob          Telnet Login        Current: 2
            Session 1    Telnet:ATHENA       Interactive     (Cr,Del)
            Session 2    Telnet:HERCULES     Interactive     (Cr,Del)
```

6.5.1 Telnet and Rlogin Sessions

Telnet is an industry-standard protocol that enables users anywhere on a network to access a remote host and start a terminal session. Telnet connections do not require that either end of the connection know the hardware/software used on the other end; for example, if user Bob connects to host athena's platform (see Figure 6-20), athena doesn't know what terminal type Bob is using, and Bob doesn't know athena's platform or operating system.

Figure 6-20: Telnet Connections



Rlogin connections are similar to Telnet connections, however, Rlogin enables trusted users to log into a host without password verification.

6.5.1.1 Outgoing Telnet/Rlogin Connections

To establish an outgoing Telnet connection, use the Telnet command. To establish an outgoing Rlogin connection, use the Rlogin command. Either a text host name or an IP address may be specified.

Figure 6-21: Outgoing Telnet/Rlogin Connections

```
Local>> TELNET athena
Local>> TELNET 192.0.1.15
Local>> RLOGIN 192.0.1.15
```

Note: *For information on resolving host names, see Name Resolving on page 6-6.*

By default, Telnet and Rlogin connections will be made to a preset port number. To connect to a different port number, use the Telnet/Rlogin commands in conjunction with a port number (prefaced by a colon).

Figure 6-22: Telnetting to a Specific Port Number

```
Local>> TELNET athena:145
```

If the SCS port has been configured with a terminal type (such as VT100), this information will be sent to the remote host during the session. To configure the terminal type, use the **Set/Define Ports TermType** command.

Figure 6-23: Setting Terminal Type

```
Local>> DEFINE PORT 2 TERMTYPE VT100
```

Rlogin can be a security problem. When the SCS attempts an outgoing Rlogin connection, the SCS will send the username specified when the user logs into the SCS. If a user is not authenticated during the SCS login process, an unauthorized username may be used to Rlogin to remote hosts. The easiest way to avoid this problem is to disable outgoing Rlogin connections.

Figure 6-24: Disabling Outgoing Rlogin Connections

```
Local>> DEFINE SERVER RLOGIN DISABLED
```

Another way to secure your network is to ensure that the SCS is not a trusted host on any UNIX hosts on the network. This solution is not foolproof, however, as a user could still add the SCS to a UNIX host's .rhost file.

6.5.1.2 Incoming Telnet/Rlogin Connections

By default, the SCS will permit incoming Telnet and Rlogin connections. If this poses a security problem on your network, these connections can be disabled, restricted with a password requirement, or restricted using the IP security table.

To disable incoming Telnet/Rlogin connections, use the **Set/Define Server Incoming** command.

Figure 6-25: Disabling Incoming Telnet/Rlogin Connections

```
Local>> DEFINE SERVER INCOMING NONE
```

To require the login password for incoming Telnet/Rlogin connections, use the Password parameter:

Figure 6-26: Requiring the Login Password

```
Local>> DEFINE SERVER INCOMING PASSWORD
```

To restrict incoming Telnet and Rlogin connections using the IP security table, see *IP Security* on page 6-17. To restrict incoming connections to SSH, see Disabling HTTP and FTP, page 6-17.

6.5.2 SSH Sessions

SSH, or Secure Shell, is a secure transport protocol based on public-key cryptography. Unlike Telnet and Rlogin connections, SSH connections are encrypted, and require both the server and the user to be authenticated before a connection is allowed. The SCS currently supports SSH Protocol versions 1 and 2 with 3DES encryption**.** Compression is not supported.

To use SSH with the SCS, you must have SSH client software installed on the host that you are connecting from. Incoming SSH sessions will obey applicable virtual port settings (port 0), which are discussed on page 8-22.

When the SCS first powers on, it generates an ephemeral host key that is regenerated every hour. Incoming SSH connections are not permitted until this key generation is complete. Outgoing SSH is not affected.

6.5.2.1 Permanent Host Keys

When you power on the SCS for the first time, the SCS generates two permanent host key pairs. These keys will be used to identify the server and will only be replaced if the file storing the key is deleted and the SCS is rebooted. These key pairs are stored in **/flash/ssh/host_rsa_key.pub, /flash/ssh/host_rsa_key, /flash/ssh/host_dsa_key.pub,** and **/flash/ssh/host_dsa_key**.

The SCS may take a few minutes to generate new server host keys if they are ever deleted. Clients connecting to an SCS with new host keys may display appropriate warning or error messages.

6.5.2.2 Supported SSH Connections

By default, the SCS is configured to allow both SSH version 1 and SSH version 2 connections. In the default mode, the remote client is prompted to choose the version to use when an SSH connection attempt is made to or from the SCS. From the command prompt of the SCS, you can change this setting and specify the types of SSH connections allowed . Use the syntax: **Set/Define Protocol SSH Mode [V1ONLY | V1PREFER | V2PREFER | V2ONLY]**.

In conjunction with the **Set/Define /SSH Mode** command, you can use the following parameters:

Table 6-3: SSH Parameters

Parameter	Incoming (Host to SCS)	Outgoing (SCS to Host)
V1ONLY	SCS offers only SSHv1 connections	SCS only connects using SSHv1
V2ONLY	SCS offers only SSHv2 connections	SCS only connects using SSHv2
V1PREFER	SCS offers both v1 and v2 and the client chooses	If both SSHv1 and SSHv2 are available, chooses SSHv1
V2PREFER	SCS offers both v1 and v2 and the client chooses	If both SSHv1 and SSHv2 are available, chooses SSHv2

If a compatible protocol version is not agreed upon (one node wants SSH v1 and the other wants SSH v2), the connection does not occur.

6.5.2.3 Creating an Authorized_Keys File

RSA and DSA are commonly used Internet encryption and authentication systems included as part of the web browsers from Netscape and Microsoft. To use RSA and DSA user authentication for connections to the SCS, you must create an **AUTHORIZED_KEYS** file and store it in the **/flash/ssh/** directory of the SCS.

The **AUTHORIZED_KEYS** file consists of each user's public keys. For example, on a UNIX host, your public key is stored in a file called **.ssh/identity.pub**. The SSH client's key generation software creates both an unreadable private key file (often called identity) and human readable public key file (**identity.pub**).

Note: Not all clients come with this program. If yours does not, you may need to use the Username/Password Authentication method described below.

Copy the contents of the public key file to a text file, and save the file with the name **AUTHORIZED_KEYS**. (**AUTHORIZED_KEYS** is case sensitive).

Note: *Make sure there is no file extension. In Windows, you may need to save the file as a .txt file and then rename the file to remove the extension.*

6.5.2.4 Shared Key Authentication

RSA, DSA, and/or username/password authentication can be used to ensure that only authorized users access the SCS and connected equipment. The following sections explain how to configure each of these.

Following is an example of how public/private key authentication works on the SCS. In this example, RSA user authentication is used. DSA authentication is similar.

1. The SSH client on the user's computer sends the public half of its identity key to the SCS.
2. The SCS checks to see if this user's identity key is listed in the **AUTHORIZED_KEYS** (or **AUTHORIZED_KEYS2)** file on the SCS.

   If the user identity key is not listed in the **AUTHORIZED_KEYS** file on the SCS, then the authentication attempt fails. If the identity key is listed, the process continues.
3. The SSH client then sends the private half of its identity key to the SCS.
4. The SSH compares the private half of the user's identity key to the key stored in the **host_rsa_key** (or **host_dsa_key**) file on the SCS.
5. If the private keys match, the user's identity is confirmed and an SSH connection forms.

If RSA or DSA user authentication fails, the SCS prompts for a username and password (or just a password, if the SSH client forwarded the username). The user's name and password are then checked against the Radius, Secure ID, or local user databases, in order of their precedence settings. See Changing the Precedence on page 12-10.

6.5.2.5 Setting up RSA Shared Key Authentication (for SSH v1)

If you plan on using RSA user authentication for connections to the SCS, you must make an **AUTHORIZED_KEYS** file and store it in the SCS's **/flash/ssh/** directory before you attempt your first SSH connection. The **AUTHORIZED_KEYS** file consists of each SSH user's public keys. For example, on a UNIX host, your public keys are stored in a file called **.ssh/identity.pub**.

Create a file including the complete text of your **identity.pub** file, plus the public keys of any other users you want to authenticate for connections to the SCS. Save it in the SCS's **/flash/ssh/** directory as follows:

1. FTP to the IP address of the SCS.
2. Log in with the usernname of **root** and enter the privileged password (**system** by default).
3. Change directories to **/flash/ssh/**.
4. "**Put**" the AUTHORIZED_KEYS FILE into that directory.

5 Reboot the SCS.

Figure 6-27: RSA Method from Unix (OpenSSH) - No Passphrase

```
sshuser@UNIXHOST/# SSH -1 SSHUSER 172.19.21.51

Lantronix SCS Version B1.0/405(011102)

Type HELP at the 'Local_33>' prompt for assistance.

Username>
```

Figure 6-28: RSA Method from Unix (OpenSSH) - with Passphrase

```
sshuser@UNIXHOST/# SSH -1sysadmin
172.19.21.51
sysadmin@172.19.21.51's password:
Lantronix SCS200 Version B1.0/405(011102)
Type HELP at the 'Local_34>' prompt for assistance.

Username>
Username/Password Authentication Setup
```

New authentication keys are generated within a few minutes based on the list of authorized user public keys. A file called **host_rsa**_key contains the authorized users' private identity keys. A file called **host_rsa_key.pub** contains the authorized users' public identity keys.

Note: *Key generation, especially of host keys, can take a significant amount of time. When the SCS boots for the first time or is factory defaulted, it must generate all the keys. Depending on your SCS model, key generation could take between one and five minutes.*

As you add individual users, add their public keys to the **AUTHORIZED_KEYS** file on your workstation and FTP the updated file to the SCS.

If this file is located at SSH connection time, and the public key of the user is valid, the user will automatically be logged into the **Local>** prompt or, if user authentication is configured on that port, the user may be prompted for his username and password. See *Database Configuration* on page 11-9 for information on configuring user authentication.

If the file is not located at connection time, the SCS proceeds to password authentication.

6.5.2.6 Setting up DSA Shared Key Authentication (for SSH v2)

If you plan on using RSA user authentication for connections to the SCS, you must make an **AUTHORIZED_KEYS2** file and store it in the SCS's **/flash/ssh/** directory before you attempt your first SSH connection. The **AUTHORIZED_KEYS2** file consists of each SSH user's public keys. For example, on a UNIX host, your public keys are stored in a file called **.ssh/identity.pub**.

Create a file including the complete text of your **identity.pub** file, plus the public keys of any other users you want to authenticate for connections to the SCS. Save it in the SCS's **/flash/ssh/** directory as follows:

1 FTP to the IP address of the SCS.

2 Log in with the usernname of **root** and enter the privileged password (**system** by default).

3 Change directories to **/flash/ssh/**.

4 "**Put**" the **AUTHORIZED_KEYS2** FILE into that directory.

5 Reboot the SCS.

New authentication keys are generated within a few minutes based on the list of authorized user public keys. A file called **host_dsa**_key contains the authorized users' private identity keys. A file called **host_dsa_key.pub** contains the authorized users' public identity keys.

Note: *Key generation, especially of host keys, can take a significant amount of time. When the SCS boots for the first time or is factory defaulted, it must generate all the keys. Depending on your SCS model, key generation could take between one and five minutes.*

As you add individual users, add their public key to the **AUTHORIZED_KEYS2** file on your workstation and FTP the updated file to the SCS.

If this file is located at SSH connection time, and the public key of the user is valid, the user will automatically be logged into the **Local>** prompt or, if user authentication is configured on that port, the user may be prompted for his username and password. See *Database Configuration* on page 11-9 for information on configuring user authentication.

If this file is not located at connection time, the SCS proceeds to password authentication.

6.5.2.7 Username/Password Authentication (SSHv1 or SSHv2)

If RSA or DSA authentication fails, the SCS prompts the user for a password (or just a password, if the SSH client forwarded the username). The user's name and password are then checked against the internal user database, Radius, or Secure ID, in order of their precedence settings (if configured).

Figure 6-29: Username/Password Authentication

```
% ssh scs2
 paul@scs2's password:
```

Note: *Expired local passwords cannot be updated and login scripts will not be run at this point of the SSH process.*

Once the username and password are verified, SSH authentication is complete. The user will be moved on to any previously configured user authentication (as enabled with the **Set/Define Ports Authenticate** command) that would normally apply to a login on that port. At this point, all authentication methods, including RADIUS and SecurID, will be available, and expired local passwords will be prompted for updates.

For example, if authentication is enabled on virtual ports (port 0), the user in Figure 6-30 will be prompted again for the username and password.

Figure 6-30: Previously Configured User Authentication

```
% ssh scs2
 paul@scs2's password:(not echoed)

Lantronix Version n.n/n (yymmdd)
Type Help at the 'Local_>' prompt for assistance.

Username> paul
Password> (not echoed)
```

6.5.2.8 SSH Incoming Connections (Unix and Non-Unix)

Note: *For a successful incoming SSH connection, RSA, DSA, and/or local password user authentication must be configured.*

To form an SSH connection from a Unix platform to an SCS, your computer must have an SSH client installed (OpenSSH, for example).

1. At the command prompt, enter **ssh** followed by the SCS host name or IP Address. You may also specify a username by adding **a –l(username)** or **(username)@hostname**.

Figure 6-31: Forming an SSH Connection (UNIX)

```
% ssh -l(username) (hostname or IP)
% ssh (username)@(hostname or IP)
```

2. If your RSA or DSA key is passphrase protected, enter your password.
3. If you are not using an RSA or DSA key, specify the username and password that the SCS will use to authenticate you.
4. If connecting directly to a serial port on the SCS, specify the port number as **22xx**, where xx is the port number. For the appropriate SSH options for your system, enter **man ssh** or view your client software's help files for a full listing of instructions and syntax requirements.

Figure 6-32: Forming an SSH Connection to a Port

```
% ssh -p2202 (hostname or IP)
```

To form an SSH connection from a non-Unix platform to an SCS:

1. Start your SSH Client software.
2. Enter the SCS host name or IP Address and specify the public key file to use.
3. Enter the **ssh** command followed by the SCS name.
4. If connecting directly to a serial port on the SCS, specify the port number as **22xx,** where xx is the port number. In the example below, an SSH connection is formed to port 2 of scs2. For the appropriate SSH options for your system, enter **man ssh** or view your client software's help files for a full listing of instructions and syntax requirements.

5 If your RSA or DSA key is passphrase protected, enter your password.

6 If you are not using an RSA or DSA key, specify the username and password that the SCS will use to authenticate you.

Figure 6-33: Forming an SSH Connection

```
% ssh -p2202 scs2
```

6.5.2.9 Outgoing SSH Connections

To form an SSH connection to another host from the SCS, enter the **ssh** command followed by the desired host's hostname or IP address.

The first time you SSH to a remote host from the SCS, the SCS notes that the host is not recognized, but permits the connection. If you are not the privileged user, you will be allowed to use the host's key for the current session, but the key will not be permanently saved in the list of known hosts.

Figure 6-34: Outgoing SSH Connections for Nonprivileged User

```
Local_9> ssh athena
%Info: The authenticity of host 'athena' can't be established.
RSA key fingerprint is 5f:d0:d7:69:39:d1:ca:fb:71:eb:g4:33:b1:ba:8c:e9.
%Warning: Failed to add the host to the list of known hosts
/flash/ssh/known_hosts: Permission denied
mary@athena's password:
```

If you are the privileged user, the host's key is permanently added to the table of known hosts (stored in /flash/ssh/known_hosts).

Figure 6-35: Outgoing SSH Connections for Privileged User

```
Local_9>> ssh athena
%Info: The authenticity of host 'athena' can't be established.
RSA key fingerprint is 5f:d0:d7:69:39:d1:ca:fb:71:eb:g4:33:b1:ba:8c:e9.
%Warning: Added 'athena' (RSA) to the list of known hosts.
mary@athena's password:
```

For each following connection between the SCS and that host, the host's key will be compared to that stored in the known host table. If the key is authentic, the connection will automatically proceed to user authentication.

If the key has changed, you will receive a warning and a brief list of possible explanations including a possible man-in-the-middle attack. To successfully connect, erase that host's public key from the known_hosts file on the SCS, then attempt the connection again. The SCS will note that the host is not recognized.

The **ssh** command can be followed by an optional command that will be executed on the remote machine, and then the session will end. **Place the command in quotes to maintain capitalization.** The following command will log user mary into host athena, provide a complete list of files including modification dates and ownership, and then log mary out of the host.

Figure 6-36: Outgoing SSH Connection with Command

```
Local_2>> ssh athena mary “ls -l”
 mary@athena’s password: (not echoed)
```

Outgoing SSH connections may be set as the preferred or dedicated service for a port. For more information, see *Preferred/Dedicated Protocols & Hosts* on page 8-8.

6.5.3 Restricting Connections to SSH

To restrict incoming connections SSH and block non-encrypted logins, use the Set/Define Server Incoming **Secure** command. The **Server Incoming Secure** command disallows unsecure Telnet and TCP connection attempts. Access is through SSH only.

Figure 6-37: Restricting Connection to SSH

```
Local_2>> define server incoming secure
```

To re-enable Telnet, use the Set/Define Server Incoming **Telnet** command. SSH is always enabled.

Figure 6-38: Re-enabling Telnet

```
Local_2>> define server incoming telnet
```

6.5.4 Disabling HTTP and FTP

You can make the SCS into a highly secure host by turning off the FTP and HTTP services. For information on disabling HTTP and FTP, see *Disabling the FTP and HTTP Servers* on page 11-23.

Note: *The web interface will no longer be available.*

6.6 IP Security

The SCS’s IP security features allow an administrator to restrict incoming and outgoing TCP/IP sessions, access to ports, and print jobs. Connections are allowed or denied based upon the source IP address for incoming connections and print jobs and the destination IP address for outgoing connections.

IP security for connections can be set to Incoming Enabled/Disabled, Outgoing Enabled/Disabled, or Both. Incoming refers to users on other hosts attempting to log into the SCS. Outgoing refers to local users connecting to other TCP/IP hosts. The Both parameter enables or disables both Incoming and Outgoing connections. IP security for printing can be set to Enabled or Disabled. The printing setting affects both LPR and RTEL print jobs from the specified hosts.

Note: *The SCS has no default IP security restrictions.*

6.6.1 Configuring the Security Table

The IP security table provides rules for checking a TCP/IP connection for legality. To configure the IP security table, use the **Set/Define IP Security** command. To add an entry to the table, specify a valid IP address, a list of affected ports, and what type of restriction is desired.

Figure 6-39: Set/Define IP Security Commands

```
Local>> DEFINE IP SECURITY 192.0.1.255 OUTGOING DISABLED PORT 3
Local>> DEFINE IP SECURITY 192.0.5.255 PRINTING DISABLED
```

The first command prevents port 3 from beginning sessions with hosts whose addresses range from 192.0.1.1 through 192.0.1.254. A 255 in any segment applies to all numbers in that range—192.0.1.255 includes 192.0.1.1, 192.0.1.2, and so on. The second command prevents nodes with IP addresses from 192.0.5.1 through 192.0.5.254 from sending print jobs to the server.

A more specific rule takes precedence over a less specific one. For example, if connections to 192.0.1.255 are disabled but connections to 192.0.1.78 are enabled, a connection to 192.0.1.78 will succeed. If no entries are defined in the table, all connection attempts will succeed. To ensure that all connections will fail unless directly specified in another entry, enter the following command:

Figure 6-40: Set/Define IP Security Commands

```
Local>> SET IP SECURITY 255.255.255.255 INCOMING DISABLED OUTGOING DISABLED
```

Note: *If the user making the connection is the privileged user (see the Set Privileged/ Noprivileged command), the connection will be allowed regardless of the entries in the table.*

A trailing zero in any address segment is shorthand for “all addresses in this range, both incoming and outgoing disabled, for all ports.” For example, the following two commands are equal.

Figure 6-41: Set/Define IP Security Commands

```
Local>> DEFINE IP SECURITY 192.0.1.0
Local>> DEFINE IP SECURITY 192.0.1.255 OUTGOING DISABLED INCOMING DISABLED
```

Finally, port zero corresponds to the virtual ports (that is, users who log into the server from the network). If no ports are specified on the command line, the command will affect all local and virtual ports.

Note: *For a description of virtual ports, see Virtual Ports on page 8-22.*

6.6.2 Clearing Table Entries

Individual entries can be cleared by entering **Clear (or Purge) IP Security** with no parameters other than the address.

Figure 6-42: Clear IP Security Command

```
Local>> CLEAR IP SECURITY 192.0.1.102
```

The entire security table can be cleared with the following command.

Figure 6-43: Clearing the Security Table

```
Local>> CLEAR IP SECURITY ALL
```

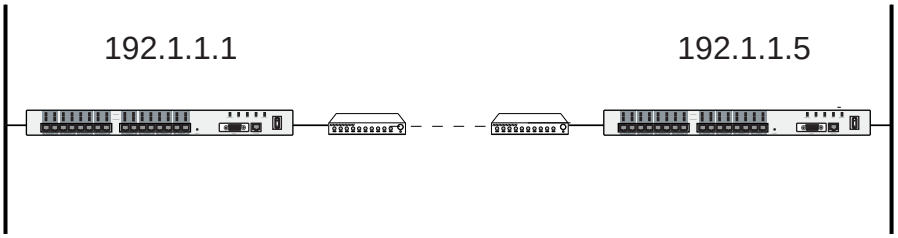
6.7 IP Routing

TCP/IP internets are usually broken down into networks. Each host on a particular network can only see hosts on its network; to transfer network traffic to other networks, routers (also called gateways) are required. Routers are typically connected to two or more networks.

The SCS serves as a router for the networks that it is directly connected to. To determine the path to other routers on the network, the SCS will listen to network broadcast packets (for example, RIP packets); routers will advertise themselves in these packets.

The SCS must be positioned between two networks in order for routing to work correctly. If two or more SCSs are used, the units cannot be on the same network (as in Figure 6-44).

Figure 6-44: Two Units Used to Link the Same Network



6.7.1 How Packets are Routed

When an IP host tries to send a packet, it looks to see if the destination address is on the same network as the host's IP address. If it is, the host sends the packet directly to its destination. If the packet is destined for a different network, the host sends it to a router (in this case, the SCS).

When the SCS receives the packet, it examines the packet's destination address, determines the most efficient route to this address, and forwards the packet to this location. The "most efficient route" is determined using two factors: the network that the address is part of and the SCS routing table, which is discussed in the following section.

6.7.2 Routing Tables

The SCS uses a routing table to keep track of which networks are reachable, and the shortest route to each network. A typical routing table entry consists of the destination network, and which router is the best path to that network. Routing tables also keep track of the cost or metric required to get to a given network.

6.7.2.1 Types of Routes

There are three types of routes: host, network, and default.

Host Routes A Host Route is a route to a single host. Generally, a host route is entered for each Remote Node that logs into the SCS.

Network Routes A network route is a route to another network. A network route is used if a host route to the destination doesn't exist.

Default Routes A default route is used if a more specific host or network route isn't available. It is used to cut down on the size of routing tables and dynamic routing protocol updates. If, for example, the SCS is the only path for network packets to reach a much larger group of networks, the SCS can be configured to advertise itself as the default route.

Note: *See Set/Define IP Route Default on page 12-42 and Define Site IP Default on page 12-140.*

An SCS in a small sales office might have a default route that points to the corporate headquarters. The SCS doesn't need to know about all of the routes on the headquarters network. It only knows to send all otherwise unspecified traffic to the central location, where it will be routed to the final destination.

6.7.2.2 Adding Routes to the Table

Entries may be added to the routing table in three ways: locally, statically, or dynamically.

Locally When a route is added locally, it is automatically determined from the SCS IP address and network mask. The SCS always keeps a local route to the Ethernet that is attached to; this route is never deleted.

Statically

Statically-entered routes are entered and removed by the administrator. These routes are used when dynamic routes are unavailable.

To add a static route to the routing table, use the **Set/Define IP Route** command. A destination and a path to that destination must be specified. The destination may be an IP network, subnetwork, or host.

The path may be another router on the Ethernet or a site. To specify that the route is another router, use the **Nextrouter** parameter. To specify that the route is to a site, use the **Site** parameter. The Site parameter indicates that a particular site should be started to forward the packet. The site will handle any remote connections necessary to forward the packet (for example, dialing another LAN).

A metric will be associated with the route to indicate its "cost." The SCS will use the route to determine the most efficient route; routes with a lower cost will be chosen over routes with a higher cost. If a metric is not specified, the SCS will assign a metric of 1 to the route.

Figure 6-45: Adding Static Routes

```
Local>> DEFINE IP ROUTE 192.5.4.0 NEXTROUTER 192.0.1.1 4
Local>> DEFINE IP ROUTE 192.5.3.0 SITE dallas
```

In Figure 6-45, the first command specifies that the route to network 192.5.4.0 is through another router, 192.0.1.1. The route was assigned a metric of 4.

The second command specifies that the route to network 192.5.3.0 is through site dallas. As a metric is not specified, the SCS will assign this route a metric of 1. When the SCS receives traffic destined for network 192.5.3.0, if this route is determined to be the most efficient route, site dallas will be started and will forward the packet.

To enter a static default route, use the **Set/Define IP Route Default** command.

Figure 6-46: Adding Default Routes

```
Local>> DEFINE IP ROUTE 192.0.1.0 DEFAULT SITE internet
Local>> DEFINE IP ROUTE 192.0.2.0 DEFAULT NEXTROUTER 192.0.1.1 2
```

Dynamically

These routes are automatically learned from other routers on the network and are managed by a dynamic routing protocol. The SCS currently supports one dynamic routing protocol, RIP. Routes are automatically entered when new networks come online, and automatically removed if the networks are no longer reachable.

Dynamic routes learned via sites are the exception; they are never timed out. The SCS assumes that these networks are reachable by bringing up a link. This allows the SCS to learn about extended networks at the remote site without the administrator's intervention.

6.7.3 Using RIP

RIP (Routing Information Protocol) is the dynamic routing protocol supported by the SCS. Throughout this manual, the term “RIP” refers to RIP version 1. RIP is automatically enabled on all SCS interfaces, including sites. For a complete discussion of RIP options, including disabling RIP, see *Configuring RIP for Sites* on page 4-10.

Note: *RIP is described in RFC-1058.*

Normally, RIP listens to routing table updates from any source. This can lead to problems if a misconfigured host accidentally begins sending incorrect information via RIP. It may also lead to security or denial of service attacks by a malicious user who is capable of sending false RIP messages.

The SCS can be configured to listen only to RIP updates from a list of trusted IP addresses. See **Set/Define IP Trusted** on page 12-47 for details. This is not entirely foolproof however, as a sophisticated attacker could still send RIP updates as one of the trusted addresses and potentially defeat the system.

6.7.4 Proxy ARP

Every TCP/IP host will reply to any ARP request that is for its own IP address. Proxy-ARP enables a device to also respond to ARP requests for addresses that it is “responsible for.” In the case of the SCS, enabling proxy ARP allows the SCS to respond to requests for hosts and networks that it is the gateway for. For example, if there are remote node connections into the SCS, any ARP requests for those nodes will be replied to by the SCS itself.

Proxy ARPing allows remote nodes to appear as if they were on the same Ethernet segment as the SCS. This feature is particularly useful for ethernet hosts that do not support RIP; those hosts will not need to learn host-route information to forward traffic destined for the remote node devices.

To enable proxy ARP, use the **Set/Define IP All/Ethernet Proxy-ARP** command.

Figure 6-47: Enabling Proxy ARP

```
Local>> DEFINE IP ETHERNET PROXY-ARP ENABLED
```

The SCS will not respond to ARP requests for routes learned from the Ethernet, or for routes that aren’t explicitly listed in the SCS routing table.

6.7.5 Using the NetBIOS Nameserver (NBNS)

Microsoft Windows users can run NetBIOS over IP and use the DNS for name resolution, or a primary or secondary NetBIOS nameserver (NBNS). This allows Windows clients to use the Network Neighborhood browser without any additional configuration on the Windows host.

To specify a NetBIOS nameserver, use the following command. A secondary NetBIOS nameserver can be configured if desired.

Figure 6-48: Setting the Domain Name Server

```
Local>> DEFINE IP NBNS 192.0.1.178
```

NBNS will allow Windows clients to use the Network Neighborhood browser without any additional configuration on the Windows host.

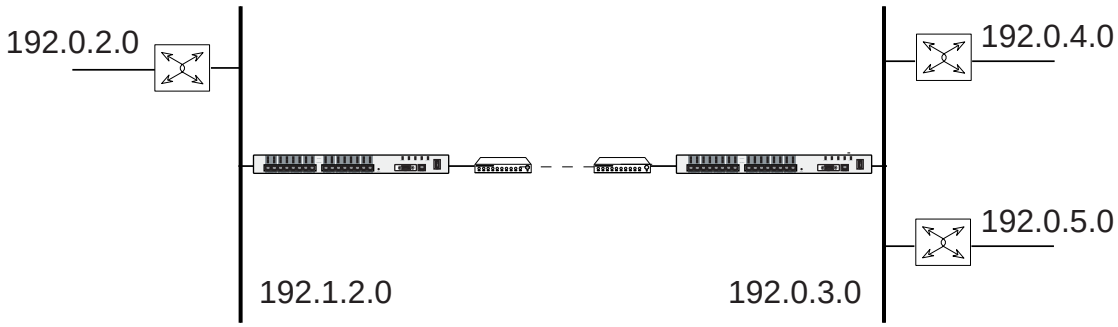
Note: *NBNS is also called WINS.*

6.7.6 Routing and Subnetworks

When dividing a network into subnetworks, ensure that subnetworks are contiguous. The SCS uses RIP to learn routing information; if subnetworks are not contiguous, RIP cannot correctly inform the SCS of the route to a particular network.

Figure 6-49 gives an example of discontinuous subnetworks.

Figure 6-49: Discontinuous Subnetworks



6.8 Displaying the IP Configuration

The **Show IP** commands display IP configuration information, including information about the IP router, IP interfaces, and IP address of the remote host. To display the basic IP configuration, use the **Show IP** command without any additional parameters.

Figure 6-50: Show IP Output

```
Local>> SHOW IP
   SCS Version B1.1/102int(951128)Name:DOC_SERVER
       Hardware Addr: 00-80-a3-0b-00-5b          Uptime:      3 Days      02:07

       IP Address:          192.0.1.53           Subnet Mask:           255.255.255.0
       Nameserver:          (undefined)          Backup Nameserver:     (undefined)
       Domain Name:         (undefined)          Host Limit:            200
       Timeserver:          (undefined)          Backup Timeserver:     (undefined)
       IP Routing:          Enabled

                            Received    Sent     Seconds since zeroed   270144
IP     Frames:              431535      13520    Errors:                0
       Fragments:           0           0

TCP    Frames:              4616        4046     Connect Failure Reasons:0000
       Invalid Frames:  1   0                    Invalid Packet Reasons: 0030
       Retransmissions:     0

ICMP   Frames:53    ICMP Reasons:0045
```

The **Show IP Interface** command displays a one-line summary for each of the router's interfaces. There will always be an interface for the Ethernet, as displayed in Figure 6-51. When sites are active, interfaces to these sites will be displayed.

The **Uptime** field displays how long (in days:hours:minutes format) each interface has been active. The **Lastin** field displays the duration since the last packet arrived on a particular interface. The **Lastout** field displays the duration since the interface sent outgoing traffic.

Figure 6-51: Show IP Interface Output

```
Local>> SHOW IP INTERFACE
   SCS Version B1.1/102int(951128)     Name:DOC_SERVER
        Hardware Addr: 00-80-a3-0b-00-5b                Uptime:      3 Days 02:07
Name            IP Address      Remote IP Address       Uptime          Lastin      Lastout
Ethernet                        192.0.1.221             74:07:04        0:00        0:00
```

When used in conjunction with a particular site's name, the **Show IP Interface** command displays information about the site's interface, including its IP address, subnet mask, IP address of the remote host, and RIP statistics.

Figure 6-52: Show IP Interface for a Particular Site

```
Local>> SHOW IP INTERFACE irvine
   SCS Version B1.1/102int(951128)              Name:              DOC_SERVER
      Hardware Addr: 00-80-a3-0b-00-5b          Uptime:            3 Days   02:07
                                    20:42:54
      Name                bob                   Type:              Dialup
      Netstate:           Running               Device/Refcount:   lm0:/002
      IP Address:         192.0.1.221           Remote Address:    192.0.1.245
      Netmask:            255.255.255.0         Network:           192.0.1.0
      TimeToLive Cost:    0                     Largest Packet (MTU)1500
      Pool Range Start:(undefined)              Pool Range End:    (undefined)
      Pool Status:        Invalid               Pool Addresses In Use:0

      Listen to RIP Packets:          Enabled   Send RIP Packets:  Enabled
      Rip Update Time (seconds):      30        Rip Metric:        1
      Default Interface:              Disabled  Trusted Routers:   Disabled
      Proxy Arp:                      Disabled

      Packets In:         622                   Packets Out:       1190
      Packets In Filtered:0                     Packets Out Filtered:0
      Packet Errors:      0                     Uptime:            04:03
      Last Packet In:     0:00                  Last Packet Out:   0:00
      Last Routed Packet In:0:00                Last Round Packet: 0:00
```

The **Show IP Route** command displays the routes currently in the SCS routing table.

Figure 6-53: Show IP Route Output

```
Local>> SHOW IP ROUTE
        SCS Version B1.1/102int(951128)                 Name:       DOC_SERVER
        Hardware Addr: 00-80-a3-0b-00-5b                Uptime:     3 Days 02:07
Destination     Next Router     Metric  Source  Timer   Interface
Default Route   192.0.1.70      3       RIP     02:31T  Ethernet
192.4.4.0       192.0.1.202     3       RIP     02:51T  Ethernet
192.0.1.0       192.0.1.57      2       Local   ------  Ethernet
192.3.5.0       192.0.1.238     1       RIP     02:48T  Ethernet
```

The **Source** field indicates how the route was added to the table; statistically, locally, or from RIP.

The **Timer** field displays how long (in minutes:seconds format) the SCS will continue to use this route. For static and local routes, this field will display a series of dashes (----); these routes are never timed out.

If a "T" is displayed on the right of the Timer value, the value represents the route's time-to-live. If a RIP update for the route is not received within this time period, the route will be marked as unreachable, and the T will be changed to a "D" to denote that the route is invalid, but isn't ready to be deleted yet. If "Exp" is displayed, the route is about to be deleted from the table.

The **Interface** field displays the interface used to forward packet traffic.

6.9 Examples

6.9.1 IP Address Assignment for Remote Networking

An SCS handles incoming calls from a series of remote node users. Two of these users, Bob and Frank, have special IP address requirements.

The SCS must be configured to do the following:

- Assign the same IP address to Bob each time he logs in.
- Permit Frank to select his own IP address.

  Note: *In general, allowing user-selected IP addresses is not recommended. It poses some security risks and could result in duplicate IP addresses.*

- Dynamically assign IP addresses to the remaining remote node users from an IP address pool. Only five SCS ports have been configured to accept incoming calls, therefore, only five IP addresses must be included in the pool.

Bob will use site **bob** when he logs into the SCS. At authentication time, he will be prompted for the site's local password, **badger**. He will be assigned IP address **192.0.1.108**.

Figure 6-54: Configuring Site bob

```
Local>> DEFINE SITE bob IP REMOTEADDRESS 192.0.1.108
Local>> DEFINE SITE bob AUTHENTICATION LOCAL “badger”
```

When Frank logs into the SCS, he will use site **frank**, which requires that he enter the password **wallaby**. No remote IP address is defined for this site, therefore, Frank may use any IP address he wishes.

Figure 6-55: Configuring Site frank

```
Local>> DEFINE SITE frank AUTHENTICATION LOCAL “wallaby”
```

To create the IP address pool, use the following command:

Figure 6-56: Creating IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.100 192.0.1.105
```

All incoming callers that do not specify a particular site (such as bob or frank) will use the default site for the connection. To require that default site users use an IP address from the pool, use the **Define Site Default IP Remoteaddress** command.

Figure 6-57: Using the Address Pool for the Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.100 192.0.1.105
```

6.9.2 General IP Setup

The following figure illustrates the commands required for the average IP setup:

Figure 6-58: General IP Configuration

```
Local>> DEFINE IP ADDRESS 192.0.1.11
Local>> DEFINE IP SUBNET 255.255.255.0
Local>> DEFINE IP NAMESERVER 192.0.1.45
Local>> DEFINE IP SECONDARY NAMESERVER 192.0.1.184
Local>> DEFINE IP DOMAIN “ctcorp.com”
Local>> DEFINE IP TIMESERVER 192.0.1.45
Local>> DEFINE IP SECONDARY TIMESERVER 192.0.1.455
```

6.9.3 Adding Static Routes

All IP packets to unknown networks must be forwarded to Internet gateway router **192.0.1.110**. A default route to this router must be configured on the SCS, and the route must be included in RIP updates to other routers. The route must have a metric of 2.

Figure 6-59: Default Route to Router

```
Local>> DEFINE IP ROUTE DEFAULT NEXTROUTER 192.0.1.110 2
```

Another router, **192.0.1.99**, provides access to the network **192.1.1.0**. This route must also be assigned a metric of 2.

Figure 6-60: Static Route to Router

```
Local>> DEFINE IP ROUTE 192.1.1.0 NEXTROUTER 192.0.1.99 2
```

6.9.4 Default Routes to a Site

All IP packets to an unknown network must be forwarded to the Internet access provider. Site **internet** is used to manage connections to this location.

A default route to internet must be configured on the SCS. The route must be included in RIP updates to other routers; it must have a metric of two.

Figure 6-61: Default Route to Site

```
Local>> DEFINE IP ROUTE DEFAULT SITE internet 2
```

7: PPP

The SCS can use PPP, the Point-to-Point Protocol, to transmit high layer protocols over a serial link, ISDN connection, or other point-to-point based connection. Unlike SLIP (the Serial Line Internet Protocol), which can also be used with the SCS, PPP supports authentication, escape sequences for flow control characters, loopback detection, and per-packet checksums.

Two major components of PPP are discussed in the following sections:

- *LCP* on page 7-1 discusses the Link Control Protocol (LCP).
- *NCP* on page 7-3 discusses Network Control Protocols (NCPs).

The final section discusses *Starting PPP* on page 7-3. PPP is also discussed in Chapter 4, *Basic Remote Networking*, and PPP authentication (PAP and CHAP) are described in *PPP Logins* on page 11-3.

7.1 LCP

The Link Control Protocol (LCP) is used by PPP to negotiate basic characteristics of the connection. These characteristics include packet size, header compression, control character escaping, and authentication mechanisms.

Note: *LCP is documented in RFCs 1661 and 1662.*

7.1.1 Packet Sizes

Both sides of a connection negotiate the size of the packets each can receive. Packet size is also known as **Maximum Receive Unit** (MRU). The MRU need not be the same in each direction. The SCS MRU is 1522 bytes.

To configure the maximum packet size that can be received from a remote node, set the **Maximum Transmission Unit** (MTU), or maximum packet size, with the **Define Site MTU** command.

7.1.2 Header Compression

PPP frames each packet with certain data fields, some of which may be omitted or compressed (see **Define Ports PPP** on page 12-81 for details). PPP header compression is enabled by default on all SCS ports. To disable header compression, use the following command.

Figure 7-1: Disabling PPP Header Compression

```
Local>> DEFINE PORT 2 PPP HEADERCOMPRESSION DISABLED
```

7.1.3 Character Escaping

PPP can be configured to substitute a two byte sequence of characters for specific characters. The substituted characters are sent instead and the recipient translates them back into the original characters. This substitution is called character escaping.

Escaping characters is often used with XON/XOFF flow control. This method of flow control, used with many modems, involves treating two characters (hex 0x11 and hex 0x13) in a special manner.

Applications that use these characters (such as certain text editors) may incorrectly trigger XON/XOFF flow control. If a user enters Ctrl-S (hex 0x13) or Ctrl-Q (hex 0x11), these characters won't be transmitted; they'll be interpreted as flow control characters and removed from the data stream.

PPP can escape values between 0x00 and 0x1f, inclusive. To do this, PPP uses a 32-bit **Asynchronous Character Control Map** (ACCM). For each character to be escaped, that corresponding bit is set in a hexadecimal format in the ACCM. For XON/XOFF flow control, the ACCM would be 0x000A0000.

Note: *The values 0x7d and 0x7e are always escaped.*

To escape a particular character, use the **Define Ports PPP ACCM** command. To automatically escape the XON/XOFF flow control characters, use the XONXOFF parameter. To escape all control characters, enter 0xffffffff as the ACCM value. These options are all shown in Figure 7-2.

Figure 7-2: Escaping Characters

```
Local>> DEFINE PORT 2 PPP ACCM 0X000A0000
Local>> DEFINE PORT 2 PPP ACCM XONXOFF
Local>> DEFINE PORT 2 PPP ACCM 0xffffffff
```

If the port is set for XON/XOFF flow control, the XON/XOFF characters are automatically added to any configured ACCM.

7.1.4 PPP Authentication

PPP supports two authentication methods: the Challenge Handshake Authentication Protocol (CHAP) and the Password Authentication Protocol (PAP). Both protocols involve a pre-assigned password.

- **CHAP** authentication begins with a challenge message from the unit to verify its peer. The peer receives the challenge, uses its password to encrypt the challenge, and responds. The authenticating unit then checks the response against what is expected, and either accepts or rejects the authentication attempt. At no time is the password transmitted over the link.
- **PAP**, a simpler protocol, involves transmitting the username and password over the link in plain text. If the unit is authenticating to an unauthorized peer, the password could be compromised.

7.1.4.1 Configuring CHAP and PAP

The SCS may be configured for PPP authentication in one of three ways:

1. Remote hosts must authenticate themselves
2. The SCS authenticates itself to remote hosts
3. Remote hosts and the SCS authenticate each other

PAP and CHAP may be enabled on each port and each site. If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the peer does not support CHAP, PAP will be attempted instead.

On incoming connections, the port's CHAP or PAP configuration will be used to determine the authentication required for the connection. For example, if a remote node was logged into port 2 on the SCS and port 2 was configured to use PAP to authenticate remote hosts, the remote node would be prompted to authenticate itself.

Outgoing connections use the site's CHAP or PAP configuration. For example, if site **irvine**, which has CHAP enabled, initiated an outgoing connection to a remote router, and the remote site required the SCS to authenticate itself using CHAP, the SCS would offer its username and password to the remote site.

Use caution with CHAP/PAP authentication because configuring both a local and a remote password on the same site could compromise security. If a site with both local and remote passwords defined receives an incoming call, during the LCP negotiation process the site will say that it is willing to transmit both passwords. The passwords will not be automatically transmitted, but the site will let the user know that it is willing to do so if required. If the user requires the SCS to authenticate itself, the SCS will transmit the remote password over the link, thereby give the user a password to access the server.

Note: *For a complete description of authentication, refer to Chapter 11, Security.*

7.1.5 CBCP

The SCS supports the Microsoft Callback Control Protocol (CBCP) for dial-in PPP clients that request it. In conjunction with the CBCP, you can configure the SCS to allow the PPP client to choose a dialback telephone number to reverse phone charges.

For more information, see *Dialback Using CBCP* on page 11-7.

7.2 NCP

Network Control Protocols (NCPs) govern use of a specific network protocol over the PPP link. On the SCS, PPP uses the IP protocol. PPP uses the IP Control Protocol (IPCP) to negotiate the use of IP over a link. IPCP allows for dynamic address assignment and Van Jacobson TCP header compression.

Note: *IP over PPP is described in RFC 1332. Van Jacobson TCP compression is covered in RFC 1144.*

If, during the negotiation process, the SCS receives a request for more IP compression slots than are configured on the site (using the **Define Site IP Slots** command), the SCS will NAK (negative acknowledge), and request the number of slots configured on the site.

7.3 Starting PPP

PPP can be started in a number of ways. For a detailed discussion of the PPP startup sequence, see *Starting PPP/Slip for Incoming Connections* on page 4-11 and *Using Sites for Outgoing Connections* on page 4-6.

7.3.1 User-Initiated PPP

If PPP is enabled for a port, you can start a PPP session from Local> mode using the **Set PPP** command. You can specify a site to connect to by appending the site name to the command.

7.3.2 Automatic Detection of PPP

A port may be configured to automatically detect a PPP packet and, if PPP is enabled on the port, run PPP when the packet is received. This eliminates the need for callers to explicitly start PPP.

To enable this PPP autodetection feature, use the **Define Ports PPPdetect** command.

Figure 7-3: Enabling Automatic Protocol Detection

```
Local>> DEFINE PORT 2 PPPDETECT ENABLED
```

If you enable PPP protocol detection, you should also configure PPP authentication (CHAP or PAP) wherever possible. If PPP authentication is not possible, enable user authentication and the **Set PPP** command to authenticate incoming calls instead.

7.3.3 Dedicated PPP

If a port is dedicated to PPP (see *Preferred/Dedicated Protocols & Hosts* on page 8-8), the protocol runs automatically when the port is started. The autodetection setting is ignored.

7.4 Multilink PPP

When an incoming PPP connection requires additional bandwidth, the SCS can add ports to the connection and combine the two or more physical streams of PPP data into one logical stream. This is called multilink PPP.

Two Servers are needed for multilink PPP connections, one to initiate the call and one to receive it. All multilink packets for a given connection must originate from the SCS that brought up the link and be received by another single SCS. The following sections explain how to configure a calling SCS and a receiving SCS for a one-way multilink connection.

Note: *Multilink PPP is described in RFC 1990.*

When a port that is enabled for multilink PPP receives a multilink call and more bandwidth is needed for the connection, the SCS will add other ports, if available, to reach the necessary bandwidth. For more information, see *Bandwidth On Demand* on page 5-4.

7.4.1 Configuring the Calling SCS

1 Enable Multilink PPP on all ports that may be used for a multilink connection.

Figure 7-4: Enabling Multilink PPP

```
Local>> DEFINE PORT 1-4 PPP MULTILINK ENABLED
```

Note: *Ensure that other port parameters (such as speed, parity, and flow control) are properly configured for the connection.*

2 Create a site for the outgoing multilink PPP connection.

Figure 7-5: Creating the Calling Site

```
Local>> DEFINE SITE irvine
```

Note: *All other desired site parameters should be set up, and a static route should be defined for the site, before the site is used for connections.*

3 Configure the ports associated with the multilink site.

A Associate the site with two or more ports, giving each port a priority. Higher priority ports will be used first.

Figure 7-6: Configuring Port Priority

```
Local>> DEFINE SITE irvine PORT 1 PRIORITY 1
Local>> DEFINE SITE irvine PORT 2 PRIORITY 2
Local>> DEFINE SITE irvine PORT 3 PRIORITY 3
Local>> DEFINE SITE irvine PORT 4 PRIORITY 4
```

B Estimate the bandwidth of each port associated with the site.

The estimate should be based on the fastest data transfer that the attached modem can support, adjusted for expected compression.

The following example assumes a 28.8 kbps modem attached to port 2 with about a 2:1 compression rate (28800 x 2 = 57600 bps = 5760 bytes per second, rounded to 5800 bytes per second).

Figure 7-7: Estimating Port Bandwidth

```
Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 5800
```

See *Estimate Each Port's Bandwidth* on page 5-6 for in-depth instructions on calculating bandwidth amounts.

C Specify a telephone number for each port.

When the site is brought up, the SCS will attempt a connection by dialing the telephone number associated with the highest priority port (in this case, 555-1001).

Figure 7-8: Configuring Port Telephone Numbers

```
Local>> DEFINE SITE irvine PORT 1 TELEPHONE 555-1001
Local>> DEFINE SITE irvine PORT 2 TELEPHONE 555-1002
Local>> DEFINE SITE irvine PORT 3 TELEPHONE 555-1003
Local>> DEFINE SITE irvine PORT 4 TELEPHONE 555-1004
```

4 Configure the site bandwidth parameters.

Note: *The SCS will only modify bandwidth if it initiated the connection.*

A Specify the initial and maximum bandwidths.

The maximum bandwidth should not exceed the sum of the bandwidths for all of the ports.

Figure 7-9: Configuring Initial and Maximum Bandwidths

```
Local>> DEFINE SITE irvine BANDWIDTH INITIAL 2800
Local>> DEFINE SITE irvine BANDWIDTH MAXIMUM 11500
```

For more information about site bandwidth settings and how to fine-tune them, see *Configuring Bandwidth Allocated to Sites* on page 5-6.

B Specify when to add and remove bandwidth from a connection.

In the following example, the bandwidth should remain between 40% and 90% of the maximum value, 11500 bytes per second. The bandwidth will be measured every 60 seconds and compared to the add and remove values to see if an adjustment is necessary.

Figure 7-10: Configuring Site Bandwidth Settings

```
Local>> DEFINE SITE irvine BANDWIDTH ADD 90
Local>> DEFINE SITE irvine BANDWIDTH REMOVE 40
Local>> DEFINE SITE irvine BANDWIDTH PERIOD 60
```

5 Configure site authentication.

All of the ports raised for a multilink connection should be added to the connection and authenticated together. A username and remote authentication password will be needed, and CHAP and/or PAP authentication should be enabled.

Figure 7-11: Configuring Site Authentication

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME "sidney"
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE "k0ala"
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE irvine AUTHENTICATION PAP ENABLED
```

7.4.2 Configuring the Receiving SCS

1 Configure the ports that will be used for the multilink connection.

A Enable Multilink PPP on all ports that will be used.

Figure 7-12: Enabling Multilink PPP

```
Local>> DEFINE PORT 1-4 PPP MULTILINK ENABLED
```

B Ensure that the telephone numbers of the modems attached to the receiving ports match those configured in the calling site.

C Enable PPP CHAP and/or PAP authentication on the ports.

Figure 7-13: Enabling PPP Authentication

```
Local>> DEFINE PORT 1-4 PPP CHAP REMOTE
Local>> DEFINE PORT 1-4 PPP PAP REMOTE
```

2 Create a site to receive the multilink traffic.

The site's name must match that of the incoming multilink user (see Figure 7-11).

Figure 7-14: Creating the Receiving Site

```
Local>> DEFINE SITE "sidney"
```

3 Configure site authentication.

A local authentication password will be needed (it should match the incoming site's remote password, see Figure 7-11), and CHAP and/or PAP authentication should be enabled.

Figure 7-15: Configuring Site Authentication

```
Local>> DEFINE SITE sidney AUTHENTICATION LOCAL "k0ala"
```

Note: *Use the same authentication protocol on the receiving SCS as on the calling SCS.*

7.5 Restoring Default PPP Settings

To restore a port to its default PPP settings, enter the **Purge Port PPP** command.

Figure 7-16: Restoring Default PPP Settings

```
Local>> PURGE PORT 2 PPP
```

7.6 Pocket PC PPP Support

To enable or disable client/server negotiation when starting a PPP connection with a PocketPC type device, use the **Set/Define Ports PocketPC** command.

7.7 Character Mode Sites

The SCS allows you to create a character mode site. A character mode site is treated as a normal site that does not run a serial protocol. The site still allows modems to be dialed, and can have a chat script and other functions, but once the site is up, it does not run PPP. The character mode site is normally used to associate an IP address with a particular serial port or to control an external device using a chat script.

To create a character mode site, use the **Set/Define Site <sitename> Protocol None** and **Set/Define Site <sitename> IP Remoteaddr <ip_address>** commands and then create a host route that points to it with the Set/Define IP Route **<ip_address> Site <sitename>** command. The <ip_address> must be on the same IP subnet as the SCS itself. To make a text mode connection to the serial port, Telnet to <ip_address.

Character mode sites still obey time-of-day restrictions and idle time-outs. All Site Authentication options for the site are ignored, as are settings for MTO, bandwidth, and packet filters. Sites without protocols cannot be started by users logging in serially. Such sites can only be started by network traffic or with the **Test Site** command.

7.8 Troubleshooting

The SCS **event logging** feature enables you to monitor network and user activity and troubleshoot problems. Configure a destination for logging information using the **Set/Define Logging** command, described on page 12-172.

To view PPP LCP and NCP negotiations with the remote host, use logging level 4 or 6. Level 4 logs PPP negotiation activity, and is adequate for most PPP troubleshooting. Level 6 logs all PPP events; this is generally only required to troubleshoot faulty PPP implementations.

Figure 7-17: Enabling PPP Event Logging

```
Local>> DEFINE LOGGING PPP 4
```

Once a connection is made, problems may be monitored using the **Show/Monitor/List Ports** command. The following table explains the counters useful for PPP troubleshooting.

Table 7-1: Port Counters

Counter(s)	Information Displayed
Packets Input	Packets from the remote host to the SCS.
Packets Output	Packets from the SCS to the remote host.
Packet-Too-Long	Number of packets longer than the Maximum Receive Unit (MRU) negotiated with LCP. In most situations, this counter will be 0. To correct this error, the remote node should configure a smaller Maximum Transmission Unit (MTU).
Bad FCS (Frame Checksum)	Number of corrupted packets. This problem may be due to line noise, flow control problems, and so on. This number should be less than 1% of the Packets Input counter; if it is not, performance is suffering greatly.

8: Ports

Each SCS port can be configured in a number of ways. Configuration options include a port's start method, available sessions, access, serial parameters, and flow control.

8.1 Using Port Commands

Most port commands require you to be the privileged user. To become the privileged user, use the **Set Privileged/Noprivileged** command. This command is discussed in detail on page 12-92.

Many port commands require that the Define commands be used instead of the Set commands. Set commands take effect immediately for the current session. Define commands do not take effect until the port is logged out (with the Logout Port command) or the Server is rebooted.

> **Note:** *For a more detailed explanation of the difference between Set and Define commands, see Command Types on page 2-3.*

A number of Define Port commands are designed to control modems (for example, Define Port Modem Answer). These commands are covered in Chapter 9, *Modems*, and in *Modem Commands* on page 12-3.

8.2 Setting Port Access

A port's access may be set to one of the following: dynamic, local, remote, or none. **Dynamic** (the default) permits both local and remote logins, **local** allows only local logins, and **remote** permits only remote logins. **None** prevents all incoming and outgoing connections, rendering the port unusable.

If a user wants to Telnet to an SCS port and dial out using an attached modem, the port must have dynamic or remote access. If the user wants to log into a port locally and Telnet to a remote host, the port must have local or dynamic access.

To configure access to a port, use the **Set/Define Ports Access** command.

Figure 8-1: Configuring Connection Type

```
Local>> DEFINE PORT 2 ACCESS LOCAL
```

8.3 Starting a Port

When the SCS is booted, the ports can start up in one of two ways: they can automatically start, or wait for character input. Each port can be individually configured; for example, one port may wait for character input before starting while another may automatically start when the SCS is booted.

A port's start-up procedure may involve a combination of factors. For example, if modem control is enabled, the port will wait until the modem asserts the DSR signal, then it could either automatically start, or wait for character input before starting (depending on the port configuration).

8.3.1 Waiting for Character Input

By default, each SCS port is idle until character input is received (e.g. if a remote user presses the Return key). If automatic protocol detection is enabled (see *Automatic Protocol Detection* on page 8-4), and the SCS recognizes a PPP or SLIP character in a packet for an enabled protocol, the SCS automatically runs that protocol.

8.3.2 Starting Automatically

To configure a port to start automatically when the SCS is booted, or as soon as the SCS receives a predetermined trigger character, use the **Set/Define Ports Autostart** command.

8.3.2.1 Enabling Autostart

When Autostart is enabled, the port starts up and executes any configured commands or connections. No user input or serial data is necessary for the port to start up; it occurs automatically.

To enable Autostart for a port, use the following command.

Figure 8-2: Enabling Autostart

```
Local>> DEFINE PORT 2 AUTOSTART ENABLED
```

Once Autostart is enabled, the port start ups without waiting for character input. The port then performs any operations that it's configured to run at start-up. For example, the port may connect to a particular host, run an authentication sequence, or run a particular protocol.

Note: *To dedicate a port to a host, see Preferred/Dedicated Hosts on page 8-9.*

If PPP is enabled on the port, the port starts when a PPP packet is received. See *PPP Mode* on page 8-3 for details. If both Autostart and modem control are enabled, the port starts as soon as the DCD signal is raised.

8.3.2.2 Setting an Autostart Trigger

Autostart can also be triggered by a specific input character. As the SCS does not have a default Autostart character, you will have to configure one. For example, you may want to use **A** so that Autostart will occur as soon as an **AT** modem command is entered. Keep in mind that when you configure an Autostart character, you can no longer use press Return to get to the **Local>** prompt.

The following example configures "A" as the Autostart character for the first serial port.

Figure 8-3: Configuring an Autostart Character

```
Local>> DEFINE PORT 1 AUTOSTART CHARACTER "A"
```

A two-character sequence can also be defined as an autostart trigger.

To specify a control character, using escaped hex. For example, Ctrl-B (ASCII character 0x02) is "\02" in escaped hex.

8.4 Port Modes

An SCS port can be used in one of three modes: character mode, PPP mode, or SLIP mode. The default port mode is character mode.To configure a port to run PPP or SLIP, see the corresponding sections below.

Note: *Enabling PPP or SLIP on the serial console port is not recommended.*

8.4.1 Character Mode

By default, the SCS ports will start character mode when the Return or Line Feed key is pressed at startup. Users logging into the SCS will see a Username> prompt followed by a Local> prompt. SCS commands can be entered at this prompt to configure the unit, control logins, Telnet or Rlogin to remote hosts, start PPP or SLIP, or display information.

Note: *If the Altprompt characteristic is enabled, users will see a Login: prompt instead of the Username> prompt. See Set/Define Server Altprompt on page 12-115 for more details.*

8.4.2 PPP Mode

A port in PPP mode runs the Point-to-Point Protocol. A port can be configured to run PPP in a number of ways; for example, users can be authenticated, headers can be compressed, and negotiation can take place. Because PPP isn't designed for user interaction, the Local> prompt will not be displayed.

Both PPP and PPPDetect are enabled for all serial ports by default. PPP will automatically run once a port's has started up and a PPP packet is received. Because running PPP in this manner bypasses a port's usual authentication (using a login password or username/password combination), you should configure CHAP or PAP authentication.

To enable a port to run PPP, use the **Define Ports PPP** command.

Figure 8-4: Enabling PPP

```
Local>> DEFINE PORT 2 PPP ENABLED
```

Note: *For more information on PPP, refer to Chapter 7, PPP.*

8.4.3 SLIP Mode

When SLIP (Serial Line Internet Protocol) and SLIPdetect (see *Automatic Protocol Detection* on page 8-4) are enabled on a port, SLIP will run once that port's start-up procedure is complete and a SLIP packet is received.

Running SLIP in this manner bypasses a port's usual authentication process (login password, etc.). As SLIP doesn't support authentication, no authentication will occur in this situation. To use authentication with SLIP, see Chapter 11, *Security*.

To enable a port to run SLIP, use the following commands.

Figure 8-5: Enabling SLIP

```
Local>> DEFINE PORT 2 SLIP ENABLED
```

8.5 Automatic Protocol Detection

An SCS port may be configured to automatically detect a PPP or SLIP packet and, if PPP or SLIP is enabled on the port, run the appropriate protocol when the first packet is received. This eliminates the need for callers to explicitly start PPP or SLIP.

In some situations, autodetection should be disabled. For example, SLIP doesn't support authentication. To authenticate users, autodetection of SLIP could be disabled; incoming callers would be presented with the Local> prompt and could be forced to enter the login password. Once authenticated, they could manually start SLIP by entering the **Set SLIP** command.

Figure 8-6: Enabling and Disabling Automatic Protocol Detection

```
Local>> DEFINE PORT 2 PPPDETECT DISABLED
Local>> DEFINE PORT 3 SLIPDETECT ENABLED
```

Because PPP protocol detection is enabled by default, you should also configure PPP authentication (CHAP or PAP) wherever possible. CHAP and PAP are enabled by default for all serial ports. If PPP authentication is not possible, enable user authentication and the **Set PPP** command to authenticate incoming calls.

If a port is dedicated to PPP or SLIP (see *Dedicated Protocols* on page 8-8), the protocol will run automatically when the port is started. Any authentication settings will be ignored.

8.6 Port-Specific Session Configuration

When you log into an SCS port to connect to a network service, your connection is referred to as a session. A network service may be an interactive login to a TCP/IP host, a connection to a modem or another SCS, another server, etc. Sessions describe interactive connections; PPP or SLIP connections are not referred to as sessions.

Session configuration may apply only to the current session, or to all sessions run on a particular port. Session-specific configuration meets needs that apply only to an active session; for example, if binary files are being transferred, you could disable interpretation of the switch characters and XON/XOFF flow control characters.

Note: *Only one session at a time will be displayed.*

Port-specific session configuration includes the number of sessions permitted on a port, the keys used to switch between sessions, and the key used to exit from a session to character mode. The commands used to configure these options are discussed in the following sections.

8.6.1 Multiple Sessions

Each port may have a number of sessions running at once. By default, each port is configured to permit up to 4 simultaneous sessions. The maximum number of simultaneous sessions, called the **session limit**, may be changed; up to 8 sessions may be run on each port.

To change the session limit, use the **Set/Define Ports Session Limit** command.

Figure 8-7: Changing the Session Limit

```
Local>> DEFINE PORT 2 SESSION LIMIT 6
```

8.6.2 Switching Between Sessions

Sessions are organized in the order that they were created. Commands or keyboard equivalents are used to switch back and forth between active sessions. Switching to a session with an earlier creation date is called switching backward; conversely, switching to a later session is called switching forward. Sessions are arranged in a circular list; switching forward from the last session created will switch to the first session in the list, and vice-versa.

The command used to switch to the previous session is **Backwards**. Its keyboard equivalent is called the backward switch. To define a backward switch, use the following command:

Figure 8-8: Defining Backward Switch

```
Local>> DEFINE PORT 2 BACKWARD SWITCH \02
```

To specify a control character to use as a switch, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

The Forwards command is used to switch to the next session. Its keyboard equivalent, the forward switch, as specified as follows:

Figure 8-9: Specifying Forward Switch

```
Local>> DEFINE PORT 2 FORWARD SWITCH \03
```

The characters you define for the backward switch and forward switch should not conflict with each other or with characters used for editing commands (see *Command Line* on page 2-2). In addition, the characters should not conflict with characters used on the host.

8.6.3 Exiting Sessions

The Break key is used to suspend a session. When a session is suspended or exited, the Local> prompt will be displayed. SCS commands can be entered at this prompt to configure the unit, start a new session, or display information.

8.6.3.1 Breaking from a Session

When the Break key is pressed, the port will do one of three things: suspend the session and display the Local> prompt, pass the character to the remote service, or ignore it all together (pressing the key will have no result).

To configure the processing of the Break key, use the **Set/Define Ports Break** command. Break can be set to one of the following: Local, Remote, or None.

Figure 8-10: Configuring Break Key Processing

```
Local>> DEFINE PORT 3 BREAK LOCAL
```

If your keyboard doesn't have a Break key, an equivalent can be specified with the **Set/Define Ports Local Switch** command, or with the **Set/Define Ports Break Character** command.

Figure 8-11: Specifying a Local Switch

```
Local>> DEFINE PORT 2 LOCAL SWITCH '
```

Figure 8-12: Specifying an Alternate Break Character

```
Local>> DEFINE PORT 2 BREAK CHARACTER '
```

There are several examples of how the Port Break command and the alternate Break character work together. The effect of the Break character depends on the type of connection and how Break processing is configured. The examples assume that an alternate Break character has been defined for the user's port.

- An SCS serial port user Telnets to a network host and types the alternate Break character.

  Local Break: The user is returned to the SCS Local> prompt.

  Remote Break: A Telnet Break IAC sequence will be sent to the host.

- An SCS serial port user makes an SSH connection to a network host and types the alternate Break character.

  Local Break: The user is returned to the SCS Local> prompt.

  Remote Break: Nothing happens, because there is no way to generate a Break across an SSH connection.

- An SCS user on serial port 2 issues a command to port 3 and types the alternate Break character.

  Local Break: The user is returned to the SCS Local> prompt.

  Remote Break: A Break condition will be generated on port 3.

- A user Telnets into the SCS, has a default alternate Break character from template port 0, and types the alternate Break character at the Local> prompt.

  Local or Remote Break: Nothing happens, because the user is already at the Local> prompt.

- A user forms a TCP connection from a network host to port 7 on the SCS (for which an alternate Break character has been defined) using socket 2007, then types the alternate Break character.

  Note: *The 20xx range of sockets performs Telnet IAC interpretation.*

  Local Break: If the alternate Break character is detected in the datastream, nothing happens. If a Break condition is detected on the serial port, nothing happens.

  Remote Break: If the alternate Break character is detected in the datastream, a serial Break condition is generated on the port. If a Break condition is detected on the serial port, a Telnet Break IAC condition will be sent on the network connection.

- A user forms a TCP connection from a network host to port 7 on the SCS (for which an alternate Break character has been defined) using socket 3007, then types the alternate Break character.

Note: The 30xx range of sockets is 8-bit clean. If a Break condition is detected on the serial port, nothing happens, because there is no way to propagate a Break condition across an 8-bit clean connection.

Local Break: If the alternate Break character is detected in the datastream, nothing happens.

Remote Break: If the alternate Break character is detected in the datastream, a serial Break condition will be generated on the port.

8.6.3.2 Disconnecting Sessions

To disconnect the current session, use the **Disconnect** command. To disconnect a particular session, specify the session number; to disconnect all sessions, use the All parameter.

Figure 8-13: Disconnecting Sessions

```
Local>> DISCONNECT
Local>> DISCONNECT SESSION 2
Local>> DISCONNECT ALL
```

8.6.4 Monitoring Session Activity

When the Verification characteristic is enabled on a particular port, messages will be issued whenever a session on that port is connected, disconnected, or switched. Use the following command to enable verification:

Figure 8-14: Enabling Verification

```
Local>> DEFINE PORT 3 VERIFICATION ENABLED
```

8.6.5 Setting Session Characteristics

You can configure a session either at the moment you make the connection, or from within a connection once it is already running.

8.6.5.1 Configuring a Session at Connection Time

To configure a session when a connection is made, an environment string may be specified. This string may be used in conjunction with the **Connect** command, or saved as part of a preferred or dedicated hostname. The environment string consists of a series of key letters, some prefaced by a plus (+) or minus (-) All environment strings are discussed in Appendix A, *Environment Strings.*

To use an environment string with the **Connect** command, specify the host, TCP port, or service to connect to, then specify the environment string prefaced by a colon. For example, to Telnet to host athena in Backspace and Passall mode, use the following command:

Figure 8-15: Using Environment Strings with Connect

```
Local>> CONNECT TELNET athena +D+P
```

To set an environment string to use with a preferred or dedicated host/service, use the following syntax:

Figure 8-16: Using Environment Strings with Preferred/Dedicated Hosts

```
Local>> DEFINE PORT 2 DEDICATED RLOGIN athena:480+E
```

Note: *For more information on preferred and dedicated hosts/services, see Dedicated Protocols on page 8-8.*

8.6.5.2 Configuring a Session Once It's Running

The **Set Session** command enables users to configure a currently-running session. Areas that may be configured include:

- The character sent as the delete character
- Local echoing
- SCS interpretation of messages and server-specific keys
- The character sent to the remote device when the Return key is pressed
- SCS interpretation of switch characters, messages, and flow control

For more information, see **Set Session** on page 12-94.

8.7 Preferred/Dedicated Protocols & Hosts

8.7.1 Dedicated Protocols

A **dedicated protocol** is a protocol (PPP or SLIP) that will automatically run when a port is started. No other protocol can be run on the port; it will continue to run PPP or SLIP until it is logged out.

To dedicate a port to PPP or SLIP, use the following command:

Figure 8-17: Dedicating a Port to PPP/SLIP

```
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 3 SLIP DEDICATED
```

When a port is dedicated, the local prompt cannot be accessed, therefore, commands can't be entered to disable the Dedicated characteristic. Take caution when dedicating ports; if you're going to dedicate all SCS ports, be sure that you have another way to log into the server (such as a Telnet login).

Note: *If you cannot log into the SCS, you'll need to restore the server to its factory default settings. See Initialize Server on page 12-111.*

8.7.2 Preferred/Dedicated Hosts

A port can be assigned a preferred or dedicated SSH, Telnet, or Rlogin host using the **Set/Define Ports Preferred** and **Define Ports Dedicated** commands. By entering a sequence of key letters (environment strings) after the TCP parameter, you can specify the type of connection (e.g. SSH, Telnet, etc.). If the TCP parameter is entered without an environment string, the connection will default to Telnet.

Figure 8-18: Specifying a Preferred/Dedicated Host

```
Local>> DEFINE PORT 2 PREFERRED TCP 192.75.1.0:T
Local>> DEFINE PORT 3 DEDICATED RLOGIN 192.0.1.221:R
Local>> DEFINE PORT 4 DEDICATED SSH 192.0.4.52:S
```

For SSH connections, the port name will be used as the username for the remote host.

See *Environment Strings* on page A-1 for more information on available strings.

8.7.3 Saving Autostart Characters

When a port is in dedicated mode and is configured to use an Autostart character (see *Starting Automatically* on page 8-2 for more information on Autostart), you can forward the autostart characters to the host as the first bytes of data. Enable this option with the **Set/Define Ports Autostart Save** command

Figure 8-19: Sending Autostart Characters to a Dedicated Host

```
Local>> DEFINE PORT 4 AUTOSTART SAVE 1
```

If you have a two-character autostart trigger, you can instruct the SCS to pass along both, one, or none of the characters as part of this command.

The full syntax of **Set/Define Ports Autostart** is discussed on page 12-60.

8.8 Port Restrictions

Ports may be restricted in a number of ways. These methods include locking a port, username/password protection, restriction of connection type, automatic logouts, control of session interruption, restriction of commands, and receipt of broadcast messages.

8.8.1 Locking a Port

The **Lock** command may be used to secure a port without disconnecting sessions. When you enter Lock, you will be prompted to enter a password. The port will then be locked until that same password is used to unlock it. Figure 8-20 displays an example.

Figure 8-20: Locking and Unlocking a Port

```
Local> LOCK
Password> donut (not echoed)
Verification> donut (not echoed)
Unlock password> donut (not echoed)
Local>
```

Note: *Secure ports (set using the Set/Define Ports Security command) cannot be locked.*

To unlock a port without the Lock password, a privileged user must use the **Unlock Port** command or log out the port using the **Logout Port** command. Logout will disconnect all sessions.

Note: *Unlock Port is discussed on page 12-100. Logout Port is discussed on page 12-53.*

The **Set/Define Server Lock** command, which is discussed on page 12-120, controls whether or not local users are permitted to lock ports.

8.8.2 Enabling Signal Check

The Signal Check characteristic can be used to prevent remote connections to a port unless DSR is asserted. This is often used to prevent Telnet logins to a port until the device attached to the port (for example, a terminal) asserts the DSR signal, indicating that it is connected and powered on.

To enable Signal Check, use the following command:

Figure 8-21: Enabling Signal Check

```
Local>> DEFINE PORT 3 SIGNAL CHECK ENABLED
```

8.8.3 Username/Password Protection

You can configure a port to require either a login password or a username/password pair before a login is permitted.

Note: *For detailed information on authentication, refer to Chapter 11, Security.*

8.8.3.1 Login Password

The login password can be required of users who want to log in to the Server from the serial ports or the network. The password is defined with the **Set/Define Server Login Password** command.

Figure 8-22: Setting the Login Password

```
Local>> SET SERVER LOGIN PASSWORD
Password> platyp (not echoed)
Verification> platyp (not echoed)
Local>>
```

The **Set/Define Ports Password** command controls whether or not the login password is required to log into the specified port. To require the password, use the following command:

Figure 8-23: Requiring the Login Password

```
Local>> DEFINE PORT 2 PASSWORD ENABLED
```

By default, incoming connections are not required to enter a login password. To require the login password for those connections, use the **Set/Define Server Incoming** command (discussed on page 12-119).

8.8.3.2 Username/Password Authentication

The **Set/Define Ports Authenticate** command is used to authenticate individual users. When this command is enabled, incoming logins will be prompted for a username/password pair. The username and password entered will be compared to authentication databases configured with the **Set/Define Authentication** command. If a match is found, the login will be permitted; otherwise, the login attempt will fail.

Figure 8-24: Set/Define Port Authentication Commands

```
Local>> DEFINE PORT 3 AUTHENTICATE ENABLED
```

Note: *Set/Define Authentication is described in Chapter 11, Security.*

8.8.4 Automatic Logouts

When a device connected to the SCS is disconnected or powered off, the DSR signal is dropped. The SCS can be configured to automatically log out a port when this occurs to prevent users from accessing other sessions by physically swapping terminal cables and using someone else's privileges. Ports can also be configured to automatically log out when they've been inactive for a specified period of time.

8.8.4.1 DSR Logouts

To configure a port to log out when the DSR signal is dropped, use the **Set/Define Ports DSRLogout** command.

Figure 8-25: Enabling DSRLogout

```
Local>> DEFINE PORT ALL DSRLOGOUT ENABLED
```

DSRLogout is implied when modem control is enabled.

8.8.4.2 Inactivity Logouts

To configure a port to log out after a specified period of inactivity, use the **Set/Define Ports Inactivity Logout** command. This command works in conjunction with the **Set/Define Server Inactivity** command. The latter defines a particular number of minutes; after this period of time, a port with Inactivity Logout enabled will be considered inactive and automatically logged out.

Note: *Set/Define Server Inactivity is described on page 12-118.*

To enable Inactivity Logout, use the following command:

Figure 8-26: Enabling Inactivity Logout

```
Local>> DEFINE PORT 3 INACTIVITY LOGOUT ENABLED
```

The SCS will only perform an inactivity logout when the port is in character mode (not running PPP or SLIP). To configure idle time logouts for PPP and SLIP connections, you must configure an idle time for the site; after the site is idle for the specified time, the link will be shut down. Use the **Define Site Idle** command and specify the length of the idle time limit in seconds.

Figure 8-27: Enabling Idle time Logouts for PPP/SLIP

```
Local>> DEFINE SITE irvine IDLE 60
```

8.8.5 Restricting Commands

The Security characteristic may be used to limit a user's access to information about other ports. When Security is enabled, only a limited number of commands may be typed at the Local> prompt. A user on a secure port are unable to get information about other ports using the Show/List commands and can not perform commands which require privileged access.

To enable Security on a particular port, use the **Set/Define Ports Security** command.

Figure 8-28: Enabling Security

```
Local>> DEFINE PORT 3 SECURITY ENABLED
```

8.8.6 Receipt of Broadcast Messages

The **Set/Define Ports Broadcast** command enables or disables a port's receipt of broadcast messages from other users, including the superuser. Broadcast messages are enabled by default.

Figure 8-29: Disabling Broadcast Messages

```
Local>> DEFINE PORT 3 BROADCAST DISABLED
```

Broadcast messages are also discussed in *Sending a Broadcast Message* on page 2-5.

8.8.7 Dialback

The Dialback feature allows a system manager to set up a dialback list of authorized users for incoming modem connections. When a username matching one in the list is entered, the port is logged out and the phone number will be sent out the serial port using the port's modem profile.

For a complete description of dialback, see *Security* on page 11-1.

8.8.8 Enabling Menu Mode

If you want to limit user access to the Local> prompt, you can set up a menu with restricted options. The **Set/Define Ports Menu** enables menu mode for the specified ports.

Figure 8-30: Enabling Menu Mode

```
Local>> DEFINE PORT 3 MENU ENABLED
```

When Menu mode is enabled, the Local> prompt cannot be accessed. Be sure that you have another way to log into the SCS before enabling Menu mode on all ports.

Note: *For a complete discussion of menu mode, see Configuring Menu Mode on page 3-4.*

8.9 Serial Port Configuration

There are a number of configurations that apply specifically to serial transmission. These configurations are a port's parity, baud rate, and bits per character. The bits per character is set using the **Set/Define Ports Character Size** command, described on page 12-64. **Set/Define Ports Parity** (discussed on page 12-77) sets a port's parity, and **Set/Define Ports Speed** (discussed on page 12-88) sets the baud rate.

Note: *Use of these commands is relatively straightforward. Please refer to the designated page references for the appropriate syntax.*

The Autobaud characteristic enables a port to detect an incoming baud rate, character size, and parity and configure its characteristics to match. This characteristic cannot be enabled if the port's Access is set to Remote or Dynamic (see *Setting Port Access* on page 8-1) or if the specified port offers a service. To enable Autobaud, use the **Set/Define Ports Autobaud** command, discussed on page 12-58.

The following sections discuss other configuration settings.

8.9.1 Naming a Port

To assign a particular name to a port, use the **Set/Define Ports Name** command.

Figure 8-31: Assigning a Port Name

```
Local>> DEFINE PORT 3 PORT NAME "highspeed_modem"
```

The default name for each port is Port_*n*, where *n* denotes the port number (for example, Port_2).

8.9.2 Specifying a Username

A username can be specified for a port using the **Set/Define Ports Username** command. When the username is specified with the Define Port Username command, users will not be prompted for a username upon login.

Figure 8-32: Specifying a Username

```
Local>> DEFINE PORT 3 USERNAME fred
```

8.9.3 Notification of Character Loss

When the **Loss Notification** characteristic is enabled, a bell character (Ctrl-G) will be sent when data error or overrun causes the loss of a character.

Figure 8-33: Enabling Loss Notification

```
Local>> DEFINE PORT 2 LOSS NOTIFICATION ENABLED
```

8.9.4 Padding Return Characters

By default, the SCS will pad Carriage Returns entered in Telnet sessions with null characters. To disable this characteristic, use the **Set/Define Ports Telnet Pad** command.

Figure 8-34: Disabling Telnet Pad

```
Local>> DEFINE PORT 3 TELNET PAD DISABLED
```

8.9.5 Setting the Device Type

The **Type** characteristic is used to specify the device types compatible with the port. Type must be one of the following device types: ANSI, Hardcopy, or Softcopy. To set a Type, use the following command:

Figure 8-35: Configuring the Device Type

```
Local>> DEFINE PORT 3 TYPE ANSI
```

Note: *For more information about Type options, refer to Set/Define Ports Type on page 12-90*

8.9.6 Specifying a Terminal Type

A terminal type, to be sent to the remote host for Telnet and Rlogin sessions, can be specified for a port using the **Set/Define Ports Termtype** command. The terminal type should be entered as a string, for example, VT100.

Figure 8-36: Specifying a Terminal Type

```
Local>> DEFINE PORT ALL TERMTYPE IBM1000
```

Note: *By default, no specific terminal type is specified.*

Termtype information is used for outbound sessions; the SCS doesn't use this information. For example, a remote host might use the terminal type to configure your terminal to run a particular application.

8.9.7 Transmitting Serial Data

Serial data can be handled a couple of different ways. The default settings will discard all data. Other options include setting various triggers to transmit the accumulated data to a host.

Once a connection has been started, several different triggers can be used to transmit all accumulated serial data to the host. These options are controlled with the **Set/Define Ports Datasend** command. The datasend process used by the SCS balances network traffic with latency concerns.

One kind of trigger can be set by specifying a "timeout" condition of either the time since the last character was received or the time since the current character burst was started. For example, to trigger data transmission 150 milliseconds after the current character burst began, enter the following command:

Figure 8-37: Transmitting Serial Data with Trigger Delay

```
Local>> DEFINE PORT 2 DATASEND TIMEOUT FRAME 150
```

The example in Figure 8-37 can be visualized as:

```
x x x xxx xx (data) x x xx xxxxxxxx xx xxxx xx xxxx
|-------------------------------------------------|
                150 milliseconds                  transmit packet
```

Another option is to set a one- or two-character trigger that will cause the SCS to transmit the data. You can also specify whether the trigger characters will be sent to the host as part of the serial data or whether they should be discarded (the default). For example, the following commands will cause the accumulated serial data to transmit as soon as the "Z" character is detected in the data stream and to send the matched character ("Z") to the host as part of that data.

Figure 8-38: Transmitting Serial Data with a Character Trigger

```
Local>> DEFINE PORT 2 DATASEND CHARACTER Z
Local>> DEFINE PORT 2 DATASEND SAVE 1
```

The example in Figure 8-38 can be visualized as:

```
x x x xxx xx (data) x x xx xxxxxxxx xx xxx Z xx xxxx
|-------------------------------------------------|
                                                  transmit packet
```

The **Set/Define Ports Datasend** command is also discussed on page 12-66.

8.9.8 Restoring Default Port Settings

To restore all ports to their default settings, use the **Purge Port** command. Use caution with this command; any changes that you've made with the Set and Define commands will be erased.

Figure 8-39: Restoring Default Port Settings

```
Local>> PURGE PORT 2
```

If the Purge Port command cannot be used (for example, if authentication has been defined on all ports), the settings can only be restored by using the Boot Configuration Program. See your *User Guide* for details.

8.10 RS-485 Configuration

Note: *This section only applies to the SCS200.*

While the SCS serial ports are is initially configured for RS-232 networking, they can also be configured for RS-485 networking. The RS-485 standard allows a serial connection to be shared like a "party line." As many as 32 devices can share the multidrop network. Typically, one device is the master and the other devices are slaves. There are a few important things to note about RS-485 networking with the SCS.

- The SCS can be used in either two-wire or four-wire mode. Refer to the following sections to determine which mode to use.
- The maximum RS-485 network cabling length (without repeaters) is 4,000 feet. Lantronix recommends the use of shielded twisted-pair cabling.

- A large number and varieties of protocols run over RS-485. However, the SCS does not convert or interpret serial data. It only moves data between serial and Ethernet. Any RS-485 protocol will have to be implemented by host software.

Note: *See your Installation Guide for the RS-485 pinouts.*

To enable RS-485 mode on the SCS, enter the **Define Protocols RS485** command. RS-232 mode is enabled by default.

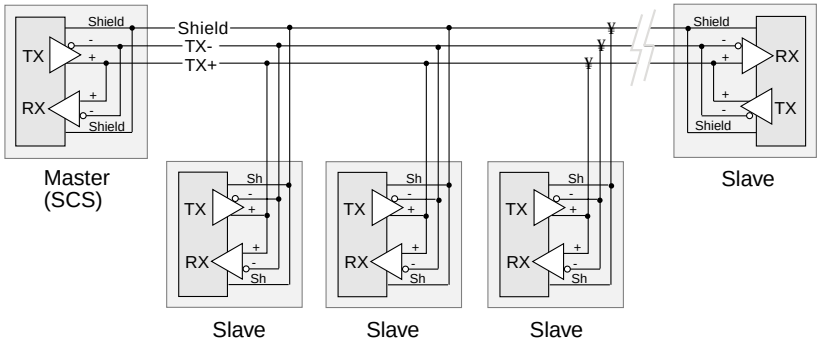
Figure 8-40: Enabling RS-485 Mode

```
Local>> DEFINE PROTOCOLS RS485 ENABLED
```

8.10.1 Two-wire Mode

In two-wire mode, the SCS operates in half duplex: one pair of wires shares transmit and receive signals, and an optional third wire can be used for shield/ground. The main advantage of using two-wire mode is reduced cabling costs.

Figure 8-41: Example Two-wire Mode Network



In a two-wire RS-485 network, the SCS must turn its transmitter on when it is ready to send data and then off for a certain period of time after the data has been sent so that the line is available to receive again. At most baud rate settings, the timing delay is typically one character length with a maximum of 1.5 character lengths.

Figure 8-42: Enabling Two-Wire RS-485 Mode

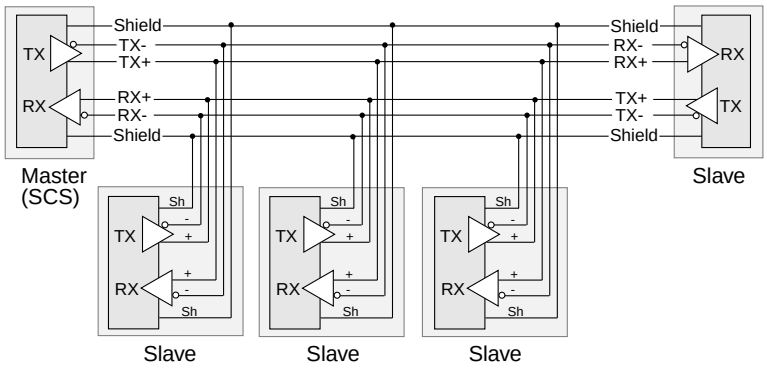
```
Local>> DEFINE PROTOCOLS RS485 MODE 2WIRE
```

Note: *For two-wire mode, the TXDrive setting must be set to Automatic (see TXDrive on page 8-17). If you enable two-wire mode and TXDrive is set for Always, the SCS returns an error.*

8.10.2 Four-wire Mode

In four-wire mode, the SCS operates in full duplex: one pair of wires functions as the transmit pair, another pair of wires functions as the receive pair, and there is a shield/ground wire for each pair. The SCS is able to send and receive data simultaneously. In a four-wire RS-485 network, one device acts as a master while the other devices are slaves. The advantages of four-wire mode are double the throughput of two-wire mode and a guaranteed open path to each slave device's receiver.

Figure 8-43: Example Four-Wire Mode Network



It is important to connect the transmitter of the master device to the wire that is connected to the receive terminals on the slave devices, and connect the receiver of the master device to the wire that is connected to the transmit terminals on the slave devices. In essence, the master device will be connected to the slave devices with a *swapped* cable.

Figure 8-44: Enabling Four-Wire RS-485 Mode

```
Local>> DEFINE PROTOCOLS RS485 MODE 4WIRE
```

8.10.2.1 TXDrive

The SCS can be configured to either always drive the TX (transmit) signal or to let the attached device control the TX signal (tristate) when not actively transmitting. The **Define Protocols RS485 TXDrive** command takes one of two parameters. The **Always** parameter sets the SCS for continuous TXDrive, so TX will never be tristated. The **Auto** parameter sets the SCS for TXDrive when transmitting and tristate while idle.

Figure 8-45: Changing TXDrive

```
Local>> DEFINE PROTOCOLS RS485 TXDRIVE AUTO
```

Note: *You can only set TXDrive for Always when using four-wire mode. The Always parameter returns an error in two-wire mode.*

8.10.3 Termination

RS-485 connections must be terminated properly in order to work. Termination is necessary when using long cable runs, although **only** end nodes should be terminated. The termination option is disabled by default.

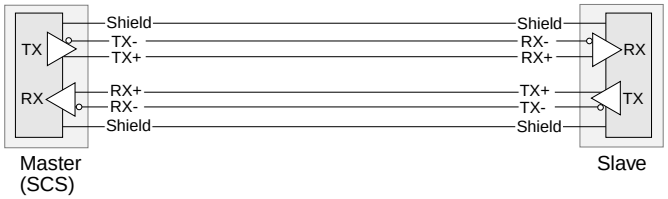
Figure 8-46: Enabling RS-485 Termination

```
Local>> DEFINE PROTOCOLS RS485 TERMINATION ENABLED
```

8.10.4 RS-422 Networking

The SCS is compatible with RS-422 networks in four-wire RS-485 mode. Connect the SCS to a single slave device using a swapped cable, as shown below, and configure the SCS as if you were going to use it for four-wire RS-485 networking.

Figure 8-47: RS-422 Connection



8.11 Flow Control

Flow control enables two connected devices to control the amount of data transmitted between them. When flow control is enabled on an SCS port and a connected device such as a modem, flow control ensures that data sent from the sending device does not overflow the receiving device's buffers. Consider the following example.

An SCS port is connected to a modem. The SCS port transfers data to the modem at 115,200 bits per second, but the modem can only send data over the phone line at 15,000-30,000 bits per second. In a short period of time, the modem's buffer fills with data. The modem sends a signal to the SCS to stop sending data, and the SCS does not send data until it receives a signal from the modem that it can receive data again.

The SCS supports hardware and software flow control. The hardware flow control option is RTS/CTS and the option for software flow control is XON/XOFF. Both flow control methods are described below.

Note: *When the SCS is communicating with a device, the SCS and the device must agree on the type of flow control used.*

8.11.1 Hardware Flow Control

When hardware flow control is used, the flow of data is controlled by two serial port signals (typically RTS and CTS). Two connected devices will assert and deassert RTS and CTS to indicate when they are ready to accept data.

For example, the SCS will assert RTS when it is ready to accept data. When it can no longer accept data (its buffers are full) it will deassert this signal. A connected modem will monitor the assertion and deassertion of this signal; it will only send data when RTS is asserted.

A modem will assert CTS when it is ready to accept data. When its buffers are full, it will deassert CTS to indicate to the SCS that it should stop sending data. The SCS will only send data when CTS is asserted.

RTS/CTS is the most reliable method of flow control and is the recommended method for the SCS. In the event that RTS/CTS flow control cannot be used, XON/XOFF flow control is recommended.

8.11.2 Software Flow Control

XON/XOFF controls the flow of data by sending particular characters through the data stream. The characters sent to signify the ability or inability to accept data are Ctrl-Q (XON) and Ctrl-S (XOFF).

Applications that use the Ctrl-Q and Ctrl-S characters (such as certain text editors) will conflict with XON/XOFF flow control. If a user enters a Ctrl-Q or Ctrl-S, these characters won't be transmitted; they'll be interpreted as flow control characters and removed from the data stream.

Protocols that require an 8-bit clean data path cannot use XON/XOFF flow control. Data passes through an 8-bit clean data path unchanged. SLIP requires an 8-bit clean data path; PPP may have the same requirements if the Asynchronous Character Control Map (ACCM) isn't set properly. To configure the ACCM, see Chapter 7, *PPP*.

8.11.3 Setting Up Flow Control

To use flow control on an SCS port, complete the following steps.

1 Set Appropriate Line/Serial Speeds

Consider the line speed and the serial speed of the modem; if data is being compressed, the serial speed should be higher than the line speed. If you're connecting a terminal to the port, ensure that the speed of the terminal matches the port speed.

Note: *See Chapter 9, Modems, for a discussion of line speeds, serial speeds, and data compression. See your modem's documentation for information on configuring the modem's line and serial speeds.*

2 Disable Autobaud

In order to ensure that the set speeds are always used, disable any automatic speed selection or autobaud options on your modem.

In addition, disable autobaud on the SCS port you're configuring. To do this, use the **Set/Define Ports Autobaud** command. This command requires that you be a privileged user.

Figure 8-48: Disabling Autobaud

```
Local>> DEFINE PORT 2 AUTOBAUD DISABLED
```

Note: *If you aren't currently a privileged user, use the Set Privileged command.*

3 Determine the Appropriate Flow Control Method

Refer to *Flow Control* on page 8-18 for a description of the different methods. Choose the method that's most compatible with the modem and applications you'll be using.

4 Configure Flow Control

To configure your modem, refer to the modem's documentation. To configure flow control on the SCS, use the **Set/Define Ports Flow Control** command. Figure 8-49 displays an example.

Figure 8-49: Configuring RTS/CTS Flow Control

```
Local>> DEFINE PORT 2 FLOW CONTROL CTS
```

Note: *For this command's complete syntax, see Set/Define Ports Flow Control on page 12-72.*

8.12 Serial Signals

Two of the modem signals (DSR and DCD) can be used to control when the SCS ports are active. By monitoring when these signals are asserted or deasserted (dropped), SCS ports can be logged out or kept from starting. The SCS uses DTR to control attached devices.

All of the SCS's DB25 and RJ45 signals are displayed in the following figures.

Figure 8-50: DB25 Serial Signals

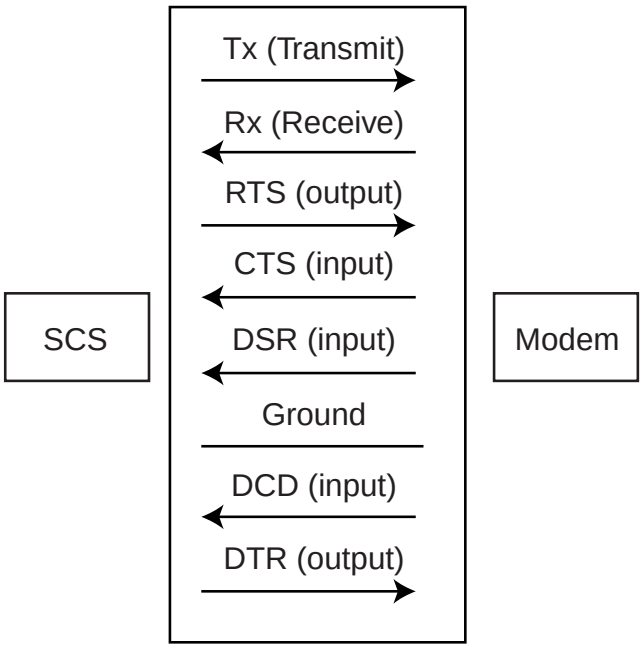
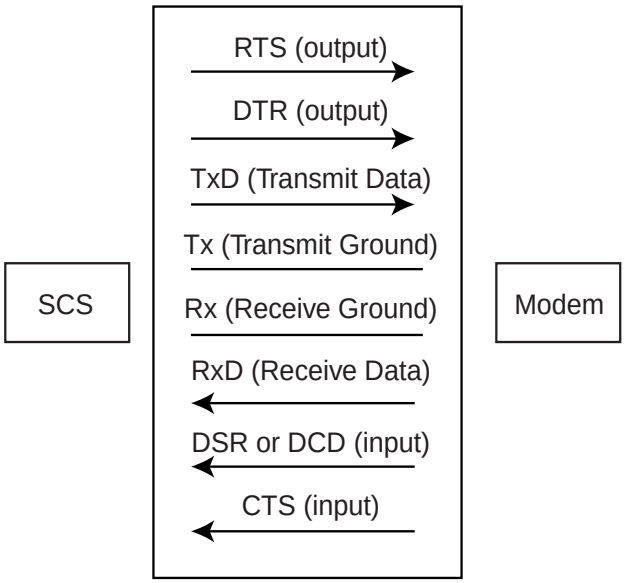


Figure 8-51: RJ45 Serial Signals



8.12.1 DSR (Data Set Ready)

8.12.1.1 DSR for Automatic Logouts

An SCS port can be configured to automatically log itself out when DSR is no longer asserted; in other words, the port will log out when the modem is disconnected. This can help ensure port security; users will be prevented from unplugging terminal lines and using sessions that are still active. See *Automatic Logouts* on page 8-11 for more information.

8.12.1.2 DSR for Controlling Remote Logins

The DSR signal can also be used to determine whether or not a remote login to a port will be permitted. When enabled, the Signal Check characteristic will require the assertion of the DSR signal before a remote login is permitted on a particular port.

Signal check is generally enabled for use with printers; if the printer doesn't assert the DSR signal, it's assumed to be disconnected or powered off. In this case, the remote login isn't permitted, and print jobs are not sent from the SCS to the printer.

To enable Signal Check, use the following command:

Figure 8-52: Enabling Signal Check

```
Local>> DEFINE PORT 3 SIGNAL CHECK ENABLED
```

8.12.2 DCD (Data Carrier Detect)

The DCD signal is asserted by the local modem when it detects a connection from a remote modem. If you're using a DB25 port, no wiring is required in order to use the DCD signal.

RJ45 ports have one pin that can be used for either DSR or DCD. If you are using modems, this pin must be wired to the modem's DCD pin. If you are using another type of device (such as a terminal or printer), this pin should be wired to the device's DSR pin. Refer to the *Pinouts* appendix of your User Guide for instructions.

8.12.3 DTR (Data Terminal Ready)

The SCS asserts DTR when it is ready to accept incoming data or connections. It also uses DTR to cycle the modem when modem control is enabled by temporarily dropping the signal.

SCS ports can be configured to assert DTR only when a user logs into the port by enabling the DTRWait characteristic. See **Set/Define Ports DTRWait** on page 12-71 for details.

8.13 Virtual Ports

Incoming SSH, Telnet, and Rlogin connections are not associated with a physical port. Instead, they are associated with a **virtual port** which serves for the duration of the connection. Virtual port connections can be made only if incoming connections are enabled on the SCS.

Figure 8-53: Enabling Incoming Connections

```
Local>> DEFINE SERVER INCOMING TELNET
```

Note: *An incoming login password can be configured with the Set/Define Server Incoming command, which is discussed on page 12-119.*

Each virtual port is created with a default set of characteristics. The default settings for port 0 connections are remote processing of the Break key, local switch set to ASCII 12 (Ctrl-L), forward switch set to ASCII 6 (Ctrl-F), and backward switch set to ASCII 2 (Ctrl-B). The **Set Port** commands can be used to customize a virtual port during the session, but these customizations cannot be saved.

To make configurations that apply to all virtual ports (all future SSH/Telnet/Rlogin connections), use **Define Port** commands, specifying **port 0** as the port number. When the command in Figure 8-54 is used, all future network logins will be required to enter a username and password.

Figure 8-54: Configuring Virtual Ports

```
Local>> DEFINE PORT 0 AUTHENTICATION ENABLED
```

Note: *Port 0 can only be configured using Define, not Set, commands.*

To display the characteristics used for virtual ports, enter the following command:

Figure 8-55: Displaying Virtual Port Characteristics

```
Local>> LIST PORT 0
```

8.14 Modem Emulation

Modem mode allows the SCS to emulate a modem for performing network connections. To configure specific ports to emulate modems, use the Set/Define Ports Modem Emulation command.]

When the port is in modem mode, the following modem commands are available:

Table 8-1: Modem Mode Commands

Command	Function
ATC	Provides passthru to the normal CLI
ATDT ipaddress	Forms a TCP connection
ATEx	Enables or disables echo command: 0 = echo off 1 = echo on (default)
ATH	Hangs up (disconnects) network session
ATI	Displays software version information
ATQx	Enables or disables result codes: 0 = result codes on (default) 1 = result codes off
ATS[xx=yy]	Sets/shows register 0: 0 means ATA answers; otherwise SCS autoanswers All other registers are unimplemented
ATSxx?	Shows register value
ATVx	Bit 0 sets response type: 0 = numeric responses 1 = text responses (default) Bit 1 sets response to unknown AT commands: 0 = do not accept unknown AT commands 1 = accept unknown AT commands (default)
ATX[y]	Accepted and ignored
ATZ	Restores settings from NVR
AT&F	Restores modem NVR to factory settings
AT&V	Views current and NVR settings
AT&W	Writes settings to NVR
AT&Z	Restores settings from NVR

Note: *When a port is configured in modem emulation mode, a comma in the dial string is interpreted as a colon. The ability to use a comma allows you to specify socket numbers as nnn-nnnn,3001 for modem software that does not work well with colons.*

9: Modems

This chapter discusses how to configure your modem and the SCS to work together.

If you have an SCS200, you can configure a supported modem card to form PPP dialup connections.An installed modem card on the SCS200 can be accessed using port number 3. Because the SCS does not support PC card hot swapping, you must reboot the SCS anytime you remove a modem card.

Note: *For a current list of supported modem cards, see the Lantronix web site, www.lantronix.com.*

This chapter is divided as follows:

- *Setup and Wiring*, page 9-1, describes any necessary physical connections.
- *Modem Speeds*, page 9-2, covers both a modem's serial speed and line speed.
- *Modem Profiles*, page 9-2, shows how the SCS can use a modem profile to interact properly with a modem.
- *Modem and SCS Interaction*, page 9-8, describes the interaction between an SCS and modem during incoming and outgoing calls.
- *Terminal Adapters*, page 9-12, discusses the additional configurations necessary when using an ISDN Terminal adapter instead of a modem.
- *Caller-ID*, page 9-12, shows the commands that will provide the SCS with Caller-ID functionality.
- *Examples*, page 9-13, gives examples of how to configure the modem profiles.
- *Troubleshooting*, page 9-16, suggests solutions for any difficulty you may encounter with your modem configuration.

9.1 Setup and Wiring

Communication devices (modems, printers, servers, etc.) are divided into two types: DTE (Data Terminal Equipment) and DCE (Data Communications Equipment). DTE and DCE are designed to work together, much as a male connector works with a female connector. The SCS is a DTE device. Modems are DCE devices. This means that they use opposite signals; the SCS uses a particular signal to send data, and the modem uses that same signal to receive data.

Some devices that the SCS will connect to (such as printers) are DTE devices. Transmitting data between two DTE devices requires the use of a null modem cable to swap the signals; for complete wiring instructions, refer to the *Pinouts* appendix of your User Guide.

The SCS must be wired to the DCD pin on your modem. See the *Pinouts* appendix of your *User Guide* for complete wiring information.

Note: *For more information, see Serial Signals on page 8-20.*

9.2 Modem Speeds

The modem's serial speed, measured in bits per second (bps), is the rate at which the modem sends data to a host computer or other device (such as the SCS) over its serial port. The modem's line speed, also measured in bits per second, is the rate at which the modem sends data through a telephone line to another modem or communications server. Although the two are related, they are not the same thing.

9.2.1 Serial Speed

The modem and the SCS must agree on the serial speed used for the connection to avoid corrupted data. However, the SCS may speak to a remote modem at a different speed due to error correction and flow control techniques used for the connection. In general, the serial speed should be set higher than the line speed, and higher still if compression is used.

Commonly used serial speeds include 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, and 230,400 bps. The SCS's default serial speed is 9600 bps, but can be changed with the **Set/Define Ports Speed** command. When a modem profile is defined, the SCS will automatically select the highest possible serial speed.

Note: *See your modem's documentation for more information about supported serial speeds and configuration options.*

9.2.2 Line Speed

Common line speeds include 9600, 14400, 28800, and 33600 bps. 9600 and 14400 are sometimes referred to by the names of the modem standards that define them (v.32 and v.32bis, respectively).

Notice that the faster line speeds do not have corresponding serial speeds. If there is not matching serial speed, the next highest serial speed should be used because faster serial speeds make the most efficient use of the given line speed. For example, a v.32bis modem (14400 bps) should use at least a 19200 bps serial speed.

To configure the proper serial and line speeds for a connection, see the *Examples* section on page 9-13.

Note: *Flow control must be used when the line speed and serial speed do not match. For more information on flow control setup, see Flow Control on page 8-18.*

9.3 Modem Profiles

The SCS interacts with a modem by sending commands to and expecting responses from the modem. This communication consists of strings or of simple commands to enable or disable modem features.

In order to communicate properly with a particular modem (this varies from modem to modem), the SCS consults a list of appropriate commands and responses for that modem. This compilation is called a **modem profile**.

9.3.1 Using a Profile

Preconfigured profiles are available for a number of modem types. Each profile contains all settings necessary to appropriately configure that type of modem. To display the list of available profiles, use the **Show Modem** command. If your modem is listed, copy it to the port using the **Define Ports Modem Type** command.

Figure 9-1: Associating Modem Profile With a Port

```
Local>> DEFINE PORT 3 MODEM TYPE 5
```

All configurations in the modem profile will be applied to the specified port. The above command enables modem control for that port, changes the port's flow control to RTS/CTS, disables Autobaud if it's currently enabled, and changes the port's serial rate to the highest rate the modem can support.

If your modem isn't in the list of profiles, use a modem profile for a modem that is similar to your modem type (for example, a modem from the same manufacturer). If there isn't a similar modem listed, use the Generic profile.

Note: *Be sure to verify the provisions mentioned in Modem Security on page 9-11.*

New modem profiles will be added to the lists as they become available from users and our engineering staff. If your modem isn't included in the list of profiles, contact Lantronix to see if it will be added in a later version of the software.

Note: *If you configure a modem profile that is not available on the list, please email it to support@lantronix.com.*

To view the modem profile, or verify that changes have been successfully made to the profile, use the **List Port Modem** command.

Figure 9-2: Verifying Modem Configuration

```
Local>> LIST PORT 3 MODEM
```

9.3.2 Editing a Profile

If a profile isn't available for your modem, editing a profile for a similar modem (e.g. one from the same manufacturer) is recommended. However, if a similar modem profile isn't available, you can edit a preconfigured "generic" modem profile. This is explained in detail in *Profile Settings* on page 9-5.

Note: *Very few modems can use all commands in the generic modem profile. The generic profile is only meant as a starting point.*

Profiles can also be edited to "fine-tune" your modem's performance. For example, dialing performance can be increased by adjusting the DMTF (touch tone) duration and spacing. To edit a modem profile, complete the following steps.

9.3.2.1 Examine the Profile

Display the modem profile by entering the **List Port Modem** command.

Figure 9-3: Displaying Modem Configuration

```
Local>> LIST PORT 3 MODEM
```

A series of settings will be displayed. For example, the Attention string may be currently set to **at**, and Error Correction may be enabled. Read through the configuration options discussed in *Typical Modem Configuration* on page 9-13 and determine which options you'll need to enable or disable to meet your needs. Consult your modem's documentation for the appropriate strings.

9.3.2.2 Edit the Init String

The Init string configures your modem at initialization. This string should do the following:

Table 9-1: Commands in Initialization String

Command Should	Example String
Set the modem to factory defaults.	&f
Set the modem to ignore any character that may force it to return to command mode (for example, +++).	s2=128
Set carrier detect (DCD) to "follow carrier."	&cl
Set the modem to hang up phone and return to command mode when the DTR signal is dropped.	&d2
Set the modem to use hardware flow control	&k3
Set the modem to determine its serial speed from the Attention command (rather than using a constant serial speed).	s20=0
Set the modem to return as many result codes as possible (known as "all progress"). Result codes will be returned in text rather than numbers.	w1
If desired, set the modem to pass Caller-ID information to the SCS.	%ccid=1

Note: *The example strings given in Table 9-1 are not for all modems: consult your documentation for appropriate commands.*

If the Init string in your profile needs to be edited, use the **Define Ports Modem Init** command. The following example uses the example strings from Table 9-1.

Figure 9-4: Sending Initialization String

```
Local>> DEFINE PORT 3 MODEM INIT "&fs2=128&c1&d2&k3s20=0w1"
```

Often, initialization commands are sent individually, prefaced by the modem's Command Prefix string (commonly "at"). In order for the SCS to correctly send the information to your modem, all commands must be sent in one string. Do not include the Command Prefix string in the init string.

Note: *DSR should always be on.*

9.3.2.3 Edit Other Settings

All settings in a modem profile can be edited with the **Define Ports Modem** commands. For example, to configure the Dial string, use the **Define Ports Modem Dial** command.

Figure 9-5: Configuring a String

```
Local>> DEFINE PORT 3 MODEM DIAL "DT"
```

9.3.2.4 Enable Modem Control

Before a port can control a modem, modem control must be enabled. Use the following command.

Figure 9-6: Enabling Modem Control

```
Local>> DEFINE PORT 3 MODEM CONTROL ENABLED
```

9.3.2.5 Initialize the Modem

Log out the port to which the modem is connected. The modem will be initialized, incorporating any changes that you've made to the modem's profile.

Figure 9-7: Initializing the Modem

```
Local>> LOGOUT PORT 2
```

9.3.3 Profile Settings

These settings can be configured with the **Define Port Modem** commands.

Answer Enabled/Disabled

This setting configures whether or not the modem will automatically answer the telephone line.

Answer Command string

This string causes the modem to answer upon ring or to never answer. It is directly preceded by the Commandprefix string and is commonly set to "A."

Attention string The attention string is sent to the modem each time the port is logged out or when the server first boots. The modem must return the OK string. Otherwise, it is assumed that the modem is disconnected or unavailable. The string is commonly set to "at."

Busy string The modem should respond with this string if the remote telephone line is busy. It is commonly set to "BUSY."

Carrier wait string This setting determines the amount of time (in seconds) that the modem will wait for a carrier. If a carrier isn't received within this period of time, the call will fail. By default, Carrierwait is set to 60 seconds.

Commandprefix string

This string is placed before all commands sent to the modem except for the Attention string. In the unlikely event that your modem doesn't use a common command prefix for all commands, this string should be left blank; include the appropriate command prefix in every string sent to the modem. It is commonly set to "at."

Compression Enabled/Disabled

This setting enables or disables the modem's data compression.

Note: *See Compression on page 9-9 for a complete description.*

Compression Command disablestring enablestring

These strings cause the modem to compress data or to let data pass uncompressed. Note that compression often causes higher latency on a line in return for higher throughput.

Connected string The modem must respond with this string after it connects with a remote modem. The modem may respond with other strings as well, but they will be ignored. It is commonly set to "CONNECT."

Dial string This string is sent after the Command Prefix but before the telephone number to be dialed. Commonly, touch tone dialing is activated with "dt" and pulse dialing is activated with "dp."

Error string The modem should respond with this string when it detects an error. It is commonly set to "ERROR."

Errorcorrection Enabled/Disabled

This setting enables or disables the modem's error detection and error correction.

Note: *See Error Correction on page 9-10 for a complete description.*

Errorcorrection Command disablestring enablestring

These strings cause the modem to use error correction or to let data pass uncorrected. Note that correction often causes higher latency on a line in return for data integrity.

Getsetup string This string displays the modem's current configuration. The SCS uses this information to determine if the modem's configuration has changed. It is commonly set to "&v."

When most modems receive the Get Setup string, they'll return one page that lists their configuration. The SCS will not function properly if more than one page of configuration information is sent (prompting the user to press a key to continue to the next page); if your modem is configured in this manner, the Get Setup string will need to be set to "". When Get Setup is set to "", the modem will not be queried for its configuration; instead, the SCS will write the modem's NVR each time the SCS is booted.

Note: *The AT&T Paradyne Comsphere and AT&T Dataport pose this problem.*

Use caution when configuring Get Setup in this manner. A modem's NVR can only be written a particular number of times; if the SCS is rebooted too often, setting Get Setup to "" could wear out the modem's NVR.

Init string The initialization (Init) string must be configured in a specific manner in order for your modem to work with the SCS. See *Editing a Profile* on page 9-3 for instructions.

Nocarrier string The modem should respond with this string if the remote modem doesn't present a carrier. It is commonly set to "NO CARRIER."

Nodialtone string The modem should respond with this string if no dial tone is present and the modem cannot dial. It is commonly set to "NO DIAL."

OK string The modem must respond with this string after receiving the Attention string. It is commonly set to "OK."

Reset string This string resets the modem and reloads its setup from nonvolatile memory (NVR). It is commonly set to "Z."

Ring string The SCS will expect this string when the modem is ringing. If set to "", any characters from an idle modem will be interpreted as a ring. It is commonly set to "RING."

Save string When the modem receives the Save string, it will save its configuration to nonvolatile memory (NVR). It is commonly set to "&w."

Speaker Enabled/Disabled

This setting enables or disables the modem's speaker.

Speaker Command disablestring enablestring

These strings turn the modem's speaker on or off. The speaker on switch may also set the speaker volume. It is commonly set to "m11 1" and "m0."

Statistics string This string is sent to the modem after each call to gather statistics on that call. The resulting information from the modem is sent to the server's logging system for later analysis.

9.3.4 Profiles for Modems with External Switches

Some modems, such as USRobotics Sportster and Courier, have external switches that control the modem's behavior. Modems that have external switches but do not have predefined modem profiles on the SCS should be set not to autoanswer. The SCS answers the phone; the modem should never pick up the phone on its own.

Sometimes the switch settings can be overridden by command strings, but sometimes they cannot. If your modem has switches, the SCS will tell you how to set the switches when you define the modem profile, as seen in Figure 9-8.

Figure 9-8: Enabling Modem Compression

```
Local>> DEFINE PORT 3 MODEM TYPE 30
%Info: Switch settings 1-8: UUDU DUUD
%Info: Port speed changed to 115200.
%Info: Port flow control changed to CTS.
```

In the example, "U" stands for up and "D" stands for down. Duplicate these settings on your modem, then power cycle the modem before logging out of the port or rebooting the SCS.

9.4 Modem and SCS Interaction

9.4.1 Initialization

When the SCS is booted, the DTR signal will be held low so that the modem will reset and will not answer incoming calls. All SCS ports with Modem Control enabled will be checked to see if a modem is connected and powered up. To determine this, the SCS will send the Attention string to the modem and wait for the OK string to be sent in response.

The modem will then be asked for its current configuration. The Init string will be sent followed by a request for the modem's configuration. If the current modem profile on that port does not match the configuration sent from the modem, it will be assumed that the modem's setup has changed. The Save string will be sent, and the setup contained in the profile will be saved in the modem's permanent memory (NVR).

Note: *The NVR on some modems will wear out with repeated use. This limitation is avoided by only writing the setup to the modem if it has changed.*

The SCS will raise DTR so that the modem will answer incoming calls. The port then waits to start an outgoing call and waits to receive the Ring string from the modem to start an incoming call.

9.4.2 Outgoing Calls

On outgoing calls, the SCS will send the Attention string until the modem responds with the OK string (up to three times). If the modem does not send the OK string, the attempt will fail and the modem will be reset. If the OK string is received, the SCS will send the Command Prefix, the Dial String, and the telephone number to the modem.

Note: *To set the telephone number, refer to Assign a Telephone Number to the Port or Site on page 4-19.*

If the modem responds with the Connect String, the call will succeed. If the modem responds with the No Carrier, Error, No Dial Tone, or Busy strings, or if no response is received in 60 seconds, the call will fail and the modem will be reset (60 seconds is the default wait period; this can be configured using the **Define Ports Modem Carrierwait** command).

Note: *Define Ports Modem Carrierwait is discussed on page 12-5.*

9.4.3 Incoming Calls

The SCS will detect an incoming call when a port receives the Ring string. The port will then be in a "ringing" state; outgoing calls cannot be made from this port during this period. The SCS will send the Command string followed by the Answer string forcing the modem to answer the call.

When a modem asserts the DCD signal, the incoming call will be permitted. If more than 60 seconds pass between ring signals or before the assertion of DCD, the SCS will assume that the caller hung up or that the connection attempt failed. Sixty seconds is the default wait period; this can be configured using the **Define Ports Modem Carrierwait** command. The port will then be available for outgoing calls.

9.4.4 When a Port is Logged Out

Each time a port is logged out (for example, when a user hangs up), the SCS will send the Attention string to the modem. The OK string is expected in return. When this string is received, the SCS will send the Command Prefix string and the Reset string.

When the modem receives the Reset string, it will read its configuration from NVR. Any temporary configuration, such as changes made by an outbound modem user, will be cleared at this point. If a user made changes during an outbound call and saved them to the modem's NVR, the modem will be returned to that changed state.

9.4.5 Compression

The compression setting in a modem profile enables or disables **data compression** in the modem. Data compression enables a modem to transfer a larger amount of data in the same amount of time. When compression is used, uncompressed data arrives on the modem's serial port and the modem compresses the data before sending it over the phone line.

The advantage of compression is increased throughput. For example, a modem might compress data to 1/2 its original size, doubling the modem's **throughput**; twice the data could be sent in the same amount of time required to send uncompressed data.

The disadvantage of compression is increased **latency**. Latency is the delay before data transfer occurs, caused by the additional time the modem requires to compress the data before it is sent. In situations where the delay is undesirable (for example, during interactive use over a long distance line), compression should not be used.

The "compressability" of data depends on what is being compressed. Some data can be compressed to less than half its original size, while other data cannot be compressed at all. As the type of data to be sent changes, the modem's throughput will change.

Before compression can be enabled, flow control must be enabled (see *Flow Control* on page 8-18). In addition, the modem's serial speed must be set higher than the line speed. This enables the SCS to keep the modem's internal data buffer filled with data to compress. As lower compression ratios decrease the effective line speed, the modem will flow control the SCS more often. When compression ratios and the effective line speed rise, the modem will flow control the SCS less often.

Note: *On many modems, error correction must be enabled for data compression to work properly. Error Correction is discussed on page 9-10.*

To enable modem compression, use the following command:

Figure 9-9: Enabling Modem Compression

```
Local>> DEFINE PORT 2 MODEM COMPRESSION ENABLED
```

Note: *For this command's complete syntax, see Define Ports Modem Compression on page 12-6.*

When modem compression is enabled on a port, the SCS will send a string to the modem to instruct it to enable modem compression. When compression should be disabled, a disable string may be sent. The default enable and disable strings vary, depending upon the modem profile used. To display the default strings for a particular modem profile, use the List Modem command.

To modify these strings, use the **Define Ports Modem Compression** command. The first string specified is the disable string; the second is the enable string.

Figure 9-10: Changing the Disable and Enable Strings

```
Local>> DEFINE PORT 2 MODEM COMPRESSION "s46=12b" "q5"
```

The compression mode used varies from modem to modem, however, the most common mode is **V.42bi**s. This is the recommended method of data compression.

V.42bis encoding offers an automatic 20% savings on all data send, regardless of how compressible it is. Some text files can be compressed down to 1/4 or less of their original size. In addition, V.42bis will enable or disable compression according to whether or not it's required.

Other compression modes, such as MNP, may not give the same results as V.42bis. To obtain the best results, experiment with different modes of compression.

9.4.6 Error Correction

A modem profile's Error Correction setting enables or disables the modem's error correction mode. Error correction modes enable modems to ensure data integrity in the presence of telephone line noise. These modes work by checking the data for errors at the receiving modem. If an error is detected, the receiving modem requests that the sending modem retransmit the data.

When errors are not detected, data flows through the modem at a normal rate. When an error occurs, the sending modem must retransmit the data and not send any new data. The sending modem must be able to flow control the SCS during the retransmission. Ensure that flow control is enabled on the SCS before enabling error correction.

Note: *To configure flow control, see Flow Control on page 8-18.*

To enable error correction, use the following command:

Figure 9-11: Enabling Error Correction

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION ENABLED
```

Note: *For this command's complete syntax, see Define Ports Modem Errorcorrection on page 12-10.*

When error correction is enabled on a port, the SCS will send a string to the modem to instruct it to enable error correction. When error correction should be disabled, a disable string may be sent. The default enable and disable strings vary, dependent upon the modem profile used. To display the default strings for a particular modem profile, use the **List Modem** command.

To modify these strings, use the **Define Ports Modem Errorcorrection** command. The first string specified is the disable string; the second is the enable string.

Figure 9-12: Changing the Disable and Enable Strings

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION "&q5" "q0"
```

9.4.7 Modem Security

If security precautions aren't properly configured, unauthorized callers may be able to gain access regardless of the port's security measures. In order to prevent this, the following features should be enabled:

- If a remote user hangs up without logging out, the modem will sense the loss of carrier, and deassert the DCD signal. The server will then log the port out.
- If the remote user logs out, the server will force the modem to hang up immediately and reset.

These items should be carefully verified for each port that a modem is attached to, even if a preconfigured modem profile is used.

Dialback security, discussed on page 9-11, can be used in conjunction with these techniques on modem ports for an additional layer of security.

The *Ports* and *Security* chapters cover security features in detail. The best tools for securing modem ports are username and password pairs, server passwords, and idle timeouts.

9.4.8 Autostart

A port with Autostart and modem control enabled will not run the specified mode (for example, PPP) until the modem asserts the DCD signal. This prevents the port from sending data to the local modem before a remote modem is connected.

Note: *For information on Autostart or the DCD signal, see Chapter 8, Ports.*

9.4.9 Dialback

Dialback allows a system manager to set up a dialback of authorized users for incoming modem connections. When a username matching one in the list is entered, the port will be logged out and the user will be called back at the predefined number.

For a complete discussion of Dialback, see *Dialback* on page 11-5.

9.5 Terminal Adapters

ISDN Terminal adapters (TAs) are similar to modems. Modems convert asynchronous serial signals to a form that can be transmitted via regular phone lines, while terminal adapters convert asynchronous serial signals to a form that can be transmitted by ISDN phone lines. The main difference between using these devices with the SCS is the complexity of TA setup, which varies by telephone service provider.

For the most part, the SCS interacts with a TA in the same way that it interacts with a modem. However, two things must be taken into account when using a TA with the SCS:

- Although some TAs can autodetect certain settings, it is not always possible to auto-configure information needed for the connection, such as the caller's own phone number. Therefore, no TA profiles are preconfigured for the SCS itself. TA users must edit the generic modem profile so that it can be used with their specific TAs and ISDN service providers.

  Note: *Lantronix provides Tech Tips that outline the configuration needed for certain specific terminal adapters. To find out if your TA's configuration is included in a Tech Tip, contact your dealer or Lantronix technical support.*

- B-channel ISDN connections are much faster than modem connections. Those who wish to use the SCS bandwidth-on-demand functionality should take this speed increase into consideration when configuring bandwidth settings.

9.6 Caller-ID

Three commands provide the SCS with basic Caller-ID functionality, provided that Caller-ID is available and the SCS is attached to a modem capable of decoding Caller-ID signals.

Define Ports Modem CallerID Enabled allows the SCS to parse Caller-ID information that it receives from the attached modem.

Figure 9-13: Turning on Caller-ID

```
Local>> DEFINE PORT 2 MODEM CALLERID ENABLED
```

Note: *The modem should be configured for either Single or Multiple Message Format; the SCS cannot parse information in raw data format (ASCII coded hexadecimal). See your modem's documentation for configuration.*

Define Ports Modem Answer Rings configures the number of rings, either 1 or 3, that the SCS will wait for before answering the line. The telephone company sends Caller-ID information between the first and second rings, so the SCS must be set to wait for 3 rings before answering in order for Caller-ID functionality to work.

Figure 9-14: Setting Modem Ring Value for Caller-ID

```
Local>> DEFINE PORT 2 MODEM ANSWER RINGS 3
```

Note: *The modem init string must be modified to tell the modem to pass Caller-ID information to the SCS. See Editing a Profile on page 9-3 for more information.*

Finally, **Show/Monitor/List Modem Status** displays status information about modems connected to SCS ports, including the most recently collected Caller-ID information. A sample modem status display is shown in Figure 9-15.

Figure 9-15: Modem Status Display with Caller-ID Information

```
Local>> SHOW PORT 2 MODEM STATUS
Port 2: Username: Stephan
Last Connect Speed: 28800/ARQ/V34/LAPM/V42BIS
Last Caller ID Information:
Date:
Number:
Name:
Local>>
```

Caller-ID information is also recorded by modem logging level 2 (see **Set/Define Logging** on page 12-172) and sent to RADIUS servers (see Appendix D, *Supported RADIUS Attributes*).

9.7 Examples

9.7.1 Typical Modem Configuration

Figure 8-16 lists the commands required for a typical modem setup. In this example, an SCS modem profile exists for this brand of modem. All modem strings in this profile are acceptable; no special configuration is required.

Figure 9-16: Typical Modem Configuration

```
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 4
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> LOGOUT PORT 2
```

9.7.2 Modem Configuration Using Generic Profile

In this example, a V.34 modem is attached to SCS port 2. A modem profile does not exist for this brand of modem; the generic modem profile must be used. This modem will support incoming and outgoing connections.

Port 2's speed must be set properly for the modem. To determine the appropriate port speed, examine the following table:

Table 9-2: Maximum Baud Rates

Modem	Typical Maximum Line Rate
V.32	19200
V.32bis	57600
V.fast	115200
V.34	115200

To determine the maximum baud rate supported by the modem, the port speed must be set and tested. Modem handling must be disabled on the port; if it is enabled, the SCS will attempt to initialize the modem when the port is logged out.

Figure 9-17: Configuring Port Speed

```
Local>> DEFINE PORT 2 MODEM DISABLED
Local>> DEFINE PORT 2 SPEED 115200
```

The port speed is tested by logging into the port and sending an attention ("at") command. The modem should respond with "OK". If it does not send "OK", the port speed should be set to a lower baud rate (see Table 9-2).

Figure 9-18: Testing the Port Speed

```
Local>> SET PORT 2 LOCAL SWITCH ^\
Local>> CONNECT LOCAL PORT_2
Local protocol emulation V2.2
at
OK

Local>>
```

After the appropriate port speed is determined, the port must be configured using the generic modem profile. In addition, modem operation must be enabled.

To determine which profile number is the generic profile (the number will change as new profiles are added), enter the **List Modem** command:

Figure 9-19: Displaying Modem Profiles

```
Local>> LIST MODEM
1- Modem 1
2- Modem 2
3- Modem 3
4- Generic
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 4
%Info: Port speed changed to 57600.
%Info: Port flow control changed to CTS.
```

The generic modem profile made a series of configurations to port 2. To determine the current configuration of port 2, use the **List Port** or **List Port Modem** command.

Figure 9-20: Current Port Configuration

```
Local>> list port 2

Port 2: Username:                              Physical Port 2 (Idle)
        Char Size/Stop Bits:        8/1        Input Speed:          57600
        Flow Ctrl:                  Cts/Rts    Output Speed:         57600
        Parity:                     None       Modem Control:        Disabled

        Access:                     Local      Local Switch:         None
        Backward:                   None       Port Name:            Port_2
        Break Ctrl:                 Local      Session Limit:        4
        Forward:                    None       Terminal Type:        Soft ()

        Preferred Services:         (Telnet)
        Characteristics:  Broadcast Loss Notify Telnet Pad Verify
```

The speed for port 2 is now 57600. This speed must be set to the appropriate speed (determined earlier by setting and testing the speed), 115200.

Figure 9-21: Configuring Port Speed

```
Local>> DEFINE PORT 2 SPEED 115200
```

Port 2 will be used for incoming and outgoing connections, therefore, access must be set to Dynamic.

Figure 9-22: Configuring Local Switch and Port Access

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

After entering this command, log out the port to ensure that the changes will be in effect when the next user logs into port 2.

9.7.3 Editing Modem Strings

The current init string on port 2 is **&fw1&c1&d2&k3s2=128**. This string must be changed to work with a particular modem:

Figure 9-23: Changing Init String

```
Local>> DEFINE PORT 3 MODEM INIT "&fw1&c1&d2s2=128s38=0"
```

Note: *To see what the above modem initialization string is configured to do, refer to Table 9-1 on page 9-4.*

Consult your modem's documentation for the exact items to include in the modem init string.

9.8 Troubleshooting

To help diagnose any difficulty with your modem setup, it is a good idea to do the following:

- Install a breakout box between the modem and the SCS. Set all modem switches to the “normal” position, and remove all jumpers. When the modem and SCS are powered on, the box’s LEDs will display the state of the signals, enabling you to more easily diagnose the problem.
- Enable event logging for modems. *Event Logging* is discussed on page 11-25.
- Use the **List Port** command to ensure that modem control is enabled on the port. Many of the port’s characteristics will be displayed; modem control is the third item listed in the left column.
- Ensure that all modems have been reset by rebooting the SCS.
- Verify the cable connections.

The following table lists some common problems that occur with modem configuration and proposes solutions for them.

Table 9-3: Modem Troubleshooting

Problem	Possible Cause(s)	Remedy
The modem won’t answer the phone.	The modem isn’t configured to answer the phone.	Enable answering with the **Define Ports Modem Answer** command (discussed on page 12-3).
	The DTR signal isn’t attached.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.
	The SCS isn’t asserting the DTR signal.	Ensure that the Dtrwait characteristic (discussed on page 12-71) is disabled on the SCS port used.
	The modem has hung.	Cycle power on the modem.
The modem doesn’t respond to the SCS’s configuration requests.	The modem’s flow control isn’t set properly, or the modem’s autobaud isn’t functioning properly.	Reset the modem’s NVR to the factory default state (the at&f string is commonly used). For further instructions, refer to your modem’s documentation.
	The modem isn’t wired correctly.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
The modem answers, but cannot connect to the SCS.	The Access characteristic on the SCS port is set to None or Remote.	Set Access (discussed on page 12-57) to Local or Dynamic.
	The modem’s serial speed does not match the serial speed on the SCS port used.	Ensure that the serial speeds of the modem and SCS port match.
	A network user is connected to the modem.	Use the **Show Ports** command (discussed on page 12-96) to verify that the SCS port is idle. If it is not idle, log out the port using the **Logout Port Port** command (discussed on page 12-53).
	The modem has hung.	Cycle power on the modem.
	The SCS cannot detect the DCD signal.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.

Table 9-3: Modem Troubleshooting, cont.

Problem	Possible Cause(s)	Remedy
All data is corrupted.	The ground pins aren't wired correctly.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.
	The modem's serial speed does not match the serial speed on the SCS port used.	Ensure that the serial speeds of the modem and SCS port match.
	Flow control isn't working properly.	Ensure that the modem and SCS port are configured to use the same flow control method.
	The modem is set to the wrong baud rate.	Cycle power on the modem.
The first few lines of data are transmitted properly, but the subsequent data is corrupted.	Flow control isn't working properly.	Ensure that the modem and SCS port are configured to use the same flow control method. Flow control is discussed in detail in *Flow Control* on page 8-18.
	The ground pins aren't wired correctly.	Verify the wiring. On RJ45 ports, ensure that the ground pins are wired together.
When the port is logged out, the modem doesn't hang up the phone line.	Modem Control isn't enabled on the SCS port used.	Ensure that Modem Control is enabled. See **Define Ports Modem Control** on page 12-8 for details.
	The DTR signal isn't attached.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
	The modem isn't configured to reset when the DTR signal is dropped.	Check the modem's configuration.
When the phone is hung up, the SCS doesn't log out the port.	Modem Control isn't enabled on the SCS port used.	Ensure that Modem Control is enabled. See **Define Ports Modem Control** on page 12-8 for details.
	The DCD signal isn't attached.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
	The modem isn't configured to deassert DCD upon loss of carrier.	Check the modem's configuration.
The modem answers, but won't connect to the remote modem.	One or both modems are configured not to connect unless some feature is enabled (for example, error correction).	Check the documentation for both modems; verify their configuration.
	The two modems cannot be connected. (Some modems are incompatible with one another.)	Replace one or both of the modems. Verify that the modem is using the correct and current version of its software.

10: Modem Sharing

Modem sharing provides users with individual modem/phone line functionality at a reduced cost. When modems are shared, a group of IP users may use a modem pool to dial out of a LAN and connect to a remote host; for example, to connect to a bulletin board service (BBS). This eliminates the need for phone lines for each user's computer.

10.1 Services

A **service** represents a resource accessible to network users, such as a modem or a pool of modems attached to the SCS.

Services provide links for TCP connections to SCS serial ports. They are employed in modem sharing to establish connections to the SCS modems.

10.1.1 Creating a Service

Each SCS service must have a unique name. To create a service, use the **Set/Define Service** command. An example is displayed below.

Figure 10-1: Creating a New Service

```
Local>> DEFINE SERVICE fastmodems
```

Service names are not case-sensitive, may be up to 16 alphanumeric characters long, and cannot include spaces.

10.1.2 Associating Ports with a Service

Each service must be associated with at least one port. To associate a port with a service, use the **Set/Define Service Ports** command.

Figure 10-2: Associating a Port with a Service

```
Local>> DEFINE SERVICE fastmodems PORTS 2
```

Note: *Set/Define Service Ports is discussed in detail on page 12-105.*

To use a service for modem sharing, the service should be associated with multiple ports; this permits multiple connections to the service. Connections will be made to the first available port.

Figure 10-3: Associating a Service with Multiple Ports

```
Local>> DEFINE SERVICE fastmodems PORTS 2-4
```

Ports associated with a service used for modem sharing must support outgoing connections. To support outgoing connections, the port access must be set to Dynamic or Remote.

Figure 10-4: Configuring a Port for Outgoing Connections

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

A port associated with a service used for modem sharing must also be configured to operate the modem attached to it. To configure modem operation on a port, use the following commands:

Figure 10-5: Configuring Modem Operation on a Port

```
Local>> DEFINE PORT 2 MODEM CONTROL ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 5
```

To display a particular modem type's settings, use the **Define Ports Modem Type** command, discussed in detail on page 12-16.

Note: *For more information on modem configuration, see Chapter 9, Modems. For more information on port configuration, see Chapter 8, Ports.*

10.1.3 Displaying Current Services

To display a list of the current services, use the **Show/Monitor/List Services** command.

To display specific information about a service, the following parameters may be used with the **Show/ Monitor/List Services** command: Characteristics, Summary, and Status. For example, to display a service's characteristics (including the ports associated with it), use the following command:

Figure 10-6: Displaying a Service's Characteristics

```
Local>> LIST SERVICES fastmodems CHARACTERISTICS
```

The command above shows the ports associated with the service **fastmodems**, the characteristics enabled for the service, and the **service rating**.

Generally, a service rating of 255 means that the service is available, and a rating of zero means that it is busy or otherwise unavailable. A rating between 255 and zero indicates that the service is partially available. For example, fastmodems may be a modem pool containing three high-speed modems, one of which is available. In this case, the service rating for fastmodems would be 85.

Note: *Show/Monitor/List Services is discussed in detail on page 12-108.*

10.2 Sharing Modems

To share SCS modems, you must do one of the following:

- Use the Lantronix COM Port Redirector application.
- Form a TCP connection to a TCP listener socket associated with a service.
- Form a TCP connection directly to an SCS serial port.
- Log into the SCS and connect to a local service or port.

These methods are discussed in the following sections.

10.2.1 Configuring an IP Modem Pool Service

Creating a service allows you to set up a modem pool on several SCS ports. To create an IP modem pool service, enter the **Set/Define Service Ports** command.

Figure 10-7: Creating an IP Modem Pool Service

```
Local>> DEFINE SERVICE modempool PORT 8-10 TCPPORT 4008
```

Note: *The complete syntax of Set/Define Service Ports is described on page 12-105.*

10.2.2 Using the COM Port Redirector

To use the Redirector on an IP network, you must create a modem pool service that is associated with a TCP listener socket. Refer to Figure 10-8 for the necessary command.

10.2.3 Connecting to a TCP Listener Service

Each service may be associated with a TCP listener socket. TCP connections to the socket are connected to the service. Once a connection is established, a user may issue commands to the modem.

To associate a service with TCP listener socket, use the **Set/Define Service TCPport** command. Socket numbers must be between 4000 and 4999.

Figure 10-8: Specifying a Raw TCP Listener Socket

```
Local>> DEFINE SERVICE fastmodems TCPPORT 4999
```

Note: *The complete syntax of Set/Define Service TCPport is listed on page 12-107.*

If the socket should perform Telnet IAC character-escaping negotiations on the data stream, use the **Set/Define Service Telnetport** command.

Figure 10-9: Specifying a Telnet TCP Listener Socket

```
Local>> DEFINE SERVICE slowmodems TELNETPORT 4500
```

Note: *Set/Define Service Telnetport is discussed in detail on page 12-108.*

Connecting to a TCP listener service is recommended if more than one modem is being used. The SCS will automatically connect the user to the next available modem, avoiding the trail and error process of finding an available port (see *Connecting to a Serial Port* on page 10-4).

10.2.4 Connecting to a Serial Port

To connect directly to an SCS serial port, specify a port number of 30*nn* or 200*nn*. The *nn* represents the number of the SCS serial port; for example, port 2002 represents SCS serial port 2.

If you're using Telnet to connect to the SCS, connect to port 20*nn*. The 2000 port is intended for Telnet connections; it performs Telnet IAC character-escaping negotiations on the data stream. In the example below, the Telnet command is used to connect to the SCS serial port 3.

Figure 10-10: Telnetting Directly to Port 3

```
% TELNET server_name 2003
```

If you're connecting via a host application, connect to port 30*nn*, where nn is the port number. This port provides an 8-bit clean connection, required by most host applications.

10.2.5 Connecting to a Service or Port

To connect to a local service or port from an SCS login, use the Connect Local command at the Local> prompt.

Figure 10-11: Connecting to a Local Service/Port

```
Local>> CONNECT LOCAL fastmodems
Local>> CONNECT LOCAL PORT_2
```

If a service name is specified, a connection is made to the first available port associated with the service. If a port name is specified, the connection is made to the port unless the port is in use.

Once the connection is established, commands may be issued to the modem attached to the serial port.

10.3 Examples

Users on an IP network need to connect to both a BBS and a commercial online service. The following modems are available:

- Two 28,800 bps modems, reserved for connections to the online service
- Four 14,400 bps modems, available for connections to both services
- One 9,600 bps modem, reserved for connections to the BBS

The modems are connected to an SCS as follows:

Table 10-1: Modems Connected to the SCS

Speed	Connected to	SCS Modem Type
28,800 bps (2)	Ports 2 and 3	6
14,400 bps (4)	Ports 4 through 7	5
9,600 bps (1)	Port 8	4

Three services will be created for the modems: **fastmodems**, **slowmodems**, and **slowestmodem**. These will be used for the 28,800, 14,400, and 9,600 modems, respectively.

Figure 10-12: Configuring the SCS fastmodems Service

```
Local>> DEFINE SERVICE fastmodems PORTS 2-3 ENABLED
Local>> DEFINE PORT 2-3 ACCESS REMOTE
Local>> DEFINE PORT 2-3 MODEM TYPE 6
Local>> DEFINE PORT 2-3 MODEM CONTROL ENABLED
```

Figure 10-13: Configuring the SCS slowmodems Service

```
Local>> DEFINE SERVICE slowmodems PORTS 4-7 ENABLED
Local>> DEFINE PORT 4-7 ACCESS REMOTE
Local>> DEFINE PORT 4-7 MODEM TYPE 5
Local>> DEFINE PORT 4-7 MODEM CONTROL ENABLED
```

Figure 10-14: Configuring the SCS slowestmodem Service

```
Local>> DEFINE SERVICE slowestmodem PORT 8 ENABLED
Local>> DEFINE PORT 8 ACCESS REMOTE
Local>> DEFINE PORT 8 MODEM TYPE 4
Local>> DEFINE PORT 8 MODEM CONTROL ENABLED
```

When all of the configurations have been entered, log the ports out and initialize the server.

10.3.1 Configuring the Redirector

The following table shows how the Redirector setup utility should be configured for this example. All three SCS services (fastmodems, slowmodems, and slowestmodem) appear in the Service Selection window.

Table 10-2: Redirector Configuration

COM Port #	Redirect?	Selected Services
COM Port 1	Yes	fastmodems slowmodems
COM Port 2	Yes	slowmodems slowestmodem

10.3.2 Configuring the PC Communications Software

The communication software must be configured to connect to the online service by dialing out through COM Port 1 and to the BBS by dialing out through COM Port 2

11: Security

The SCS enables you to secure your network in a number of ways. Supported security features include:

- Authentication of incoming connections, discussed on page 11-1.
- Authentication of outgoing LAN to LAN connections, discussed on page 11-4.
- Dialback during incoming connection attempts, discussed.
- Databases which store authentication information, discussed on page 11-9.
- Restriction of user access to commands and functions, discussed on page 11-19.
- Event logging, discussed on page 11-25.

11.1 Incoming Authentication

Incoming connections may be one of the following types: character mode (Local> prompt) logins, PPP logins, SLIP logins, or virtual port logins. When incoming authentication is configured, users must prove their identity before their connection to the SCS is permitted.

The connection type affects the authentication sequence and how the authentication information is transferred.

11.1.1 Character Mode Logins

Each SCS serial port may be configured to support any combination of the following:

- A server-wide login password
- A username/password pair
- Dialback on serial ports with modems attached

This section describes the login password and the username/password pair. Dialback will be discussed in the following section.

Note: *To configure a port to support character mode, see Port Modes on page 8-3.*

11.1.1.1 Login Password

To set the login password, use the **Set/Define Server Login Password** command.

Figure 11-1: Defining the Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
```

Note: *The login password can be up to 16 characters long. The default password is "access."*

To require that users enter the login password when logging into a particular port from another serial port, use the **Set/Define Ports Password Enabled** command.

Figure 11-2: Requiring Login Password on a Port

```
Local>> DEFINE PORT 2 PASSWORD ENABLED
```

By default, incoming Telnet and Rlogin connections are not required to enter the login password. To require the login password for virtual port connections, use the **Set/Define Server Incoming Password** command:

Figure 11-3: Requiring a Login Password for Telnet/Rlogin Connections

```
Local>> DEFINE SERVER INCOMING PASSWORD
```

11.1.1.2 Username/Password Pair

In addition to the login password, each port may be configured to prompt users for a personal username and password. When the user enters the username/password pair, the SCS scans the authentication databases (see *Database Configuration* on page 11-9) for a matching pair. If a match is not found, the login will not be permitted.

Figure 11-4: Enabling Username/Password Authentication

```
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
```

To require username/password authentication for virtual port logins, use the **Set/Define Ports Authenticate** command, specifying port 0 as the port number. This command prompts the incoming user for a username and password to be checked against the authentication database.

Figure 11-5: Virtual Port Username/Password Authentication

```
Local>> DEFINE PORT 0 AUTHENTICATE ENABLED
```

11.1.1.3 Local Password

PPP or SLIP may be started when a port is in character mode using the **Set PPP** or **Set SLIP** commands. If an incoming user specifies a particular site to be started (for example, Set PPP irvine), the site may prompt the user for its local (site-specific) password.

To configure a site's local password, use the **Define Site Authentication Local** command.

Figure 11-6: Setting a Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION LOCAL "badger"
```

To prompt the user for the local password when attempting to start the site, use the **Define Site Authentication Prompt** command.

Figure 11-7: Requiring Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION PROMPT ENABLED
```

11.1.2 PPP Logins

This section covers authentication on ports dedicated to PPP or with PPPdetect enabled. If PPP will be started from character mode, see *Character Mode Logins* on page 11-1.

Note: *To dedicate a port to PPP or enable PPPdetect, see Chapter 8, Ports.*

11.1.2.1 CHAP and PAP

The username and password may be transmitted using CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). Each protocol goes through a negotiation sequence to complete the authentication; see Chapter 4, *Basic Remote Networking*, for details.

To use CHAP or PAP to authenticate incoming callers, CHAP Remote or PAP Remote must be enabled on the port accepting the call. One or both may be enabled, however, CHAP is recommended.

Figure 11-8: Enabling PAP and CHAP for Incoming Connections

```
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 PPP PAP REMOTE
```

If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the remote host does not understand CHAP, PAP will be attempted instead. If neither CHAP nor PAP successfully authenticates the caller, the connection is terminated.

11.1.2.2 Comparing Username/Password to Authentication Databases

If the username sent by the caller matches a site name, that site will be checked to determine if it has a local password defined. The local password is the password expected from the incoming caller. *Local Password* on page 11-2 describes how to configure and assign a local password to a site.

If the password entered matches the site's local password, the site will be started. If it does not match the local password, or if the site does not have a local password defined, the SCS will check the next database (according to the order of database precedence). See *Database Configuration* on page 11-9 for details.

Note: *Some databases are case-sensitive, so the login information must be entered in the proper case in order for authentication to succeed. See the Database Configuration section for more information.*

A custom site will only be started if the username matches a site name and any password in an authentication database. If the username doesn't match a site name, but matches a username/password pair in an authentication database, a temporary site will be used for the connection.

If a matching username/password pair is not found in any authentication database, the connection attempt will fail.

11.1.2.3 Offering Authentication Information to the Incoming Caller

If the incoming caller must authenticate the SCS, the port must have PAP Local or CHAP Local configured. Use the **Define Ports PPP CHAP Local** or **Define Ports PPP PAP Local** command.

Figure 11-9: Enabling CHAP and PAP Local

```
Local>> DEFINE PORT 2 PPP CHAP LOCAL
Local>> DEFINE PORT 2 PPP PAP LOCAL
```

During CHAP/PAP negotiation, the SCS will send the site's username and remote password to the incoming caller. To set a site's username and remote password, use the Define Site Authentication command:

Figure 11-10: Configuring the Site Username and Remote Password

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME seattle
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE gopher
```

Use caution when configuring a site to offer and accept authentication information (when the site has both a local and remote password). PAP does not offer complete security in this situation; if the site has PAP authentication enabled for incoming and outgoing connections, both passwords may be compromised during the LCP negotiation process.

When the SCS receives an incoming call, a site configured with a local and remote password may let the incoming caller know that it is willing to transmit these passwords. If the remote caller has PAP authentication enabled, it may persuade the SCS to transmit its passwords to the remote caller as part of the PAP authentication negotiation. At that point, the remote caller can hang up in possession of the SCS passwords. The caller may be able to use the SCS remote password to log into other networks, or to call the SCS and connect as an authorized user.

11.1.3 SLIP Logins

SLIP does not support authentication; authentication must take place before SLIP is started.

Ensure that the port will start in character mode by disabling SLIP autodetection and SLIP dedicated modes. SLIP Autodetection and dedicated SLIP are disabled by default.

Figure 11-11: Disabling SLIPdetect and SLIP Dedicated

```
Local>> DEFINE PORT 2 SLIPDETECT DISABLED
Local>> DEFINE PORT 2 SLIP DISABLED
Local>> DEFINE PORT 2 SLIP ENABLED
```

11.2 Outgoing Authentication

When the SCS attempts to connect to a remote host, the host may require that the SCS send a username and password. The method used to transmit this username/password pair depends upon the type of connection: character, SLIP, or PPP.

11.2.1 Outgoing Character Mode Connections

If the remote device is expecting the information in character mode, the username and password must be sent in a chat script. The chat script should expect the username prompt, send the appropriate username, expect the password prompt, and send the appropriate password. See Chapter 5, *Additional Remote Networking*,for information on configuring chat scripts.

11.2.2 Outgoing PPP Connections

If the remote device supports PPP, the username and password may be transmitted using CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). Each protocol goes through a negotiation sequence to complete the authentication; see *Configuring Outgoing Connections* on page 4-18 for details.

To enable CHAP and PAP authentication on outgoing connections, use the **Define Site Authentication CHAP** and **Define Site Authentication PAP** commands. One or both may be enabled, however, CHAP is recommended.

Figure 11-12: Enabling PAP/CHAP Outgoing Authentication

```
Local>> DEFINE SITE dallas AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE dallas AUTHENTICATION PAP ENABLED
```

If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the remote host does not understand CHAP, PAP will be attempted instead. If both PAP and CHAP fail, the connection will be terminated.

To define the username that the SCS sends to the remote host, use the **Define Site Authentication Username** command:

Figure 11-13: Outgoing Site Username

```
Local>> DEFINE SITE dallas AUTHENTICATION USER "seattle"
```

The password sent to the remote host is called the remote password. Configure this password with the **Define Site Authentication Remote** command.

Figure 11-14: Configuring Site Remote Password

```
Local>> DEFINE SITE dallas AUTHENTICATION REMOTE "badger"
```

11.2.3 Outgoing SLIP Connections

All outgoing SLIP authentication must be done with chat scripts before SLIP starts. SLIP does not support any authentication. To configure chat scripts, see *Chat Scripts* on page 5-3.

11.3 Dialback

When dialback is used, the SCS verifies the identity of incoming users by logging the port out and dialing the user back at a specified number. Dialback may be configured to do any combination of the following:

- Log out a port and call the user back
- Permit users to bypass the dialback process and connect immediately
- Terminate the connection when unauthorized users attempt to connect

Note: *The port must be configured to use modems; for additional information, see Chapter 9, Modems.*

11.3.1 The Dialback Process

1. When a username is entered on a dialback port, the SCS determines if it should allow the connection or dial the user back.

   If the SCS must dial the user back, it hangs up the modem by cycling DTR.

2. The SCS sends a command to the applicable serial port. The command contains the modem command prefix, the dial string, and the configured telephone number from its dialback database.

3. The dial string should perform any special configuration required for the call, then dial the remote modem number (in the example below, 555-1235). It is not necessary to precede the telephone number by strings such as "atdt."

4. The SCS waits the length of the Carrier Wait setting for the DCD signal to go high, indicating that the modem has reconnected successfully. Otherwise, DTR is dropped for 3 seconds and the port is reset.

5. The SCS waits 30 seconds for the user to enter a username when in Dialback mode. After 30 seconds, the port is logged out to keep unauthorized users from denying other users access to that port.

Note: *Dialback only applies to incoming port logins. Dialback ports can be used normally for outgoing connections.*

11.3.2 Dialback from Character Mode

To use dialback for character logins, configure a list of authorized users with the following steps:

1. Enable modem control using the **Define Ports Modem Control Enabled** command.

2. Assign a modem type to the port using the **Define Ports Modem Type** command.

3. Enable dialback using the **Define Ports Dialback Enabled** command.

4. Configure how Dialback treats users who are not in the dialback database.

   The Dialback Bypass setting controls what happens when a user that is not in the dialback database attempts to connect to the SCS. If Bypass is enabled, these users will be allowed to connect without dialback occurring. If Bypass is disabled, these users will not be able to connect.

5. Add users to the dialback database.

To add a user to the dialback database, use the **Set/Define Dialback** command and specify a username and a telephone number. If the user must bypass dialback (regardless of whether Dialback Bypass is enabled or disabled), specify the Bypass parameter.

Figure 11-15: Adding Users to the Dialback Database

```
Local>> DEFINE DIALBACK BYPASS ENABLED
Local>> DEFINE DIALBACK FRANK BYPASS
Local>> DEFINE DIALBACK BOB "555-1235"
```

In the example in Figure 11-15, user frank will bypass dialback. When user bob attempts to connect, the SCS will call him back at 555-1235. Any other user attempting to connect will be subject to dialback; if he or she is not in the dialback database, the attempt will fail.

To view the Dialback database, use the **Show/Monitor/List Dialback** command.

Figure 11-16: Viewing the Dialback Database

```
Local>> SHOW DIALBACK
```

Note: *You must be the privileged user to view the Dialback database.*

11.3.3 Dialback from SLIP/PPP Mode

To authenticate incoming PPP and SLIP callers using dialback, the site managing the incoming connection must have dialback enabled. Use the **Define Site Authentication Dialback** command.

Figure 11-17: Enabling Dialback on a Site

```
Local>> DEFINE SITE irvine AUTHENTICATION DIALBACK ENABLED
```

Ensure that the correct ports and telephone numbers are defined; the site will use the defined site-specific or port-specific telephone number to dial the incoming caller. See *Telephone Numbers* on page 4-17 for more information.

11.3.4 Dialback Using CBCP

The SCS supports the Microsoft Callback Control Protocol (CBCP) for dial-in PPP clients that request it. In conjunction with CBCP, the SCS may be configured to allow the PPP client to choose the dialback telephone number. This form of dialback is referred to as “insecure dialback” because it negates the usual security provided by dialback. It is primarily used to offer remote users a way to specify a dialback number to reverse telephone charges.

Note: *Insecure dialback may post a security risk. Use it with caution.*

After the CBCP-aware client has connected to the SCS and has passed PPP authentication, and is optionally switched to a custom site, the SCS will negotiate CBCP (this happens regardless of site dialback settings). Three callback options are available:

- If dialback is disabled for the site, the connection will proceed without the dialback step.
- If normal dialback authentication is enabled for the site, the SCS will offer to call the PPP client back at the site-specific telephone number listed in the dialback database. If the client refuses, the connection will be terminated.
- If insecure dialback is enabled for the site, the PPP client can choose to use the site-specific telephone number or specify a different telephone number to use for the return call. If the client refuses to use the site's telephone number and does not enter a valid alternate telephone number, the connection will be terminated.

Note: *The caller should have the alternate telephone number handy when connecting to the SCS to ensure that the connection does not time out before the number can be entered.*

To configure a site to allow insecure dialback, enter the following command on the SCS.

Figure 11-18: Configuring Insecure Dialback

```
Local>> DEFINE SITE irvine AUTHENTICATION DIALBACK INSECURE
```

Note: *Insecure dialback is only offered under CBCP for PPP clients. It does not apply to SLIP or Local mode dialback situations.*

11.3.5 Potential Dialback Drawbacks

The Dialback system does not absolutely guarantee security. Depending on the modem in use and its configuration, it may be possible for a determined attacker to penetrate the system. There are two windows of vulnerability where an attacker could gain unauthorized access to the SCS. The first window exists after the SCS hangs up the modem but before the modem dials the user back. The second is when a dialback attempt fails but before the server reaches the end of the configured carrier wait time-out period (the default setting is 60 seconds). Careful configuration and testing of the system during those short vulnerable periods is required to ensure a high level of security.

If a second call arrives in the few moments after the server hangs up the modem but before the server issues the dial command, security may be breached. Until the modem goes "off hook," it may answer another incoming call and remain on-line, granting access to a possibly unauthorized user. This is highly unlikely and the chances of unauthorized access can be reduced further by configuring the modem to answer only after the second or third ring. Also, the modem must not answer the phone unless DTR is asserted. If possible, the modem should be configured to only dial after detecting a dial tone, and hang up otherwise.

11.3.6 Port User Restrictions

You can constrain user access to specific ports on the SCS using the Set/Define Authentication User **<username> Port Serial <portlist>** command. This command currently only affects users authenticated against the local SCS database. The SCS rejects a user connection attempt to a port not on his or her port target list. The syntax of the command is Set/Define Authentication User **<username> Port [Target] <portlist>.**

To show the user's current port restrictions, use the Show/Monitor/List Authentication **<username>** command. To reset the permissions back to the default, use the Set/Define Authentication User **<username> Port Factory** command.

11.4 Database Configuration

Five types of databases can store authentication information. The databases can be used in any order or combination, but no more than one of each type may be used.

- Local authentication database stored in the SCS's permanent memory (NVR)
- Kerberos V4 server
- RADIUS server
- SecurID ACE/Server
- UNIX password file, via TFTP

You must assign a precedence number to each database method you wish to use. **Precedence** specifies the search order in which the configured databases will be checked. The database location with the most username/password pairs is usually given the highest precedence (1), setting it as the primary database. By default, the local authentication database has a precedence of 1.

> **Note:** *See Database Search Order on page 11-28 for an example of database precedence configuration.*

Configure your precedence settings carefully. If a database is configured for a precedence slot that has already been filled by another database, it will take over the precedence setting and return all of the previous database type's settings to their factory defaults.

> **Note:** *To check the database configuration, use the Show/Monitor/List Authentication command (discussed on page 12-177). Databases are listed according to their precedence numbers.*

As you configure the authentication settings, keep in mind that all configured authentication methods will be tried until one method succeeds or all methods have failed. If six databases are configured and the database with the first precedence denies the user access, there are still five possible chances for the user to pass authentication. Remember that when it comes to configuring multiple authentication methods, your security is only as strong as the weakest method configured.

If you want the SCS to abort the authentication process at any "invalid user" or "invalid password" error, enable Strict fail mode. Strict fail mode is disabled by default, but can be enabled with the **Set/Define Authentication Strictfail** command. By default, authentication attempts continue until either the user is successfully authenticated or all methods fail. Enabling Strictfail causes the SCS to abort the login attempt on the first failure in the authentication method list. This option is SCS-wide, not per port or per user.

Unless Strict fail mode is enabled, the SCS does not examine the reasons for authentication failures. It simply notes the failure.

11.4.1 Local (NVR) Database

The local database is stored in NVR. Storing authentication locally offers the following advantages:

- A network server is not required.
- Local authentication functions even when the network is down.

- Local authentication can execute and restrict user commands.
- CHAP may be used for authentication.

Disadvantages include:

- The SCS cannot share its databases with other servers.
- The SCS cannot share existing databases.
- The local database is limited by the size of the server's NVR.

11.4.1.1 Changing the Precedence

By default, the precedence for the local database is set to 1. To change the precedence number, use the **Set/Define Authentication Local** command.

Figure 11-19: Specifying the Precedence

```
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 3
```

11.4.1.2 Adding Username/Password Pairs

To add a username/password pair to the local database, use the **Set/Define Authentication Local** command.

Figure 11-20: Adding User and Password to Local Database

```
Local>> DEFINE AUTHENTICATION USER "elmo" PASSWORD "badger"
```

Note: *All passwords are case sensitive. All usernames are case insensitive.*

11.4.1.3 Forcing Execution of Commands

A command or series of commands may be associated with a particular username; the commands will be run when the user is successfully authenticated. For example, when user elmo logs into the SCS, he will be automatically telnetted to host 192.0.1.67 and logged out of the SCS.

Figure 11-21: Forcing Commands

```
Local>> DEFINE AUTHENTICATION USER "elmo" COMMAND "telnet 192.0.1.67; logout"
```

Commands must be enclosed in quotes. If a series of commands is specified, they must be separated by semicolons.

11.4.1.4 Permitting Users to Change Their Passwords

By default, users are not permitted to change their passwords. To enable a user to change his or her password, use the **Set/Define Authentication User Alter** command.

Figure 11-22: Permitting User to Change Passwords

```
Local>> DEFINE AUTHENTICATION USER "elmo" ALTER ENABLED
```

11.4.1.5 Forcing Selection of a New Password

Users may be forced to select a new password during their next login. This is useful when the user has forgotten his or her password, or to ensure that passwords are changed on a regular basis.

Figure 11-23: Forcing a User's Password to Expire

```
Local>> DEFINE AUTHENTICATION USER "elmo" EXPIRED
```

11.4.1.6 Displaying the Local Database

Local database entries can be checked with the **Show/Monitor/List Authentication User** command. All users, their passwords, and other parameters are listed.

Note: *See Show/Monitor/List Authentication on page 12-177.*

11.4.1.7 Purging the Local Database

To remove a particular user from the database, use the **Clear/Purge Authentication User** command. See **Clear/Purge Authentication** on page 12-151 for a complete description of this command.

11.4.2 Kerberos

The Kerberos Authentication Service is a network-based authentication service. Passwords are always transmitted in encrypted form. The SCS supports Kerberos version 4.

Kerberos is available as public-domain software and from commercial vendors. Please refer to your Kerberos server documentation for detailed information about setting up a Kerberos server, registering Kerberos clients, and administering a Kerberos network.

Kerberos advantages include the following:

- Passwords are always encrypted; it is not possible to obtain a user's password by eavesdropping on a connection attempt.
- Kerberos is a widely-accepted standard, and is proven to be secure.
- The SCS may easily be added to an existing Kerberos network.
- A large number of users may be supported.

Disadvantages include:

- Configuring the Kerberos database can be complicated.
- Kerberos does not guard against guessing a user's password.
- If the caller attempts to use CHAP for authentication, Kerberos cannot be used.

Note: *Kerberos authentication is case-sensitive.*

11.4.2.1 Configuring Kerberos

The **Set/Define Authentication Kerberos** commands are used for most of the Kerberos configuration options.

1. Ensure that the SCS clock is synchronized with the clock on the Kerberos server. The Kerberos authentication model attaches timestamps to the packets sent between the SCS and Kerberos server to prevent replay attacks. The SCS timestamp is only allowed to deviate 5 minutes from the Kerberos server clock before the packet is considered invalid, which would result in a failed authentication attempt.

   To synchronize the SCS and the Kerberos clock, use the **Set/Define IP Timeserver** command:

   Figure 11-24: Synchronizing the Clocks

   ```
   Local>> DEFINE IP TIMESERVER 192.0.1.110
   ```

2. Designate a precedence number for the Kerberos server.

   Figure 11-25: Configuring Kerberos Precedence

   ```
   Local>> DEFINE AUTHENTICATION KERBEROS PRECEDENCE 2
   ```

3. Configure the primary and secondary Kerberos server locations by IP address:

   Figure 11-26: Configuring Kerberos Server Locations

   ```
   Local>> DEFINE AUTHENTICATION KERBEROS PRIMARY 192.0.1.52
   Local>> DEFINE AUTHENTICATION KERBEROS SECONDARY 192.0.1.53
   ```

4. Configure the realm. The **realm** is the name of the Kerberos administrative region that defines the scope of client authentication data maintained by a Kerberos server. Most installations choose realm names that mirror their Internet domain name system. To specify the realm, use the **Set/Define Authentication Kerberos Realm** command.

   Figure 11-27: Configuring the Kerberos Realm

   ```
   Local>> DEFINE AUTHENTICATION KERBEROS REALM “phred.com”
   ```

   Note: *The value for realm is case-sensitive. Enclose this string in quotes to retain case.*

5. Configure the **principle**, **instance**, and **authenticator** that enable the Kerberos server to identify the SCS. Principle, instance, and authenticator entries must be configured on the SCS to match the corresponding entries on the Kerberos server.

   The default setting for the SCS principle is **rcmd**; for the SCS instance, the default setting is **scs**.

   The authenticator is the password for the principle/instance pair. It must be defined on the SCS and the Kerberos server. A text string or an eight-byte hexadecimal value may be specified.

To specify the SCS principle, instance, and authenticator, use the Set/Define Authentication Kerberos command:

Figure 11-28: Configuring the Principle, Instance, and Authenticator

```
Local>> DEFINE AUTHENTICATION KERBEROS PRINCIPLE "kerbauth"
Local>> DEFINE AUTHENTICATION KERBEROS INSTANCE "scsname"
Local>> DEFINE AUTHENTICATION KERBEROS AUTHENTICATOR "passwd"
Local>> DEFINE AUTHENTICATION KERBEROS AUTHENTICATOR 0x08FF6D3E97735421
```

Note: *The values for principle, instance, and authenticator are case-sensitive. Enclose these strings in quotes to retain case.*

6 Configure the Key Version Number (KVNO). The key version number ensures that the SCS and Kerberos server are using the correct authenticator for the defined principle/instance pair. A KVNO must be configured on the SCS to match the KVNO on the Kerberos server.

To configure the SCS KVNO, use the **Set/Define Authentication Kerberos KVNO** command.

Figure 11-29: Configuring the SCS KVNO

```
Local>> DEFINE AUTHENTICATION KERBEROS KVNO 1
```

Note: *By default, the KVNO is set to 1.*

For additional Kerberos configuration instructions, see **Set/Define Authentication** on page 12-153.

11.4.3 RADIUS

The SCS supports the Remote Authentication for Dial-In User Services (RADIUS) protocol. RADIUS is a centrally-located client-server security system.

Note: *The SCS supports RADIUS as described in RFC 2138 and is intended to support future versions when they become available.*

RADIUS is geared towards large networks that have many communications servers, or many users for which explicit security measures must be enforced. Its advantages are:

- Authentication information for multiple users, in multiple forms, can be stored in a single RADIUS server.
- The RADIUS server can be part of a local or wide-area network.
- RADIUS can be used with Kerberos and CHAP/PAP security.
- Passwords are not transmitted across the network in readable form.

Disadvantages include:

- Keeping authentication information on one server can be dangerous; the server should be backed up regularly.
- Those wishing to use RADIUS must use one of the database types that RADIUS supports (currently local RADIUS databases, UNIX password files, NIS files, Kerberos databases, and TACACS).
- RADIUS servers are subject to security attacks from users already on the network. More information can be found in the RFC 2058 and in your RADIUS server's documentation.

RADIUS consists of two parts: authentication and accounting. Authentication is handled by the RADIUS authentication server, which stores authentication information configured by the network administrator. Accounting is handled by the RADIUS accounting server, which stores statistical information about authenticated connections. RADIUS accounting and authentication can be implemented independently of one another.

11.4.3.1 RADIUS Authentication

The general process of SCS user authentication using a RADIUS server is explained below.

1. A user connects to the SCS. The SCS prompt the user for a username and password, or CHAP/PAP authentication information if CHAP or PAP is configured.
2. The SCS creates an Access-Request packet that includes the username/password pair, an identification string for the SCS, the port being used for the modem connection, the port type, and other information as needed (see *Authentication Attributes* in Appendix D for more information). The SCS then encrypts the password and sends the packet to the RADIUS authentication server.

   Note: *CHAP responses sent from the user's PPP software to the SCS are not encrypted beyond what is inherent to the operation of CHAP.*

3 The RADIUS authentication server decrypts the Access-Request packet and routes it to the appropriate security checking mechanism, such as a UNIX password file or Kerberos database. Based on the information returned from the security check, one of the following occurs:

A If authentication is successful, the server sends an authentication acknowledgement (Access-Accept) packet to the SCS. The packet may contain additional information about the user's network system and connection requirements, such as the type of connection required and filtering information. The user is connected to a site or destination node if appropriate.

Note: *See Appendix D, Supported RADIUS Attributes, for more information about using filters with RADIUS.*

B If authentication fails, the server sends an Access-Reject packet to the SCS. The SCS will move on to the authentication method at the next precedence level, or terminate the connection if all methods have been tried.

C The server may be configured to send a challenge to the user after attempting to log in. If this is the case, the SCS will print the server's challenge and prompt the user to enter a response. The user must respond to the challenge, at which time step 3 is repeated using the response in place of the password in the Access-Request Packet.

Note: *In order to respond to the challenge, the user must be in character mode which precludes the use of PAP or CHAP for authenticating the user. See RADIUS and Sites on page 11-16.*

To configure the SCS for RADIUS authentication, use the **Set/Define Authentication RADIUS** commands.

Figure 11-30: Configuring the SCS to use RADIUS Authentication

```
Local>> DEFINE AUTHENTICATION RADIUS PRECEDENCE 5
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.77
Local>> DEFINE AUTHENTICATION RADIUS SECONDARY 192.0.1.78 PORT 1620
```

In the example above, the third command tells the SCS to use port 1620 on the secondary RADIUS authentication server rather than the default RADIUS authentication port (port 1812).

Note: *See Set/Define Authentication RADIUS on page 12-157 for complete syntax and information.*

The secret string configured for the SCS must match that of the RADIUS server being used for authentication.

Figure 11-31: Configuring the RADIUS Server

```
Local>> DEFINE AUTHENTICATION RADIUS SECRET "ok829dsnva1843qx"
```

For security reasons, it is recommended that you choose a secret string of at least 16 characters containing no obvious or easily-guessable items (such as names, phone numbers, or words that can be found in a dictionary).

11.4.3.2 RADIUS and Character Logins

When a user attempts to log into the SCS via a character-mode session (i.e. not through PPP or SLIP), the SCS reports a Service-Type of **Login:** to the RADIUS server. Once the server authenticates the user, it will send one of three possible Service-Types to the SCS:

Login	The SCS allows the user to log into the SCS, but immediately connects the user (via Telnet or Rlogin) to a remote host. To specify the remote host, see *Login-IP-Host* on page D-3. If no host is found, the user receives an error message and is logged out.
Callback-Login	The SCS disconnects the user, then attempts to dialback to the user. If dialback succeeds, the user will be connected to a remote host as in the normal "Login" described above.
Prompt	The SCS assumes that the user is an administrative user, and presents the user with a Local> prompt. The user will not be forced to a remote host.

Different RADIUS software packages may have different names for these Login types. In particular, the "Prompt" type may be referred to as "Administrative User" or "Admin." It will be distinct from the basic "Login" type. Consult your RADIUS server's documentation for specifics.

11.4.3.3 RADIUS and Sites

When a user logs in via PPP or SLIP, the SCS looks for a site that has the same name as the user. If it finds a matching site, it starts the site and modifies it with whatever additional setup information the RADIUS server sends it in its Access-Accept packet (see Step A under). If it does not find a matching site, it starts and modifies a copy of the default site.

Note: *Unless RADIUS specifically overrules a setting, the site's settings apply.*

If a user logs in using local mode but the RADIUS server indicates that the user should be using PPP or SLIP, the Set Site sitename Logout command will be executed where sitename is the name of the RADIUS site created for this user.

Note: *Setting up sites for specific users should be done sparingly, and only when a user has special connection requirements that can't be met otherwise.*

If, on the other hand, the RADIUS server detects that a user logging in via PPP should actually be a local mode user, the connection will be denied. The reason for this is two-fold: the user would not be able to return to the local prompt once in PPP mode, and allowing the connection may create a security hole.

11.4.3.4 RADIUS Accounting

A RADIUS accounting server creates an accounting log based on information that it gets from its client, such as an SCS. The server also responds to the client so that the client knows its packets reached the accounting server intact.

The SCS sends four types of packets to the accounting server:

Accounting-On	Sent each time accounting is enabled or re-enabled on the SCS, and when the SCS boots with accounting enabled.

Accounting-Start Send when a user logs into the SCS. This type of packet includes the user's name, port number, and current configuration.

Note: *EZWebCon users are logged as administrators.*

Accounting-Stop Send when a connection is logged out or otherwise terminated. This type of packet includes the user's name, reason for logout, length of connection, and the counts of bytes and packets sent and received.

Accounting-Off Sent when accounting is disabled on the SCS, and when the SCS is about to shut down or reboot.

Accounting-Start and Accounting-Stop packets contain session IDs that are used to match them together. In order to generate the proper session IDs, the SCS must know the current time. It can be told the correct time by a timeserver (configured with **Set/Define IP Timeserver**) or by its internal clock (configured with **Set/ Define Server Clock**). If the current time is not set properly, accounting packets may carry non-unique session IDs and cause problems in the accounting log.

Note: *See Supported RADIUS Attributes, Appendix D, for more information on the types of information that are included in accounting packets.*

To configure the SCS to send accounting information to the RADIUS accounting server, enter the **Set/ Define Authentication RADIUS Accounting** command.

Figure 11-32: Configuring the SCS to use RADIUS Accounting

```
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING ENABLED
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING PRIMARY 192.0.1.130
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING SECONDARY 192.0.1.131
```

The default RADIUS Accounting port is port 1646. A different port can be specified by adding the Port parameter to the command as shown in the third line of Figure 11-30.

11.4.4 SecurID

The SCS supports the ACE/Server security system manufactured by Security Dynamics Technologies Inc. ACE/Server is a system of UNIX-based client-server software and accompanying token cards.

Note: *Refer to your Security Dynamics documentation for ACE/Server installation instructions.*

The SecurID card generates single-use, unpredictable numerical codes. These "cardcodes," together with the user's PIN, form the basis of the SecurID authentication. The PIN and generated cardcodes are referred to collectively as SecurID passcodes. To gain access to a network protected by SecurID, both elements of the passcode must be entered correctly.

SecurID advantages include the following:

- Three items are required for authentication: the token card, PIN, and user ID.
- The card's cardcode is constantly changing, thus changing the passcode that the user enters.

- If someone eavesdrops on a connection attempt and obtains a passcode, the passcode will not be useful; a new passcode will be required in a few minutes. This enhances the security of Telnet connections.

Disadvantages include:

- If the caller attempts to use CHAP for authentication, SecurID cannot be used.
- Users are required to carry the token card.
- SecurID cannot be used for LAN to LAN connections, as the SCS has no way to generate passcodes.
- The SecurID server must be configured.

Note: *SecurID authentication is case-sensitive.*

The Security Dynamics SecurID system requires communication between the ACE/Server and the end-user. For example, the user must enter a new PIN when a SecurID card is first used, and a second passcode when locked out.

PAP does not allow for these types of messages or additional user input. Therefore, it is strongly recommended that SecurID be run from character mode only. It is possible to use SecurID with PAP, provided that situations like those mentioned above are either prevented or handled in text mode on the next call.

11.4.4.1 Configuring SecurID

To log into the SCS, the user must enter a username at the username prompt, and the passcode at the password prompt.

To specify the SecurID ACE/Server for authentication of username/passcodes, use the Set/Define Authentication SecurID command:

Figure 11-33: Configuring the SCS to Use SecurID

```
Local>> DEFINE AUTHENTICATION SECURID PRECEDENCE 4
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.50
Local>> DEFINE AUTHENTICATION SECURID SECONDARY 192.0.1.51
```

After SecurID is configured on the SCS, the SCS will receive further configuration information from the ACE/Server. However, this only happens the first time that the SCS and ACE/Server communicate. If you purge the authentication information on the SCS or change the precedence of SecurID, this learned information will be lost. You will need to have your ACE/Server administrator reinitialize the SCS with ACE/Server for SecurID to function properly again.

If SecurID receives repeated authentication requests for an invalid username/password pair, it assumes that a login attack is taking place. SecurID will react by continually slowing its responses to the SCS. This problem can be avoided by ensuring that SecurID has the highest precedence number. For example, if you're using SecurID, Kerberos, and a UNIX password file, set SecurID's precedence to 3.

For additional SecurID configuration instructions, see **Set/Define Authentication SecurID** on page 12-159.

11.4.5 UNIX Password File

Trivial File Transfer Protocol (TFTP) can be used to retrieve files from remote systems. During authentication, the SCS can TFTP a UNIX password file and check the username and password fields for the pair provided by a user. The SCS cannot add, modify, or delete password file entries.

Note: *The TFTP file is stored in UNIX /etc/passwd format. It must be in a location reachable via TFTP.*

UNIX password files are advantageous because existing UNIX password files can be used. Their main disadvantage is that TFTP poses a security risk. If the SCS can retrieve the file, chances are that other hosts on the network can retrieve the file and potentially crack the passwords. If your network is not trusted, you may not want to use TFTP authentication.

Note: *UNIX password file authentication is case-sensitive.*

To use a UNIX password file to authenticate users, use the **Set/Define Authentication TFTP** command:

Figure 11-34: Configuring the SCS to Use a UNIX Password File

```
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 5
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.50
Local>> DEFINE AUTHENTICATION TFTP SECONDARY 192.0.1.51
```

Specify the full pathname of the password file using the **Set/Define Authentication TFTP Filename** command:

Figure 11-35: Specifying the Pathname of the Password File

```
Local>> DEFINE AUTHENTICATION TFTP FILENAME "/tftpboot/passwd"
```

11.5 User Restrictions

Individual SCS users may be restricted in a number of ways. They may be prevented from using particular commands, forced to use a certain configuration, or forced to use a particular IP address.

11.5.1 Privileged Commands

Many of the SCS commands require privileged user (superuser) status. To become the privileged user, use the **Set Privileged** command. The default privileged password is system.

Figure 11-36: Set Privileged Command

```
Local>> SET PRIVILEGED
Password> system (not echoed)
Local>>
```

Note: *To change the privileged password, use the Set/Define Server Privileged Password command, described on page 12-123.*

Only one user may have privileged status at any time. If another user currently has privileged status, the **Set Privileged Override** command may be used to forcibly become the privileged user. To stop being the privileged user, use the **Set Noprivileged** command.

11.5.2 IP Address Restriction

To avoid routing problems and enhance security, the SCS can restrict incoming remote networking callers to a particular address or range of addresses.

Each site may specify a particular range of acceptable IP addresses. When an incoming caller requests to use a specific address, it will be compared to this range. If the address falls within the range, the connection will be permitted, if not, the connection attempt will fail.

To specify the beginning and end of the range, use the **Define Site IP Remoteaddress** command. Two addresses must be specified: the beginning of the range and the end of the range.

Figure 11-37: Specifying Range of Addresses

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.254
```

Callers will not be permitted to use IP addresses with the host part of the address set to all zeroes or all ones. These addresses are reserved to identify broadcast packets. If the range that you specify includes such an address (for example, 192.4.5.0 or 192.4.5.255) and a caller requests this address, the connection will not be permitted.

Note: *For more information on IP address assignment, see IP Address Negotiation on page 4-7.*

11.5.3 Controlling Use of Set PPP/SLIP Commands

In order for incoming callers to start PPP or SLIP with the **Set PPP/SLIP** commands, PPP or SLIP must be enabled on the port receiving the call. By default, PPP and SLIP are disabled.

To enable or disable PPP or SLIP on a port, use the **Define Ports PPP/Define Ports SLIP** commands:

Figure 11-38: Disabling PPP and SLIP

```
Local>> DEFINE PORT 2 PPP DISABLED
Local>> DEFINE PORT 2 SLIP DISABLED
```

11.5.4 Securing a Port

When a port is secure, users on that port will be prevented from editing many of the port's settings. In addition, they will only be able to display a limited amount of information using Show/Monitor/List commands.

Note: *Users logged in on secure ports cannot become privileged users.*

It is recommended to secure ports used for public use; for example, ports used for public dial-in modem pools. To secure a port, use the **Set/Define Ports Security** command:

Figure 11-39: Securing a Port

```
Local>> DEFINE PORT 2 SECURITY ENABLED
```

Note: *The complete syntax of Set/Define Ports Security is discussed on page 12-85.*

11.5.5 Locking a Port

The Lock command may be used to secure a port without disconnecting sessions. When **Lock** is entered, the user will be prompted to enter a password. This port will then be locked until this password is used to unlock it. Figure 11-40 displays an example:

Figure 11-40: Locking and Unlocking a Port

```
Local> LOCK
Password> donut (not echoed)
Verification> donut (not echoed)
Unlock password> donut (not echoed)
Local>
```

Note: *Secure ports (set using the Set/Define Ports Security command) cannot be locked.*

To unlock a port without the Lock password, a privileged user must use the **Unlock Port** command (discussed on page 12-100) or log out the port using the **Logout Port** command (discussed on page 12-53). Logout will disconnect all sessions.

11.5.6 Forcing Execution of Commands

When a username is entered in the local authentication database (NVR), a series of commands may be associated with that user. These commands will be executed when the user is successfully authenticated.

To execute commands when the user logs into the SCS, first ensure that authentication databases have been configured; see *Database Configuration* on page 11-9 for instructions. Then associate commands with the username using the **Set/Define Authentication User Command** command. The commands you specify will be executed when the user is successfully authenticated.

Figure 11-41: Forcing User to Start a Particular Site

```
Local>> DEFINE AUTHENTICATION USER bob COMMAND "SET PPP dialin_users; logout"
```

In the previous example, when user bob logs into the SCS, he will automatically start PPP and run the site dialin_users.

To ensure that the user is not left at the Local> prompt after the forced command finishes executing, the string “;logout” may be added.

11.5.7 Restricting Multiple Authenticated Logins

The **Set/Define Authentication Unique Enabled** command can be used to prevent a single PPP or Local mode user from making multiple authenticated connections to the SCS.

For example, imagine that ports 1 through 8 have authentication enabled, but ports 9 through 16 do not. If user george connects to port 2 and enters the correct password, he will be permitted to login. If, while george is connected to port2, another user tries to log into port3 using george as his username, he will be rejected.

Unique authentication applies only to ports that have authentication enabled. If user george connects to port2 and then attempts a second connection to port9, the second login will be allowed because port9 does not have authentication enabled. Similarly, if george attempts an authenticated login to port 2 after another user has logged into port9 with username george, he will succeed (provided that he enters the correct password) because he is the first user to log in as george on an authenticated port.

To enable unique authentication, enter the following command:

Figure 11-42: Preventing Multiple Authenticated Logins By Single Users

```
Local>> DEFINE AUTHENTICATION UNIQUE ENABLED
```

11.6 Network Restrictions

11.6.1 Incoming Telnet/Rlogin Connections

Incoming Telnet and Rlogin connections can be permitted without restriction, password protected, or prevented entirely. By default, incoming Telnet and Rlogin connections are permitted without entering the login password; to change this configuration, use the **Set/Define Server Incoming** command:

Figure 11-43: Preventing Incoming Telnet/Rlogin Logins

```
Local>> DEFINE SERVER INCOMING NONE
Local>> DEFINE SERVER INCOMING PASSWORD
Local>> DEFINE SERVER INCOMING SECURE
```

Note: *The complete syntax of the Set/Define Server Incoming command is discussed on page 12-119.*

In Figure 11-43, the first command prevents all incoming Telnet and Rlogin connections. The second command permits the connections, but requires that the login password be entered before the connection is permitted. The third command disables incoming Telnet and Rlogin (along with 200x and 300x ports). See *Set/Define Server Incoming* on page 12-119 for more information.

When Incoming None is specified, incoming SSH connections are also denied. The other parameters do not affect incoming SSH connections.

11.6.2 Outgoing Rlogin Connections

The **Set/Define Server Rlogin** setting controls whether or not outgoing Rlogin connections are permitted. By default, outgoing Rlogin is disabled; to change this setting, use the following command:

Figure 11-44: Permitting Outgoing Rlogin Connections

```
Local>> DEFINE SERVER RLOGIN ENABLED
```

11.6.3 Limiting Port Access

A port's access may be set to one of the following: dynamic, local, remote, or none. **Dynamic** permits both local and remote logins, **local** permits only local logins, and **remote** permits only remote logins. **None** prevents all incoming and outgoing connections; the port is unusable.

To configure a port's access setting, use the **Set/Define Ports Access** command.

Figure 11-45: Configuring Connection Type

```
Local>> DEFINE PORT 2 ACCESS REMOTE
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

Note: *For more information about configuring a port's access, refer to Setting Port Access on page 8-1.*

11.6.4 Disabling the FTP and HTTP Servers

The server contains on-board FTP and HTTP servers. You can choose to disable one or both of these servers using the **Set/Define Protocol FTP** and **Set/Define Protocol HTTP** commands.

Figure 11-46: Disabling the HTTP and FTP Servers

```
Local>> DEFINE PROTOCOL FTP DISABLED
Local>> DEFINE PROTOCOL HTTP DISABLED
```

If you choose to disable the HTTP server, you will not be able to use the web browser interface for configuration. You will also not be able to use the URL to find the log file when you receive email notifications of serial events (see *Email Alerts for Serial Events* on page 3-3).

11.6.5 Packet Filters and Firewalls

Filters enable the SCS to restrict packet traffic. Each filter specifies a particular rule, for example, only IP packets will be permitted passage. Packets that pass the filter will be forwarded; packets that don't will be discarded.

Filters are organized into ordered filter lists, which are referenced by name. For example, a filter named firewall may permit forwarding of packets that match a particular IP rule, but deny passage to packets that match a generic rule.

Note: *For a complete explanation of filter rules, see Set/Define Filter on page 12-166.*

Filter lists are associated with sites. Sites use filter lists for the following purposes:

Table 11-1: Types of Filter Lists

Type of Filter List	Purpose
Idle	Determines whether the site will remain active. Packets that pass the filter will reset the site's idle timer, preventing the site from being timed out.

Table 11-1: Types of Filter Lists

Type of Filter List	Purpose
Incoming	Determines whether to forward incoming packets received from a remote site. Packets that pass the filter will be forwarded.
Outgoing	Determines whether to forward outgoing packets to a remote site. Packets that pass the filter will be forwarded.
Startup	Determines whether a site will initiate a connection to a remote site. When a packet passes the filter, the SCS will initiate an outgoing connection. (If an outgoing connection currently exists, this filter will be ignored.)

When a site with an associated filter list receives a packet, the SCS will compare the packet against each filter starting with the first filter on the list. If the packet matches any of the filters, the packet will be forwarded or discarded to the filter's specification. If the packet does not match any of the filters in the list, it will not be forwarded.

11.6.5.1 Filter Order

The order that filters appear in a list is important. For example, consider the following filter list:

- Allow any packets
- Deny all IP traffic matching a particular rule

When this filter list is associated with a site, all packets will be forwarded. Packets will be compared to the first filter in the list, and all packets will match specification "any packets." Therefore, all packets will be forwarded without being compared to the second filter.

Switching the order of the two filters will have very different effects. Examine the filter list below, where the order of the two filters is reversed.

- Deny all IP traffic matching a particular rule
- Allow any packets

When this filter list is used, any IP traffic matching the specified rule will be discarded. Therefore, some IP packets will be discarded without being compared to the second filter.

11.6.5.2 Preventing All IP Traffic

To prevent all IP packet traffic, you do not need to use a filter list. Instead, use the **Define Site IP Disabled** command.

Figure 11-47: Preventing IP Packet Traffic

```
Local>> DEFINE SITE irvine IP DISABLED
```

11.6.5.3 Setting Up a Filter List

Configuring filter lists involves two primary steps: creating the filter list, and associating the list with a particular site.

1 When a filter list is created, it must be assigned a name of no more than 12 characters. The remainder of the configuration consists of a series of rules that will filter packet traffic in a particular way.

Use the **Set/Define Filter** command to create a new filter.

Figure 11-48: Define Filter Command

```
Local>> DEFINE FILTER firewall ADD 1 DENY IP SRC 192.0.1.0 255.255.255.0
```

Each rule is assigned a particular position in the filter list, denoted by a number. In Figure 11-48, the rule **Deny IP** will be added to the **firewall** filter in the first position of the list. If a position number isn't specified with the Set/Define Filter command, the rule will be added to the end of the filter list.

Note: *Set/Define Filter has many parameters, which are described in detail on page 12-166.*

2 A single filter list can be associated with many sites. Each site may use a filter list as an incoming, outgoing, startup, or idle filter.

Note: *Filter list types are described in Table 11-1 on page 11-23.*

To associate a filter list with a site, use the **Define Site Filter** command.

Figure 11-49: Associating a Filter List With Sites

```
Local>> DEFINE SITE irvine FILTER IDLE firewall
Local>> DEFINE SITE dallas FILTER INCOMING firewall
```

In Figure 11-49, filter **firewall** will be used as an idle filter for site irvine, and as an incoming filter for site **dallas**. An example firewall is described in *Creating a Firewall* on page 11-30

Note: *Filters can also be used with RADIUS. See Filter-ID on page D-3 for more information.*

11.7 Event Logging

Event logging enables a network administrator to track network and user activity. Logging can be configured at a number of levels. For example, one level of logging may record only system problems related to authentication, and another level may record all authentication activities (all passwords).

11.7.1 Setting the Destination

In order to use logging, the SCS must be configured to send logging information to one of the following destinations:

- A TCP/IP host running syslog
- SCS memory
- The SCS serial console port, typically port 1
- A file stored locally on the SCS. The default disk location is /ram.

To specify the logging destination, use the **Set/Define LoggingDestination** command. A colon must be appended to the IP address or IP host name.

Figure 11-50: Specifying Logging Destination

```
Local>> DEFINE LOGGING DESTINATION CONSOLE
Local>> DEFINE LOGGING DESTINATION 192.0.1.5:1
Local>> DEFINE LOGGING DESTINATION MEMORY
Local>> DEFINE LOGGING DESTINATION FILE syslog
```

Note: *The complete syntax of Set/Define Logging is given on page 12-172.*

To see logging information that is stored in the SCS memory, enter the **Show/Monitor/List Logging Memory** command. The following command will display the log and update the display continuously.

Figure 11-51: Displaying Logging Saved to Memory

```
Local>> MONITOR LOGGING MEMORY
```

11.7.2 Logging Levels

The following table lists the different areas that can be logged and the logging options available for each area:

Table 11-2: Events Logged by the SCS

To Log Events Associated With:	The Following Options are Available: (Numbers Reflect Logging Level)	
Authentication	1	System Problems
	2	Failures and Successes
	3	All Logins and Logouts
	4	Incorrect Passwords
	5	All Passwords, and RADIUS Warnings
Commands		Enabled
		Disabled
Dialback	1	Problems
	2	Unauthorized Users
	3	Dialback Failures
	4	Dialback Successes
	5	Dialback Attempts
	6	Modem Chat
IP	1	Errors
	2	Packets that Trigger Remote Connections
	3	Routing Table/Interface Changes

Table 11-2: Events Logged by the SCS, cont.

To Log Events Associated With:	The Following Options are Available: (Numbers Reflect Logging Level)	
	4	Incoming/Outgoing RIP Packets
	5	Resulting Routing Table
	6	Contents of All RIP Packets
	7	Routed Packets
Modems	1	Problems
	2	Call Statistics Dump From Modem
	3	Setup
Networks		Enabled
		Disabled
PPP	1	Local System Problems
	2	Remote System Problems
	3	Negotiation Failures
	4	Negotiation Data
	5	State Transitions
	6	Full Debugging
Printers		Enabled
		Disabled
Sites	1	Usage Summary
	2	Detailed Usage Summary
	3	Errors
	4	Connections
	5	Bandwidth
	6	Network Addressing
	7	Chat Scripts
	8	Modems and Dialback
System		Enabled
		Disabled

For example, to record all logins and send the information to the console port, use the following command:

Figure 11-52: Logging All Logins

```
Local>> DEFINE LOGGING AUTHENTICATION 3
```

Note: *Logging passwords may compromise security.*

Each logging level logs all events associated with higher logging levels. For example, if logging level 6 is specified, the events associated with levels 1-5 will also be logged.

To disable all logging, use the following command:

Figure 11-53: Disabling Event Logging

```
Local>> DEFINE LOGGING DESTINATION NONE
```

11.8 Examples

11.8.1 Database Search Order

The SCS must be configured for authentication using a UNIX password file. The configuration must meet the following criteria:

- A large group of users is listed in a RADIUS authentication database. The RADIUS server's IP address is 192.0.1.55, and port 1640 is used rather than the default RADIUS authentication port.
- Two other groups of users are listed in UNIX password files; the files are on hosts 192.0.1.87 and 192.0.1.99.
- Any additional users will be added to the local database.
- A RADIUS accounting server has been set up at host 192.0.1.176 to log accounting information.

Figure 11-54 shows how to configure the SCS in this situation:

Figure 11-54: Configuring Database Order

```
Local>> DEFINE AUTHENTICATION RADIUS PRECEDENCE 2
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.55 PORT 1640
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 3
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.87
Local>> DEFINE AUTHENTICATION TFTP SECONDARY 192.0.1.99
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 4
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING ENABLED
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING PRIMARY 192.0.1.176
```

11.8.2 Terminal User Forced to Execute Command

Terminal user **jerry** does not have an existing account on UNIX. He will only use the SCS to Telnet to his own remote host, **venus**. The following figure shows the commands necessary to add jerry to the local database.

Figure 11-55: A Single User Entry

```
Local>> DEFINE AUTHENTICATION USER "jerry" PASSWORD "3no37" COMMAND "TELNET
venus;LOGOUT" ALTER DISABLED
```

When jerry connects to the SCS, he is prompted for a login password, then his own username and password. When authenticated, he is automatically telnetted to host venus and logged out of the SCS.

Jerry will see the following:

Figure 11-56: Results of User Authentication with Command

```
Type HELP at the 'Local_1>' prompt for assistance.

Login password> badger (not echoed)
Username> jerry
Password> 3no37 (not echoed)

Telnet/TCP protocol emulation v2.2
SunOS UNIX (venus)
Login:_
```

11.8.3 Multiple-User Authentication

A large number of users need to connect to the SCS. These users must be authenticated. The SCS must be configured to meet the following criteria:

- All users will connect to port 2.
- 50 users have their usernames and passwords stored in a UNIX password file.
- Another 20 users are PPP users that share site **pppUsers** for their connections. This site's password is **special**.
- There is one SLIP user that will use site **SlipMan**. This site has password **exception**; once the password is entered, the site must automatically enter SLIP mode.

Port 2 must be configured to automatically detect PPP so that it can begin running PPP and CHAP when necessary. The port must not be dedicated to PPP, however, because other connections will be using the same port.

In order to authenticate the SLIP user, SLIPdetect must be disabled. Figure 11-57 displays the commands necessary for this configuration:

Figure 11-57: Authentication for Multiple Users

```
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 1
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.88
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED

Local>> DEFINE SITE PPPusers LOCAL "special"
Local>> DEFINE PORT 2 PPPDETECT ENABLED

Local>> DEFINE PORT 2 SLIPDETECT DISABLED
Local>> DEFINE SITE "SlipMan" IP REMOTEADDRESS 192.0.1.17
Local>> DEFINE SITE "SlipMan" LOCAL "exception"
Local>> DEFINE SITE "SlipMan" PROTOCOL SLIP
```

11.8.4 Outgoing LAN to LAN Connection

An SCS in Dallas must connect to an SCS in Seattle. The Dallas SCS must be configured in the following manner:

- The SCS in Dallas must have a site for the connection to the Seattle SCS. The site's name is **seattle**.
- PPP will be used for the connection.
- PAP authentication will be used.
- To authenticate itself, the SCS in Dallas must send username **dallas** and password **texas**.

The following commands must be entered on the Dallas SCS:

Figure 11-58: Configuring Remote Site Authentication

```
Local>> DEFINE SITE seattle AUTHENTICATION PAP ENABLED
Local>> DEFINE SITE seattle AUTHENTICATION USERNAME dallas
Local>> DEFINE SITE seattle AUTHENTICATION REMOTE "texas"
```

11.8.5 Creating a Firewall

If your site involves an internet connection, it is a good idea to set up a firewall to augment current security. A firewall prevents outside users from freely accessing your network by controlling which services on your network are available to internet users.

A local network consists of addresses **192.0.1.0** through **192.0.1.24**. Site **irvine** is used to manage connections to this network. Irvine requires a firewall that does the following:

- Prevents IP spoofing
- Permits outgoing Telnet connections
- Permits SMTP (Simple Mail Transfer Protocol) traffic to the local SMTP server, **192.0.1.102**. The backup SMTP server is **192.0.1.103**
- Permits NNTP (Network News Transfer Protocol) traffic between the local NNTP server, **192.0.1.104**, and the remote NNTP server, **192.0.2.100**
- Permits outgoing FTP connections

- Denies X-Windows traffic, but permits incoming TCP/IP traffic to ports 1023 and higher.
- Permits DNS queries to the local Domain Name Server, **192.0.1.101**
- Permits ICMP (Internet Control Message Protocol) messages
- Permits outgoing finger requests

The firewall will be named **fw_i**. Packets that do not specifically match the filters in fw_i will be denied passage through the SCS.

Note: *Due to the length of the commands in the following examples, the keywords Define and Filter are shortened to Def and Filt.*

The **Set/Define Filter Create** command is used to create the firewall.

Figure 11-59: Creating the Filter List

```
Local>> DEF FILT fw_i CREATE
```

To prevent IP spoofing, the **Define Filter Add Deny IP SRC** command is used. This filter will block any packets from an outside network that claim to have originated from the local network. This filter is placed at the beginning of the filter list; if it were not, spoofed IP packets could be permitted passage by filters positioned before this rule.

Figure 11-60: Preventing IP Spoofing

```
Local>> DEF FILT fw_i ADD DENY IP SRC 255.255.255.0 192.0.1.0
```

Note: *The CERT advisory on IP spoofing is available from ftp://cert.org/pub/cert_advisories/CA-95:01.IP.spoofing.*

To permit outgoing Telnet connections initiated from the local network, the following command is used:

Figure 11-61: Permitting Outgoing Telnet Connections

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ TELNET DPORT GT 1023 ACK
```

To permit SMTP traffic between the SCS and the local and backup SMTP servers, the following commands are required:

Figure 11-62: Permitting SMTP Traffic to SMTP Servers

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ SMTP SPORT GT 1023 DST 255.255.255.255 192.0.1.102
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ SMTP DPORT GT 1023 ACK DST 255.255.255.255. 192.0.1.102
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ SMTP SPORT GT 1023 DST 255.255.255.255 192.0.1.103
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ SMTP DPORT GT 1023 ACK DST 255.255.255.255 192.0.1.103
```

To permit NNTP traffic between the local and remote NNTP servers, the following commands are required:

Figure 11-63: Permitting Traffic Between NNTP Servers

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ NNTP SPORT GT 1023 DST 255.255.255.255 192.0.1.104 SRC
255.255.255.255 192.0.2.100
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ NNTP DPORT GT 1023 ACK DST 255.255.255.255 192.0.1.104
SRC 255.255.255.255 192.0.2.100
```

To permit outgoing FTP connections, the following commands are used:

Figure 11-64: Permitting Outgoing FTP Connections

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FTP DPORT GT 1023 ACK
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FTPDATA DPORT GT 1023
```

The following three commands deny incoming X-Windows traffic to well-known ports 6000-6023, but permit incoming TCP/IP connections to ports greater than 1023. This configuration also allows PASV-mode FTP data.

Figure 11-65: Controlling X-Windows Traffic

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT GT 1023 DPORT GT 6024 ACK
Local>> DEF FILT fw_i ADD DENY IP TCP SPORT GT 1023 DPORT GE 6000 ACK
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT GT 1023 DPORT GT 1023 ACK
```

The three commands below permit UDP- and TCP-based queries and answers to the local Domain Name Server:

Figure 11-66: Permitting DNS Queries

```
Local>> DEF FILT fw_i ADD ALLOW IP UDP DPORT EQ DNS DST 255.255.255.255 192.0.1.101
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ DNS SPORT GT 1023 DST 255.255.255.255 192.0.1.101
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ DNS DPORT GT 1023 ACK DST 255.255.255.255
192.0.1.101
```

To permit ICMP messages (except for redirect messages), a generic IP rule is defined:

Figure 11-67: Permitting ICMP Messages

```
Local>> DEF FILT fw_i ADD ALLOW IP ICMP IPGENERIC OFFSET 0 MASK 0xf0000000 NE 0x50000000
```

Outgoing finger requests are permitted and incoming requests are prevented using this command:

Figure 11-68: Permitting Outgoing Finger Requests

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FINGER DPORT GT 1023 ACK
```

To use firewall fw_i as an incoming filter list for site **irvine**, the **Define Site Filter Incoming** command is used:

Figure 11-69: Configuring a Firewall

```
Local>> DEF SITE irvine FILTER INCOMING fw_i
```

11.8.6 Dialback

An SCS must be configured to prevent all users from connecting with the exception of two users, **sam** and **paul**. When sam and paul attempt to connect to the SCS, the modem must dial them back to verify their identities.

The modem is connected to SCS port 2, and there isn't a corresponding modem profile. The generic modem profile must be used. The following example assumes that modem profile type 3 is the generic modem profile (Use the List Modem command to view available modem profiles).

Figure 11-70: Enabling Modem Handling/Selecting a Modem Type

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 3
%Info: Port speed changed to 57600.
%Info: Port flow control changed to CTS.
```

The following commands are used to configure dialback:

Figure 11-71: Configuring Dialback

```
Local>> DEFINE PORT 2 DIALBACK ENABLED
Local>> DEFINE DIALBACK sam "123-4567"
Local>> DEFINE DIALBACK paul "867-5309"
Local>> DEFINE DIALBACK BYPASS DISABLED
Local>> LOGOUT PORT 2
```

11.9 Troubleshooting

To troubleshoot authentication problems, use event logging. To configure event logging, use the **Set/Define Logging** command, discussed on page 12-172.

The following example assumes the terminal is connected to the console port (port 1).

Figure 11-72: Configuring Authentication Event Logging

```
Local>> SET LOGGING DESTINATION CONSOLE
Local>> SET LOGGING AUTHENTICATION 4
Fri Jan 26 13:44:40 1996 SCS_00DD12: SYSTEM: notice: log closed
Fri Jan 26 13:44:40 1996 SCS_00DD12: SYSTEM : notice: syslog started
Fri Jan 26 13:44:49 1996 SCS_00DD12: AUTH: info: Denied Port 4 User john Password badpass Method Local
Fri Jan 26 13:45:27 1996 SCS_00DD12: AUTH: info: Granted Port 4 User john Password goodpass Method Local
Fri Jan 26 13:45:39 1996 SCS_00DD12: AUTH: notice: Port 4 user john privilege password denied.
Fri Jan 26 13:45:49 1996 SCS_00DD12: AUTH: notice: Port 4 user john privilege password granted.
```

12: Command Reference

This chapter describes all commands that can be used with the SCS. To recap the types of commands (Set/Define, Show/Monitor/List, Clear/Purge), see Chapter 2, *Getting Started*.

Most Define commands are documented with their corresponding Set commands, but some are listed separately under the Define keyword. Monitor and List commands are documented with their corresponding Show commands. Most Purge commands are documented with their corresponding Clear commands, but some are listed separately under the Purge keyword.

The sections of this command reference chapter are divided as follows:

- *Navigation/Help Commands*, page 12-180, covers commands that provide basic navigation, help, and global status information.
- *IP/Network Commands*, page 12-18, includes commands for forming and configuring connections that use the IP protocol. This section also covers 802.11 networking, which is applicable only to the SCS200
- *Port Commands*, page 12-52, contains commands for serial and virtual port configuration.
- *Modem Commands*, page 12-3, describes the commands necessary for configuring the SCS to use an attached modem.
- *Service Commands*, page 12-101, covers commands that setup various services.
- *Server Commands*, page 12-111, includes commands that affect the whole SCS.
- *Site Commands*, page 12-132, describes the commands necessary to set up sites.
- *Security Commands*, page 12-151, includes the necessary instructions for enabling the SCS's security features.

12.1 Command Descriptions

Each command description includes the following:

- The command's full syntax, shown in diagram form
- Any restrictions on the command, such as whether you must be the privileged user to use it

  Note: *For information on becoming the privileged user, see Set Privileged/Noprivileged on page 12-92.*

- Potential errors that may be encountered when using the command
- Descriptions of each associated parameter. Multiple optional parameters can be entered on the same command line, subject to the maximum command line length of 312 characters.
- Default settings, where applicable

- Examples of the command
- Cross-references to related commands

12.2 About Strings

When a command calls for a string, the following two things must be taken into consideration.

First, any user-entered strings should be enclosed in quotes to retain the case entered. If a string is not enclosed in quotes, it will be changed to all uppercase characters, and any spaces will cause the SCS to interpret the different parts of the string as different command parameters.

In addition, string lengths are generally limited to thirty-one alphanumeric characters for pathnames and file server names, fifteen alphanumeric characters for filenames, and six alphabetic characters for the privileged and login passwords. When a string limit differs from the norm, its limitations are noted.

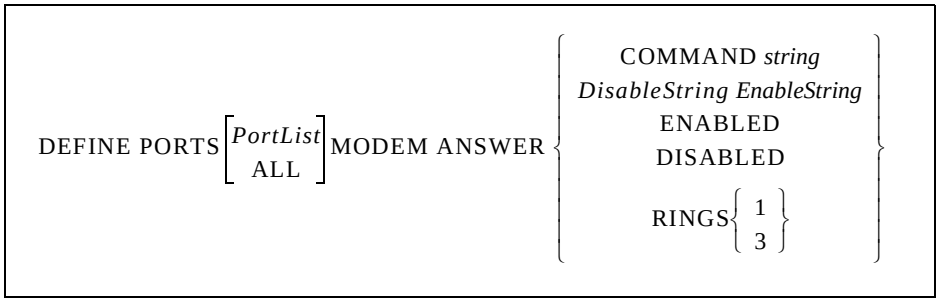
12.3 Conventions Used in This Chapter

The following conventions are used to explain the syntax of the commands:

- Optional parameters are enclosed in brackets **[]**; one or more of these parameters may be used, or the command can be used without adding any of these parameters.
- Required parameters are enclosed in curly braces **{}**; one and only one of these parameters must be used.
- User-supplied parameters, such as a particular port number or host name, are shown in *italics*.

12.4 Modem Commands

12.4.1 Define Ports Modem Answer



Permits or prevents a modem from automatically answering the line, optionally after a specified number of rings.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Command
Changes the answer command that is actually sent to the modem to make it answer the line. Commonly set to “A” or “ATA.”

DisableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be disabled. Commonly set to “s0=0.”

EnableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be enabled. Commonly set to “s0=1.”

Rings
Either enter 1 or 3 to tell the SCS how many rings to wait before answering the line. When Caller-ID is enabled, the ring value should be set to 3 to give the SCS time to gather Caller-ID information.

Defaults Disabled (no strings defined), 1 Ring

Examples

```
Local>> DEFINE PORT 2 MODEM ANSWER ENABLED
Local>> DEFINE PORT 2 MODEM ANSWER “s0=0” “s0=1”
```

See Also Define Ports Modem CallerID, page 12-5; *Profile Settings*, page 9-5; *Caller-ID*, page 9-12

12.4.2 Define Ports Modem Attention

Defines a string to get the modem's attention.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

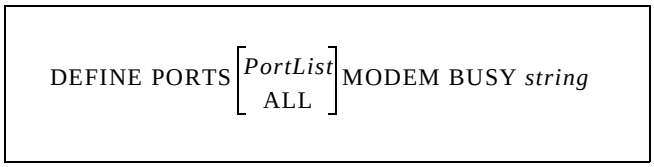
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM ATTENTION "at"
```

See Also *Profile Settings*, page 9-5

12.4.3 Define Ports Modem Busy



Defines a string that the SCS will expect from the modem on outbound calls to signal that the remote number is busy or otherwise unavailable.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to "BUSY."

Defaults Depends on modem and modem profile.

See Also *Profile Settings*, page 9-5

12.4.4 Define Ports Modem CallerID

Configures whether the SCS will look for and attempt to decode Caller-ID information for incoming calls. The SCS should be set to wait for three rings before answering the line so that it has enough time to gather the Caller-ID information. The ring setting can be configured with the Rings command.

Restrictions Requires privileged user status.

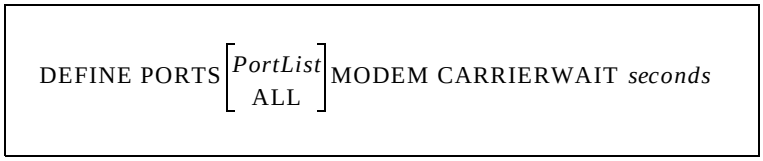
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Define Ports Modem Answer, page 12-3*; Caller-ID*, page 9-12

12.4.5 Define Ports Modem Carrierwait



Defines the length of time that a server will wait for a carrier on incoming and autodialed calls. If a carrier is not received in that length of time, the SCS assumes that it will not be received. The call will fail and the modem will be reset.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

seconds
A time value between 1 and 250 seconds.

Defaults 60 seconds

Examples Local>> DEFINE PORT 2 MODEM CARRIERWAIT 40

See Also *Profile Settings—Carrierwait String*, page 9-5

12.4.6 Define Ports Modem Commandprefix

DEFINE PORTS [*PortList* / ALL] MODEM COMMANDPREFIX *seconds*

Defines a string to send before the “Init” and other configuration strings.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to “at.”

Defaults Depends on modem and modem profile.

Examples Local>> DEFINE PORT 2 MODEM COMMANDPREFIX “at”

See Also *Profile Settings*, page 9-5

12.4.7 Define Ports Modem Compression

DEFINE PORTS [*PortList* / ALL] MODEM COMPRESSION { ENABLED / DISABLED / *DisableString EnableString* }

Enables or disables data compression in the modem.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

DisableString
A string of up to 12 characters. When this string is received by the modem, data compression will be disabled

Note: *The DisableString and the EnableString must be entered together.*

EnableString
A string up to 12 characters. When this string is received by the modem, data compression will be enabled.

Defaults Disabled (no strings defined)

Examples
```
Local>> DEFINE PORT 2 MODEM COMPRESSION ENABLED
Local>> DEFINE PORT 2 MODEM COMPRESSION "%c" "%c1"
```

See Also *Profile Settings*, page 9-5; *Compression*, page 9-9

12.4.8 Define Ports Modem Connected

DEFINE PORTS [*PortList* / ALL] MODEM CONNECTED *ConnectString*

Defines a string to expect on outbound calls when the modem is connected to the remote location.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

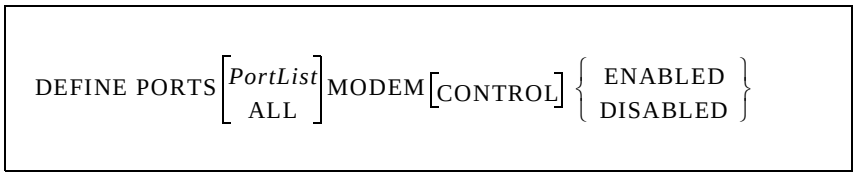
ConnectString
A string of up to 12 characters. Commonly set to "CONNECT."

Defaults Depends on modem and modem profile.

Examples
```
Local>> DEFINE PORT 2 MODEM CONNECT "CONNECT"
```

See Also *Profile Settings*, page 9-5

12.4.9 Define Ports Modem Control



Enables or disables modem handling on the specified port(s). When modem handling is enabled, the assertion and deassertion of modem signals (DSR, DTR, and DCD) control the port's interaction with the modem, including initializing the modem upon booting and resetting the modem between uses. The SCS monitors DCD to determine if a connection exists. If DCD drops, the SCS will log the port out and drop DTR.

Note: *Modem control is automatically enabled on ports that have modems attached (i.e. when you set the modem type with Define Ports Modem Type).*

Restrictions Requires privileged user status.

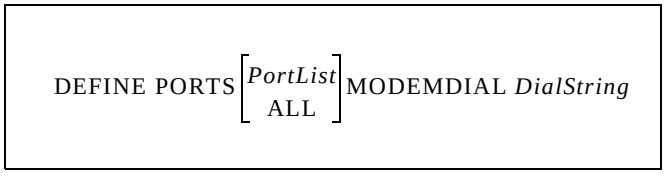
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Set/Define Ports DSRLogout, page 12-70; Show/Monitor/List Ports Modem, page 12-96; Chapter 9, *Modems*

12.4.10 Define Ports Modem Dial



Defines a string to send to the modem to cause it to dial. This string is preceded by the Commandprefix string.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

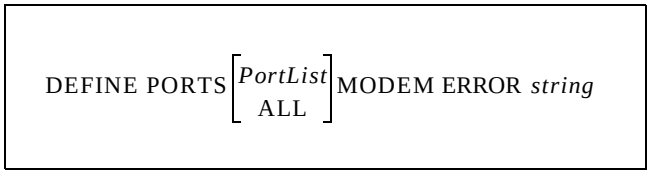
DialString
A string of up to 12 characters. Often touch tone dialing is activated with “dt” and pulse dialing is activated with “dp.”

Defaults Depends on modem and modem profile.

Examples
```
Local>> DEFINE PORT 2 MODEM DIAL “dt”
```

See Also Define Ports Modem Commandprefix, page 12-6; *Profile Settings*, page 9-5

12.4.11 Define Ports Modem Error



Defines a string to expect on outbound calls when the modem encounters an error.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

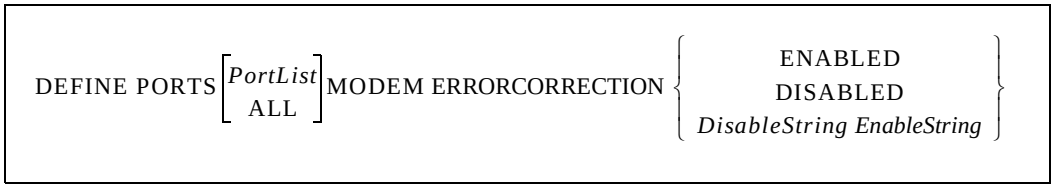
string
A string of up to 12 characters set to “ERROR” by default.

Defaults Depends on modem and modem profile.

Examples
```
Local>> DEFINE PORT 2 MODEM ERROR “ERROR”
```

See Also *Profile Settings*, page 9-5; Define Ports Modem Errorcorrection, page 12-10

12.4.12 Define Ports Modem Errorcorrection



Enables or disables error correction in the modem

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

DisableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be disabled.

EnableString
A string of up to 12 characters. When this string is received by the modem, error correction will be enabled.

Note: *The DisableString and the EnableString must be entered together.*

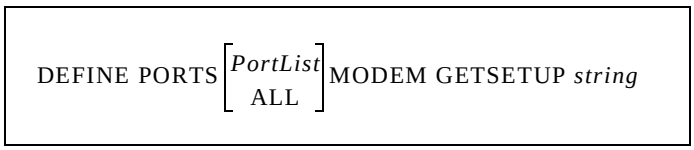
Defaults Disabled (no strings defined)

Examples

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION ENABLED
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION "&q5" "q0"
```

See Also *Profile Settings*, page 9-5; Define Ports Modem Error, page 12-9

12.4.13 Define Ports Modem Getsetup



Defines a string to send to the modem to cause it to return its setup. This string is preceded by the Commandprefix string. If the string is set to "", the SCS will not attempt to get the modem's setup. The SCS will always send the Save string after configuration. Modems that do not return their configuration in a single screen should do this.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to "&v."

Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM GETSETUP "&v"
```

See Also Define Ports Modem Commandprefix, page 12-6; *Profile Settings*, page 9-5

12.4.14 Define Ports Modem Init

DEFINE PORTS [*PortList* | ALL] MODEM INIT *string*

Defines an initialization string to send to the modem. The string is preceded by the **Commandprefix** string.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 64 characters.

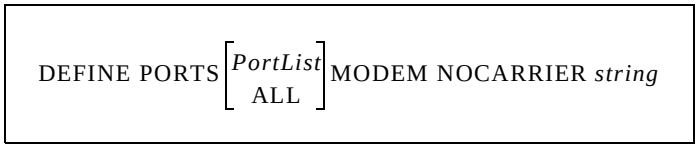
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM INIT "&fw1&c1&d3s2=128"
```

See Also *Define Ports Modem Commandprefix*, page 12-6; Profile Settings, page 9-5

12.4.15 Define Ports Modem Nocarrier



Defines a string to expect on outbound calls when the modem can dial but doesn't connect.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to "NO CARRIER"

Defaults Depends on modem and modem profile.

Examples Local>> DEFINE PORT 2 MODEM NOCARRIER "NO CARRIER"

See Also *Profile Settings,* page 9-5

12.4.16 Define Ports Modem Nodialtone

Defines a string to expect on outbound calls when the modem can't detect a dial tone.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

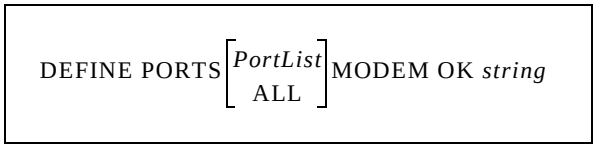
string
A string of up to 12 characters. Commonly set to "NO DIAL."

Defaults Depends on modem and modem profile.

Examples Local>> DEFINE PORT 2 MODEM NODIAL "NO DIAL"

See Also *Profile Settings,* page 9-5

12.4.17 Define Ports Modem OK



Defines a string to expect after the **Attention** string is sent to the modem.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to "OK."

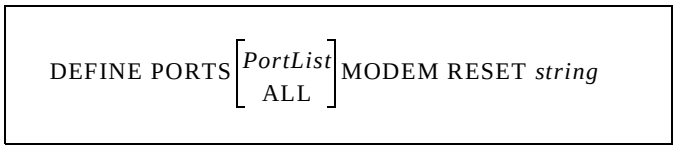
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM OK "OK"
```

See Also Define Ports Modem Attention, page 12-4; *Profile Settings*, page 9-5

12.4.18 Define Ports Modem Reset



Defines a string that will cause the modem to reset and reload its configuration from NVR.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to "Z."

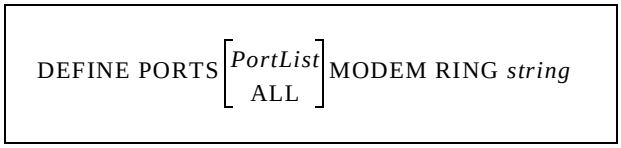
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM RESET 2
```

See Also *Profile Settings*, page 9-5

12.4.19 Define Ports Modem Ring



Defines a string that the modem returns if it rings.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to “RING.”

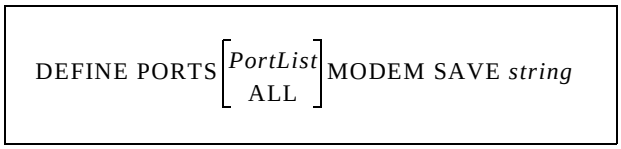
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM RING “M&M”
```

See Also *Profile Settings*, page 9-5

12.4.20 Define Ports Modem Save



Defines a string that forces the modem to save its configuration to NVR.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

string
A string of up to 12 characters. Commonly set to “&w.”

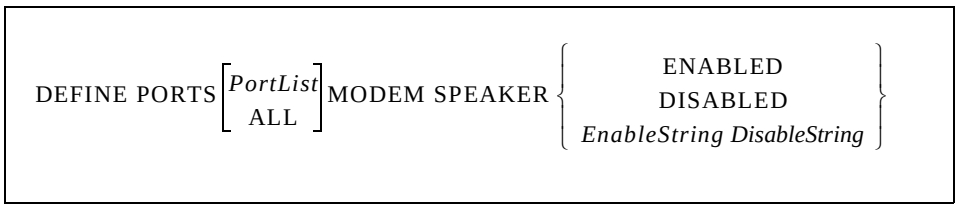
Defaults Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM SAVE “&w”
```

See Also *Profile Settings*, page 9-5

12.4.21 Define Ports Modem Speaker



Enables or disables the modem's speaker. The speaker allows the user to hear the modem's dialup and connect sequences for debugging purposes.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

EnableString
A string of up to 12 characters. Commonly set to "m1/1." When this string is received by the modem, the modem's speaker will be enabled.

DisableString
A string of up to 12 characters. Commonly set to "m0." When this string is received by the modem, the modem's speaker will be disabled.

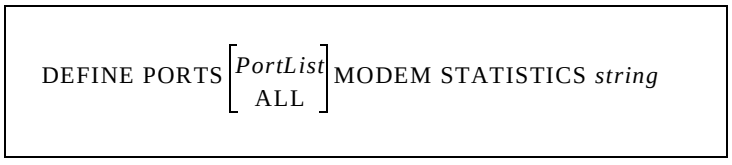
Defaults Disabled (no strings defined)

Examples

```
Local>> DEFINE PORT 2 MODEM SPEAKER ENABLED
Local>> DEFINE PORT 2 MODEM SPEAKER "m11" "m0"
```

See Also *Profile Settings*, page 9-5

12.4.22 Define Ports Modem Statistics



Defines a string to send to the modem to collect connection statistics after each call. This string is preceded by the **Commandprefix** string.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

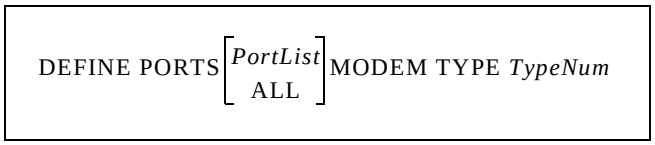
string
A string of up to 12 characters.

Defaults Depends on modem and modem profile.

Examples
```
Local>> DEFINE PORT 2 MODEM STATISTICS "statreport"
```

See Also Define Ports Modem Commandprefix, page 12-6; Set/Define Logging, page 12-172

12.4.23 Define Ports Modem Type



Specifies a predefined modem profile. Use the **Show Modem** command to see a list of available profiles.

This command automatically enables modem control for the specified port, if not enabled already.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

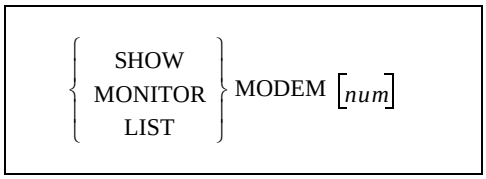
TypeNum
A predefined modem profile number.

Defaults Depends on modem and modem profile.

Examples
```
Local>> DEFINE PORT 2 MODEM TYPE 12
```

See Also Show/Monitor/List Modem, page 12-16; *Modem Profiles*, page 9-2

12.4.24 Show/Monitor/List Modem



Displays a list of modem profiles.

Restrictions You must be the privileged user to use the Monitor command.

Parameters **num**
A particular modem profile type to display.

Examples
```
Local> SHOW MODEM 3
```

See Also *Modem Profiles*, page 9-2

12.5 IP/Network Commands

12.5.1 Clear/Purge Hosts

Removes a TCP/IP host entry from the SCS table of known hosts. If Clear is used and the host was seen through the **rwho** facility, it will reappear as soon as that machine broadcasts again. A host will also reappear if a user Connects to it.

Restrictions Requires privileged user status.

Errors Clear Telnet Hosts will fail if there are any active Telnet connections on the server.

Parameters

All
Removes the names of all known hosts.

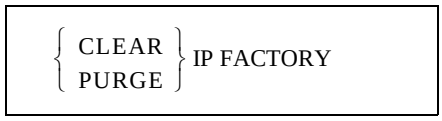
HostName
The name of a Telnet host to be removed.

Examples

```
Local>> CLEAR HOSTS alex
```

See Also Set/Define Hosts, page 12-34; Show/Monitor/List Hosts, page 12-48

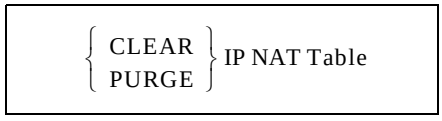
12.5.2 Clear/Purge IP Factory



Resets IP router options to their factory defaults.

Restrictions Requires privileged user status.

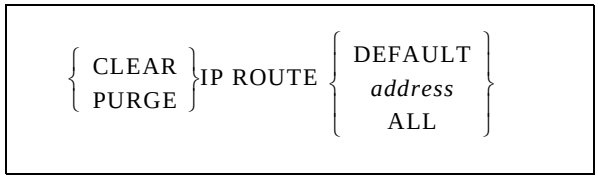
12.5.3 Clear/Purge IP NAT Table



Clears entire NAT table.

Restrictions Requires privileged user status.

12.5.4 Clear/Purge IP Route



Removes a static IP route.

Restrictions Requires privileged user status.

Parameters

Default
Clears or purges default IP routes.

address
An IP address in standard numeric format (for example, 193.53.2.2).

All
Clears or purges static IP routes.

Examples

```
Local>> PURGE IP ROUTE 192.0.1.1
Local>> PURGE IP ROUTE DEFAULT
```

See Also Set/Define IP Route, page 12-42; Show/Monitor/List IP Routes, page 12-49; *IP Routing*, page 6-19

12.5.5 Clear/Purge IP Security

Removes entries from the trusted router table.

Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.53.2.2).

All
Clears or purges the entire security table.

Examples

```
Local>> CLEAR IP SECURITY 192.0.1.2
```

See Also Set/Define IP Security, page 12-43; Show/Monitor/List IP, page 12-49; *IP Address Restriction*, page 11-20

12.5.6 Clear/Purge IP Trusted

Removes all entries from the trusted router table.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.53.2.2).

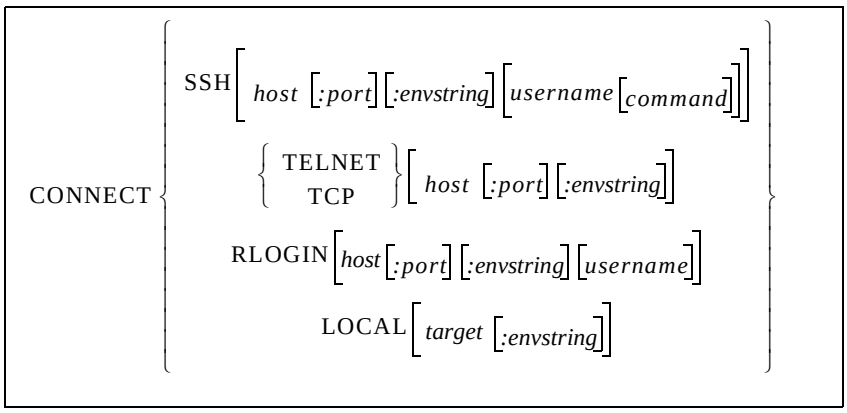
All
Clears or purges the entire security table.

Examples

```
Local>> PURGE IP TRUSTED 192.0.1.1
Local>> PURGE IP TRUSTED ALL
```

See Also Set/Define IP Trusted, page 12-47; Show/Monitor/List IP Trusted, page 12-49; *Routing Tables*, page 6-19

12.5.7 Connect



Establishes a connection with a TCP/IP host. If no hostname is specified, a connection to any preferred host is attempted.

Note: *The keyword "Connect" is not needed for Telnet or Rlogin connections, but must be included in the command for TCP or Local connections.*

Outgoing SSH connections can specify a host, optional port, optional username, and optional command to be executed on the remote machine. After the command is executed, the SSH connection will end.

A colon and session environment string can be added to the connect request (see *Setting Session Characteristics* on page 8-7). A colon and a port number can be added to the hostname for TCP/Telnet/Rlogin sessions; in this case, the specified port number will be used for the connection. There should be no spaces between the hostname, colon, and port number or environment string.

Parameters

SSH
Establishes an SSH connection to the specified host or, if no hostname is entered, to the preferred host.

host
Enter a text host name or an IP address in a standard numeric format (for example, 192.0.1.183).

username
Enter a user name that will be passed to the remote host.

command
Enter a command that will be executed on the SSH host. Put the command in **quotes** to retain any capitalization.

Telnet
The port is dedicated to the specified Telnet host or, if no hostname is entered, to the preferred host.

TCP
Establishes a raw TCP connection to the host/port number specified. This is useful for non-standard applications that do not desire any interpretation of the data stream.

Rlogin
Forces an Rlogin connection to the remote host or, if no hostname is entered, to the preferred host. May also take a **username** after the host parameter, in which case a username is sent to the remote Rlogin host.

host
Enter a text host name or an IP address in a standard numeric format (for example, 192.0.1.183).

envstring
Sets up the connection environment before the session is started. The string is constructed with a sequence of key letters, some of which are prefaced by either the "+" or "-." For the available key letters and usage instructions, see Appendix A, *Environment Strings*.

Local
Establishes a connection to a local service or port specified with the **target** parameter.

target
A local service or port name.

Examples

```
Local> CONNECT
Local> CONNECT TELNET 145.34.35.11:245
Local> CONNECT TCP labsun
Local> CONNECT RLOGIN 145.34.35.14
Local> CONNECT RLOGIN docserver mary
Local> CONNECT SSH ogun nathan "ls -l"
```

See Also Set/Define Ports Password, page 12-78; Disconnect, page 12-22; *Preferred/ Dedicated Protocols & Hosts*, page 8-8

12.5.8 Disconnect

Terminates the current session (if no session is specified), the specified session, or all sessions.

Examples
```
Local> DISCONNECT
Local> DISCONNECT SESSION 3
```

See Also Connect, page 12-20; Show/Monitor Sessions, page 12-98; *Exiting Sessions*, page 8-5

12.5.9 Purge IP Ethernet

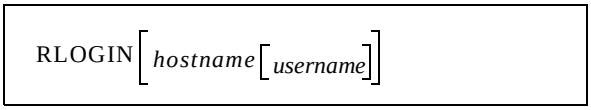
Removes the specified secondary Ethernet from the SCS permanent memory.

Restrictions Requires privileged user status.

Parameters **num**
An integer specifying a secondary Ethernet. Numbering begins at 1.

See Also Set/Define IP All/Ethernet, page 12-35; Show/Monitor/List IP Interface, page 12-49

12.5.10 Rlogin



Requests an Rlogin connection to a specified host, or the preferred TCP host if no host is specified.

Note: *Rlogin is an abbreviation for Connect Rlogin, described on page -20.*

Errors An error is returned if Rlogin is not enabled. Secure users may only use the Rlogin command if it has been enabled by the server by a privileged user.

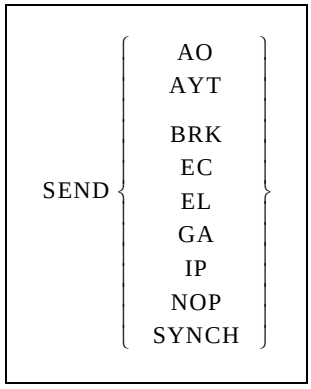
Parameters

hostname
A text hostname or an IP address in standard numeric format (for example, 192.0.1.183).

username
A username to use as the login name.

See Also Connect, page 12-20; Set/Define Ports Password, page 12-78; *Telnet and Rlogin Sessions*, page 6-9

12.5.11 Send



Sends Telnet commands through a session.

Note: *This command is only functional for Telnet TCP connections.*

Parameters

AO
Abort Output.

AYT
Are You There

BRK
Break

EC
Erase Character

EL
Erase Line

GA
Go Ahead

IP
Interrupt Process

NOP
No Operation

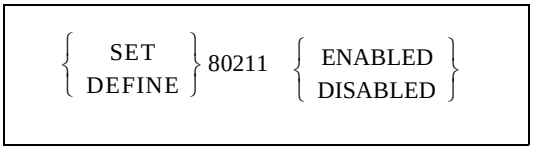
SYNCH
Synchronize

12.5.12 Set/Define 80211

After you enter an 80211 configuration command, you must reboot the unit for the changes to take effect. You can also enter the **Set 80211 Reset** command for all configuration commands except the Set/Define 802.11 Enabled/Disabled command, which requires a reboot.

Note: *These commands are only valid on the SCS200.*

12.5.12.1 Set/Define 80211 Enabled



When 802.11 is enabled, the SCS checks for a compatible 802.11 wireless Ethernet PC card at startup and, if one is present, uses the card instead of a wired Ethernet port. If no valid PC card is detected at startup, the SCS uses the 10/100BASE-T network connection.

When 802.11 is disabled, the SCS will ignore an installed 802.11 card and will only look for a compatible wired Ethernet connection.

You must reboot the SCS before those changes will take place.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Parameters

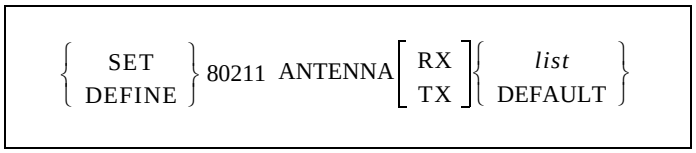
Enabled
Prompts the SCS to check for a compatible 802.11 wireless Ethernet networking PC card at startup. If one is present, wireless networking will be used instead of the wired Ethernet connection. You must reboot the SCS after entering this command.

Disabled
Prompts the SCS to only look for a compatible 10/100BASE-T wired Ethernet connection at startup. You must reboot the SCS after entering this command.

Defaults Enabled

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.2 Set/Define 80211 Antenna



Controls the antenna(s), if any, on the installed wireless card. Not all antennas can be used for both receive and transmit, so be sure to read your card documentation completely. The default settings should work in most applications.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200 and SCS400.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

RX
Specifies the antennas used to receive

TX
Specifies the antennas used to transmit.

list
Enter an integer or group of integers separated by commas (e.g. 1,2,3) to specify the affected antenna(s). Antennas are numbered consecutively starting with antenna number one. See the documentation that came with your card for antenna numbering information.

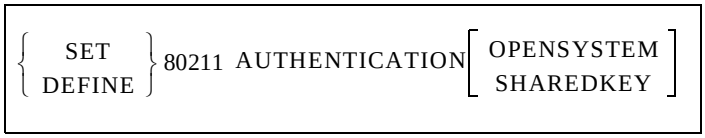
Default
Sets the antennas to their default transmit and receive values.

Examples

```
Local>> DEFINE 80211 ANTENNA DEFAULT
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.3 Set/Define 80211 Authentication



On products that support an 802.11 PC card, the wireless configuration alows either open or shared mode authentication styles. Use this command to change the authentication mode.

Restrictions Requires privileged user status.

Only applies to the SCS200 and SCS400.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

OPENSYSTEM
Access point will provide the WEP key to the SCS.

SHAREDKEY
Static WEP key is configured on the SCS.

Defaults Opensystem

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.4 Set/Define 80211 Channel

Sets the SCS operating frequency within the 2.4 GHz band allotted to wireless networking. A direct-sequence 802.11 network on one channel will affect reception on channels up to two numbers away. For best performance on collocated wireless networks, you should select channels that are at least five channels apart from each other. For example, three networks could be put on channels 1, 6, and 11 (depending on your regulatory region). See your PC card documentation for specific information about which channels are available in your area.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200 and SCS400.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

num
Enter a valid channel for your regulatory region. This number should be an integer between 1 and 14. Recommended for ad-hoc network mode.

Any
Tells the SCS to set itself for the channel used by the strongest AP with the same ESSID. Recommended for infrastructure network mode.

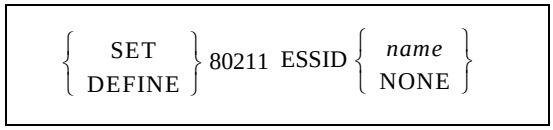
Defaults Any

Examples

```
Local>> CHANGE 80211 CHANNEL 6
Local>> CHANGE 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.5 Set/Define 80211 ESSID



Configures the ESSID, which tells the SCS the name of the Extended Service Set (ESS) to which it belongs. Setting an ESSID ensures that the SCS will stay on the desired network subsegment.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

name
Enter a string of up to 32 characters. If the string contains lowercase letters or non-alphanumerics, it may need to be enclosed in **quotes** to be processed properly.

None
If no ESSID string is set, the SCS will communicate with whichever Access Point (AP) gives the strongest signal, regardless of ESS association. Setting the ESSID to none allows the SCS to associate with any AP within range.

Defaults ESSID=None

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.6 Set/Define 80211 Fragmentation

```
{ SET    }
{ DEFINE } 80211 FRAGMENTATION num
```

Changes the fragmentation threshold.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters **num**
Enter an integer between 256 and 2346 to change the fragmentation threshold.

Defaults 2346

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.7 Set/Define 80211 MAC Address

```
{ SET    }
{ DEFINE } 80211 MACADDRESS { CARD }
                            { SCS  }
```

Configures which of the two available MAC addresses the SCS will use on the network—its own or that of the attached 802.11 wireless networking PC card. The SCS MAC address, which is the same as its hardware address, is printed on bottom label of the SCS.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters **Card**
Instructs the SCS to use the MAC address of the wireless PC card that is inserted into one of its PC card slots.

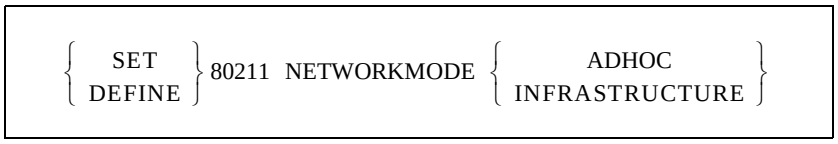
SCS
Instructs the SCS to use its own internal MAC address.

Defaults SCS

Examples
```
Local>> DEFINE 80211 MACADDRESS CARD
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.8 Set/Define 80211 Network Mode



Denotes whether the SCS operates in a peer-to-peer (AdHoc) or managed (Infrastructure) network environment.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

AdHoc
Specifies that the SCS is communicating with other wireless devices in a peer-to-peer capacity.

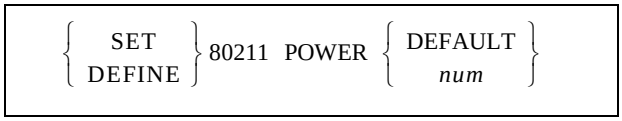
Infrastructure
Specifies that the SCS is communicating with an Access Point (AP).

Defaults Infrastructure

Examples
```
Local>> DEFINE 80211 NETWORKMODE ADHOC
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.9 Set/Define 80211 Power



Controls the card's transmit power settings. The numeric power setting specified must exactly match a value supported by the card.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

Default
Sets the card to its default transmit power setting.

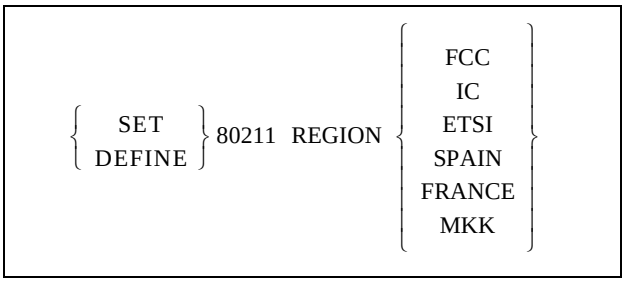
num
Enter a specific milliWatt power setting.

Examples

```
Local>> DEFINE 80211 POWER DEFAULT
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.10 Set/Define 80211 Region



Sets the regulatory region under which you will operate the SCS. Users in the United States can leave this at the default setting (FCC). Other users should set it to correspond with their region.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a region that will not work with your 802.11 card, an error bit will be displayed when you enter the **Show 80211** command.

Parameters

Regions
IC: Canada
ETSI: Europe, most countries (verify with your local regulatory body)
SPAIN: Spain
FRANCE: France
MKK: Japan

Defaults FCC

Examples

```
Local>> DEFINE 80211 REGION FRANCE
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.11 Set 80211 Reset

```
SET 80211 RESET
```

Resets the SCS so any configuration changes will take effect immediately.

Restrictions Requires privileged user status.

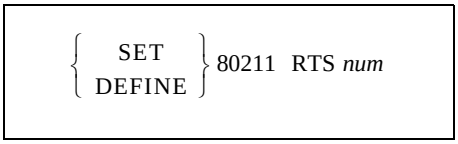
Only applies to the SCS200.

Parameters

Reset
Resets the SCS to make all 802.11 changes take effect immediately. This command should be entered anytime you make an 802.11 configuration change. It also clears out any previous errors and starts over with the current 802.11 parameters.

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.12 Set/Define 80211 RTS



Changes the RTS threshold value.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions Requires privileged user status.

Only applies to the SCS200.

Errors If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

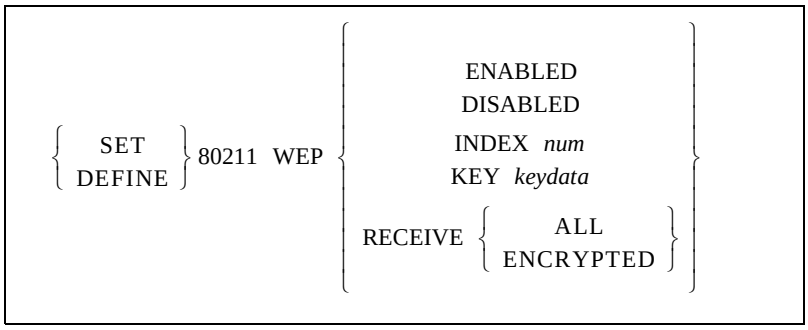
Parameters **num**
Enter a value between 0 and 3000.

Defaults 3000

Examples
```
Local>> DEFINE 80211 RTS 0
Local>> SET 80211 RESET
```

See Also Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.12.13 Set/Define 80211 WEP



Enabling WEP (Wireless Equivalent Privacy) means the SCS will only connect to an AP (in infrastructure mode) or communicate with other ad-hoc peers (in ad-hoc mode) that have been programmed with the same WEP key as the SCS. All wireless network traffic the SCS sends will be encrypted with its WEP key and any encrypted wireless network traffic the SCS receives will be decrypted with its WEP key. Disabling WEP causes the SCS to ignore its WEP key and only receive and transmit unencrypted network traffic.

Any configuration changes you make with the above commands will not take place until you reboot the SCS or issue the **Set 80211 Reset** command.

Restrictions

Requires privileged user status.

Only applies to the SCS200.

Errors

If you enter a command that is not applicable to the 802.11 card currently in use, you will receive an Error message.

Parameters

Enabled
Enables WEP.

Disabled
Disables WEP.

Index
Assigns the index number that should be used with the WEP key.

num
Enter an integer between 1 and 4. For two keys to match, both their key data and their index number must be identical.

Key
Sets the WEP key. The SCS allows both 40-bit and 128-bit keys, and will determine which key length is being set by the length of the key data.

keydata
Enter the WEP key. The key format should be entered as "xx-xx-xx-xx..." where each x is a hexadecimal digit (0 through 9 and A through F). Each pair of hex digits (xx) defines a byte of key data, and each byte is separated from the next by a dash. For a 40-bit key, 5 bytes of key data must be given. For a 128-bit key, 13 bytes of data must be given.

Receive
Determines whether the SCS will receive unencrypted data while WEP is enabled.

All
Allows reception of encrypted traffic while WEP is enabled. The SCS will accept unencrypted wireless network frames, as well as frames encrypted with its WEP key. This is the default setting once WEP has been enabled.

Encrypted
Refuses to accept unencrypted data while WEP is enabled. The SCS will discard and ignore unencrypted wireless network frames, accepting only frames encrypted with its WEP key.

Defaults

Disabled, Receive all

Examples

```
Local>> DEFINE 80211 WEP ENABLED
Local>> DEFINE 80211 INDEX 3
Local>> DEFINE 80211 RECEIVE ENCRYPTED
Local>> SET 80211 RESET
```

See Also

Show 80211, page 12-48; *802.11 Configuration*, page 2-11

12.5.13 Set/Define Hosts

Associates a TCP/IP hostname with an IP address in the local host table, allowing you to use the text name for Telnet connections even if there is no name server to resolve it. If the given host name has already been configured, the new IP address will replace the previous value.

Restrictions Requires privileged user status.

Errors You will receive an error if you enter an IP address in a questionable format.

Parameters

hostname
The hostname string you wish to define, limited to 64 alphanumeric characters with only 16 characters between any period delimiters.

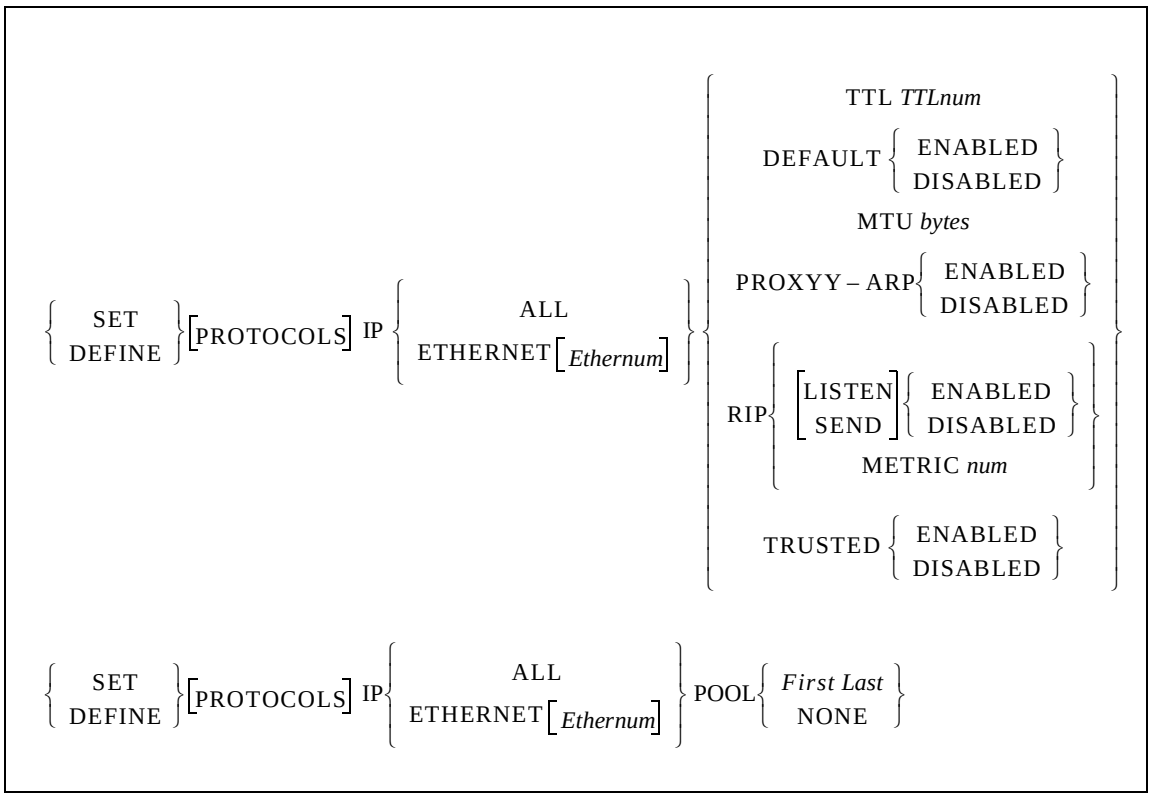
IPaddress
Standard, numeric IP address of the machine referred to by the hostname.

Examples

```
Local>> SET HOST spectre 192.0.1.11
```

See Also Clear/Purge Hosts, page 12-18; Show/Monitor/List Hosts, page 12-48

12.5.14 Set/Define IP All/Ethernet



Configures all interfaces on an Ethernet interface.

Restrictions Requires privileged user status.

Parameters

All
Configures all IP interfaces.

Ethernet
Configures an Ethernet interface. To specify the number of the Ethernet, the **Ethernum** parameter must be used. If no number is entered, the configuration will affect the primary interface.

Note: *Servers with one Ethernet port do not need the optional Ethernum parameter; when omitted, it defaults to zero.*

Ethernum
Enter the number of a specific secondary Ethernet interface. If a zero is entered, the configuration will affect the primary interface.

TTL
Sets the amount of time that the IP Time-To-Live value should be decremented by when routed through this interface. The specific amount must be set using the **TTLnum** parameter.

TTLnum
An integer between 1 and 127, inclusive.

Default
If enabled, IP routing updates will advertise this router as the "default" route. Default is commonly used to avoid large routing tables when there is only one possible path to a large number of networks.

MTU
Sets the maximum Transmission Unit, or "packet size" for this interface. Packets larger than this value will be IP fragmented when transmitted. Must be used in conjunction with the **bytes** parameter, discussed below.

bytes
An integer between 40 and 1500, inclusive.

Proxy-ARP
If enabled, an ARP response will be sent in reply to ARP requests for non-local networks to which the SCS knows a valid path. Commonly used to allow end hosts that don't understand routing or subnet masks to find a router.

Pool
Allocates a pool of IP addresses to dialin users. When Proxy-ARP is enabled, the SCS will respond to ARP requests to all addresses in the pool. Must be used with the **First** and **Last** parameters, or with the **None** parameter.

Note: *The pool can be set to any size, but it makes sense to restrict it to the number of available serial ports.*

First
Specifies the start of the range of IP addresses to be used.

Last
Specifies the end of the range of IP addresses to be used.

None
Disables use of the IP address pool.

RIP
Configures the IP Routing Information Protocol (RIP) for this interface. Must be used in conjunction with the **Listen**, **Send**, or **Metric** parameter.

Listen
Enables or disables RIP listening.

Send
Enables or disables RIP sending.

Metric
Configures the cost or "hop-count" of this interface. routes learned through this interface will have the value added to their metric. The value to be added must be specified using the **num** parameter.

num
An integer between 1 and 16, inclusive. Commonly used to make a given interface less desirable for backup routing situations.

Trusted
When enabled, this interface will only listen to routing updates from routers specified by the **Set/Define IP Trusted** command. Otherwise, this interface will listen to all routing updates.

Defaults

Ethernet Interface number: 0
TTLNum: 1
Default, Proxy-ARP, and Trusted: Disabled
MTU: 1500 bytes
Listen and Send: Enabled

Examples

```
Local>> DEFINE IP ALL MTU 1500
Local>> DEFINE IP ETHERNET MTU 1500
Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

See Also

Clear/Purge IP Trusted, page 12-20; Show/Monitor/List Hosts, page 12-48; *Defining an IP Address Pool*, page 6-3

12.5.15 Set/Define IP Create

{ SET / DEFINE } [PROTOCOLS] IP CREATE ETHERNET 0 *IPaddress Netmask*

Creates a secondary interface—an interface that shares a physical device, such as an Ethernet port, but has a different IP address. The secondary interface is commonly used to allow more than one IP network on a given Ethernet.

Restrictions

Requires privileged user status.

Parameters

0
The number zero represents the primary Ethernet interface for which the secondary interfaces are created. The number zero must be included in the command.

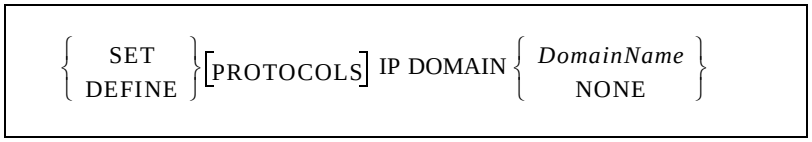
IPaddress
An IP address in standard numeric format (for example, 193.0.1.50).

Netmask
A subnet mask; for example, 255.255.255.0.

Examples

```
Local>> SET IP CREATE ETHERNET 0 192.73.220.183 255.255.255.0
```

12.5.16 Set/Define IP Domain



Sets the default domain suffix. This suffix is appended to host names during IP name resolution.

Restrictions Requires privileged user status.

Parameters

DomainName
A string of up to 64 characters.

None
Clears an existing domain suffix.

Defaults None (no domain defined)

Examples

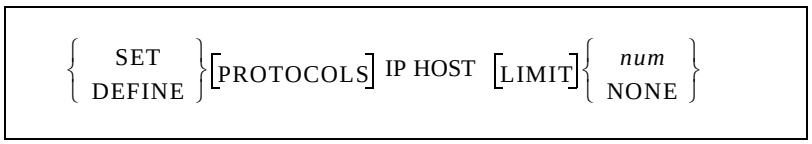
```
Local>> SET IP DOMAIN your.domain.com
```

See Also Show/Monitor/List IP, page 12-49; *Specifying a Default Domain Name*, page 6-7

12.5.17 Set/Define IP Ethernet

See *Set/Define IP All/Ethernet*, page 12-35.

12.5.18 Set/Define IP Host Limit



Sets the maximum number of TCP/IP hosts that the SCS will add to its host table as a result of Rwho and DNS lookups. Hosts from the preset host table are exempt from this limit.

Restrictions Requires privileged user status.

Parameters

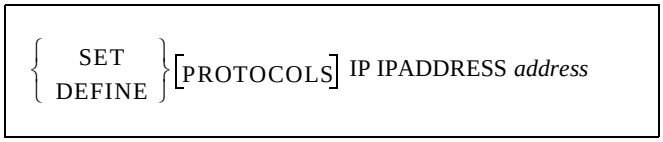
num
An integer between 0 and 200.

None
Clears any current host limit.

Defaults Limit: 200 hosts

See Also Show/Monitor/List IP, page 12-49; *Adding Hosts to the Host Table*, page 6-7

12.5.19 Set/Define IP IPaddress



Specifies the server's IP address for TCP/IP connections.

Restrictions Requires privileged user status.

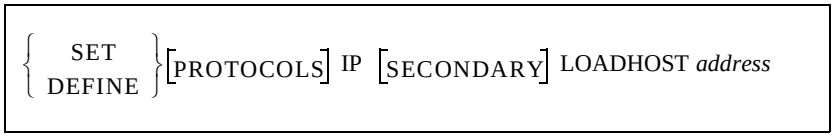
Errors An error is returned if there are active connections to the SCS. An error is returned if the address is in use by another node.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Show/Monitor/List IP, page 12-49; *IP Addresses*, page 6-1

12.5.20 Set/Define IP Loadhost



Specifies the IP address of the host used for TFTP loading.

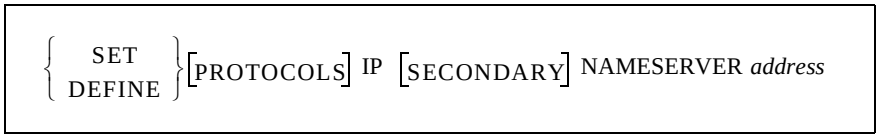
Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.5).

See Also Set/Define Server Loadhost, page 12-120

12.5.21 Set/Define IP Nameserver



Specifies the IP address of the local nameserving host for use on IP connections and NetBIOS connections that use IP. The host's address must be specified using the address parameter, described below.

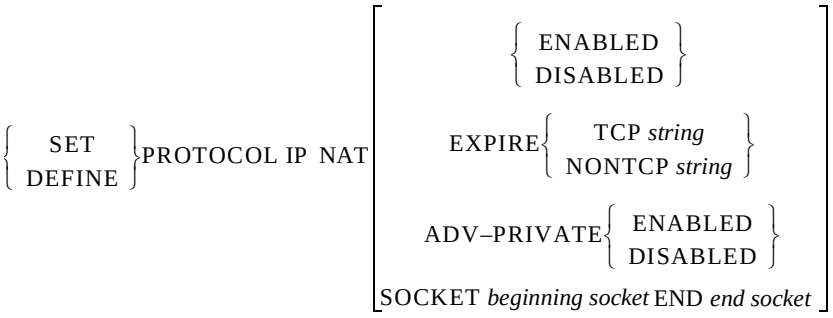
Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.5).

See Also *Configuring the Domain Name Service (DNS)*, page 6-7

12.5.22 Set/Define IP NAT



Enables and configures basic Network Address Translation (NAT) features.

Restrictions Requires privileged user status.

Parameters

EXPIRE
Time, in minutes, before a NAT entry is removed from the mapping table.

TCP string
Time, in minutes, to expire TCP NAT mappings.

NONTCP string
Time, in minutes, to expire non-TCP NAT mappings.

ADV-PRIVATE
Specifies whether to advertise private networks.

SOCKET
Specifies beginning of socket range used by NAT.

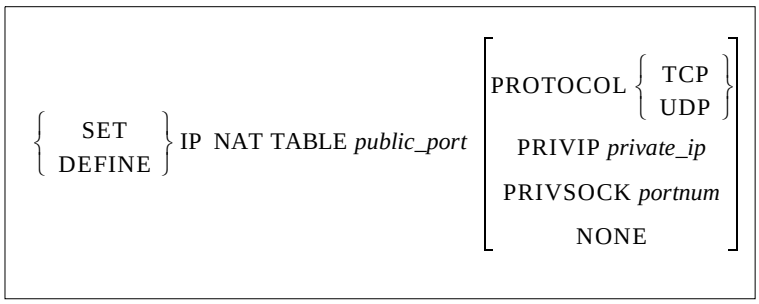
beginning socket
First socket number or IP port number

END
Specifies last of socket range used by NAT.

end socket
Last socket number or IP port number.

See Also *Set/Define IP NAT Table*, page 12-41;Show/Monitor/List IP, page 12-49; ISP Site Connections with NAT on page 4-6

12.5.23 Set/Define IP NAT Table



Specifies the IP address of the local nameserving host for use on IP connections and NetBIOS connections that use IP. The SCS also allows connections from public IP networks to specific IP address/port combinations on the private IP interface. The NAT table can contain 10 mappings. The host's address must be specified using the address parameter described below.

Restrictions Requires privileged user status.

Parameters

public_port
A socket number or IP port number on public network (Internet).

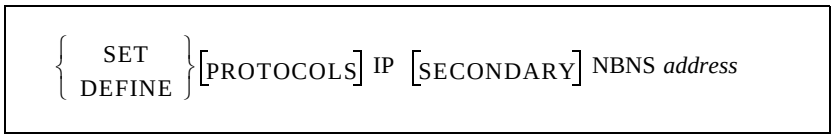
PRIVIP
An IP address in standard numeric format (for example, 193.0.1.50).

PRIVSOCK
A socket number or IP port number at the PRIVIP address.

NONE
Clears an entry in the NAT table.

See Also Show/Monitor/List IP, page 12-49, ISP Site Connections with NAT on page 4-6

12.5.24 Set/Define IP NBNS



Specifies the address of the NetBIOS Name Server (NBNS) used for NetBIOS over an IP network. NBNS addresses are passed via PPP to remote users who want to locate the name server dynamically. The SCS does not use this information itself.

Note: *NBNS is also known as WINS.*

NetBIOS over IP can also use DNS; the nameserver address set with the **Set/Define IP Nameserver** command will also be passed on to remote node users who ask for them.

Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also *Set/Define IP Nameserver*, page 12-39*; Configuring the Domain Name Service (DNS)*, page 6-7

12.5.25 Set/Define IP Route

Configures a static route. Static routes are used to tell the IP router the path toward other IP networks that cannot be learned by a dynamic routing protocol such as RIP. Static routes commonly point to sites (see the **Define Site** commands), which represent the best path to the destination. The destination can be an IP network, a subnetwork, or a host.

Restrictions Requires privileged user status.

Parameters

Default
Configures a default route. If an explicit route to a destination network doesn't exist, the packet will be routed according to the default route.

Static default routes are used when another router is the designated default route. If this router is to advertise itself as the default router, see **Set/Define IP All/Ethernet Default**, page 12-35.

destination
An IP address in standard numeric form.

Nextrouter
Sets the router that packets to the destination will be sent to.

router
A router name or IP address.

Note: *If the route points to a site, use the Site parameter.*

Site
Specifies the site that packets to the destination will be sent to. When a packet arrives for the destination, a connection will be formed to the specified site, if one does not currently exist.

The site must be defined before a route can be created that points to the site. To configure a site, use the **Define Site** commands.

SiteName
A site name of up to 12 characters.

Note: *If the next "hop" is a router available on the LAN, use the Nextrouter parameter.*

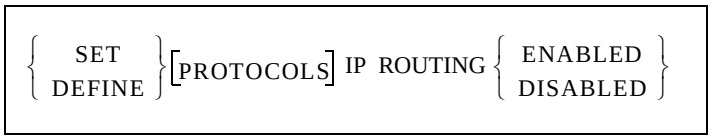
num
An integer from 1 through 16 representing the metric for this route.

Defaults Metric: 16 (unreachable)

Examples
```
Local>> SET IP ROUTE 198.8.8.0 NEXT 192.0.1.9
```

See Also Clear/Purge IP Route, page 12-19; Show/Monitor/List IP Route, page 12-49; *IP Routing*, page 6-19

12.5.26 Set/Define IP Routing



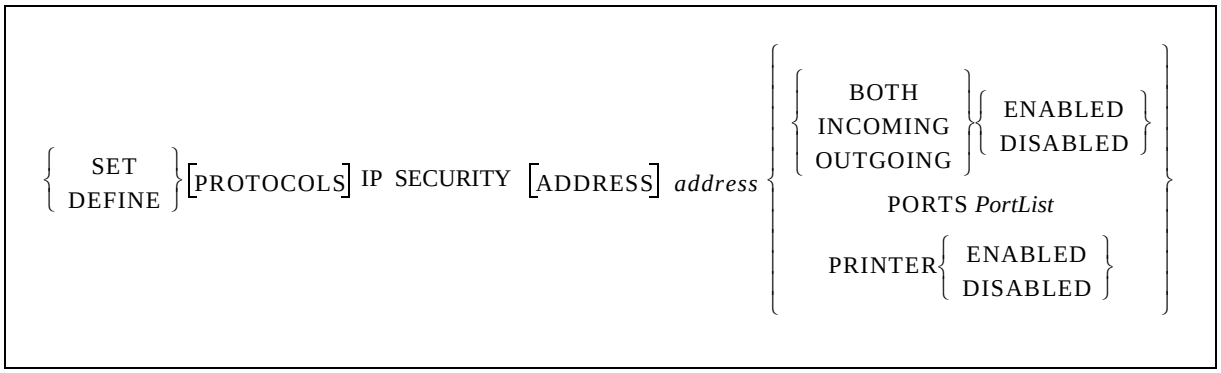
Configures the routing of IP packets. If routing is disabled, any packets requiring routing on the SCS will be rejected. The router will still learn routes via RIP (if enabled) for its own use.

Restrictions Requires privileged user status.

Defaults Enabled

See Also *IP Routing*, page 6-19

12.5.27 Set/Define IP Security



Adds or changes entries in the IP security table.

Restrictions Requires privileged user status.

Parameters

address
The IP address to be restricted. The address can be a full IP address, such as 192.0.180, to restrict one address; it can also be expressed as a partial address, such as 192.0.1.255, to restrict whole subnetworks.

An address with a 255 in any segment means the restriction applies to all the addresses in that range. Any address with a 0 in any segment implies Incoming and Outgoing Disabled for all ports.

Both
Restricts both logins from the network to the server and Telnet sessions to the network from the server.

Incoming
Restricts logins from the network into the server.

Outgoing
Restricts Telnet sessions from the network into the server.

Ports
A list of ports for which the restriction applies. To specify a port or list of ports, use the **PortList** parameter. If **PortList** is not specified, all physical and virtual ports apply. A port number of 0 i used to apply to the virtual (incoming login) ports.

PortList
A port or series of ports to be restricted. Multiple ports must be specified with a comma; ranges of ports must be specified with a dash (-).

Printer
Enables or disables LPR and RTEL printing from the specified host(s).

Defaults

Both Enabled, Printing Enabled

Examples

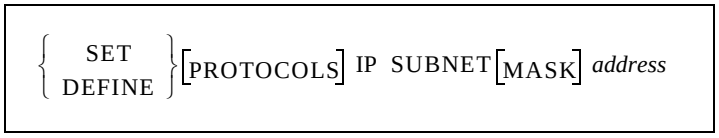
```
Local>> SET IP SECURITY ADDRESS 192.0.1.255 INCOMING ENABLED OUTGOING
DISABLED

Local>> SET IP SECURITY 134.0.1.255 PORT 3,5-7
```

See Also

Clear/Purge IP Security, page 12-19; Show/Monitor/List IP Security, page 12-49; *IP Security*, page 6-17

12.5.28 Set/Define IP Subnet



Specifies a subnet mask as an IP address. The mask must be specified using the **address** parameter.

Restrictions Requires privileged user status.

Parameters

Mask
Specifies a subnet mask. Must be used in conjunction with the address parameter. If a subnet mask isn't specified, a default subnet mask will be inferred from the server's current IP address.

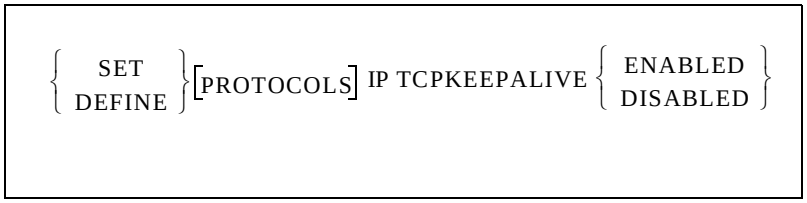
address
An IP address in standard numeric format (for example, 255.255.192.0).

Examples

```
Local>> SET PROTOCOL IP SUBNET MASK 255.255.255.0
```

See Also *IP Addresses*, page 6-1

12.5.29 Set/Define IP TCP Keepalive



Enables or disables TCP keepalive packets. By default, TCP keepalive packets are enabled and are transmitted every minute.

Restrictions Requires privileged user status.

Parameters

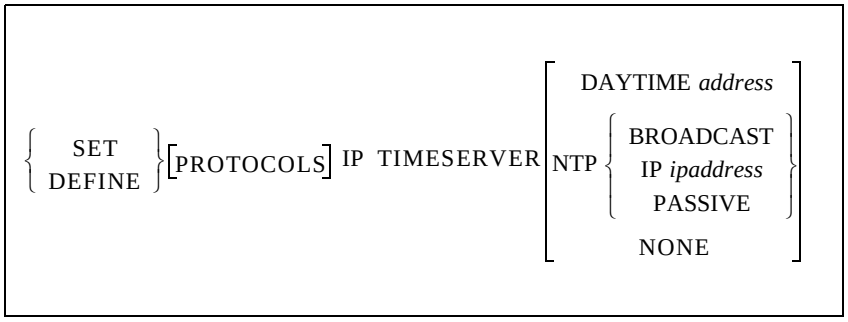
Enabled
Transmits keepalives.

Disabled
Does not transmit keepalives.

Defaults Enabled

See Also Show/Monitor/List IP, page 12-35

12.5.30 Set/Define IP Timeserver



Configures a timeserver for the SCS to use to update its internal clock. The SCS can communicate with either Daytime or Network Timeserver Protocol (NTP) servers. For NTP, the SCS can periodically broadcast a message asking for time information and wait for an NTP timeserver to reply, periodically query a specific NTP timeserver, or just listen for NTP broadcasts on the network.

Restrictions Requires privileged user status.

Parameters

Daytime
Specifies a daytime server. The SCS will listen for a possible daytime server, then send packets querying that server for time information.

Note: *Daytime is only supported over UDP.*

address
An IP address in standard numeric format (for example, 193.0.1.50).

None
Clears a previous timeserver setting.

NTP
Specifies an NTP server. There are three types of NTP.

Broadcast
The SCS periodically broadcasts a message that asks for time information, and waits for an NTP timeserver to reply.

IP
Use this method if you have a single NTP timeserver on your network. You must enter an IP address in standard numeric format.

Passive
The SCS will listen for NTP timeserver announcements on the network.

Examples

```
DEFINE IP TIMESERVER NTP IP 192.0.1.122
```

12.5.31 Set/Define IP Trusted

Configures a list of trusted routers. When **Set/Define IP All/Ethernet Trusted** is enabled, the SCS will only listen to RIP updates from routers in this list.

Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

RIP
When enabled, sets the specified IP address as a trusted routers. By default, routers are not trusted.

See Also Set/Define IP All/Ethernet, page 12-35; Show/Monitor/List HostsTrusted, page 12-48; Clear/Purge IP Trusted, page 12-20; *Types of Routes*, page 6-19

12.5.32 Set/Define IP Trusted

Configures a list of trusted routers. When **Set/Define IP All/Ethernet Trusted** is enabled, the SCS will only listen to RIP updates from routers in this list.

Restrictions Requires privileged user status.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

RIP
When enabled, sets the specified IP address as a trusted routers. By default, routers are not trusted.

See Also Set/Define IP All/Ethernet, page 12-35; Show/Monitor/List HostsTrusted, page 12-48; Clear/Purge IP Trusted, page 12-20; *Types of Routes*, page 6-19

12.5.33 Show IP Counters

Displays current TCP/IP traffic counters.

12.5.34 Show/Monitor/List Hosts

Displays either the currently available TCP/IP (Telnet/Rlogin) hosts (Show) or the ones that have been Defined locally in the host table (List). Hosts will be shown with the method of discovery (rwho, connection, host table, etc.) and will also be marked if they are the current nameserver and/or gateway. Specifying a particular host name will show only that host's information. Wildcards for the hostnames are allowed. The All option is the default, and it displays all known TCP/IP hosts.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

hostname
Specifies a particular TCP/IP host.

All
Displays all the TCP/IP nodes that this server currently knows about. These include hosts from the local host table, as well as hosts seen by Rwho broadcasts and those resolved after a Connect/Telnet request.

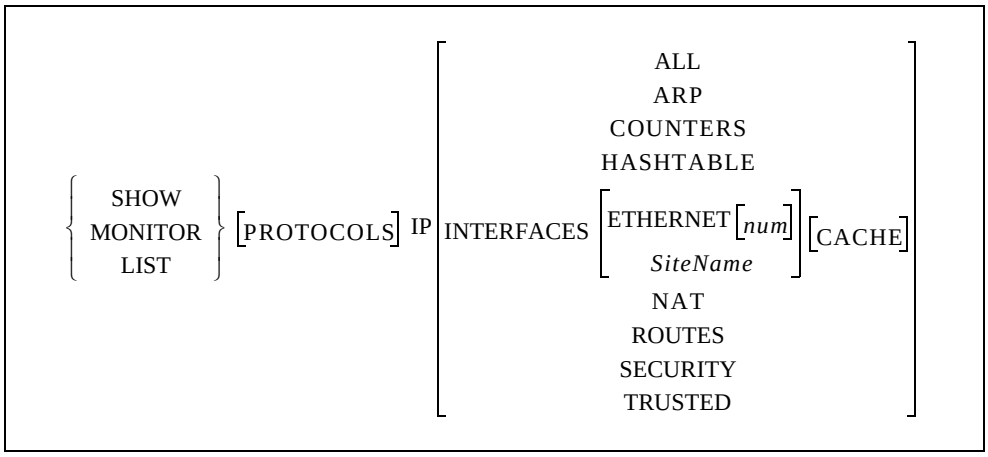
Local
Displays local TCP/IP nodes.

Examples

```
Local> SHOW HOSTS ALL
```

See Also Set/Define Hosts, page 12-34; *Adding Hosts to the Host Table*, page 6-7

12.5.35 Show/Monitor/List IP



Displays the current operating characteristics of the targets. Use the **List** command to see the permanent attributes that will take effect upon reboot/login.

Restrictions You must be the privileged user to use the Monitor command.

Parameters **[No Parameters]**
Entering the **Show IP** command without additional keywords will display general IP protocol information, including the following counters.

The Reasons fields show counters in hexadecimal with the rightmost bit being 0. For example, a Connect Failure Reason of 0040 represents 0000 0000 0100 0000 in binary, which means that bit 6 is set. The meaning of each bit is explained in Table 12-1.

Table 12-1: IP Failure and Message Reasons

Bit	Connect Failure Reasons	Invalid Packet Reasons	ICMP Message Reasons
0	Internal failure, should be 0	Data received outside window	Echo message received
1		Connection terminated abnormally	Echo reply received
2	No nameserver defined (for text host name)	Packet received with an invalid data checksum	Destination unavailable; see bits 4-7
3	Attempted name service failed	Packet received with an invalid data header	Unknown ICMP type received
4	No gateway was configured for a non-local connection	RST packet sent to remote node	Network unreachable; usually from a gateway host

Table 12-1: IP Failure and Message Reasons, cont.

Bit	Connect Failure Reasons	Invalid Packet Reasons	ICMP Message Reasons
5	Attempted ARP failed	Packet received for an unknown local user	Host unreachable
6	Remote host did not answer	Unused, should be 0	Port unreachable; usually due to failed name service
7	Remote host rejected the connection		Protocol unreachable
8-15	Unused, should be 0		Unused, should be 0

All
Displays all defined IP information.

ARP
Displays the current state of the ARP table.

Counters
Displays the IP-related counters.

Hashtable
Displays the routing table's hash table statistics.

Interfaces
Displays IP router interfaces. To display IP router information about a specific interface, Interfaces may be used in conjunction with one of the following parameters: Ethernet, Cache, or **SiteName**.

Ethernet
Displays information about a particular Ethernet interface. To specify the interface, use the **num** parameter.

num
An integer specifying a particular Ethernet interface.

SiteName
A particular site whose IP information will be displayed.

Cache
Displays cache statistics.

NAT
Displays the settings related to NAT support.

Routes
Displays the IP routing table.

Security
Displays the active (Show, Monitor) or permanent (List) IP security entries.

Trusted
Displays trusted IP routers.

Timeserver
Displays the timeserver.

Examples

```
Local> SHOW IP HASHTABLE
Local>> SHOW IP INTERFACES ETHERNET
Local>> SHOW IP INTERFACES ETHERNET 4
```

See Also Netstat, page 12-187; *IP/Network Commands*, page 12-18; Chapter 6, *IP*

12.5.36 SSH

SSH is a shorthand for the **Connect SSH** command. For a description of the command, see **Connect**, page 12-20.

12.5.37 Telnet

Telnet is a shorthand for the **Connect Telnet** command. For a description of the command, see **Connect**, page 12-20.

12.6 Port Commands

12.6.1 List Email

LIST EMAIL [*emailsite* | ALL]

When entered without any parameters, displays all emailsite configurations that will take place the next time that emailsite is used. Using the emailsite parameter will show the configurations for that specific site, while the All parameter will show a detailed listing of all emailsites.

Restrictions Requires privileged user status.

Parameters **emailsite**
Enter the name of an emailsite.

See Also Purge Email, page 12-54; Define Email, page 12-55; Define Ports Event Email Serialdata, page 12-71; *Event Port Logging*, page 3-2

12.6.2 Lock

LOCK

Locks a port without disconnecting sessions. When you enter this command, you will be queried for a password (6 alphanumeric characters maximum) and asked to verify it. The port is then locked until that password is used to unlock it. If a user forgets the password, the privileged user must either logout the port using the Logout command (disconnecting all sessions) or use the **Unlock Port** command.

Note: *The password and verification are not displayed as the user types them.*

Restrictions Secure users may not lock their ports.

Examples

```
Local> LOCK
Password> donut
Verification> donut

Unlock password> donut
Local>
```

See Also Set/Define Server Lock, page 12-120; Unlock Port, page 12-100; Logout Port, page 12-53; Set/Define Ports Security, page 12-85; *Locking a Port*, page 8-9

12.6.3 Logout Port

```
LOGOUT [PORT Portlist]
```

Logs out a port. Active sessions are disconnected, and all site circuits are closed.

Restrictions Only privileged users can log out a port or site other than their own.

Parameters

Port
Logs out the list of ports specified with the PortList parameter.

PortList
Specifies a port or series of ports to be logged out. Multiple ports must be separated by commas (for lists) or dashes (for ranges).

Note: *If the PortList parameter isn't specified, the current port will be logged out.*

Examples

```
Local> LOGOUT
Local>> LOGOUT PORT 2,4-6
```

See Also *Automatic Logouts,* page 8-11

12.6.4 Purge Port

```
PURGE PORT { PortList } [ PPP ]
           { ALL     } [ MODEM ]
```

Resets a port to the factory default PPP or Modem settings, but without affecting any other port settings. When used without the PPP or Modem parameters, both PPP and Modem settings are purged.

Restrictions Requires privileged user status.

Parameters

PPP
Resets all Link Control Protocol parameters on the specified port.

Modem
Clears the specified port's modem init information.

PortNum
Specifies a particular SCS port.

See Also Show/Monitor/List Ports, page 12-96; *Port Commands,* page 12-52

12.6.5 Purge Email

PURGE EMAIL *emailsite*

Removes an emailsite.

Restrictions Requires privileged user status.

Parameters **emailsite**
Enter the name of an emailsite.

See Also Define Email, page 12-55; Define Ports Event Email Serialdata, page 12-71; *Event Port Logging*, page 3-2

12.6.6 Resume

RESUME [[SESSION] *number*]

Leaves character (Local>) mode and resumes the current (active) session. To resume a session other than the current one, specify a session number with the **number** parameter.

Errors An error is returned if there are no active or defined sessions.

Parameters **number**
A session number, which can range from one to the total number of sessions that you currently have open.

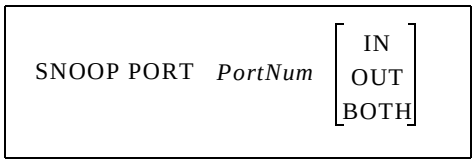
Examples
```
Local> RESUME
Local> RESUME SESSION 4
```

See Also *Switching Between Sessions*, page 8-5

12.6.7 Set Noprivileged

See **Set Privileged/Noprivileged**.

12.6.8 Snoop Port



Enables you to watch the data traffic on a local serial port.

Restrictions Requires privileged user status.

Parameters

PortNum
Specifies a particular SCS port to watch.

In
Displays only data coming into the serial port from an attached device.

Out
Displays only data going from the SCS serial port to the attached serial device.

Both
Displays both incoming and outgoing data to and from the serial port. Incoming data is displayed in inverse video.

Note: *All data may not display if you are monitoring a high speed serial port on a slower speed connection.*

See Also Show/Monitor/List Ports, page 12-96;

12.6.9 Define Email

Configures email notification in a format known as an emailsite, which contains all of the information needed when email notification for port buffering is enabled. Emailsites can be named default or portxx, where xx is the port number. The portxx sites will be used for email notification on that port, e.g. the port12 emailsite will be used for port buffering on port 12.

The default emailsite configurations will be used to fill in any blanks for the port-specific emailsites.

All of the above strings can use dynamic print variables. Available dynamic print variables are shown in the following table.

Note: *Dynamic print variables are case-sensitive. You must use all capital letters in the variables to avoid problems.*

Table 12-2: Dynamic Print Variables

Variable	Parsing Function
$FN	Displays the file name currently being accessed
$SC	Prints **Lantronix**
$SD	Adds a date stamp to the web page in the Day Month Date, Year format (e.g. Tue June 8, 1999)
$SH	Substitutes the SCS's hardware address
$SI	Print's the SCS's IP address
$SM	Prints the domain name of the network the SCS is on, as specified with the **Set/Define IP Domain** command
$SN	Prints the SCS's name, as specified with the **Set/Define Server Name** command
$SP	Prints the product name of the SCS
$ST	Adds a time stamp in the Hour:Minutes:Seconds format (e.g. 12:42:08)
$SV	Prints the version of operating software the SCS is currently using.

Restrictions

Requires privileged user status.

Parameters

emailsite
Enter the emailsite name. The only valid names are "default" and "portxx," where xx is the port number.

To
Sets the recipient(s) of the email.

address
Enter an email address, or a series of email addresses separated by commas. **Enclose the address in quotes to preserve case and spaces.** The max number of characters for this field is 64 characters. Most SMTP mail servers require a domain name on the To/From names, e.g. admin@strut.com instead of just admin.

From
Sets the text that will be displayed in the From: field of the email message. The maximum number of characters for this field is 32.

Subject
Sets the subject line that will be displayed in the email message. Enter a character string with a maximum length of 48 characters. **Enclose the string in quotes to preserve case and spaces**.

string
Enter a character string with a maximum length of 32 characters. **Enclose the string in quotes to preserve case and spaces.**

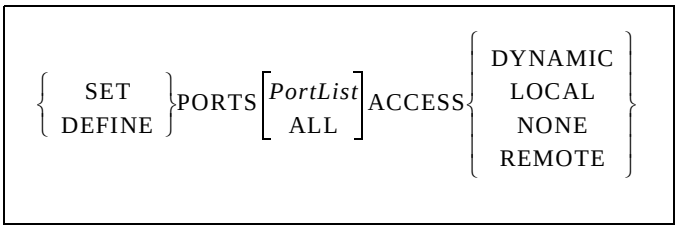
Mailhost
Sets the SMTP mailhost. Enter a string with maximum length of 24 characters. **Enclose the string in quotes to preserve case and spaces.**

Replyto
Sets the email address that any response to the email notification will be sent to. **Enclose the address in quotes to preserve case and spaces.** The max number of characters for this field is 32.

Examples DEFINE EMAIL port2 TO “ahab@strut.com, crash@strut.com”

See Also Set/Define Ports Serial Log, page 12-85; Define Ports Event Email Serialdata, page 12-71; *Event Port Logging*, page 3-2

12.6.10 Set/Define Ports Access



Sets the type of incoming connections allowed through the physical port.

Restrictions Requires privileged user status.

Errors If a port is active, its access cannot be set.

Autobaud must be disabled for Remote and Dynamic ports.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Dynamic
The ports can receive connection requests from local and remote users.

Local
The ports can only accept connection requests from local users (those connected to the serial ports). No remote logins are permitted.

None
The specified ports are unusable.

Remote
The specified ports accept only network connection requests. No local logins are permitted.

Defaults Dynamic

Examples
```
Local>> DEFINE PORTS ALL ACCESS LOCAL
```

See Also *Setting Port Access*, page 8-1; *Limiting Port Access*, page 11-22

12.6.11 Set/Define Ports Authenticate

When enabled, prompts incoming user for a username and password to be checked against the authentication database(s) set up with the **Set/Define Authentication** commands.

Restrictions Requires privileged user status.

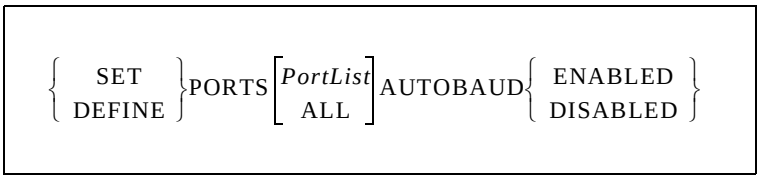
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Clear/Purge Authentication, page 12-151; Set/Define Authentication, page 12-153; Show/Monitor/List Authentication, page 12-177; *Ports Not Using Automatic Protocol Detection*, page 4-14; *Port Restrictions*, page 8-9

12.6.12 Set/Define Ports Autobaud



Enables a port to detect the incoming baud rate and change its own to match at login time. Autobaud must be disabled for Remote and Dynamic port access and for any port offering a service.

Note: *When Autobaud is enabled, you may have to press Return twice or more to allow the port to determine the baud rate.*

Restrictions Requires privileged user status.

Errors Autobaud and Autostart cannot be used together. If you try to configure both options, you will get a message saying that the previously configured option was disabled.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Autobaud works for most baud rates when both ends of the line are the same parity, or when the port is set to 8 bits with no parity and the incoming connection is 7 bits with even parity. Baud rates must be within 3 "steps" of each other, 9600 to 38400 will work, but 9600 to 115200 will not.

Defaults Disabled

Examples
```
Local>> DEFINE PORTS AUTOBAUD DISABLED
```

See Also *Configure Modems*, page 4-18; *Modem Speeds*, page 9-2

12.6.13 Set/Define Ports Autoconnect

If enabled, the port connects automatically to the preferred service upon login. To exit to character (Local>) mode, the Break command can be used. To attach other services, the **Connect** command can be used.

Restrictions Requires privileged user status to use this command on ports other than your own. Secure users may not use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

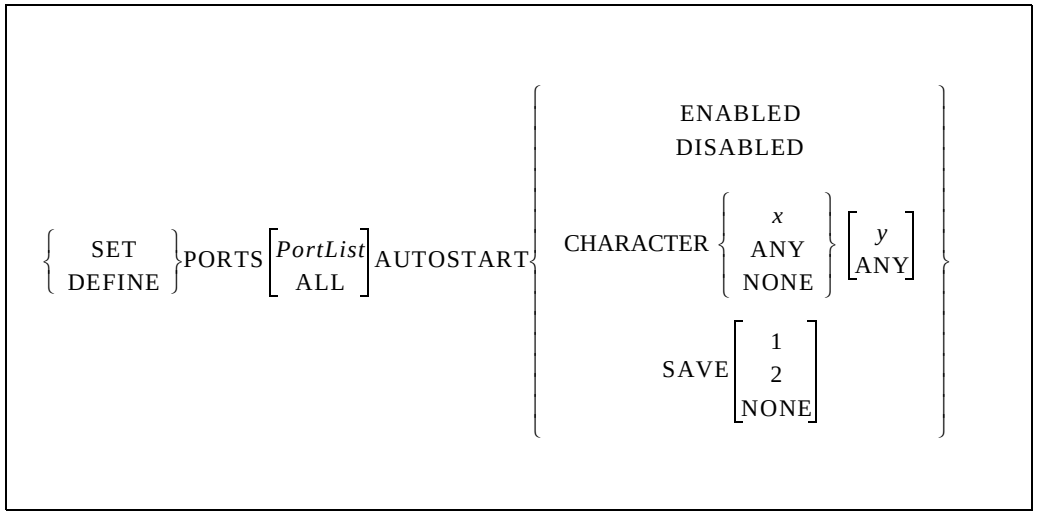
Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

Examples
```
Local>> SET PORTS AUTOCONNECT ENABLED
```

See Also Set/Define Ports Preferred, page 12-79

12.6.14 Set/Define Ports Autostart



Determines whether the specified port will wait for a carriage return or pre-set character(s) before starting a connection. Enabling Autostart causes the port to start connections automatically. Autostart can also be configured to allow a user-defined sequence of one or two characters to initiate sessions.

If the port is in Dedicated mode, the autostart characters can be sent to the host as the first bytes of data. In all other modes, autostart characters are discarded.

Restrictions Requires privileged user status.

Errors Autostart and Autobaud are incompatible. If the port is set for Autobaud, enabling Autostart will disable Autobaud and produce an error message.

The Save parameter is only applicable when the port is configured with a dedicated host.

If Modem Control is enabled, a port enabled for autostart will not be idle unless DSR is held low, and therefore will not be available for connections from the network.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Character
Sets a character that will cause a login event. Users will get the benefit of Autostart without having to hit Return or enable Autostart for extended periods of time.

x
Enter the desired alphanumeric character. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

y
Enter the optional second alphanumeric character. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

Any
Sets a wildcard character.

Note: *If you are using command abbreviation, you must enter Any. Just entering "char a" will be interpreted as setting the character "a" as the autostart trigger.*

None
Clears the autostart character.

Save
Specifies what happens to the characters that start the connection. Either the first and/or second autostart characters will be passed to the host as the first bytes of data, or the characters will be discarded.

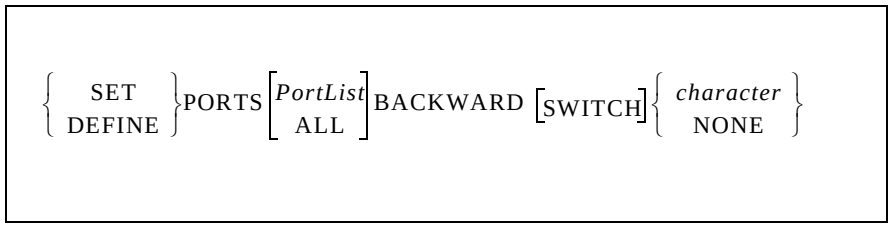
None
Discards the autostart characters.

Defaults Disabled

Examples
```
Local> DEFINE PORTS 2 AUTOSTART ENABLED
Local> DEFINE PORT 1 AUTOSTART CHARACTER A
Local> DEFINE PORT 1 AUTOSTART SAVE 1
```

See Also *Starting Automatically*, page 8-2

12.6.15 Set/Define Ports Backward Switch



Defines a "backward" key. From character (Local>) mode, typing this key functions as if the Backward command was entered; the user may switch to the previous session without entering character mode.

Any key can be specified unless it conflicts with SCS line editing or the Break or Forward keys. The key you specify will be stripped from the data stream, so while it won't interfere with remote operating systems, you will lose any functionality that key would have on local programs.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the **character** parameter.

character
The character to be used as the backward switch. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

None
Clears the current switch character.

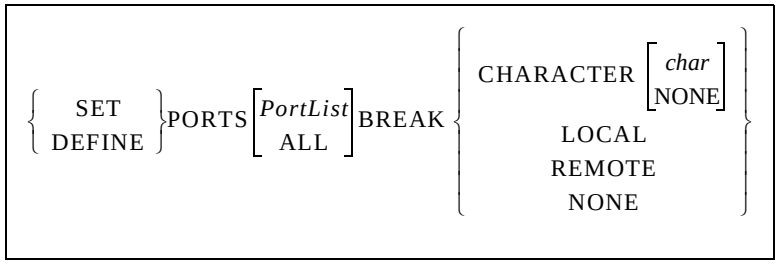
Defaults None configured for serial connections; \02 (Ctrl-B) for virtual port logins

Examples

```
Local>> SET PORT 2 BACKWARD SWITCH \02
```

See Also Backwards, page 12-180; Set/Define Ports Forward Switch, page 12-73; Set/Define Ports Local Switch, page 12-74; *Switching Between Sessions*, page 8-5

12.6.16 Set/Define Ports Break



Allows users to set an alternate Break character, and determines where the Break condition is processed. Examples of using the Break key/character with the Local and Remote settings can be found on page 8-5.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Character
Specifies an alternate Break character. This is useful for terminals that cannot generate a Break condition, Telnet clients that cannot generate a break IAC sequence, and SSH connections.

char
Specify a single character enclosed in quotes. Non-printable characters can be specified using the hexadecimal notation **\xx**.

Local
Pressing the Break key will return to character (Local>) mode.

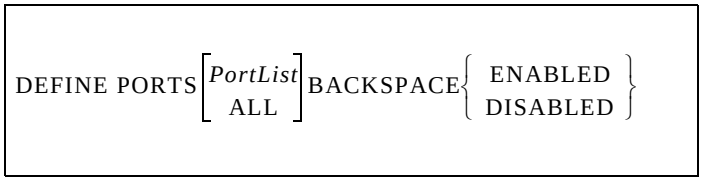
Remote
The Break key is ignored by the SCS and passed through to the remote service.

None
Removes the alternate Break character (when used with the **Character** keyword) or disables Break key processing. Pressing the Break key does nothing.

Defaults Local for serial users, Remote for virtual port connections

See Also Set/Define Ports Backward Switch, page 12-61: Set/Define Ports Forward Switch, page 12-73: Set/Define Ports Local Switch, page 12-74: *Breaking from a Session*, page 8-5: Serial Break Handling, page 3-9.

12.6.17 Define Ports Backspace



Specifies behavior of the Backspace key. If disabled, the Backspace key deletes the character to the left of the cursor. If enabled, Backspace returns the cursor to the beginning of the command line.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

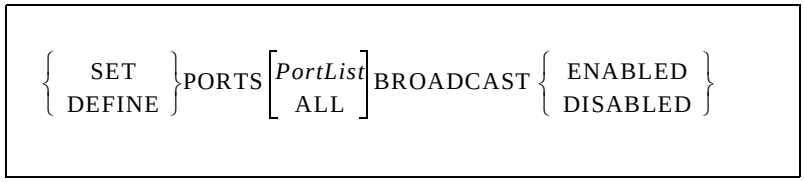
Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

12.6.18 Set/Define Ports Broadcast



Enables or disables other users' broadcasts to this port. Broadcasts are typically disabled when extra messages are not desired on the port's output device.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

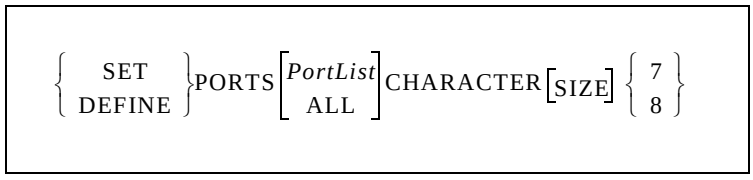
Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Enabled

Examples
```
Local>> SET PORTS BROADCAST ENABLED
```

See Also Broadcast, page 12-180; Set/Define Server Broadcast, page 12-116

12.6.19 Set/Define Ports Character Size



Sets the number of bits per character for the serial port.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Errors Autobaud only works for 8 bits, or for 7 bits with even parity.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

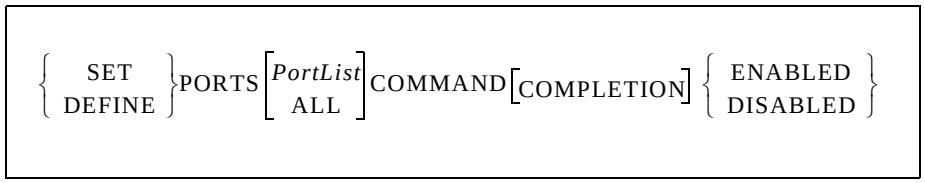
7 or 8
Character size must be either 7 or 8 bits.

Defaults 8 bits

Examples
```
Local>> SET PORTS CHARACTER SIZE 7
```

See Also Set/Define Ports Autobaud, page 12-58; Set/Define Ports Parity, page 12-77; Chapter 9, *Modems*

12.6.20 Set/Define Ports Command Completion



Enables or disables the command completion feature. If enabled, the SCS will attempt to complete partially-typed command words when the user presses the Space or Tab keys.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Errors If the partially-entered command is ambiguous (or if you are typing an optional string), the SCS sends a beep to the terminal.

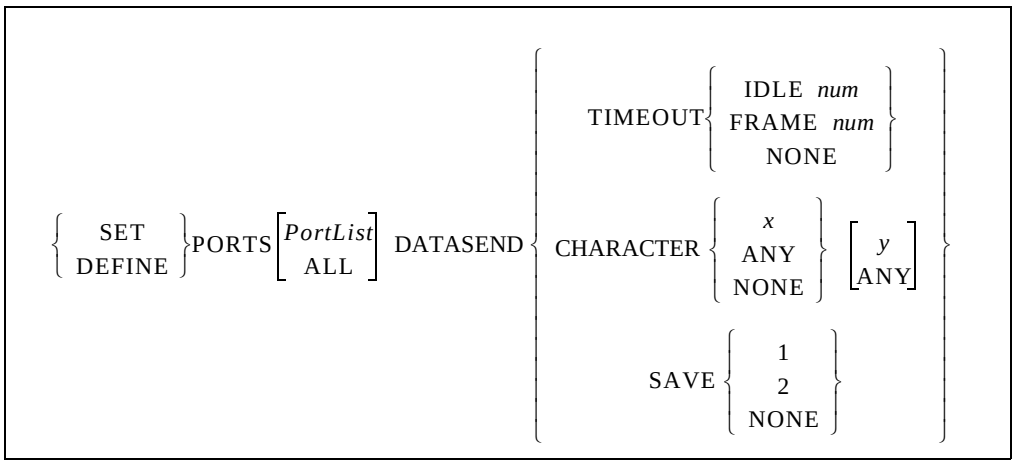
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

Examples
```
Local>> SET PORTS COMMAND ENABLED
```

12.6.21 Set/Define Ports Datasend



Changes the amount of time the SCS will allow serial characters to accumulate before sending them to the host. Several different triggers can be used to notify the SCS when to send the accumulated data. You can specify a "timeout" condition of either the time since the last character was received (the Timeout Idle parameter) or the time since the current "character burst" was started (the Timeout Frame parameters). The timer resolution on the SCS is approximately 20 milliseconds. Any timeout values lower than 30 milliseconds will be approximated as well as possible.

Another option is to set a one- or two-character trigger, specified through the Character parameter, that will cause the SCS to transmit the data. You can also specify whether the trigger characters will be sent to the host as part of the serial data or whether they should be discarded through the Save parameter.

Packets created by the serial handling rules will be queued to the ethernet driver as a single operation, but there is no guarantee that they will be received at the host in a single network read. If the serial input buffer is filled, the accumulated data will be queued to the ethernet driver regardless of the serial handling rules. The serial input buffer size is 1024 bytes.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Timeout
Sets the trigger that allows serial data to be accumulated until a "timeout" condition has been detected.

Idle
Defines the timeout as a period of time since the last character was received.

num
Sets the timeout in milliseconds.

Frame
Defines the timeout as the time since the current "character burst" was started.

None
Clears previous timeout settings, so the transmission takes place whenever the SCS decides to send the data.

Character
Sets a trigger that transmits any accumulated data as soon as the specified one or two byte character sequence is detected in the data stream.

x
Enter the desired alphanumeric character. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

Any
Sets any character as the trigger.

None
Clears any previous trigger characters.

y
Enter the optional second alphanumeric character. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

Save
Specifies what happens to the matched trigger characters. Either the first character or both characters will be passed to the host as the first bytes of data, or the characters will be discarded.

Defaults

30 (msec)

Examples

```
Local> DEFINE PORTS ALL  DATASEND DELAY CHARACTER 50
```
(Triggers data transmission for 50 milliseconds since the last character was received.)

```
Local> DEFINE PORTS ALL  DATASEND DELAY FRAME 150
```
(Triggers data transmission for 150 milliseconds since the current "character burst" was started.)

```
Local> DEFINE PORT 2 DATASEND CHARACTER Z
Local> DEFINE PORT 2 DATASEND SAVE 1
```
(Transmits any accumulated data, including "Z," as soon as the "Z" character is detected in the data stream.)

See Also

Set/Define Ports Autostart, page 12-60; *Transmitting Serial Data*, page 12-14

12.6.22 Define Ports Dedicated

Sets up a dedicated Rlogin, SSH, or Telnet host or service that the specified port will connect to whenever it is logged in. The type of dedicated connection is specified with the environment string. If no environment string is specified, the connection will be Telnet by default.

If you are logged in to a dedicated port, you will be logged off the server when the remote service is logged out.

There should be no spaces between the hostname, colon, and environment string.

Note: *Dedicating all SCS ports is dangerous, as it leaves no easy way to log into the server. (In other words, users can no longer quickly access the Local> prompt.) If all ports are dedicated, users must connect via the console ports, or the SCS must have incoming logins enabled.*

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

None
Clears any existing Dedicated service.

Rlogin
Dedicates the port to the specified Rlogin host. Must be used in conjunction with the **host** parameter.

SSH
Dedicates the port to the specified SSH host. Must be used in conjunction with the **host** parameter.

TCP
Dedicates the port. Must be used in conjunction with the **host** parameter.

host
A text host name or an IP address in standard numeric format (for example, 192.0.1.183).

envstring
Sets up the connection environment before the session is started. For a description of all available environment strings, see Appendix A, *Environment Strings*. If no environment string is specified with the TCP parameter, the connection will default to a Telnet connection.

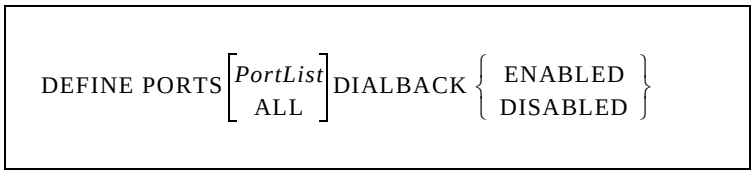
Examples

```
Local>> DEFINE PORT 5 DEDICATED 192.0.1.221
Local>> DEFINE PORT 2 DEDICATED irvine:+D
```

See Also

Connect, page 12-20; Set/Define Ports Preferred, page 12-79; Define Ports PPPdetect, page 12-84; Set/Define Ports SLIPdetect, page 12-88; Show/ Monitor/List Ports, page 12-96; *Setting Session Characteristics*, page 8-7

12.6.23 Define Ports Dialback



Turning on Dialback causes the SCS to check the dialback table (see **Set/Define Dialback**) each time a user logs in. If the entered username is not in the table, the port is logged out. If the username is in the table, the port is logged out and the SCS sends the dialback string to the port and awaits a second login. Typically, the dialback string will cause the modem attached to the port to call the user back at a certain telephone number for security reasons. Ports with dialback enabled have a 30-second time limit for entering the username when logging in.

In order to use Dialback functionality, modem control must be enabled, and a modem profile must be associated with the port. When Dialback is enabled, Modem Control is enabled by default. However, disabling Dialback does not disable Modem Control; Modem Control must explicitly be disabled if so desired.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Examples

```
Local>> DEFINE PORT 3 DIALBACK ENABLED
```

See Also Set/Define Dialback, page 12-165; Show/Monitor/List Dialback, page 12-178; Define Ports Modem Control, page 12-8; Define Ports Modem Type, page 12-16; Show/Monitor/List Ports, page 12-96; *Dialback*, page 8-12; *Dialback*, page 11-5

12.6.24 Set/Define Ports DSRLogout

When enabled, the port will be logged out when the port's DSR signal is dropped. This usually only occurs when the attached terminal device is powered off or disconnected; it is intended to keep users from switching terminal lines to access other sessions. Any open connections will be closed before logging out.

Restrictions Requires privileged user access.

Errors Modem Control and DSRLogout are mutually exclusive.

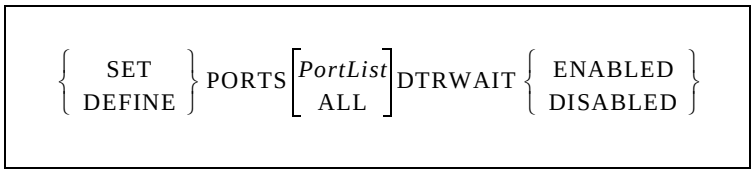
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also *DSR Logouts*, page 8-11; *Serial Signals*, page 8-20

12.6.25 Set/Define Ports DTRWait



If enabled, the SCS will not assert the DTR signal on the serial port until a user logs into the port, connects to the port via a service, or connects to the port via a Telnet connect. When the port is idle, DTR will not be asserted.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Define Ports Modem Control, page 12-8; Set/Define Ports Flow Control, page 12-72; *DTR (Data Terminal Ready)*, page 8-22

12.6.26 Define Ports Event Email Serialdata

Enables email notification for the serial buffering feature. This command automatically changes the specified port's access to Remote if not already set.

When email notification is enabled, an email is triggered when the specified serial port receives a burst of 20 or more characters in its serial log. The port will buffer the incoming data for up to 25 seconds or until the log file reaches 1500 bytes before sending the email, which contains the current contents of the log file. Any data that comes in after that 25 seconds will be discarded. Email can not be sent from the same port more than once every 10 minutes.

Restrictions Requires privileged user status.

Port buffering must be enabled (**Set/Define Ports Serial Log**) for email notification to work.

Parameters

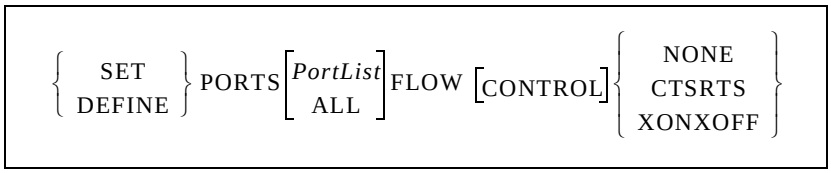
PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults set to None

See Also Set/Define Ports Serial Log, page 12-85; Define Email, page 12-55; *Event Port Logging*, page 3-2; *Email Alerts for Serial Events*, page 3-3

12.6.27 Set/Define Ports Flow Control



Sets the type of flow control on the port.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

None
No flow control will be performed.

CTSRTS
Sets the flow control type to RTS/CTS.

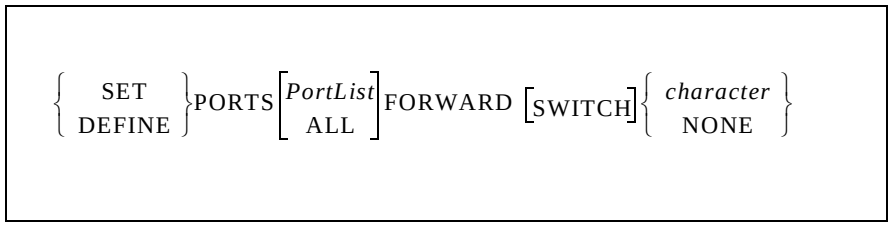
XONXOFF
Sets the flow control type to XON/XOFF.

Defaults XON

Examples Local>> SET PORTS FLOW CONTROL CTS

See Also Set/Define Ports DTRWait, page 12-71; *Flow Control*, page 8-18

12.6.28 Set/Define Ports Forward Switch



Defines a “forward” key. From character (Local>) mode, typing this key functions as if the Forward command was entered; the user may switch to the previous session without entering character mode.

Any key can be specified unless it conflicts with SCS line editing or the Break or Backward keys. The key you specify will be stripped from the data stream, so while it won’t interfere with remote operating systems, you will lose any functionality that key would have on local programs.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the **character** parameter.

character
The character to be used as the forward switch. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

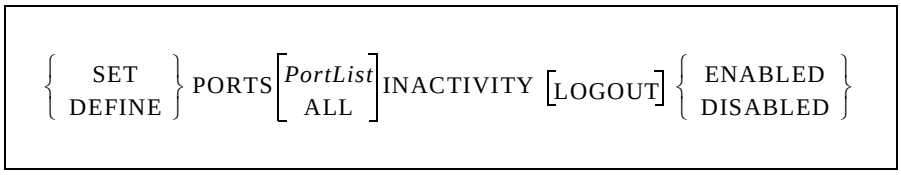
None
Clears the current switch character.

Defaults None configured for serial connections; \06 (Ctrl-F) for virtual port logins

Examples Local>> SET PORT 2 FORWARD SWITCH \02

See Also Forwards, page 12-186; Set/Define Ports Backward Switch, page 12-61; Set/Define Ports Local Switch, page 12-74; *Switching Between Sessions*, page 8-5

12.6.29 Set/Define Ports Inactivity Logout



Enables automatic logout of the port if it has been "inactive" for a set period of time. Inactive is defined as having no keyboard or network activity on the port. The port's open connections (if any) will be closed before logging out.

Note: *The inactive period is configured using the Set/Define Server Inactivity command.*

This command is ignored for remote networking connections. See the **Define Site Idle** command.

Restrictions Requires privileged user status.

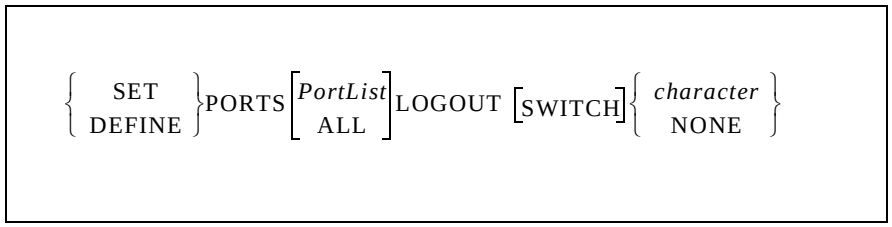
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Define Site Idle, page 12-139; Set/Define Server Inactivity, page 12-118

12.6.30 Set/Define Ports Local Switch



Defines a "local switch" key. From character (Local>) mode, typing this key functions as if the Forward command was entered; the user may switch to the previous session without entering character mode.

Any key can be specified unless it conflicts with SCS line editing or the Break or Forward/Backward keys. The key you specify will be stripped from the data stream, so while it won't interfere with remote operating systems, you will lose any functionality that key would have on local programs.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the **character** parameter.

character
The character to be used as the local switch. To specify a control character, use escaped hex (\xx). For example, Ctrl-B (ASCII character 0x02) would be specified as \02.

None
Clears the current switch character.

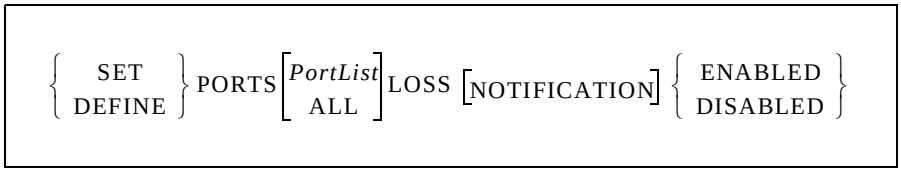
Defaults None configured for serial connections; \0c (Ctrl-L) for virtual port logins

Examples

```
Local>> SET PORT 2 LOCAL SWITCH \02
```

See Also Set/Define Ports Break, page 12-62; Set/Define Ports Backward Switch, page 12-61; Set/Define Ports Forward Switch, page 12-73; *Port-Specific Session Configuration*, page 8-4

12.6.31 Set/Define Ports Loss Notification



Sends the terminal device a Ctrl-G (Bell) when a typed character is lost due to a data error or an overrun on the SCS.

Restrictions Requires privileged user status if you want to use this command on a port other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

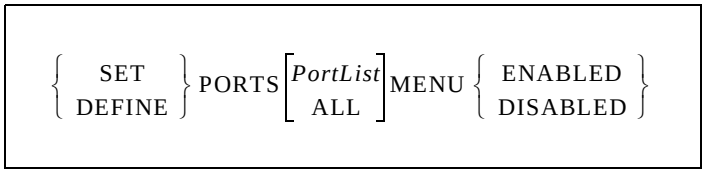
Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Enabled

Defaults Enabled

See Also *Notification of Character Loss*, page 8-13

12.6.32 Set/Define Ports Menu



Specifies whether or not the port will be placed in menu mode at login. If it is disabled, the Local> prompt will appear at login. If it is enabled, a menu screen will be displayed; the Local> prompt is not accessible.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

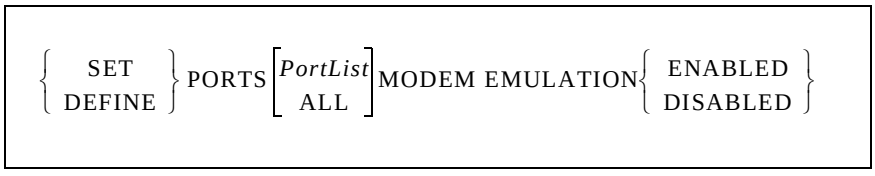
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Clear/Purge Menu, page 12-111; Set/Define Menu, page 12-112; Show/ Monitor/List Menu, page 12-129; *Enabling Menu Mode*, page 8-12; *Configuring Menu Mode*, page 3-4

12.6.33 Set/Define Ports Modem Emulation



Specifies whether or not to enable the SCS to emulate a modem for performing network connections. If it is disabled, the Local> prompt will appear at login. If it is enabled, the SCS will respond to “AT” commands.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

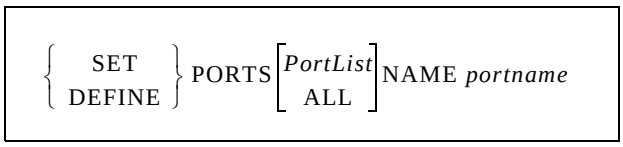
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also Modem Emulation, page 8-23

12.6.34 Set/Define Ports Name



Sets a unique name for each port, or a common name for a group of ports. Giving the same name to several ports may be desirable, for example, when you want to label them as modem connection ports or dedicated SLIP/PPP ports.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

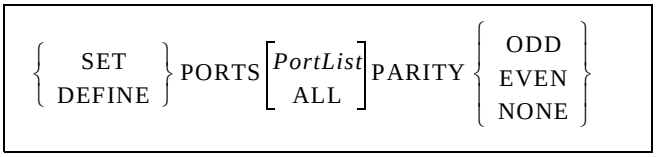
portname
A name of up to 16 characters composed of alphanumerics or the underscore ("_") character. If the name is not enclosed in quotation marks, it will be converted to uppercase.

Note: *The default portname is Port_n, where n is the port number.*

Examples Local>> SET PORT 2 NAME "highspeed_modem"

See Also *Naming a Port*, page 8-13

12.6.35 Set/Define Ports Parity



Sets the serial port's parity to Odd, Even, or None (no parity). Note that changing the parity may affect the configured character size.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Errors Autobaud will not work unless the port is using 8 bit characters, or 7 bit characters with even parity.

Parameters

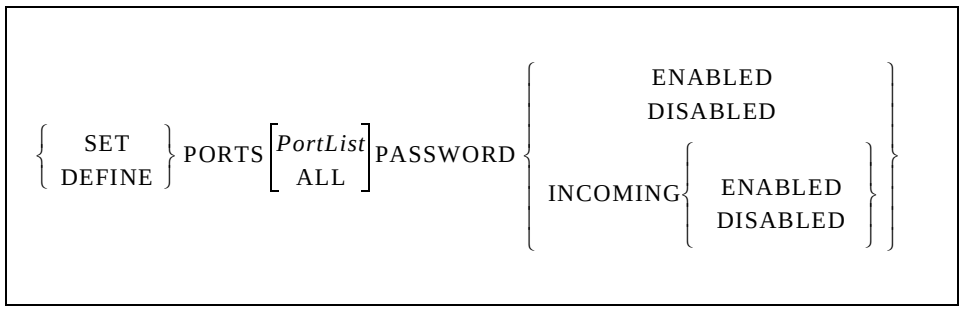
PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults None (no parity)

See Also Set/Define Ports Autobaud, page 12-58; Set/Define Ports Character Size, page 12-64; *Serial Port Configuration*, page 8-13

12.6.36 Set/Define Ports Password



Controls whether or not the login password is required to log in to an SCS port. The **Set/Define Server Login Password** command is used to set the password.

Restrictions Requires privileged user status.

Errors The virtual port (port 0) password must be enabled or disabled with the Define command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

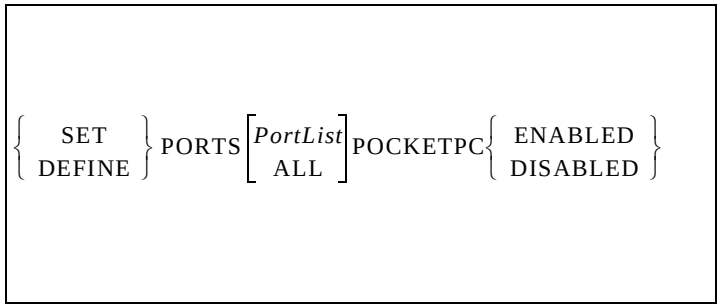
Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Incoming
When enabled, users who Telnet or SSH directly to the target serial port are forced to provide the login password.

Defaults Disabled

See Also Set/Define Server Login Password, page 12-121; *Login Password*, page 8-10

12.6.37 Set/Define Ports PocketPC



Allows the SCS to work with PocketPC type devices. Enables and disables client/server negotiation when starting a PPP connection.

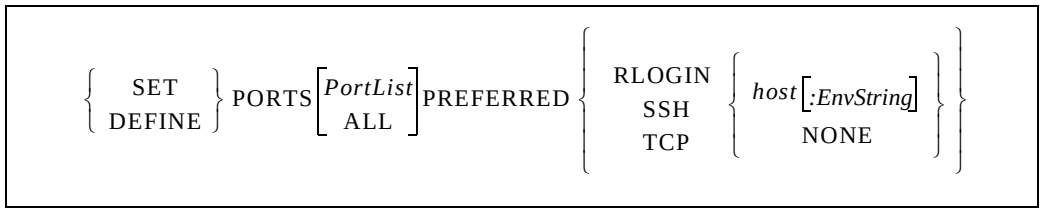
Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

See Also Pocket PC PPP Support, on page 12-7

12.6.38 Set/Define Ports Preferred



Specifies a default service for this port. The SCS will attempt to use the preferred service for Autoconnecting, as well as when no service name is specified in a **Connect**, **Telnet**, **SSH**, or **Rlogin** command.

If no environment string is specified, the service will be a Telnet connection by default.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Rlogin
Specifies that the service is a default Rlogin connection. Must be used in conjunction with the **hostname** parameter.

SSH
Specifies that the service is a default SSH connection. Must be used in conjunction with the **hostname** parameter.

TCP
Specifies that the service is a default TCP connection. If there is no local nameserver defined, the host must be specified with a numeric hostname. Must be used in conjunction with the **hostname** parameter.

hostname
TCP host name of 40 characters or less, or an IP address in standard numeric format (for example, 192.0.1.3).

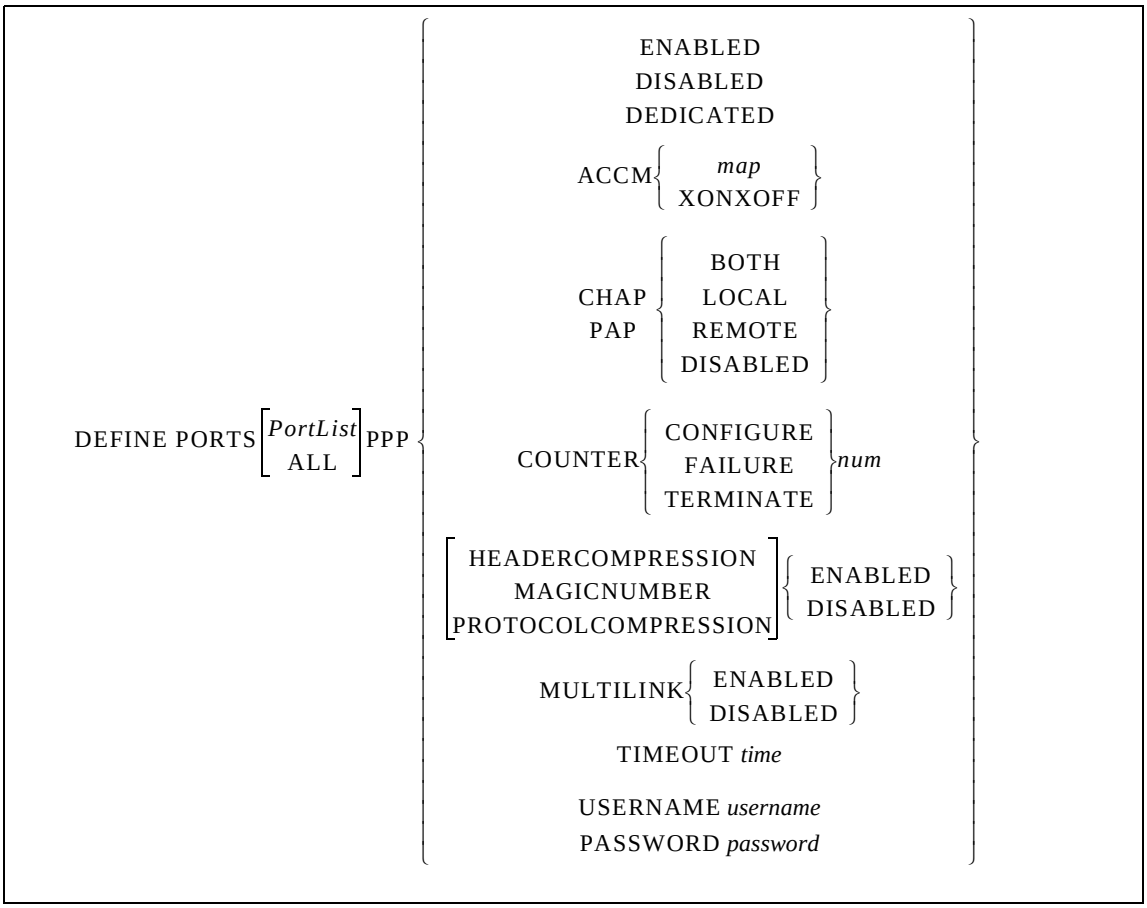
envstring
Sets up the connection environment before the session is started. The string is constructed with a sequence of key letters, some of which are prefaced by either the "+" or "-." For the available key letters and usage instructions, see Appendix A, *Environment Strings*. If no environment string is specified with the TCP parameter, the connection will default to a Telnet connection.

Defaults None

Examples
```
Local>> SET PORT 2 PREFERRED TELNET 192.0.1.3
Local>> SET PORT 3 PREFERRED todd
```

See Also Connect, page 12-20; Rlogin, page 12-22; Set/Define Ports Autoconnect, page 12-59; Define Ports Dedicated, page 12-68; *Setting Session Characteristics*, page 8-7

12.6.39 Define Ports PPP



Enables PPP to run on the specified port and configures PPP-related settings. This command does not start PPP. You can use this command to specify a per port username and password to authenticate information outbound from the SCS, for example, CHAP Secrets. If you do not specify the per port fields, the username and password from the appropriate site is used for the connection.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Enabled/Disabled
Enables or disables PPP on a specified port, but does not start PPP.

Dedicated
Configures a port to always be in PPP mode. The port will automatically run PPP when it is started. No other protocol can be run on the port; it will continue to run until it is logged out.

ACCM
Enters an asynchronous control map in hexadecimal. Bits turned on represent ASCII characters that will be escaped in the PPP data stream. See *Character Escaping* on page 7-1 for more information.

map
A hexadecimal value between 0x00000000 and 0xffffffff.

XONXOFF
A default map that escapes the XON and XOFF software flow control characters.

CHAP
Configures the Challenge Handshake Authentication Protocol (CHAP). See *PPP Authentication* on page 7-2

PAP
Configures the Password Authentication Protocol (PAP). See *PPP Authentication* on page 7-2 for more information.

Both
Enables authentication for both this node and the remote node.

Disabled
Turns off CHAP/PAP authentication.

Local
The SCS will authenticate itself to the SCS.

Remote
The remote node will authenticate itself to the SCS.

Counter
Specifies the number of configuration retries for the Link protocol and all Network Control protocols.

Configure
Specifies the number of Configure-Requests to send before giving up negotiation.

Failure
Specifies the number of Configure-Naks to send before giving up negotiation.

Terminate
Specifies the number of Terminate-Requests to send before disconnecting.

num
An integer between 1 and 255.

HeaderCompression
Enables or disables compression of PPP headers. See *Header Compression* on page 7-1 for more information.

MagicNumber
Controls PPP magic numbers.

ProtocolCompression
Configures the compression of protocol information in PPP.

Timeout
Sets the timeout value, in tenths of seconds, for the Link Control Protocol and all Network Control protocols.

time
An integer between 1 and 255, representing a length of time in tenths of seconds. For example, a setting of 25 equals 2.5 seconds.

Multilink
Allows the SCS to add the specified port to a PPP connection to increase bandwidth on demand.

Username
A specific per-port username for authenticating data outbound from the SCS, for example, CHAP Secrets.

Password
A specific per-port password for authenticating data outbound from the SCS, for example, CHAP Secrets.

Defaults

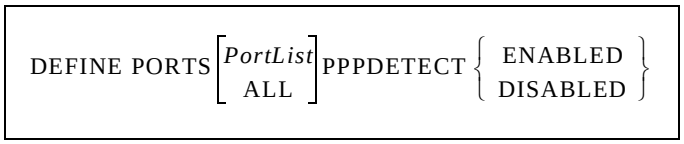
PPP: Enabled
Map value: 0x00000000
CHAP: Both
PAP: Both
Counter Configure: 10 requests
Counter Failure: 5 Configure-NAKs
Counter Terminate: 2 requests
HeaderCompression, MagicNumber, ProtocolCompression: Enabled
Timeout: 30 seconds
Multilink: Disabled

Examples

```
Local>> DEFINE PORT PPP ACCM 0X000A0000
Local>> DEFINE PORT PPP CHAP LOCAL
Local>> DEFINE PORT PPP PAP REMOTE
Local>> DEFINE PORT PPP COUNTER FAILURE 5
Local>> DEFINE PORTS 2-4 PPP HEADERCOMPRESSION ENABLED
Local>> DEFINE PORT 2 PPP MAGICNUMBER ENABLED
Local>> DEFINE PORT 3 PPP TIMEOUT 25
Local>> DEFINE PORT PPP MULTILINK ENABLED
```

See Also Define Ports PPPdetect, page 12-84; Purge Port PPP, page 12-53; Show/Monitor/List Logging PPP, page 12-179; Set PPP, page 12-95; Show/Monitor/List Ports PPP, page 12-96; Chapter 7, *PPP*

12.6.40 Define Ports PPPdetect



Automatically detects incoming PPP characters and starts running PPP.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Enabled

See Also Define Ports PPP, page 12-81; Purge Port PPP, page 12-53; Set/Define Logging PPP, page 12-172; Set PPP, page 12-95; Show/Monitor/List Ports PPP, page 12-96; Chapter 7, *PPP*

12.6.41 Set/Define Ports Printer

If enabled, the server will verify that the port is online before sending data to it.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

12.6.42 Set/Define Ports Security

Setting a port to Secure status restricts its access to SCS commands and the ability to get information about other ports using Show/List commands. Privileged commands are not available to secure users. Certain other commands cannot be entered for a port other than the secure user's own port.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also *Preferred/Dedicated Protocols & Hosts*, page 8-8; Chapter 11, *Security*

12.6.43 Set/Define Ports Serial Log

Spools idle serial data to the RAM disk, where it is logged into a file that can be accessed later. The file will be saved in the form "/ram/Port_xx.log" where xx is the port number. This command also indicates the maximum size of the log file and changes the specified port to Access Remote.

If the file size reaches the limit set by this command, the file will be truncated to half its current size, and will start logging again. The oldest data will be discarded.

To stop serial logging, enter 0 as the file size.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

number
The maximum size, in KB, of the log file. Enter an integer between 0 and 250. A value of 0 turns logging off.

Defaults No logging

See Also Set/Define Ports Access, page 12-57; Define Email, page 12-55; Define Ports Event Email Serialdata, page 12-71; Event Port Logging, page 12-2

12.6.44 Set/Define Ports Session Limit

Limits the number of active sessions on a port. The maximum number of session configured for a port cannot exceed the server session limit.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

limit
An integer between 0 and 8.

None
Allows the maximum number of sessions.

Defaults Limit: 4 sessions

See Also Set/Define Server Session Limit, page 12-126; *Port-Specific Session Configuration*, page 8-4

12.6.45 Set/Define Ports Signal Check

Determines whether or not the DSR signal will be checked for when remote connections to the port are made. If enabled, remote connections to the port will not be permitted unless the DSR signal is asserted.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also *DSR for Controlling Remote Logins*, page 8-21

12.6.46 Define Ports SLIP

The Enabled and Disabled parameters determine whether or not SLIP can be run on the specified port. The Dedicated parameter devotes that port to SLIP mode.

Restrictions Requires privileged user status.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Dedicated
The specified port will automatically run SLIP when it is started. No other protocol can be run on the port; it will continue to run SLIP until it is logged out.

Defaults Disabled

See Also Set/Define Ports SLIPdetect, page 12-88; Set SLIP, page 12-96; Show/ Monitor/List Ports SLIP, page 12-96; *Starting PPP/Slip for Incoming Connections*, page 4-11

12.6.47 Set/Define Ports SLIPdetect

Automatically detects and starts running SLIP. Be aware that automatically running SLIP is a potential security hazard.

Restrictions Requires privileged user status.

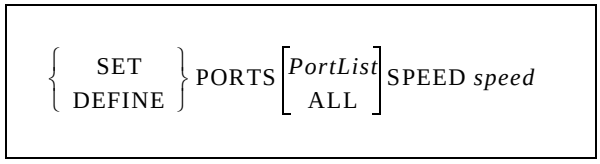
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

See Also *Starting PPP or SLIP Using Automatic Protocol Detection*, page 4-12

12.6.48 Set/Define Ports Speed



Specifies the baud rate of the port.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Errors An error is displayed for illegal baud rates.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

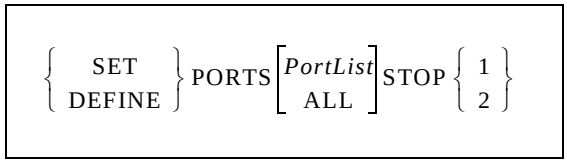
speed
One of the following baud rates: 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, and 230400.

Defaults 9600 baud

Examples Local>> SET PORTS SPEED 2400

See Also Set/Define Ports Autobaud, page 12-58; *Modem Speeds*, page 9-2

12.6.49 Set/Define Ports Stop



Specifies the stop bit count for the port. The default is to use one stop bit.

Restrictions Requires privileged user status if you want to use this command on ports other than your own. Secure users may not use this command.

Errors An error is displayed if an invalid stop bit number is entered.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults 1 stop bit

12.6.50 Set/Define Ports Telnet Pad

If Telnet Pad is enabled (the default), the server automatically pads carriage returns with null characters for Telnet sessions.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters

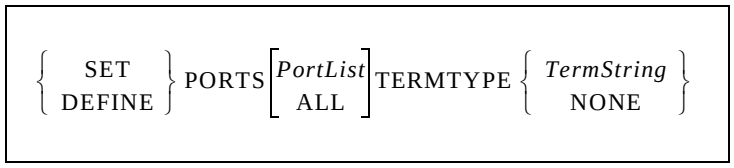
PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Enabled

See Also *Padding Return Characters*, page 8-14

12.6.51 Set/Define Ports TermType



Specifies a terminal type for the port. The terminal type is reported to the destination node in Telnet and Rlogin sessions. Example terminal types might be VT100 or IBM1000.

Restrictions Requires privileged user status if you want to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

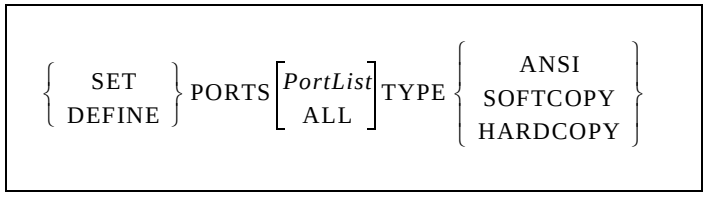
TermString
Enter a string of up to 8 characters in length.

None
Clears the field. There is no terminal type configured by default.

Defaults None defined

See Also *Specifying a Terminal Type*, page 8-14

12.6.52 Set/Define Ports Type



Describes the type of device connected to the port.

Restrictions Requires privileged user status to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

ANSI
VT100 compatible devices.

Softcopy
VT100 without clear screen or cursor controls.

Hardcopy
Deleted characters are echoed between backslashes; there is no cursor movement.

Defaults Softcopy

See Also *Setting the Device Type,* page 8-14

12.6.53 Set/Define Ports Username

Used to specify a username for the port. When the username is defined, you will not be asked for one when logging in to the port.

Restrictions Requires privileged user status to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

username
A name of up to 16 characters in length, c**onverted to all uppercase unless enclosed in quotes.**

None
Clears a current username.

Defaults None

See Also *Specifying a Username*, page 8-13

12.6.54 Set/Define Ports Verification

When enabled, the server will issue informational messages whenever a session is connected, disconnected, or switched.

Restrictions Requires privileged user status if you wish to use this command on ports other than your own.

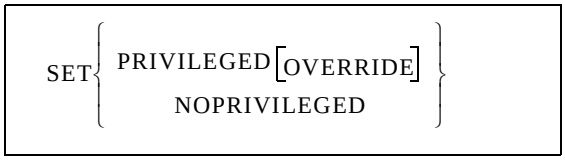
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Enabled

See Also *Port-Specific Session Configuration*, page 8-4

12.6.55 Set Privileged/Noprivileged



Changes the current port's privilege status. Only one port on the server can be privileged at any time. The Override parameter is provided to force your current port to become the privileged port (and the previously privileged port loses the privilege).

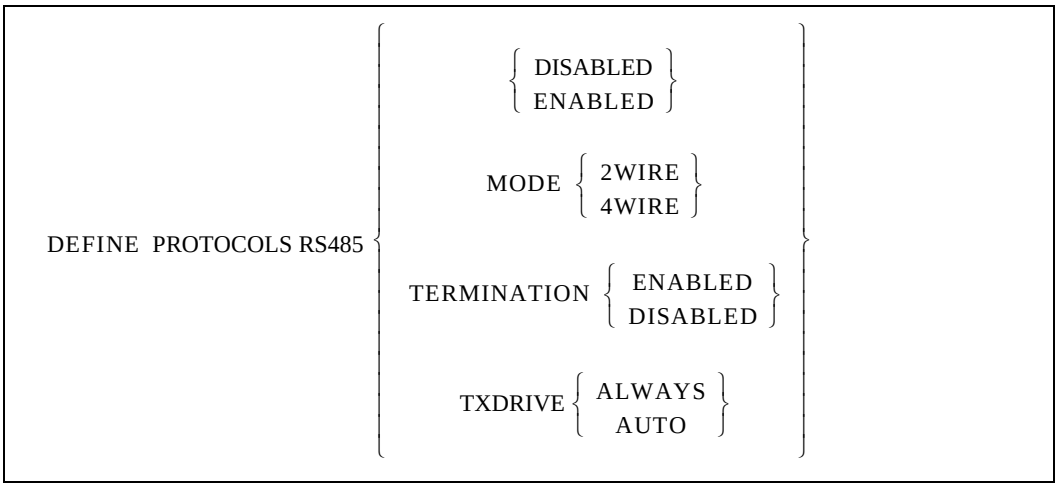
When changing your port to privileged status, you will be queried for the privileged password. The factory default privileged password is system; this password can be changed with the Set Server Privileged Password command. If the password is forgotten, the server can be reset to factory defaults using the Initialize commands.

Restrictions To use the Privileged parameter, you must know the privileged password. Secure users cannot become privileged.

Examples
```
Local>> SET NOPRIVILEGED
Local>> SET PRIVILEGED OVERRIDE
```

See Also Set/Define Ports Security, page 12-85; *Privileged Password*, page 2-8

12.6.56 Define Protocols RS485



Enables RS-485 networking and configures the necessary RS-485 parameters on the SCS200.

Restrictions Requires privileged user status.

Errors Only applies to the SCS200.

In two-wire mode, TXDrive must be set to Auto.

Parameters

Enabled/Disabled
Enables or Disables RS-485 mode. By default, the SCS is configured for RS-232 networking.

Mode
When RS-485 Mode is enabled, you must choose either two-wire or four-wire mode. If you do not explicitly set a mode with this command, the SCS will default to four-wire mode.

2Wire
Sets the SCS to use two-wire mode.

4Wire
Sets the SCS to use four-wire mode.

Termination
Enable termination whenever you are using long cable runs and Disable it at other times. Only end nodes should be terminated.

TXDrive
Controls how the SCS drives the TX pin.

Always
Sets the SCS to drive TX. The SCS will never tristate TX, even if data is not being sent. Always is only valid for four-wire mode.

Auto
Sets the SCS to drive TX only when transmitting, and tristate when not transmitting.

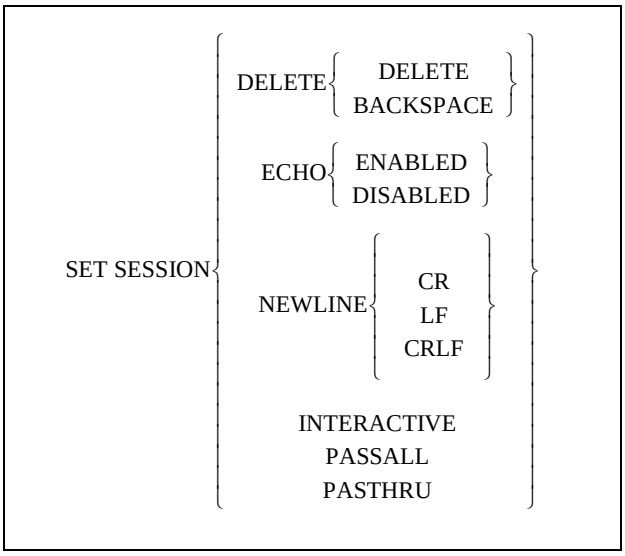
Defaults

Disabled
Mode = 4Wire
Termination disabled
TXDrive = Always

See Also

Show RS485, page 12-98; *RS-485 Configuration*, page 8-15

12.6.57 Set Session



Specifies the characteristics for the current session.

Parameters

Delete
Specifies which character to send as the delete character. Set Session Delete sends a delete character (ASCII 0x7f). This command has no effect if Pasthru or Passall are in effect. This command and the Newline command may be helpful if you are getting odd output from a Telnet session.

Backspace
Set Session Delete Backspace sends a backspace character (ASCII 0x8, or Ctrl-H).

Echo
Enabling asks the unit to echo for TCP connections. The default is Disabled, on the assumption that the remote host will provide echoing.

Newline
Changes what is sent to the remote service when you press the newline (usually <Return>) key. This command has no effect if Pasthru or Passall (see below) are in effect.

CR
Send carriage returns (ASCII 0xA) only.

LF
Send linefeeds (ASCII 0xD) only.

CRLF
Send both carriage return and linefeed.

Interactive
Allows server-specific keys (i.e. Forward, Backward, and Local) and messages to be interpreted by the unit.

Passall
Disables server interpretation of switch characters, messages, and XON/XOFF flow control. Used for binary transfers, such as executable files and graphics.

Pasthru
Disables server interpretation of switch characters and server messages, but not XON/XOFF flow control. Used for ASCII file transfers.

Defaults
Delete: Delete
Newline: CR

Examples
```
Local>> SET SESSION DELETE BACKSPACE
Local>> SET SESSION NEWLINE CRLF
```

See Also
Port-Specific Session Configuration, page 8-4

12.6.58 Set PPP

```
SET PPP [ IPADDRESS address
          SiteName ]
```

Starts PPP on this port using the specified site's configuration. If no site is specified, a site with the default site characteristics will be used.

Parameters

IPaddress
Defines the non-negotiable remote IP address.

address
An IP address in standard numeric format (for example, 193.0.1.50).

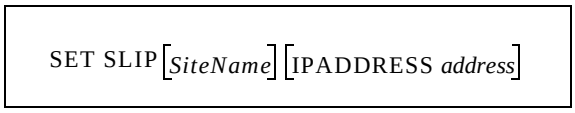
SiteName
A name of 12 characters or less. If no site name is given, a site with the default site characteristics will be used.

Examples

```
Local>> SET PPP irvine
Local>> SET PPP allison IPADDRESS 191.1.1.1
```

See Also Define Ports PPP, page 12-81; Chapter 7, *PPP*

12.6.59 Set SLIP



Starts SLIP on this port using the specified site's configuration.

Parameters

SiteName
A site name of up to 12 characters. If no site name is given, a site with the default site characteristics will be used.

IPaddress
Defines the non-negotiable remote IP address.

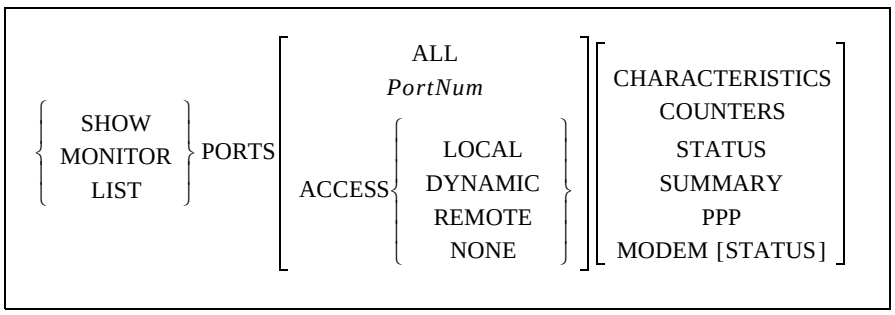
address
An IP address in standard numeric format (for example, 192.75.2.0).

Examples

```
Local> SET SLIP irvine
Local> SET SLIP allison IPADDRESS 192.0.1.221
```

See Also Set/Define Ports SLIPdetect, page 12-88; *Starting PPP/Slip for Incoming Connections*, page 4-11

12.6.60 Show/Monitor/List Ports



These commands display information about the server's ports. The current port is the default, unless another port number or All is specified. You can also get information about all the local ports having a particular Access value. If no keywords are added to the command, the current port's Characteristics will be shown.

If the port is a virtual port, irrelevant information (such as baud rate, parity, or flow control) will not be displayed. Any List command performed for a virtual port will display the template port's configuration.

Restrictions

You must be the privileged user to use the Monitor command.

Secure ports cannot Show or List ports other than their own.

Errors

Status and Counters parameters are not valid with List.

Counters is not valid for virtual ports.

Parameters

All
Displays information for all ports.

PortNum
Specifies a particular port.

Access
Display ports that match a specified access-type. Must be used in conjunction with the **Local**, **Dynamic**, **Remote**, or **None** parameter.

Local
Displays ports set to Local access. Local access restricts logins on the port to local users.

Dynamic
Displays ports set to Dynamic access. Dynamic access permits local or remote users to log into the port.

Remote
Displays ports set to Remote access. Remote access restricts logins on the port to remote (network) users.

None
Displays ports with access set to None. None prevents all access to the port, including user logins.

Characteristics
Displays information from the operational database about the specified ports, including the port's settings, such as baud rate, parity, preferred services, name, username, port buffering setting, and group codes.

Counters
Displays the port's local and remote accesses as well as any communication errors.

Status
Displays information regarding the port's serial connections, including the current flow control state and the state of the DSR and DTR signals.

Summary
Displays a one-line summary of information about the specified ports. The information includes type of access, status, and services offered. The Summary option shows the access type, any offered services, and the login status of the port.

PPP
Displays information about the Point to Point Protocol's Link Control Protocol on the specified ports.

Modem
Displays information about modem control and configuration strings on the specified ports.

Status
The Modem Status option shows the last connect speed of the modem connected to the specified port(s), and the last available Caller-ID information for the port(s). Modem control must be enabled for this command to work.

Note: *The Modem Status option is of no use for remote access or no access ports.*

Examples

```
Local> SHOW PORT ALL SUMMARY
Local> LIST PORT ACCESS DYNAMIC COUNTERS
```

See Also Chapter 8, *Chapter 8*

12.6.61 Show RS485

```
SHOW RS485
```

Displays the current RS-485 networking settings, including wire mode, termination, and TXDrive.

Restrictions Only applies to the SCS200.

See Also Define Protocols RS485, page 12-93; *RS-485 Configuration*, page 8-15

12.6.62 Show/Monitor Sessions

```
{ SHOW    } SESSIONS [ PORT PortNum ]
{ MONITOR }          [ ALL         ]
```

Displays information about the specified sessions.

Restrictions You must be the privileged user to use the Monitor command.

Secure users cannot specify Port or All.

Parameters

PortNum
Specifies a particular port.

All
Displays the sessions currently running on all ports.

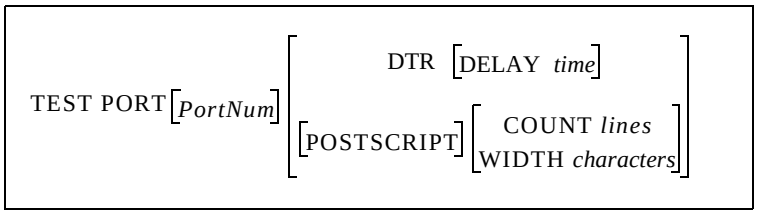
Examples

```
Local> SHOW SESSION
Local> SHOW SESSION PORT 5
```

See Also

Set/Define Ports Security, page 12-85; *Port-Specific Session Configuration*, page 8-4

12.6.63 Test Port



Tests a serial port's connection by sending a continuous stream of ASCII alphabetic characters until the number of lines specified by Count is reached. You can stop the test by pressing any key.

Restrictions

Non-privileged users may only test their own port.

Virtual and multisession-enabled ports can only be tested by the user on that port.

Parameters

PortNum
Specifies a particular SCS port.

PostScript
Sends a Postscript test page to the port instead of ASCII data.

Count
Specifies the number of test lines to be send, or if in postscript mode, the number of pages to print. Any character will terminate the test. Must be used in conjunction with the lines parameter.

lines
The number of lines to be sent to the port. There is no line limit.

Width
The number of characters per line in the test pattern. Must be used in conjunction with the characters parameter.

characters
Enter an integer between 1 and 132, inclusive.

DTR
Lowers and then raise the DTR signal on the serial port. If a delay is not specified, DTR will lower for approximately one second and then raise.

Delay
Lowers DTR will for the specified delay length, then raises DTR.

time
Enter a delay time from 50 to 3,000 (milliseconds).

Examples

```
Local> TEST PORT
Local> TEST PORT 4 WIDTH 45 COUNT 5
```

12.6.64 Unlock Port

UNLOCK PORT *PortNum*

Unlocks a locked port, which may be necessary if the user has locked the port and forgotten the password. The command does nothing if the port is already unlocked.

Restrictions Requires privileged user status.

Parameters

PortNum
The number of the locked SCS port.

Examples

```
Local>> UNLOCK PORT 6
```

See Also Lock, page 12-52; *Locking a Port*, page 8-9; *Locking a Port*, page 11-21

12.7 Service Commands

12.7.1 Clear/Purge Service

Removes an SCS service. Clearing a service only disables it until re-initialization of the SCS. For a permanent removal, the Purge command must be used.

Restrictions Requires privileged user status.

Errors Clear Service fails when there are sessions connected to the service or when there are connect requests in the service's queue. These conditions can be corrected with the Logout Port and Remove Queue commands.

Parameters

Local
Specifies that all local services should be removed.

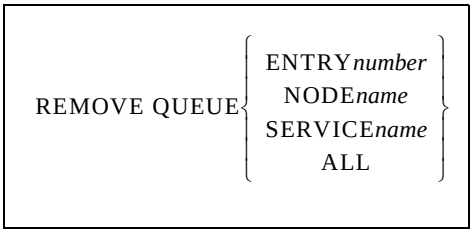
ServiceName
A specific service to be removed.

Examples

```
Local>> PURGE SERVICE LOCAL
Local>> CLEAR SERVICE FILESERVER
```

See Also Show/Monitor/List Services, page 12-108; *Port-Specific Session Configuration*, page 8-4

12.7.2 Remove Queue



Removes requests for local services from that service's queue. A particular request or all requests may be specified.

Restrictions Requires privileged user status.

Parameters

Entry
Specifies a particular queue entry to be removed. Must be used in conjunction with the **number** parameter.

number
A queue entry number.

Node
Specifies a particular node from which all connection requests will be removed. Must be used in conjunction with the **name** parameter.

Service
Specifies a particular local service; all entries queued to this service will be deleted. Must be used in conjunction with the **name** parameter.

name
A node or service name.

All
Removes all entries in the local service queue.

Examples

```
Local>> REMOVE QUEUE NODE hydra
Local>> REMOVE QUEUE ENTRY 5
Local>> REMOVE QUEUE SERVICE MODEM
Local>> REMOVE QUEUE ALL
```

See Also Show/Monitor Queue, page 12-190

12.7.3 Set/Define Service

Creates a new service. For the description and syntax of particular parameters used in conjunction with this command, refer to the individual entries that follow.

Note: *A maximum of 16 services can be created for the SCS.*

Restrictions Requires privileged user status.

Parameters

ServiceName
A string of up to 16 alphanumeric characters. Spaces are not permitted.

See Also Clear/Purge Service, page 12-101

12.7.4 Set/Define Service Banner

Specifies whether the SCS should print a banner page before starting the job. Banners should be disabled (the default) for all PostScript and plotter (binary) data.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Clear/Purge Service, page 12-101

12.7.5 Set/Define Service Binary

If the binary characteristic is enabled on a service, character translation (i.e. <cr> to <cr><lf> translation) and tab expansion will be permitted on the print data. The binary characteristic should be disabled when printing PCL data.

Restrictions Requires privileged user status.

Defaults Disabled

See Also Clear/Purge Service, page 12-101

12.7.6 Set/Define Service EOJ

Specifies a string to be sent to the attached device at the end of every job regardless of network protocol.

Restrictions Requires privileged user status.

Parameters

EndString
Any ASCII characters, or non-ASCII characters entered as hexadecimal digits (e.g. \45). The combined length of the SOJ and EOJ strings must not exceed 62 characters.

None
Clears any previously-configured string.

Defaults No string configured

See Also Clear/Purge Service, page 12-101

12.7.7 Set/Define Service Formfeed

```
{ SET    } SERVICE ServiceName FORMFEED { ENABLED  }
{ DEFINE }                              { DISABLED }
```

If enabled (the default), the SCS will append a formfeed at the end of any LPR print jobs.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Clear/Purge Service, page 12-101

12.7.8 Set/Define Service Identification

```
{ SET    } SERVICE ServiceName IDENTIFICATION { string }
{ DEFINE }                                    { NONE   }
```

Provides an information string for the specified service.

Restrictions Requires privileged user status.

Parameters **string**
Enter an information string of up to 40 characters.

12.7.9 Set/Define Service Password

```
{ SET    }
{ DEFINE } SERVICE ServiceName (PASSWORD) Password
```

Provides a password for the specified service. Local connections to service and IP connections to TelnetPort or TCPPort sockets will be prompted for this password.

Restrictions Requires privileged user status.

Parameters

Password
Enter a password of up to six characters.

ServiceName
Specifies a service name of up to 16 characters. Spaces are not permitted.

12.7.10 Set/Define Service Ports

```
{ SET    }                 { PortList }  [ENABLED ]
{ DEFINE } SERVICE ServiceName PORTS { ALL      }  [DISABLED]
```

Specifies a list of ports that will support or offer this service. If Enabled or Disabled is specified, the ports listed will be added to or removed from the current list, respectively. If neither option is specified, the new port list will replace the old port list. Note that ports offering a service must be in the correct access mode for connections to succeed.

Restrictions Requires privileged user status.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled

Examples

```
Local>> SET SERVICE lab5 PORTS 3,4,7-8 ENABLED
```

See Also Clear/Purge Service, page 12-101; Set/Define Ports Access, page 12-57

12.7.11 Set/Define Service Postscript

If enabled, the SCS will assume there is a PostScript printer attached to the service ports and will try to ensure a job is done before starting another. It will send a Ctrl-D to the attached device and wait for the new printer to return a Ctrl-D before starting the job transfer. If this is not done, slower printers may lose new jobs while interpreting the previous job. Setting PostScript mode is strongly recommended for all PostScript queues.

Restrictions Requires privileged user status.

Defaults Disabled

See Also Clear/Purge Service, page 12-101

12.7.12 Set/Define Service PSConvert

Controls whether the SCS will place a PostScript wrapper around each job. The SCS will try to detect if it is already a PostScript job, in which case it would not add an additional wrapper.

See Also Clear/Purge Service, page 12-101

12.7.13 Set/Define Service RTEL

Enables or disables RTEL access to the specified service.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Clear/Purge Service, page 12-101

12.7.14 Set/Define Service SOJ

Specifies a string to be sent to the attached device at the start of every access regardless of network protocol.

Restrictions Requires privileged user status.

Parameters

StartString
Any ASCII characters, or a backslash and two hex digits.

None
Clears any previously-configured string. No string is configured by default.

Examples

```
Local>> DEFINE SERVICE myserv SOJ \45
```

See Also Clear/Purge Service, page 12-101

12.7.15 Set/Define Service TCPport

Associates a TCP listener socket with the given service. TCP connections to this socket will be connected to the service.

Restrictions Requires privileged user status.

Parameters

SocketNum
A particular socket. The socket number can be an integer from 4000 to 4999.

None
Clears the current socket number.

Defaults None

See Also Clear/Purge Service, page 12-101

12.7.16 Set/Define Service Telnetport

Associates a TCP listener socket with the given service. TCP connections to this socket will be connected to the service. Unlike the TCPport option, a Telnetport socket will do Telnet IAC negotiations on the data stream.

Restrictions Requires privileged user status.

Parameters

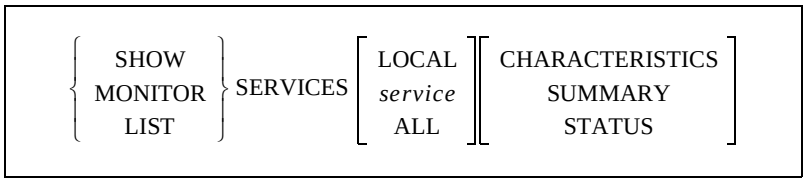
SocketNum
A particular socket. The socket number can be an integer from 4000 to 4999.

None
Clears the current socket number.

Defaults None

See Also Clear/Purge Service, page 12-101

12.7.17 Show/Monitor/List Services



This command is used to display the characteristics of the services on the network. Remember that this list is masked by the services that this port is eligible to see—users will not see services they cannot connect to.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Local
Displays those services local to this server, whether available or not.

service
Specifies a particular service. Numbers and wildcards are permitted.

All
Displays all known services usable by the current port.

Characteristics
Displays information about the known (local and remote) services. Information includes service rating, group code, and if the service is local, the service ports and service flags (such as Queueing and Connections).

Summary
Displays one-line summary information for the specified services.

Status
Displays full information for the specified services including network address, protocol version, and other services that node offers.

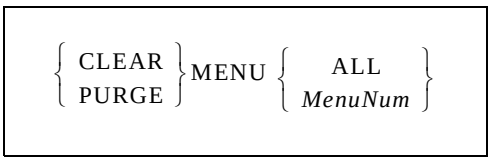
Examples

```
Local> SHOW SERVICE lab5_prtr STATUS
Local> MONITOR SERVICE LOCAL SUMMARY
```

See Also Clear/Purge Service, page 12-101

12.8 Server Commands

12.8.1 Clear/Purge Menu



Removes a specified menu entry or all menu entries.

Restrictions Requires privileged user status.

Parameters

All
Clears all menu entries.

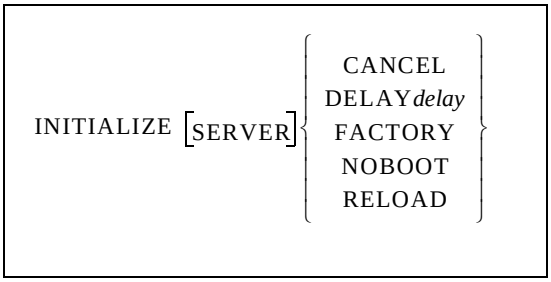
MenuNum
An integer from 1 through 36 specifying a particular menu entry to be removed.

Examples

```
Local>> CLEAR MENU ALL
Local>> CLEAR MENU 2
```

See Also Set/Define Menu, page 12-112; Set/Define Ports Menu, page 12-76; Show/ Monitor/List Menu, page 12-129; *Enabling Menu Mode*, page 8-12

12.8.2 Initialize Server



Controls SCS initialization and behavior after the unit is booted. When the server is initialized, all changes made using Set commands will be lost unless corresponding Define or Save commands were also made.

Initialization also sets local authentication in the first precedence slot (i.e. **Set/Define Authentication Local Precedence 1**).

Restrictions Requires privileged user status.

Parameters

Cancel
Cancels any pending initialization.

Delay
Schedules the initialization to take place after a specified number of minutes. Must be used in conjunction with the delay parameter.

delay
An integer between zero and 120, representing seconds before the initialization. Zero specifies an immediate reboot.

Note: *Show/Monitor/List Server will display the time remaining before a scheduled initialization.*

Factory
Reloads the factory settings. All configurations made with the Define and Save commands will be cleared and will have to be reconfigured.

Noboot
Forces the SCS to remain in the Boot Configuration Program (BCP) instead of booting.

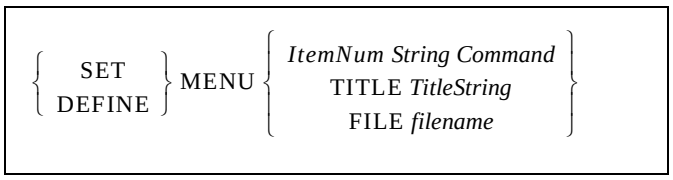
Reload
On Flash ROM equipped units, re-downloads the operational code and reprograms the Flash ROM.

Examples

```
Local>> INITIALIZE DELAY 2
Local>> INITIALIZE RELOAD FACTORY DELAY 12
Local>> INITIALIZE FACTORY
Local>> INITIALIZE CANCEL
```

See Also *Rebooting*, page 2-5; *Reloading Operational Software*, page 2-6

12.8.3 Set/Define Menu



Configures individual Menu Mode menu choices and the menu's title banner. You can also configure the menus using a preconfigured text file, which is specified using the filename parameter and is normally saved on the flash disk .

When using a configuration file, use the Set Menu command to parse the file before using Define to commit the file into use.

Note: *You should add a menu entry that allows users to log out. This can be accomplished by adding a "Logout Port Port" command to the end of the menu.*

Restrictions Requires privileged user status.

Errors The Define command only works with the File parameter if the file is saved in /flash.

Parameters

ItemNum
A number (1 through 36) and corresponds to the menu entry you are changing.

String
A text string, up to 32 characters long, that is displayed to users in the menu screen.

Command
A string of text, up to 32 characters long, that is displayed to users in the menu screen.

TitleString
An optional title for the entire menu. Enter up to 5 title lines with up to 48 characters each. The title can include dynamic print variables, as shown in the table below.

Note: *Dynamic print variables are case-sensitive. You must use all capital letters in the variables to avoid problems.*

Table 12-3: Dynamic Print Variables

Variable	Parsing Function
$FN	Displays the file name currently being accessed
$SC	Prints **Lantronix**
$SD	Adds a date stamp to the web page in the Day Month Date, Year format (e.g. Tue June 8, 1999)
$SH	Substitutes the SCS's hardware address
$SI	Print's the SCS's IP address
$SM	Prints the domain name of the network the SCS is on, as specified with the **Set/Define IP Domain** command
$SN	Prints the SCS's name, as specified with the **Set/Define Server Name** command
$SP	Prints the product name of the SCS
$ST	Adds a time stamp in the Hour:Minutes:Seconds format (e.g. 12:42:08)
$SV	Prints the version of operating software the SCS is currently using.

filename
Enter the name of the text file that contains your menu configurations.

Examples

```
Local>> SET MENU 5 "SHOW SET NODES" SHOW HOSTS"
```

See Also

Show/Monitor/List Menu, page 12-129; Clear/Purge Menu, page 12-111; *Enabling Menu Mode*, page 8-12; *Configuring Menu Mode*, page 3-4; *Menu Configuration Files*, page 3-5

12.8.4 Set/Define Protocol FTP

Enables or disables the on-board FTP server. Disabling the FTP server results in greater security.

Defaults Enabled

See Also *Disabling the FTP and HTTP Servers*, page 11-23

12.8.5 Set/Define Protocol HTTP

Controls whether the user can log in using the web browser interface.

Defaults Enabled

Parameters

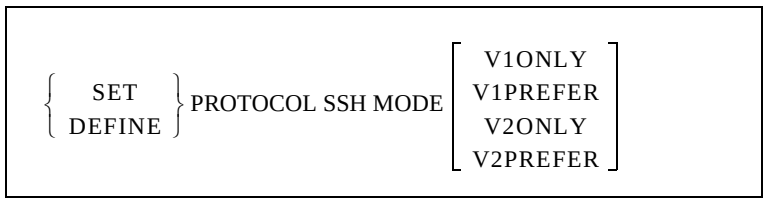
Enabled
Normal (non-privileged) users are allowed to view the web pages but must become the superuser to make any configuration changes.

Disabled
No access is allowed to the web pages.

Secure
Superuser access is required to view any web pages.

See Also *Disabling the FTP and HTTP Servers*, page 11-23

12.8.6 Set/Define Protocol SSH Mode



Allows the user to specify they types of SSH connections allowed from the command prompt of the SCS.

Restrictions Requires privileged user status.

Parameters

V1ONLY
The SCS offers only SSHv1 incoming and outgoing connections.

V1PREFER
The SCS offers both v1 and v2 incoming (host to SCS) connections, and the client chooses. If both versions are available, the SCS chooses SSHv1 for (SCS to Host) outgoing connections.

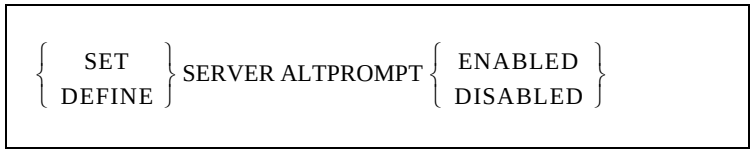
V2ONLY
The SCS offers only SSHv2 incoming and outgoing connections.

V2PREFER
The SCS offers both v1 and v2 incoming (host to SCS) connections, and the client chooses. If both versions are available, the SCS chooses SSHv2 for outgoing (SCS to Host) connections.

Defaults **V2PREFER**

See Also *Supported SSH Connections*, page 6-11

12.8.7 Set/Define Server Altprompt



Enables or disables the alternate UNIX-like prompts at login time. When enabled, the “Username>” prompt is changed to “login:” and the “Password>” prompt is changed to “Password:.”

Defaults Disabled

See Also Set/Define Server Prompt, page 12-123

12.8.8 Set/Define Server BOOTP

Enables or disables querying for a BOOTP host at system boot time.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Your SCS *User Guide*

12.8.9 Set/Define Server BOOTGATEWAY

Specifies a bootgateway, which allows a router to be used when the SCS attempts to download new code through a routed network.

Restrictions Requires privileged user status.

Parameters **IPaddress**
An IP address in standard numeric format (for example, 193.0.1.50).

Examples Local>> DEFINE SERVER BOOTGATEWAY 193.23.71.49

See Also Your *SCS User Guide*

12.8.10 Set/Define Server Broadcast

Enables or disables broadcasts from the server's ports.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Broadcast, page 12-180

12.8.11 Set/Define Server Buffering

Specifies the size of the buffer (in bytes) used for TCP/IP connections. The size can be increased for large data transfers such as file transfers.

Restrictions Requires privileged user status.

Parameters **buffersize**
Specify the buffer size in bytes between 128 and 8192.

Defaults 4096 bytes

Examples Local>> SET SERVER BUFFERING 1024

12.8.12 Set/Define Server Clock

Manually sets. the date and time information on the server clock.

Restrictions Requires privileged user status.

Parameters

time
Enter the time in 24-hour **hh:mm:ss** format. Entering seconds is optional.

date
Enter the date in **mm/dd/yyyy** format.

Examples Local>> SET SERVER CLOCK 13:23 0/3/15/1995

See Also Set/Define IP Timeserver, page 12-46; Show/Monitor/List Server Clock, page 12-129; Show/Monitor/List Timezone, page 12-131; *Setting the Date and Time*, page 2-10

12.8.13 Set/Define Server DHCP

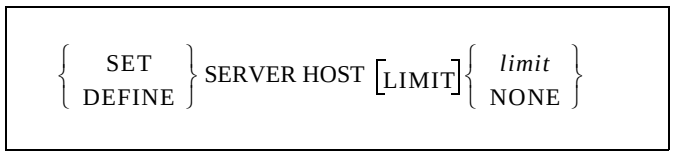
If a DHCP server exists on the network, enabling it will provide the SCS with an IP address, gateway address, and subnet mask.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Your *SCS User Guide*

12.8.14 Set/Define Server Host Limit



Sets the maximum number of TCP/IP hosts learned from Rwho that the server will keep information for. Hosts from the preset host table are exempt from this limit. If the new limit is less than the current limit and the host table is full, the limit will be slowly weeded down to the new value.

Restrictions Requires privileged user status.

Parameters

limit
A value between 0 and 200.

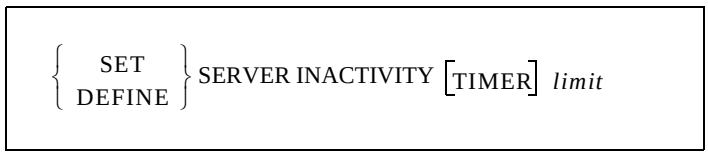
None
No limit is set.

Defaults 200 hosts

Examples

```
Local>> SET SERVER HOST LIMIT 6
```

12.8.15 Set/Define Server Inactivity



Sets the period of time after which a port with Inactivity Logout enabled is considered inactive and is automatically logged out.

Restrictions Requires privileged user status.

Parameters

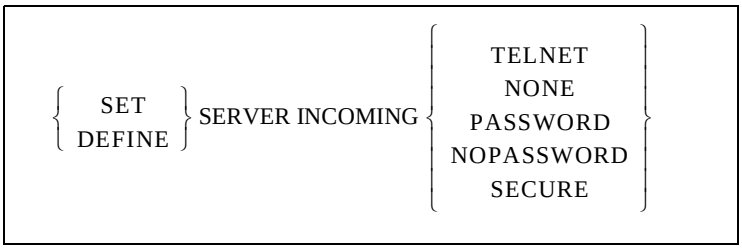
limit
Enter an inactivity period of 1 to 120 minutes.

Defaults 30 minutes

Examples Local>> DEFINE SERVER INACTIVITY LIMIT 20

See Also Set/Define Ports Inactivity Logout, page 12-74

12.8.16 Set/Define Server Incoming



Allows or denies incoming connections and enforces password protection if desired. If None is applied, incoming SSH connections will also be denied. The **Show Server** command shows the status of incoming connection parameters.

The status of the Incoming Telnet also controls incoming Rlogin sessions from remote hosts—the **Set/ Define Server Rlogin** command controls outgoing Rlogin connections.

Restrictions Requires privileged user status.

Parameters

Telnet
Enables incoming Telnet connects (logins) to the server.

None
Prevents all login attempts.

Password
Requires incoming Telnet login attempts to supply the server login password before being logged in.

NoPassword
Incoming Telnet logins are permitted and are not prompted for the login password before connecting.

Secure
Completely disables all non-encrypted connections to the server (Telnet in, Rlogin in, 200X sockets, and 300X sockets). You will not be able to connect to the server using EZWebCon.

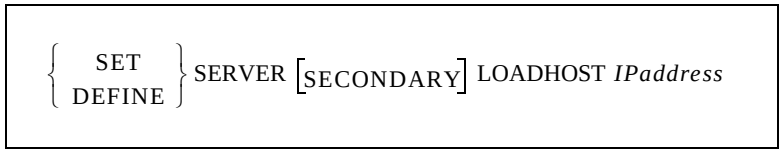
Defaults Telnet
NoPassword

Note: *The default incoming password is "access." See the Set/Define Server Login Password command for more information.*

Examples Local>> SET SERVER INCOMING TELNET INCOMING PASSWORD
(sets up password protected Telnet logins)

See Also Set/Define Server Rlogin, page 12-125; Set/Define Server Login Password, page 12-121; *Login Password*, page 8-10, *Restricting Connections to SSH, page 6-17*, *Disabling HTTP and FTP*, page 6-17

12.8.17 Set/Define Server Loadhost



Specifies the host to be used for downloads from TCP/IP hosts. The host name must be a numeric IP-style address. The SCS requests its run-time code from this host.

Restrictions Requires privileged user status.

Parameters **IPaddress**
An IP address in standard numeric format (for example, 193.0.1.50).

Examples Local>> DEFINE SERVER LOADHOST 193.23.71.49

See Also Your SCS *Installation Guide*

12.8.18 Set/Define Server Lock

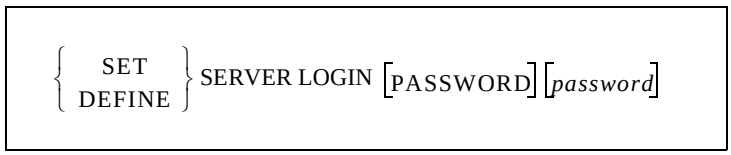
Controls whether or not local users are permitted to Lock their ports.

Restrictions Requires privileged user status.

Defaults Enabled

See Also *Locking a Port*, page 8-9

12.8.19 Set/Define Server Login Password



Specifies the password that is used to log in to the server from the serial ports or the network. If the password is not given on the command line, you will immediately be prompted to enter the password, which will not be displayed when typed.

The login password is only required on ports that have been Password Enabled.

Restrictions Requires privileged user status.

Parameters **password**
Enter a password of 16 or fewer characters.

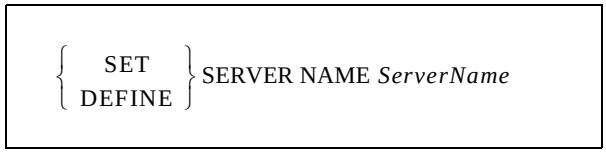
Note: *SCS passwords are case-independent, even when enclosed in quotes.*

Defaults "access"

Examples
```
Local>> SET SERVER LOGIN PASSWORD
Password> platyp (not echoed)
Verification> platyp (not echoed)
Local>>
```

See Also Set/Define Server Incoming Password, page 12-119;
Login Password, page 8-10; Set/Define Ports Password, page -78

12.8.20 Set/Define Server Name



Specifies the name of the SCS. **The name string must be in quotes if lowercase characters are used.**

Restrictions Requires privileged user status.

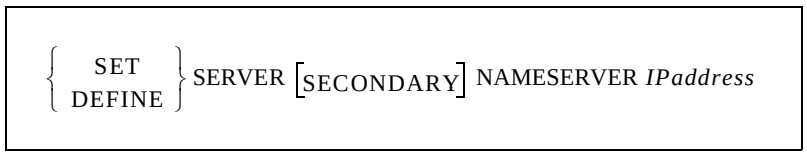
Parameters **ServerName**
Assign a name to the SCS, 16 alpahanumeric characters or less.

Defaults SCS**_xxxxxx** where **xxxxxx** represents the last 3 segments of the unit's hardware address.

Examples
```
Local>> SET SERVER NAME "docserver"
```

See Also *Changing the Server Name*, page 2-9

12.8.21 Set/Define Server Nameserver



Specifies the IP address of the name server (if any) for TCP/IP connections. This host will attempt to resolve text hostnames into numeric form if the local host table is unable to do so.

Restrictions Requires privileged user status.

Parameters

IPaddress
The network address of the nameserving host, in numeric IP format.

Examples

```
Local>> SET SERVER NAMESERVER 192.0.1.49
```

See Also Set/Define IP Host Limit, page 12-38; Set/Define IP Nameserver, page 12-39; *Configuring the Domain Name Service (DNS)*, page 6-7

12.8.22 Set/Define Server Password Limit

Limits the number of failures allowed when issuing the **Set Privileged** command, when entering the login password when logging in to a serial port, or when **Set/Define Ports Password Incoming** is enabled. After limit retries, the port will be logged out. The value is also used for determining the number of times a user can fail an authenticated user login (e.g., local database, Radius, Secure ID) when **Set/Define Ports Authenticate** is enabled.

The user can abort the password process by typing Ctrl-Z instead of the password.

Restrictions Requires privileged user status.

This limit does not apply to SSH connections, which always have a password limit of 3.

Parameters

limit
A value between 0 and 100. If zero is specified, the port is never logged out for too many password failures.

None
Sets the password limit to the default value.

Defaults 3 tries

Examples
```
Local>> SET SERVER PASSWORD LIMIT 10
```

See Also Set Privileged/Noprivileged, page 12-92; Set/Define Ports Authenticate, page 12-58

12.8.23 Set/Define Server Privileged Password

{ SET / DEFINE } SERVER PRIVILIGED [PASSWORD] [*passwd*]

Sets the password for becoming the "superuser" of the server. If the password is not given on the command line, you will immediately be prompted to enter the password, which will not be displayed when typed.

Restrictions Requires privileged user status.

Parameters

passwd
Enter a password of 16 or fewer characters.

Note: *SCS passwords are case-independent, even when enclosed in quotes.*

Defaults "system"

Examples
```
Local>> SET SERVER PRIVILEGED PASSWORD "yodel"

Local>> SET SERVER PRIVILEGED
Password: ok2bin (not echoed)
Verify: ok2bin (not echoed)
```

See Also Set Privileged/Noprivileged, page 12-92; *Privileged Password*, page 2-8

12.8.24 Set/Define Server Prompt

{ SET / DEFINE } SERVER PROMPT *PromptString*

This command allows the manager to change the prompt that users see from the default Local_x> string. A string of up to 16 characters long can be configured, **and should be enclosed in quotes.**

Restrictions Requires privileged user status.

Parameters

PromptString
The following parameters can be included in the prompt string:

String	Affect on Prompt
%p	Substitutes the current port's name
%n	Substitutes the current port's number
%s	Substitutes the current server name
%D	Substitutes the product name (SCS1600, etc.)
%C	Substitutes the company name (Lantronix)
%S	Substitutes the current session name
%P	Substitutes a > if user is currently privileged
%%	Substitutes a percent sign (%)

Defaults

Local_%n%P

Examples

(shown with the prompt that might result on the next line)

```
Local>> SET SERVER PROMPT "Port %n:"
Port 3: SET SERVER PROMPT "%D:%S!"
SCS1600:LabServ! SET SERVER PROMPT "%p%S_%n%P%%"
Port_5[NoSession]_5>% SET SERVER PROMPT "Lcl_%n>%P"
Lcl_3>>
```

See Also

Changing the Local Prompt, page 2-9

12.8.25 Set/Define Server RARP

Enables or disables querying for a RARP host at system boot time.

Restrictions Requires privileged user status.

Defaults Enabled

See Also Your *Installation Guide*

12.8.26 Set/Define Server Retransmit Limit

Specifies the number of times that a TCP packet will be resent if it is not acknowledged.

Restrictions Requires privileged user status.

Parameters **LimitNum**
An integer between 4 and 100, inclusive.

Defaults 50 tries

12.8.27 Set/Define Server Rlogin

Restricts the use of the Rlogin command from the server. If Rlogins are disabled, you may not Rlogin to remote hosts. Incoming Rlogin connections may still be permitted, depending on the current **Set/Define Server Incoming** setting.

Restrictions Requires privileged user status.

Defaults Disabled

12.8.28 Set/Define Server Session Limit

Sets the limit on active sessions per port. Each port can have an additional limit less than or equal to this limit.

Restrictions Requires privileged user status.

Parameters

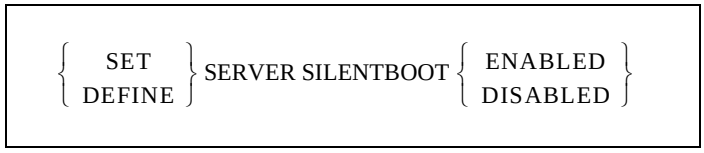
limit
A number between zero and 8.

None
The maximum possible session limit is used (8).

Defaults 4 sessions

See Also *Port-Specific Session Configuration*, page 8-4

12.8.29 Set/Define Server Silentboot



Causes the unit to attempt to boot without sending any status messages to the console port (unless there are errors).

Restrictions Requires privileged user status.

Defaults Disabled

12.8.30 Set/Define Server Software

Specifies the name of the download software file (if any) the server will attempt to load at boot time. For IP-loading hosts, this is the file that will be requested at boot time. This command is only useful if it is Defined; if it is Set, it will be cleared/reset at boot time.

For TFTP loading, the complete path of the file can also be specified if the file is located in a directory other than the default. The path name can be up to 31 characters in length not counting the file name. **The full path must be enclosed in quotes to preserve case.**

Restrictions Requires privileged user status.

Parameters

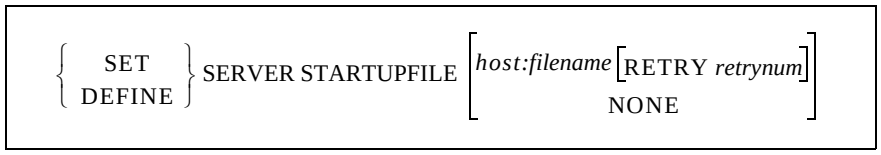
filename
Load file name, 15 characters or less. The server will automatically add the ".SYS" extension to the name.

Examples

```
Local>> DEFINE SERVER SOFTWARE SCS
Local>> DEFINE SERVER SOFTWARE "/usr/rich/tscode"
```

See Also Set/Define Server Loadhost, page 12-120; *Editing Boot Parameters*, page 2-6; Your SCS *Installation Guide*

12.8.31 Set/Define Server Startupfile



Configures the startup configuration file that the SCS will attempt to download at boot time. This file contains the SCS commands that will configure the server before the users and services are started. If no retry limit is specified in the command, the SCS will retry failed downloads forever; otherwise it will retry the specified number of times and then boot normally.

Telnet consoles are available at the time the server attempts to download the startupfile; if there is a problem with the download, you can still log into the server and determine what went wrong.

Restrictions Requires privileged user status.

Parameters

host
An IP address, or a text host name that is resolvable at boot time.

filename
A startup file name of up to 47 characters.

Retry
Configures the server retry limit. Must be used with the **retrynum** parameter.

retrynum
The number of times to retry the download attempt. The maximum number of retries is 1000. If a retrynum is not specified, the SCS will retry 5 times (the default).

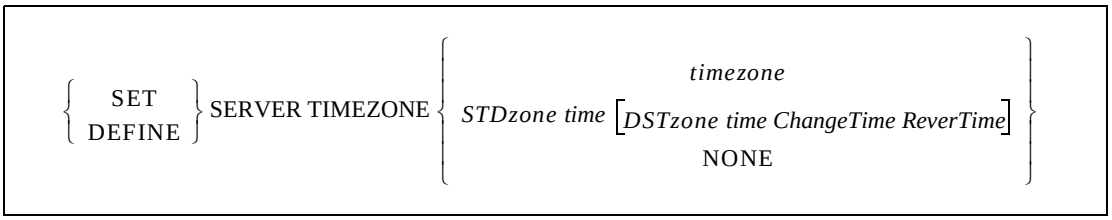
None
Clears any specified startup file.

Defaults
Startupfile: none specified
Retries: 5

Examples Local>> DEFINE SERVER STARTUPFILE “bob:start” RETRY 6

See Also *Editing Boot Parameters*, page 2-6; Your SCS *Installation Guide*

12.8.32 Set/Define Server Timezone



Manually sets the timezone for the SCS.

Restrictions Requires privileged user status.

Parameters

timezone
A pre-configured timezone name. Use the Show/Monitor/List command to see a list of available timezone names.

STDzone
A three-letter timezone name that represents your Standard Time zone (for example, use PST for Pacific Standard Time). Must be used in conjunction with the **time** parameter.

DSTzone
A three-letter timezone name that represents your Daylight Savings Time zone (for example, use PDT for Pacific Daylight Time). Must be used in conjunction with the **time** parameter.

time
The time difference from Greenwich Mean Time, entered as h:mm. Entering the minutes is optional.

ChangeTime
Enter the month, day, and time of day that the change to DST occurs, separating each element by a space (see the examples below). For the month, enter the first three letters of the month. For the day, recognized forms include:

5	The fifth day of the month
lastSun	The last Sunday in the month
Sun>=8	The first Sunday on or after the 8th of the month
Sun<=25	The last Sunday on or before the 25th of the month

For the time of day, use the same format as used for the **time** parameter.

RevertTime
Enter the month, day, and time of day

None
Specifies that no timezone will be used.

Examples

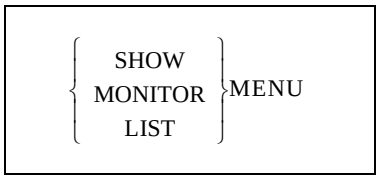
```
Local>> DEFINE SERVER TIMEZONE AMERICA/EASTERN
Local>> DEFINE SERVER TIMEZONE HST -10

Local>> DEFINE SERVER TIMEZONE MET 1:00 MET-DST 1:00 Mar lastSun 2:00 Sep
lastSun 2:00
```

(In the last example above, MET is the STDzone, and MET-DST is the DSTzone, both of which are one hour off of Greenwich Mean Time. The change to DST occurs on the last Sunday in March at 2:00, and it reverts back to standard time on the last Sunday in September at 2:00.)

See Also Set/Define Server Clock, page 12-117; Show/Monitor/List Timezone, page 12-131

12.8.33 Show/Monitor/List Menu



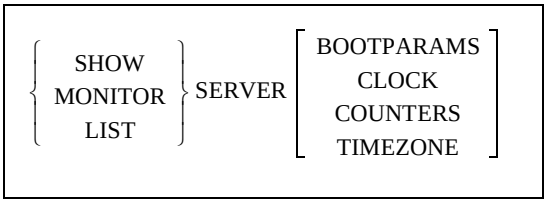
Displays the current or saved Menu entries. If you have a configuration file set, this command will only display the name of that file.

Restrictions You must be the privileged user to use the Monitor command.

Secure users may not use this command.

See Also Clear/Purge Menu, page 12-111; Set/Define Menu, page 12-112; *Enabling Menu Mode*, page 8-12; *Configuring Menu Mode*, page 3-4

12.8.34 Show/Monitor/List Server



This command is used to display the global attributes or counters for the server itself.

Restrictions You must be the privileged user to use the Monitor command. The List Server command can only be used with the Bootparams parameter.

Parameters

Bootparams
Displays parameters related to rebooting the unit and reloading the software file.

Clock
Displays the local time and date and the UTC (GMT) time and date.

Counters
Counters can be reset to zero with the Zero Counters All command. Displays the accumulated error counters for the Ethernet and TCP/IP protocols. The four-digit bit position numbers represent one of the network error reasons listed below:

Table 12-4: Server Failure Reasons

Bit	Send Failure Reason	Receive Failure Reason
0	Unused, should be 0	Unused, should be 0
1	Unused, should be 0	Packet received with CRC error
2	At least one collision has occurred while transmitting	Received packet did not end on byte boundary
3	Transmit aborted due to excessive (more than 16) network collisions	FIFO overrun: Could not write received data before new data arrived
4	Carrier sense was lost during transmission	Receive packet could not be accommodated due to lack of receive buffers
5	FIFO underrun: Ethernet controller could not access transmit data in time to send it out	Received a packet larger than the maximum Ethernet size (1536 bytes)
6	CD heartbeat not received after transmission	Unused, should be 0
7	Out-of-window collision detected	
8-15	Unused, should be 0	

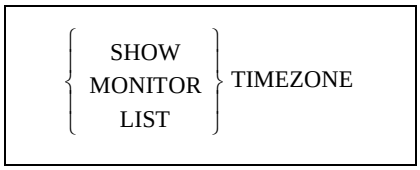
Timezone
Displays the timezone if a timezone has been specified.

Examples

```
Local> SHOW SERVER BOOTPARAMS
```

See Also Set/Define Server Clock, page 12-117; *Setting the Date and Time*, page 2-10

12.8.35 Show/Monitor/List Timezone

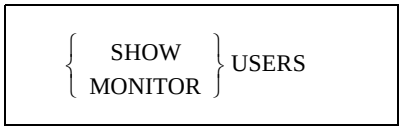


Displays a table of timezone abbreviations which can be used to select a timezone for the server.

Restrictions You must be the privileged user to use the Monitor command.

See Also *Setting the Date and Time*, page 2-10

12.8.36 Show/Monitor Users

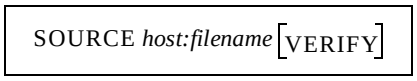


Displays the current users logged onto the server. For each user, the SCS displays the port username and current connection information.

Restrictions You must be the privileged user to use the Monitor command.

Errors List Users will cause an error.

12.8.37 Source



Source attempts to download a configuration file from a TFTP host. The file is assumed to be lines of server commands which will be executed. The Source command is most useful for trying out a configuration file before using the **Set/Define Server Startupfile** command, page 12-127.

Restrictions Requires privileged user status.

Parameters

host
Enter a TFTP host (text host name or IP address).

filename
The download path and filename, 22 characters maximum.

Note: *If filename contains lower-case letters, it must be enclosed in quotation marks.*

Verify
Displays each command from the configuration file before executing it.

Examples Local>> SOURCE “labsun:start.com”

See Also Set/Define Server Startupfile, page 12-127

12.9 Site Commands

12.9.1 Define Site

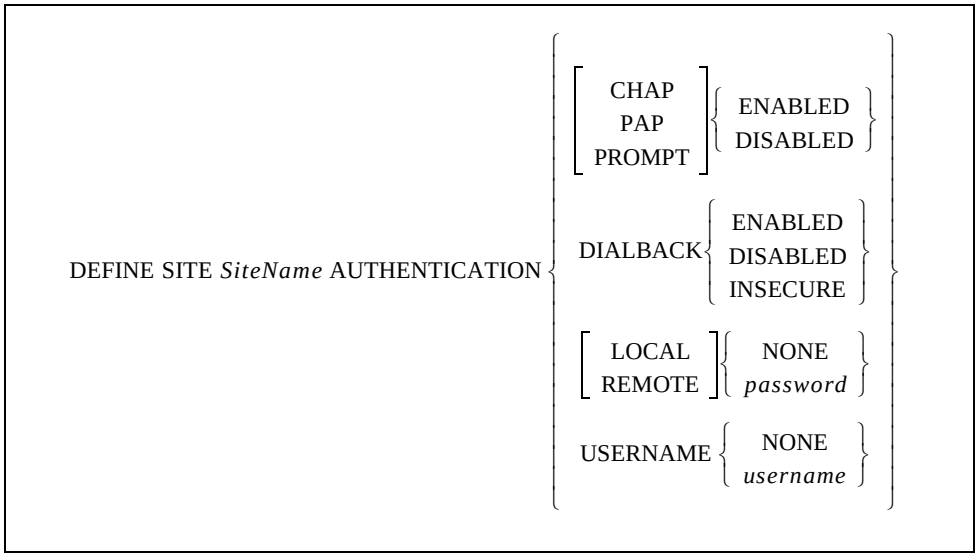
Creates a new site with the given name. See the following **Define Site** commands for additional site configuration options.

Restrictions Requires privileged user status.

Examples Local>> DEFINE SITE irvine

See Also The following Define Site commands

12.9.2 Define Site Authentication



Defines authentication information, such as site names and passwords, for link protocols that support authentication (for example, PPP).

Restrictions Requires privileged user status.

Parameters

SiteName
A site name of up to 12 characters.

CHAP
Enables or disables the Challenge Handshake Authentication Protocol for outgoing calls.

PAP
Enables or disables the Password Authentication Protocol for outgoing calls.

Note: *CHAP and PAP are part of PPP.*

Prompt
When Prompt is enabled, incoming callers will be prompted for the local password before starting PPP or SLIP.

Dialback
If Dialback is enabled, when the site receives an incoming connection, the SCS will hang up and initiate an outgoing connection to verify the caller's identity. If Insecure dialback is enabled, the caller may be given the option of specifying the dialback telephone number.

The site must have at least one port and a telephone number defined for the outgoing connection (See **Define Site Port**, page 12-143).

Insecure
Allows CBCP-aware PPP clients the option of choosing their own number for dialback. Be sure to read the cautions listed under *Dialback Using CBCP* on page 11-7.

Local
Defines the password required from the remote host. Must be used in conjunction with the **None** or **password** parameters.

Remote
Defines the password to be sent to the remote host. Must be used in conjunction with the **None** or **password** parameter.

Username
Define the username to be sent to the remote site. Must be used in conjunction with the **None** or **username** parameters.

None
Specifies that a password or username will not need to be used.

password
A password of up to 10 alphanumeric characters.

username
A username of up to 10 characters.

Defaults

Dialback, Prompt, CHAP, and PAP: Disabled
Local, Remote, and Username: None (no password or username defined)

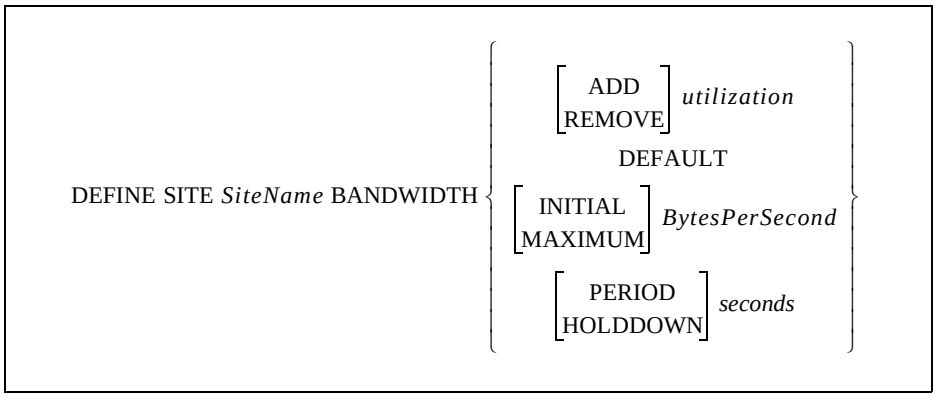
Examples

```
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE NONE
```

See Also

Set/Define Authentication, page 12-153; Show/Monitor/List Authentication, page 12-177; Chapter 11, *Security*

12.9.3 Define Site Bandwidth



Sets the initial or maximum amount of bandwidth that should be used when connecting to the specified site. Also controls how the SCS calculates the bandwidth needed, and how often it is checked to see if it is within the desired range.

This command is only useful when Multilink (bandwidth on demand) is enabled. See **Define Ports PPP Multilink**, page 12-81, and *Bandwidth On Demand* on page 5-4 for more information.

Restrictions Requires privileged user status.

Parameters

SiteName
A site name of up to 12 characters.

Add
Attempts to add bandwidth whenever usage reaches a specified percentage. Must be used in conjunction with the **utilization** parameter.

Remove
Removes bandwidth when usage falls below a certain percentage. Must be used in conjunction with the **BytesPerSecond** parameter.

utilization
The percentage of usage above which the SCS will attempt to add bandwidth and below which the SCS will remove bandwidth.

Default
Returns the bandwidth to the SCS's default setting.

Initial
Sets the initial amount of bandwidth. Must be used in conjunction with the **BytesPerSecond** parameter.

Maximum
Sets the maximum amount of bandwidth. Must be used in conjunction with the **BytesPerSecond** parameter.

BytesPerSecond
The precise bandwidth amount, up to 6,550,000 bytes per second. The server will add ports until it reaches the specified amount.

BytesPerSecond is truncated to the nearest 100. For example, a setting of 3840 is truncated to 3800.

A BytesPerSecond value below of 99 or less truncates to zero, disabling bandwidth.

Period
Sets the number of seconds (specified by the seconds parameter) used to calculate average utilization statistics. The value is expressed as percent usage over a period of time.

Holddown
Specifies the minimum amount of time, in seconds, after adding or removing bandwidth to the remote site before bandwidth can be adjusted again. Must be used in conjunction with the **seconds** parameter.

Adding bandwidth after it has been removed or removing bandwidth after it has been added requires double the number of **seconds**. For example, if a holddown value of 5 is specified, adding bandwidth after it has been removed will require a 10 second delay.

Defaults

Add and Remove: Disabled (utilization = 0).

Default: bring up one port.

Initial and Maximum: 100 bytes per second.

Period: 60 seconds.

HoldDown timer: 60 seconds.

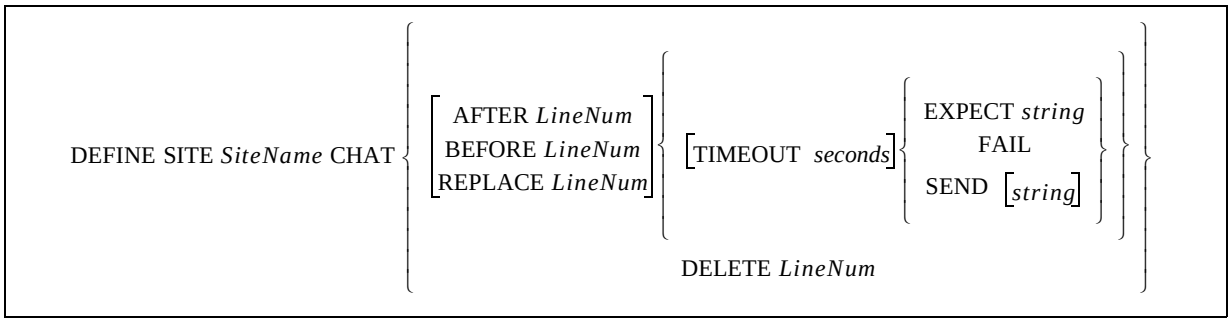
Examples

```
Local>> DEFINE SITE irvine BANDWIDTH INITIAL 123
Local>> DEFINE SITE irvine BANDWIDTH ADD 50
Local>> DEFINE SITE irvine BANDWIDTH PERIOD 6
```

See Also

Define Ports PPP Multilink, page 12-81; Define Site Port Bandwidth, page 12-143; Show/Monitor/List Sites Bandwidth, page 12-149; *Bandwidth On Demand*, page 5-4

12.9.4 Define Site Chat



Configures a chat script to automate the login sequence when connecting to a remote site. Chat scripts are a set of commands that send data to the remote site and wait for certain replies after the modems (if any) have connected. Based on the replies, other commands are executed.

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

After
Inserts a line after another line.

Before
Inserts a line before another line.

Replace
Replaces a line with another line, specified with the **LineNum** parameter.

The default is to append information to the end of the script.

Timeout
Sets the time to wait before commands, or the number of times to wait for input before giving up. Must be used in conjunction with the **seconds** parameter.

seconds
A number of seconds or tries between zero and 65500.

Expect
Looks for a **string** before executing the next line of the script.

string
The following special characters can be used in CHAT script expect strings, which are case-sensitive.

Table 12-5:

String	Meaning	String	Meaning
\N (0x0 hex)	Newline	\b (0x8 hex)	Backspace
\r (0xd hex)	Return	\n (0xda hex)	Newline
\t (0x14 hex)	Tab	\\ (0x5c hex)	\
\s (0x20 hex)	Space	\octal	Octal value (i.e., \101 = ”A“)

Fail
Uses the number specified as the Timeout **seconds** parameter to set the number of times the search for a string (specified with the Expect parameter) can fail before the whole script will give up. Each time the Expect command fails, the script continues at the last Fail command. This permits looping while waiting for a given prompt.

A sample script is displayed below.

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL
Local>> DEFINE SITE irvine CHAT SEND ""
Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT "login:"
```

This script will send a newline and wait for the string "login:" for two seconds. If found, the script will continue. If not, the script will search again three times before failing.

Send
Sends the specified string, followed by a newline character (0xd hex, 13 ASCII). If a string is not specified, only a carriage return is sent.

Delete
Removes a line.

LineNum
The line to remove.

Defaults

Timeout: 0 (None defined)
marker and string: not defined

Examples

```
Local>> CHAT REPLACE 1 EXPECT "login:"
Local>> CHAT DELETE 1
Local>> CHAT TIMEOUT 2 EXPECT "login:"
Local>> DEFINE SITE irvine CHAT SEND "hello?"
Local>> DEFINE SITE irvine CHAT REPLACE 4 TIMEOUT 3 EXPECT "login:"
```

See Also

Show/Monitor/List Sites Chat, page 12-149; *Chat Scripts*, page 5-3

12.9.5 Define Site Dial on Hangup

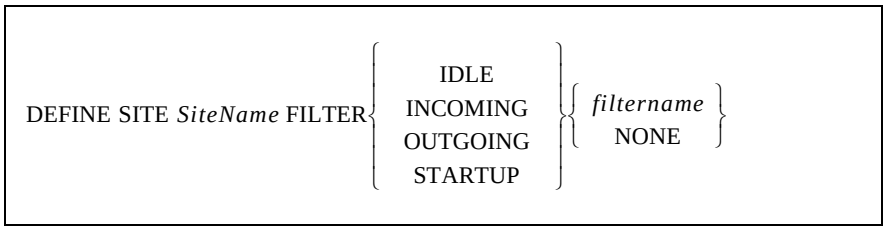
A call and hangup on any of the ports associated with this site causes the site to form an outbound call.

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

12.9.6 Define Site Filter



Configures packet filters for the site. If a particular packet filter is not configured, all packets are considered matches of that filter type and are accepted. For example, if no incoming packet filter is configured, all packets will be accepted as incoming packets and will be allowed in.

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

Idle
Configures the packet filter that resets the idle timer. Packets that pass this filter will reset the timer, keeping the site from timing out and disconnecting. Must be used in conjunction with the **filtername** parameter.

Incoming
Configures the packet filter for packets that come into the SCS from the remote site. Packets that do not pass this filter will be dropped. Must be used in conjunction with the **filtername** parameter.

Outgoing
Configures the packet filter for packets going from the SCS to the remote site. Packets that do not pass this filter will be dropped. Must be used in conjunction with the **filtername** parameter.

Startup
Configures the packet filter for regulating connections. Packets that pass this filter can cause the site to initiate a connection. Packets that do not pass this filter will be dropped if a link is not already in place, but will continue to their destination if a link has already been established. Must be used in conjunction with the **filtername** parameter.

filtername
Sets the filter to be used for a specific type of packet filtering. Filter names must be 3 characters or fewer.

None
Clears any previously-set filter for that site.

Examples

```
Local>> DEFINE SITE irvine FILTER IDLE a3f
Local>> DEFINE SITE irvine FILTER IDLE m00
Local>> DEFINE SITE irvine FILTER IDLE gb
```

See Also Set/Define Filter, page 12-166; Show/Monitor/List Filter, page 12-178; *Filter Lists*, page 5-2

12.9.7 Define Site Idle

DEFINE SITE *SiteName* IDLE *seconds*

Sets the maximum time, in seconds, that the specified site may be idle before the link is shut down ("timed out").

Note: *The SCS must be idle for at least 10 seconds before the link can be shut down.*

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

seconds
The maximum length of time (specified by an integer between 10 and 65,000) that the site can remain idle before the link disconnects. A time setting of 0 will disable timeouts.

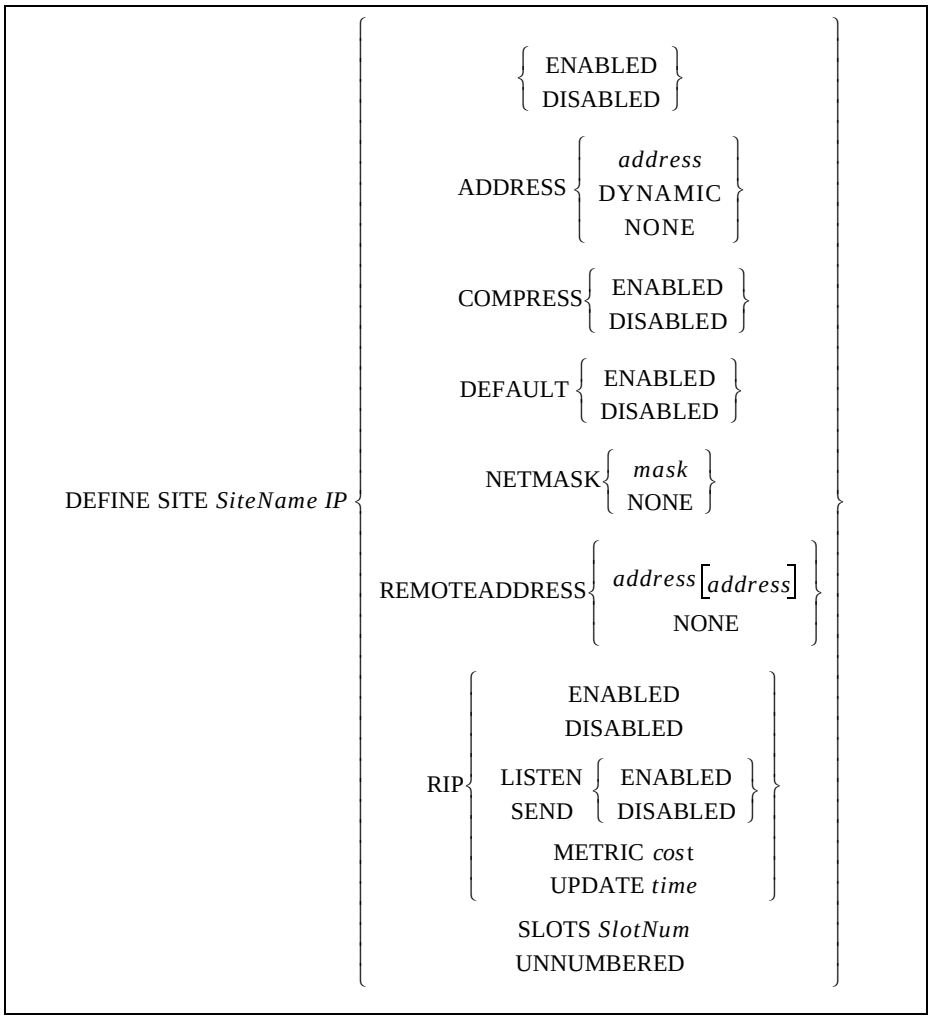
Defaults Idle time: 600 seconds.

Examples

```
Local>> DEFINE SITE irvine IDLE 600
```

See Also Define Site Filter Idle, page 12-138; Set/Define Server Inactivity, page 12-118; *Reducing Cost*, page 5-10

12.9.8 Define Site IP



Configures the Internet Protocol (IP).

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

Enabled/Disabled
Enables or disables the site's use of IP. May be used instead of packet filters to prevent all IP packets from being forwarded.

Address
Sets the IP address (specified with the **address** parameter) on this server's IP interface.

Compress
Enables or disables header compression for the specified protocol.

Dynamic
Allows the SCS to be dynamically assigned an IP address by a remote host.

Default
Advertises this server as the default route to the remote host.

Netmask
Sets the IP Netmask on this server's IP interface.

mask
A value that is used to remove bits that you do not want.

Remoteaddress
Sets the IP address (specified with the **address** parameter) of the remote host. If two address are specified, it indicates an acceptable range of addresses for the remote host.

Callers cannot use IP addresses with the host part of the address set to zero or -1; these addresses are reserved for broadcast packets. If the specified range includes such an address (for example, 192.4.5.0 or 192.4.5.255) and a caller requests this address, the connection will be denied.

address
An IP address in standard numeric format. For example, 192.0.1.3.

None
Clears a current IP address, Remoteaddress address, Othermask, or Netmask.

Unnumbered
An IP address is not to be expected from the remote site.

RIP
Enables or disables RIP parameters, and allows specification of update times and hop counts for the interface.

Enabled/Disabled
Enables or disables both listen and send at the same time.

Listen
Enables or disables RIP listening only.

Send
Enables or disables RIP sending only.

Metric
Configures the cost ("hop-count") of this interface. Routes learned through this interface will have this value added to their metric. Must be used in conjunction with the cost parameter.

cost
An integer between 1 and 16.

Note: *Metric is commonly used to make a given interface less desirable for backup routing situations.*

Update
Configures the time, in seconds, between sending a RIP packet. Must be used in conjunction with the **time** parameter.

time
An integer between 10 and 255 representing the number of seconds between updates.

Slots
Configures the number of header compression slots. Must be used in conjunction with the SlotNum parameter.

SlotNum
An integer between 1 and 254.

Defaults

IP, Compress, and RIP: Enabled
Address, Netmask, and RemoteAddress: None
Default: Disabled
RIP Metric: 1
RIP Updates: every 30 seconds
Header compression slots: 16

Examples

```
Local>> DEFINE SITE irvine IP SLOTS 16
Local>> DEFINE SITE irvine IP RIP UPDATE 30
Local>> DEFINE SITE irvine IP UNNUMBERED
Local>> DEFINE SITE irvine IP RIP METRIC 4
Local>> DEFINE SITE irvine IP COMPRESS ENABLED
Local>> DEFINE SITE irvine IP FORWARD ENABLED
```

See Also

Set/Define Logging Sites, page 12-172; Show/Monitor/List Sites, page 12-149; *Configuring RIP for Sites*, page 4-10; *Chapter 7,Character Mode Sites*

12.9.9 Define Site MTU

DEFINE SITE *SiteName* MTU *MaxSize*

Configures the maximum sized packet that the remote site may send to the SCS. Packets larger than this will be fragmented by the remote site.

Restrictions

Requires privileged user status.

Parameters

SiteName
A site name of up to 12 characters.

MaxSize
Between 32 and 1522 bytes, inclusive.

Note: *The SCS will negotiate MTU with the remote site, so the actual MTU may be lower than what is configured.*

Default
1522 bytes.

Examples Local>> DEFINE SITE irvine MTU 256

See Also Set/Define IP All/Ethernet MTU, page 12-35; Chapter 4, *Basic Remote Networking*

12.9.10 Define Site Permanent

DEFINE SITE *SiteName* PERMANENT { ENABLED | DISABLED }

Configures a permanently connected site. When enabled, the site connects immediately after the SCS boots. If the connection is interrupted and the site goes down, the site will reconnect as soon as it is able.

Restrictions Requires privileged user status.

Parameters

Enabled
Enables the specified site to be permanently connected.

Disabled
Disables a permanent connection for a site.

Examples Local>> DEFINE SITE irvine PERMANENT ENABLED

12.9.11 Define Site Port

DEFINE SITE *SiteName* PORT { *PortList* | ALL } [BANDWIDTH *BytesPerSecond* | TELEPHONE { *number* | NONE } | PRIORITY *priorityNum*]

Configures a port that a site will use for its outgoing calls. Each port must have a telephone number associated with it. If multiple ports are associated with a site, they must be prioritized.

Note: *To purge the port setting from the site, see Purge Site, page 12-148.*

Restrictions Requires privileged user status.

Parameters

SiteName
A site name of up to 12 characters.

PortList/All
Specifies a particular SCS port, a list or range of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

Note: *A port must be defined before the Bandwidth, BytesPerSecond, and Telephone parameters can be used.*

Bandwidth
Gives the SCS a bandwidth estimate for the device (for example, a modem) that is attached to the port. Must be used in conjunction with the **BytesPerSecond** parameter.

Note: *See Estimate Each Port's Bandwidth on page 5-6 for more information on how to use the port bandwidth setting.*

BytesPerSecond
The bandwidth value. The value can range from 100 to 6,550,000 bytes per second.

Telephone
Specifies a telephone number for this port. This number will override the number defined for the site as a whole. Must be used in conjunction with either the **number** parameter or the **None** parameter.

number
A telephone "number" of up to 24 characters (characters can be of any type).

None
No specific telephone number will be set for this port.

Priority
Specifies a priority level for a particular port. Higher priority ports will be dialed before ports with lower priority numbers. Must be used with the **prioritynum** parameter.

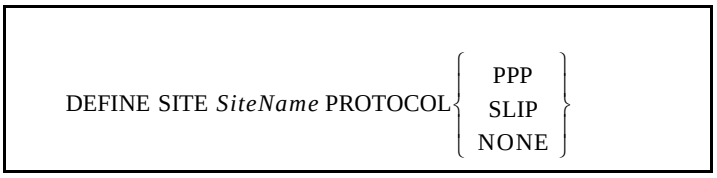
priorityNum
An integer between 1 and 100 representing the priority level of the specified port.

Defaults Bandwidth: 100 bytes per second

Examples
```
Local>> DEFINE SITE irvine PORT 2 TELEPHONE "8675309"
Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 28800
```

See Also Define Site Bandwidth, page 12-134; Show/Monitor/List Sites, page 12-149; *How Bandwidth is Controlled*, page 5-5

12.9.12 Define Site Protocol



Defines the "line" or "link layer" protocol that this site should use for outgoing calls. Reset the Maximum Transmission Unit (MTU) value to the default PPP or SLIP MTU value.

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

PPP
PPP will be used for outgoing calls.

SLIP
SLIP will be used for outgoing calls.

NONE
No protocol will be used for outgoing calls.

Defaults PPP

See Also *Incoming Connections*, page 4-11

12.9.13 Define Site Telephone

Defines the telephone number of the remote site. Before you assign a telephone number, you must associate the site with an SCS port or ports.

Restrictions Requires privileged user status.

Errors An error is returned if there is no port associated with the site.

Parameters

SiteName
Enter a site name of up to 12 characters.

number
A telephone "number" of up to 24 characters. Characters of any type can be used.

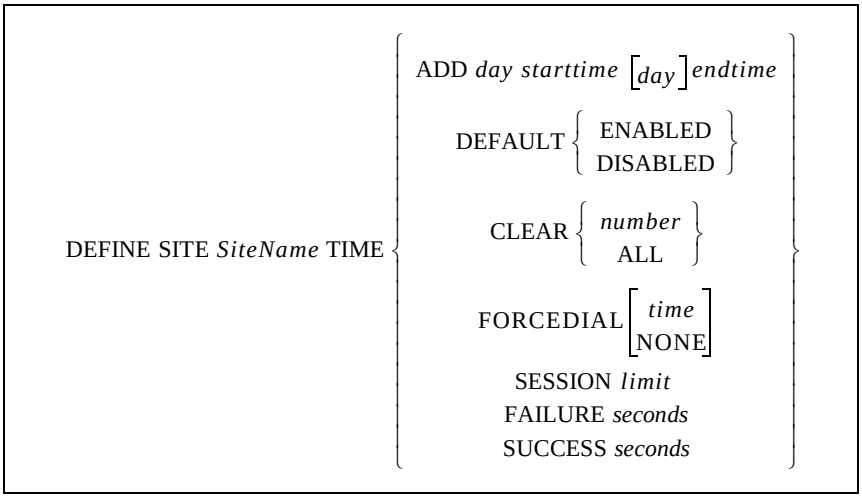
None
No telephone number will be defined for this site.

Default
None (no telephone number is defined).

Examples Local>> DEFINE SITE irvine TELEPHONE 8675309

See Also Define Site Port Telephone, page 12-143; *Assign a Telephone Number to the Port or Site*, page 4-19

12.9.14 Define Site Time



Configures the time ranges during which outgoing connections are allowed from this site, and during which bandwidth can be adjusted for this site.

Restrictions Requires privileged user status.

Parameters

SiteName
Enter a site name of up to 12 characters.

Add
When the Default setting is Enabled (see below), specifies when connections are not allowed. When the Default setting is Disabled, specifies when connections are allowed.

day
Specify the days during which Adding will start and stop. Must be followed by both starttime and endtime parameters. If a second day is not specified, it is understood that the start time and end time occur on the same day.

starttime, endtime
Specify the time when Add will go into effect, and the time when Add will end, on the specified day. Times are specified in hh:mm format and are ordered with respect to their time settings rather than the order in which they were entered. Specified times are combined if appropriate.

Note: *Show/Monitor/List Sites SiteName Time displays the specified time ranges and their order.*

Default
Set the default access parameter for the site.

If the default is enabled, connections are allowed except during the times specified. If the default is disabled, connections are restricted except during the times specified.

Clear
Remove a time range.

number
A time range to be removed. Time ranges are listed in numerical order.

Forcedial
Configures the site to dial at a particular time of day. If a time is assigned with this command, the site will always attempt to create a connection at that specified time, every day.

time
Enter a time for the Forcedial feature.

All
Remove all time ranges.

Forcedial
Creates a connection, every day, at the time set with the other parameters.

Session
Sets the total time, in seconds, that this site can be active before it is logged out. Must be used in conjunction with the **limit** parameter.

limit
Specify a time range from 10 to 65,000 seconds. A setting of zero disables the session limit.

Success
Specifies a delay after a successful connection before another connection will be attempted. Must be used in conjunction with the **seconds** parameter.

Failure
Specifies a delay after a failed connection attempt before another connection will be attempted. Must be used in conjunction with the **seconds** parameter.

Note: *The success and failure settings control the time between calls. If the connection worked, the SCS waits for the success delay to pass before attempting another connection. If the connection did not work, the SCS waits for the failure delay to pass.*

seconds
A delay time of 1 to 65000 seconds.

Connection
Specifies the minimum amount of time, in seconds, after a connection drops or fails before attempting to form another connection. Must be used in conjunction with the seconds parameter.

Defaults Default: Disabled (connections are allowed only when specified).
Success: 1 second.
Failure: 30 seconds.
Session: 0 seconds (disabled).

Examples
```
Local>> DEFINE SITE irvine TIME ADD mon 8:00 mon 17:00
Local>> DEFINE SITE irvine CLEAR TIME 3
```

See Also Set/Define Server Clock, page 12-117; Set/Define Server Timezone, page 12-128; Show/Monitor/List Sites Time, page 12-149; *Getting Timesetting Information*, page 5-11

12.9.15 Logout Site

Logs out a site on the server. Active sessions are disconnected, and all site circuits are closed.

Restrictions Only privileged users can log out a port or site other than their own.

Parameters

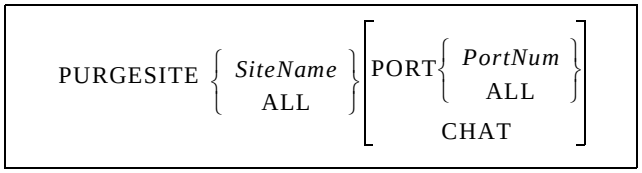
Site
Logs out a site, closing all circuits. Must be used in conjunction with the SiteName parameter.

SiteName
A site name of up to 12 characters.

Examples
```
Local> LOGOUT
Local>> LOGOUT SITE irvine
```

See Also *Automatic Logouts*, page 8-11

12.9.16 Purge Site



Removes a site, or removes ports from a site.

Restrictions Requires privileged user stats.

Parameters

SiteName
Enter a site name of up to 12 characters.

All
When used before the Port parameter, removes all ports from the specified site. When used either before the Port parameter or both before and after the Port parameter, removes all ports from all sites.

Port
Removes a port from a site. Must be used in conjunction with the **PortNum** or **All** parameters.

PortNum
An integer between 1 and 16.

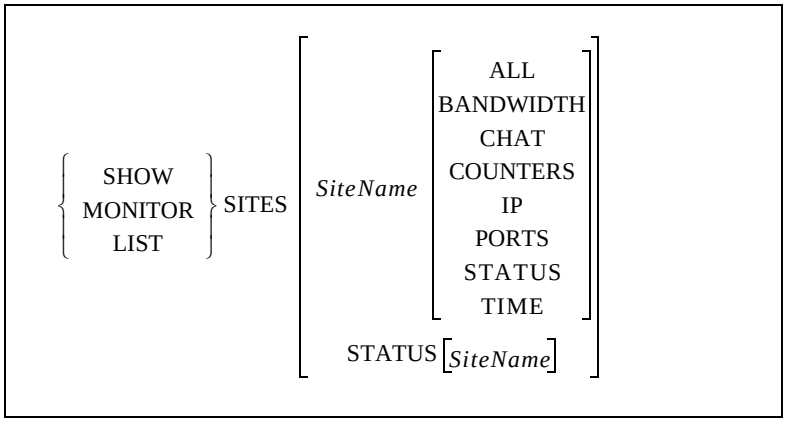
Chat
Clears the specified site's chat scripts.

Examples

```
Local>> PURGE SITE irvine PORT 2
```

See Also Define Site Port, page 12-143

12.9.17 Show/Monitor/List Sites



In general, displays information about a specified site. The **All** keyword is a special case, as described below.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
A particular site name of up to 12 characters.

All
Displays all accumulated statistics for all sites that have started since the SCS was last booted, not just those that are running.

Bandwidth
Displays the specified site's bandwidth configuration and related statistics.

Chat
Displays a site's chat script.

Counters
Displays a site's counters.

IP
Displays a site's IP configuration.

Ports
Displays a site's ports.

Time
Displays time configuration for the specified site, including.

Status
Displays statistics for sites that have been active since booting.

Examples

```
Local> SHOW SITE irvine CHAT
Local> SHOW SITE irvine IP
```

See Also Define Site commands, page 12-132

12.9.18 Test Site

TEST SITE *SiteName*

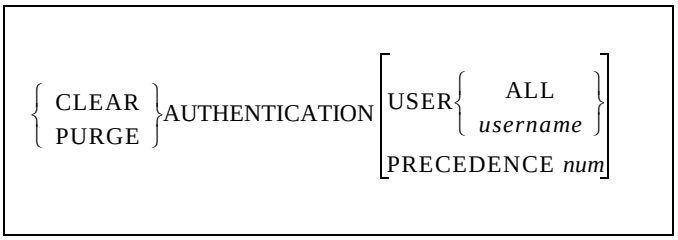
Tests a site without having to force packet traffic. When the command is issued, the SCS will attempt a connection to the site and return basic status. The site must then be shut down manually.

Errors An error will be returned if the site is unavailable. For more detailed information, use the Logging feature.

See Also Define Site commands, page 12-132; Set/Define Logging, page 12-172; *Creating a New Site*, page 4-3

12.10 Security Commands

12.10.1 Clear/Purge Authentication



Removes information stored in the local authentication database.

Restrictions Requires privileged user status.

Parameters

User
Clears or purges a user from the local authentication database.

All
Clears or purges all users.

username
A specific username to clear or purge.

Precedence
Clears or purges a given precedence slot. Must be used in conjunction with the **num** parameter.

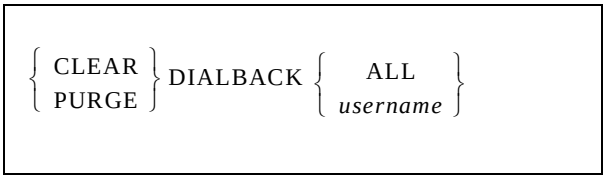
num
A precedence number of 1 through 6.

Examples

```
Local>> CLEAR PURGE AUTHENTICATION USER “bob”
Local>> PURGE AUTHENTICATION PRECEDENCE 2
```

See Also Set/Define Authentication, page 12-153; Set/Define Authentication Unique, page 12-163; Show/Monitor/List Authentication, page 12-177; Chapter 11, *Security*

12.10.2 Clear/Purge Dialback



Removes a dialback setting for a particular username, or for all usernames.

Restrictions Requires privileged user status.

Errors Clear Dialback will return an error if the specified username isn't found, or if All is specified and no entries are configured.

Parameters

All
Clears dialback settings for all usernames.

username
Clears dialback settings for the specified username.

Examples

```
Local>> CLEAR DIALBACK ALL
Local>> PURGE DIALBACK robert
```

See Also Define Ports Dialback, page 12-70; Set/Define Dialback, page 12-165; Show/Monitor/List Dialback, page 12-178; *Dialback*, page 11-5.

12.10.3 Clear/Purge Filter

Removes a specified packet filter.

Restrictions Requires privileged user status.

Parameters

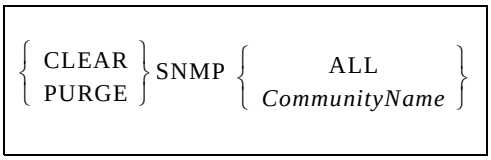
filtername
A particular packet filter to be removed.

Examples

```
Local>> PURGE FILTER abc
```

See Also Set/Define Filter, page 12-166; Show/Monitor/List Filter, page 12-178; *Filter Lists*, page 5-2

12.10.4 Clear/Purge SNMP



Removes entries from the SNMP security table.

Restrictions Requires privileged user status.

Parameters

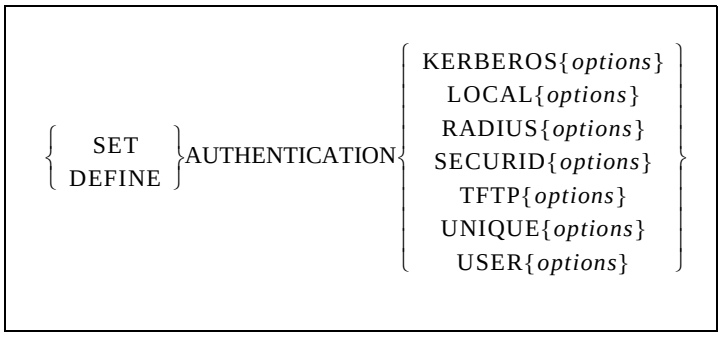
All
Removes all SNMP table entries.

CommunityName
Enter the name of the SNMP community to be removed.

Examples Local>> CLEAR SNMP “nycomm”

See Also Set/Define SNMP, page 12-177; Set/Define Filter IP, page 12-169; Show/ Monitor/List SNMP, page 12-179; ,

12.10.5 Set/Define Authentication



Configures the authentication system. Logins on ports with authentication enabled will be prompted for a username and password pair, which will be checked sequentially against up to six databases: a Kerberos database, the SCS local database (NVR), a RADIUS server, a SecurID server, or a UNIX password file (TFTP).

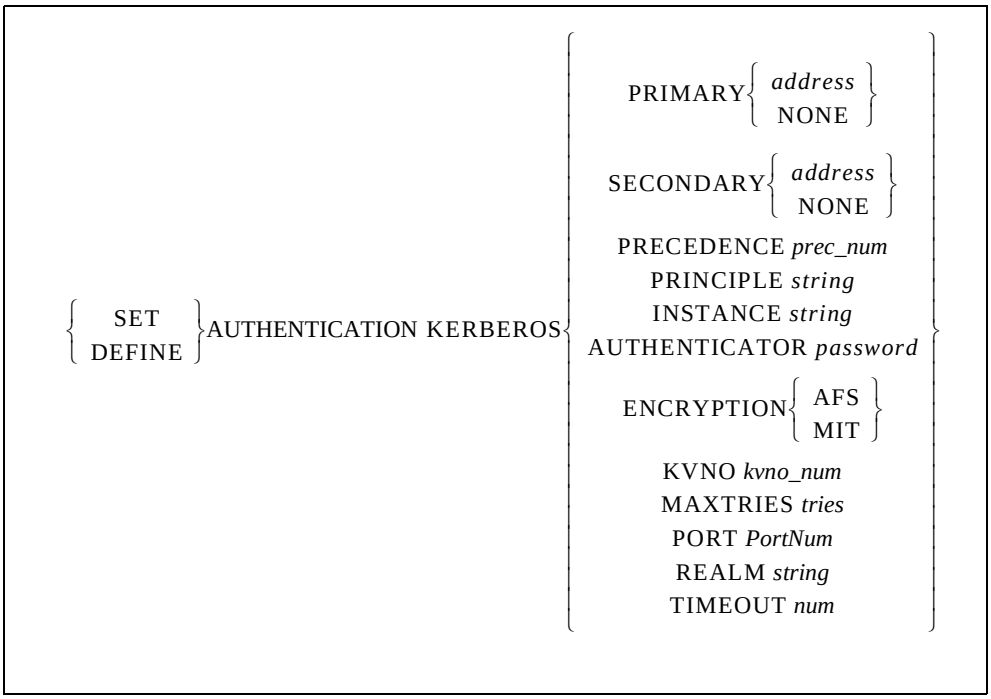
To configure one or more of the six databases, refer to the appropriate command in this section.

Note: *Precedence settings should be configured carefully. If a database is configured for a precedence slot that has already been filled by another database, it will take over the precedence setting and return all of the previous database’s settings to their factory defaults.*

Restrictions Requires privileged user status.

See Also Define Site Authentication, page 12-132; Chapter 11, *Security*

12.10.6 Set/Define Authentication Kerberos



Specifies that a Kerberos database will be used for authentication. Specific Kerberos options are explained in detail in the *Kerberos* section on page 11-11.

Restrictions Requires privileged user status.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

If the SCS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/ password), the secondary database or server (discussed below) will be checked. If the user is authenticated at any point, the search process will stop and the login will be permitted.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

Secondary
Sets the secondary database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 192.23.71.49).

None
Clears the current server address.

Precedence
Sets the precedence in which this database or server is checked. The precedence number must be specified using the **prec_num** parameter.

prec_num
A precedence number between 1 and 6.

Principle
A label that identifies the authentication service that the SCS requests from the Kerberos server. Must be used in conjunction with the **string** parameter.

Instance
A label that is used to distinguish among variations of the principle. Must be used in conjunction with the string parameter.

string
A case-sensitive string of up to 40 alphanumeric characters. **To preserve case, enclose the string in quotes.**

Authenticator
Specifies the password for the principle/instance pair. Must be used in conjunction with the password parameter.

password
A case-sensitive password of up to 40 alphanumeric or 8 hexadecimal characters. **To preserve case, alphanumeric passwords must be enclosed in quotes.**

Encryption
Specifies that either the Andrew File System (AFS) or MIT Encryption algorithm will be used to create the Kerberos keys. The SCS encryption method should match the Kerberos server encryption method.

MIT
Enables use of the MIT encryption algorithm.

AFS
Enables use of the Andrew File System encryption algorithm.

Port
Specifies the UDP/IP Port number used to communicate with the Kerberos server. The number applies to both the primary and secondary servers. Must be used in conjunction with the PortNum parameter.

PortNum
An integer between 1 and 65535.

Timeout
Specifies the timeout period for a response from the Kerberos server. Must be used in conjunction with the *seconds* parameter.

seconds
An integer between 1 and 255, inclusive.

Maxtries
Specifies the maximum number of times that the SCS will attempt to contact the Kerberos server.

tries
An integer between 1 and 255, inclusive.

Realm
Sets the Kerberos realm that the SCS resides in. Often set to a name that mirrors the Internet domain name system. Must be used in conjunction with the **string** parameter, discussed earlier.

KVNO (Key Version Number)
Ensure that the SCS and the Kerberos server are using the correct authenticator for the defined principle/instance pair. The KVNO for the SCS must match the Kerberos server's KVNO. Must be used in conjunction with the **kvno_num** parameter.

kvno_num
An integer between 1 and 255, inclusive.

Defaults

Principle: rcmd
Instance: SCS
Encryption: MIT
PortNum: 750
Timeout: 3 seconds
MaxTries: 5

See Also

Define Site Authentication, page 12-132; *Kerberos*, page 11-11

12.10.7 Set/Define Authentication Local

Specifies that an SCS database (saved in NVR or RAM) will be used for authentication. The precedence number is set to 1 by default.

Restrictions

Requires privileged user status.

Parameters

Precedence
Sets the precedence in which this database or server is checked. Must be used in conjunction with the prec_num parameter.

prec_num
A precedence number between 1 and 6, usually set to 1.

Defaults

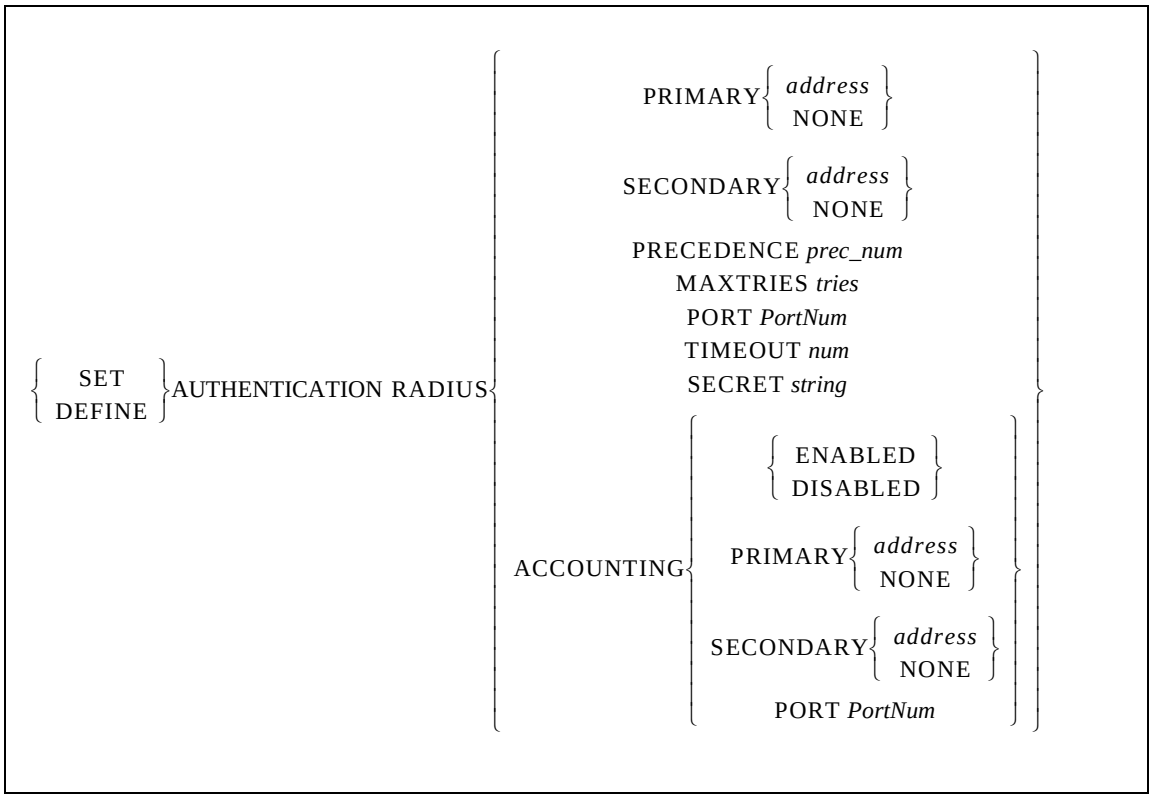
Precedence: 1

Examples

```
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 2
```

See Also Define Site Authentication, page 12-132; Set/Define Authentication Unique, page 12-163; *Local (NVR) Database*, page 11-9

12.10.8 Set/Define Authentication RADIUS



Specifies that a RADIUS server will be used for authentication and/or accounting.

Restrictions Requires privileged user status.

Parameters

Primary
Specifies the first server to be checked. A specific address must be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

If the SCS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/password), the secondary database will be checked. If the user is authenticated at any point, the search process stops and the login is permitted.

If the user cannot be authenticated using the secondary server, the dataserver with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

Secondary
Sets the secondary server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

address
A text host name (if DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Sets the precedence in which this database or server is checked. The precedence number must be specified using the **prec_num** parameter.

prec_num
A precedence number between 1 and 6.

Maxtries
Specifies the maximum number of times that the SCS will attempt to contact the RADIUS server. Maxtries must be used in conjunction with the **tries** parameter.

tries
An integer between 1 and 255, inclusive.

Port
Specifies that authentication or accounting information should be sent to a specific port on the server, specified with the **PortNum** parameter.

PortNum
A port number between 0 and 65535, inclusive.

Timeout
Specifies the timeout period for a response from the RADIUS server. Must be used in conjunction with the **num** parameter.

num
An integer between 1 and 255, inclusive.

Note: *For accounting, the SCS has to hold onto packets until they can be verified. If the Maxtries and Timeout values are too large, you can overflow the SCS and it will begin to drop accounting packets. This can be avoided by setting retries and timeouts to lower values.*

Secret
Specifies the Secret to be Shared between the RADIUS client and server. Must be used in conjunction with the string parameter.

string
A string of up to 64 characters. This string must be identical to that used by the RADIUS server for the SCS.

Accounting
Specifies that RADIUS accounting information will be sent to a RADIUS accounting server. Accounting can be enabled even if the SCS does not use a RADIUS server for authentication.

Primary
Specifies the primary accounting server to which accounting information will be sent. If the primary server cannot be reached, the secondary server will be tried.

Secondary
Specifies the secondary accounting server to which accounting information will be sent when the primary server cannot be reached.

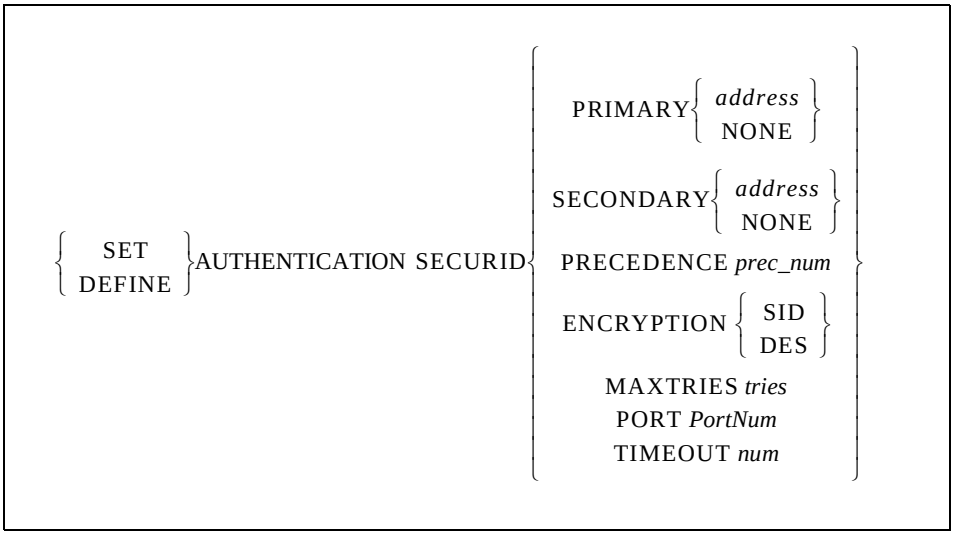
PortNum
A port number between 0 and 65535, inclusive.

Defaults
Authentication port: 1645
Maxtries: 3
Timeout: 1 (second)
Accounting port: 1646

Examples
```
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.55:1234
Local>> DEFINE AUTHENTICATION RADIUS TIMEOUT 10 MAXTRIES 4
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING ENABLED
```

See Also
Clear/Purge Authentication, page 12-151; Define Site Authentication, page 12-132; Show/Monitor/List Authentication, page 12-177; *RADIUS*, page 11-14

12.10.9 Set/Define Authentication SecurID



Specifies that a Security Dynamics ACE/SecurID server will be used for authentication.

Restrictions

Requires privileged user status.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

Secondary
If the SCS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/ password), the secondary database or server will be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 192.23.71.49).

None
Clears the current server address.

Precedence
Sets the precedence in which this database or server is checked. The precedence number must be specified using the **prec_num** parameter.

prec_num
A precedence number between 1and 6.

Encryption
SecurID (SID) or DES encryption will be used for authentication.

SID
Enables use of SecurID encryption.

DES
Enables use of DES encryption.

Maxtries
Specifies the maximum number of times the SCS will attempt to contact the SecurID server. Must be used in conjunction with the **tries** parameter.

tries
An integer between 1 and 255, inclusive.

Port
Specifies the UDP/IP port number used to communicate with the primary and secondary SecurID servers. Must be used in conjunction with the PortNum parameter.

PortNum
An integer between 1 and 65535.

Timeout
Specifies the timeout period for a response from the SecurID server. Must be used in conjunction with the seconds parameter.

seconds
An integer between 1 and 255, inclusive.

Defaults

Encryption: DES
Maxtries: 5
UDP/IP port: 5500
Timeout: 3 seconds

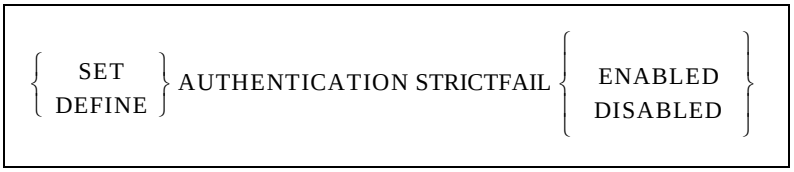
Examples

```
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.55
Local>> DEFINE AUTHENTICATION SECURID TIMEOUT 10 MAXTRIES 4
Local>> DEFINE AUTHENTICATION SECURID ACCOUNTING ENABLED
```

See Also

Define Site Authentication, page 12-132; *SecurID*, page 11-17

12.10.10 Set/Define Authentication Strictfail



Strict fail mode aborts the authentication process if any method returns an error of “invalid error” or “invalid password.”

Restrictions

Requires privileged user status.

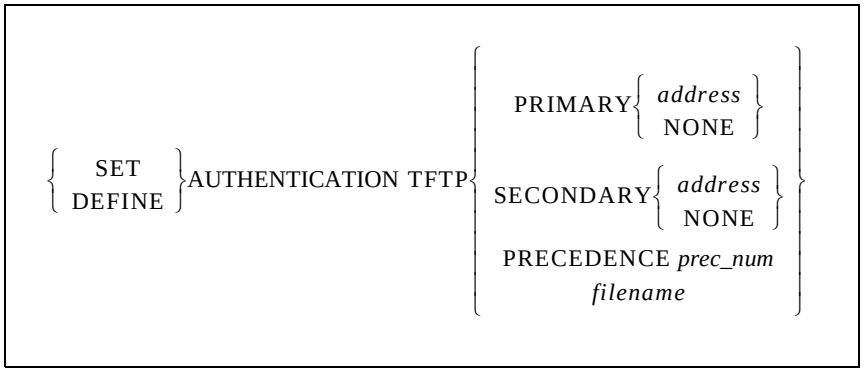
Defaults

Disabled

See Also

Show/Monitor/List Authentication, page 12-177; *Database Configuration*, page 11-9, *Disabling HTTP and FTP*, page 6-17

12.10.11 Set/Define Authentication TFTP



Specifies that a UNIX password file will be used for authentication. This file will be read via the TFTP protocol.

Note: *A TFTP-readable password file may reduce network security.*

Restrictions Requires privileged user status.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

Secondary
If the SCS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/password), the secondary database or server will be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 192.23.71.49).

None
Clears the current server address.

Precedence
Sets the precedence in which this database or server is checked. The precedence number must be specified using the **prec_num** parameter.

prec_num
A precedence number between 1 and 6.

filename
Specify a TFTP password file name of up to 32 characters. **If spaces or lowercase characters are used, the filename must be enclosed in quotes.**

Examples Local>> SET AUTHENTICATION TFTP FILENAME radicchio

See Also Define Site Authentication, page 12-132; *UNIX Password File*, page 11-19

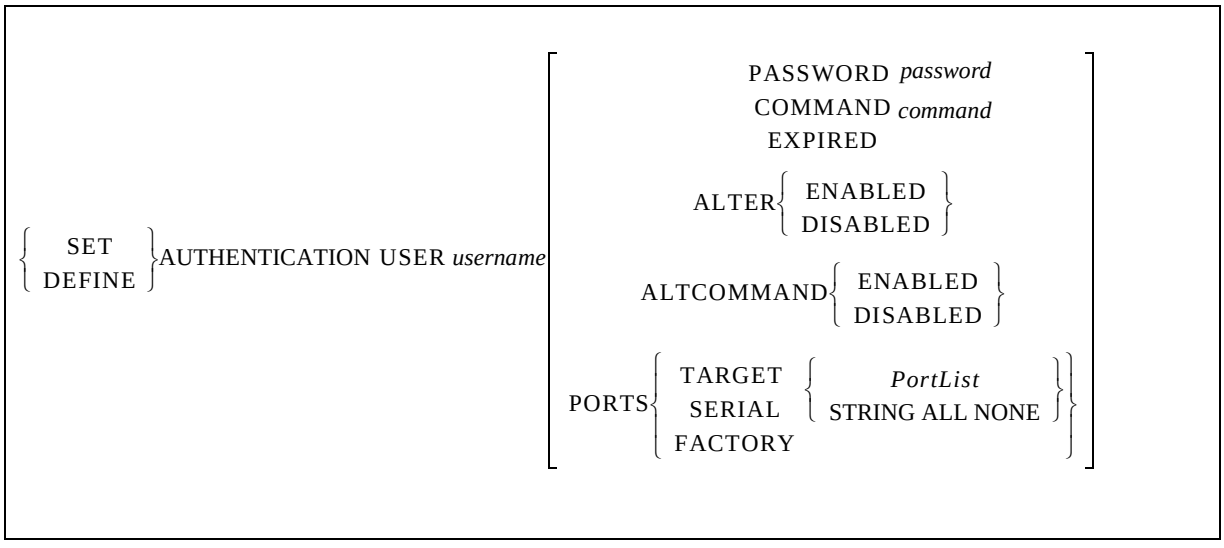
12.10.12 Set/Define Authentication Unique

When enabled, the authentication code prevents multiple incoming authenticated logins by the same user. It does not prevent the user from making additional non-authenticated connections.

Restrictions Requires privileged user status.

See Also *Restricting Multiple Authenticated Logins*, page 11-21

12.10.13 Set/Define Authentication User



Configures entries to the local database. To indicate which username entry will be modified, a username must be specified using the username parameter.

Restrictions Requires privileged user status.

Parameters

username
A username of up to 16 characters. ***The name is converted to all uppercase unless it is enclosed in quotes.***

Password
Configures a password for an authenticated user. **The password is converted to all uppercase unless it is enclosed in quotes.**

Note: *Users who don't have passwords configured for them will always be granted access.*

Command
Runs a command or commands immediately after login. The Altcommand feature must be enabled for this to work. **Commands must be enclosed in quotes and separated by semicolons.** The combined length of a series of commands cannot exceed 100 characters.

Expired
Forces a user to select a new password upon next login.

Alter
Enables or disables a user's ability to change his password. The password can be changed with the Set/Define Password command.

Altcommand
Enables the use of the command specified with the *command* parameter.

None
Removes port list from specified user.

Ports Target
Rejects user connection attempt from the network or "connect local" to a port not on the user's port target list.

Ports Serial
Rejects user connection attempt from the serial (character or PPP) not on the user's serial port list.

Ports Factory
Resets current port restrictions back to the default.

Portlist/All
Specifies a particular port or group of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

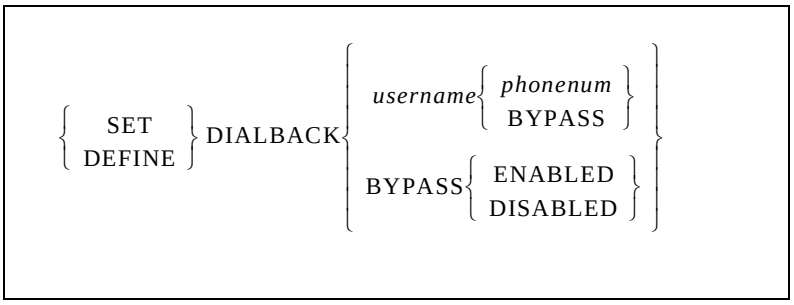
Examples

```
Local>> SET AUTHENTICATION USER "fred" COMMAND "TELNET athena;LOGOUT"
```

See Also

Define Site Authentication, page 12-132; Set/Define Password, page 12-176; *Local (NVR) Database*, page 11-9; Port User Restrictions, page 11-8

12.10.14 Set/Define Dialback



The Dialback feature enables a system manager to set up a dialback list of authorized users for incoming modem connections. Dialback lists include usernames and corresponding phone numbers. When a username entered matches one in the list, the port is logged out and the SCS sends the corresponding phone number to the serial port, at which time the port's modem profile initiates the modem connection.

Restrictions Requires privileged user status.

Parameters

username
A text name, up to 16 characters long. **If white space or lowercase characters are used, the username must be enclosed in quotes.**

phonenum
A telephone number.

Note: *The ATDT command should not be entered in the telephone number string. The modem profile will prepend any necessary command prefixes.*

Bypass
When the Bypass parameter is associated with a username, the port will not be logged out, and the user will not be dialed back, when attempting to connect to the SCS. The word "bypass" must be associated with the username in the dialback database in order for dialback to be bypassed.

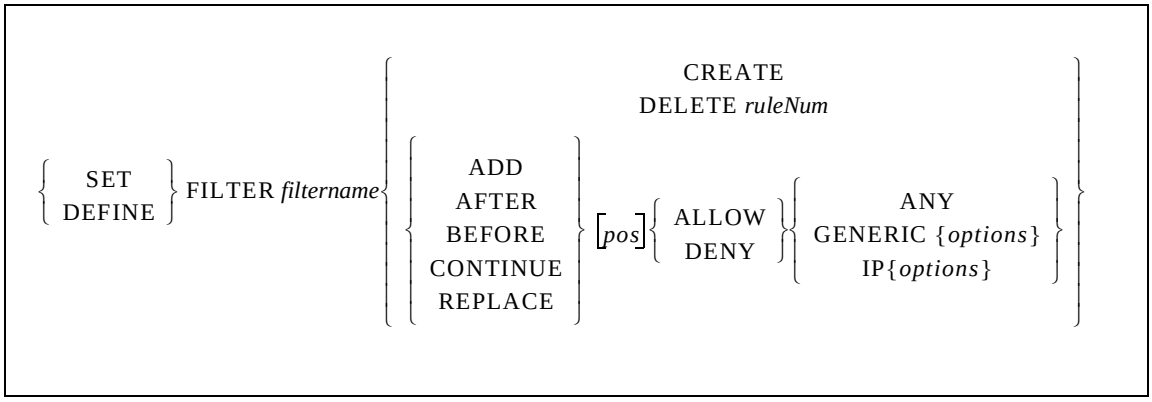
When Bypass is used with the Enabled parameter (that is, not associated with a username), users not in the dialback database are immediately given the Local> prompt. When disabled, users not in the database are denied access.

Examples

```
Local>> SET DIALBACK "susan" 867-5309
```

See Also Define Ports Dialback, page 12-70; *Dialback*, page 9-11; *Dialback*, page 11-5

12.10.15 Set/Define Filter



Creates or deletes a packet filter, or configures a rule in that filter that is used to manage network traffic. These packet filters are applied to packets arriving from or going to remote dialup sites.

Each rule consists of a name, a position, an action (allow or deny) and a protocol segment. To configure protocol options, refer to the appropriate command on the following pages. Due to space considerations, the command syntax from the Add braces to the Allow/Deny braces in the above diagram is represented by an ellipse (...) in the remaining Set/Define Filter commands.

In-depth protocol-related examples are given with the subcommands listed on the following pages.

Restrictions Requires privileged user status.

Parameters

filtername
The name of the filter in which the new rule will be included, up to 12 letters in length.

Create
Creates a new filter with the specified filtername. Filters must be created before their rules can be added, deleted, or otherwise modified.

Delete
Removes the specified rule from the named filter.

ruleNum
The number of the rule to be deleted.

Add
Adds a rule after another rule. If no position is specified, the rule is added to the end of the list of rules.

After
Inserts a rule after another rule. If no position is specified, the rule is added to the end of the list of rules.

Before
Inserts a rule before another rule. If no position is specified, the rule is added to the beginning of the list of rules.

Continue
Continues a long filter that won't fit in the 132-character line limit for commands.

Replace
Replaces an existing rule with a new one. If no position is specified, the first rule in the list is replaced.

pos
A location in the filter list to perform a specific function, such as Add.

Allow
Allows passage of data packets that meet the defined filter criteria. The criteria consists of all specified parameters after Allow.

Deny
Denies passage of data packets that meet the defined filter criteria. The criteria consists of all specified parameters after Deny.

Examples

```
Local>> DEFINE FILTER abc CREATE

Local>> DEFINE FILTER abc DELETE 2
(Removes the second rule in filter list abc)

Local>> DEFINE FILTER abc ADD DENY IP TOS 0xE0 0x80
Local>> DEFINE FILTER abc CONTINUE DENY IP TOS 0xf0 0x40
```

See Also Define Site Filter, page 12-138; Clear/Purge IP Security, page 12-19; Define Ports Dialback, page 12-70; *Packet Filters and Firewalls*, page 11-23.

12.10.16 Set/Define Filter Any

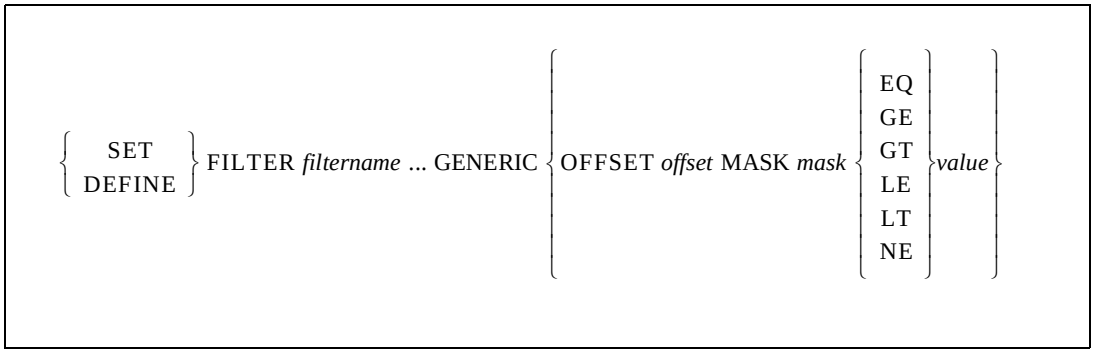
{ SET / DEFINE } FILTER *filtername* ... ANY

Specifies that every packet will be allowed or denied passage through the SCS. Using the Any parameter along with either Allow or Deny will affect all packets regardless of any filter specifications that follow. Usually, an Any rule is placed at the end of a filter list to process data packets not specifically identified by the previous rules in the list.

Restrictions Requires privileged user status.

See Also Define Site Filter, page 12-138; Clear/Purge IP Security, page 12-19; Define Ports Dialback, page 12-70; *Packet Filters and Firewalls*, page 11-23

12.10.17 Set/Define Filter Generic



Specifies a general filter rule that applies to any packet regardless of protocol. A Generic rule starts at a location **offset** bytes from the beginning of the packet, applies the specified **mask**, and then compares the result with a specified value. Multiple generic offset segments can be included in a single rule, subject to the maximum command line length of 132 characters (see the example below).

Restrictions Requires privileged user status.

Parameters

offset
Defines where in the data packet to apply the mask. May be a decimal value from 0 to 1500, where 0 indicates the first data position in the packet.

mask
A hexadecimal or decimal number.

operator
(EQ, GE, GT, LE, LT, NE)
The options are: equal to (EQ), greater than or equal to (GE), greater than (GT), less than or equal to (LE), less than (LT), and not equal to (NE).

value
A hexadecimal or decimal number.

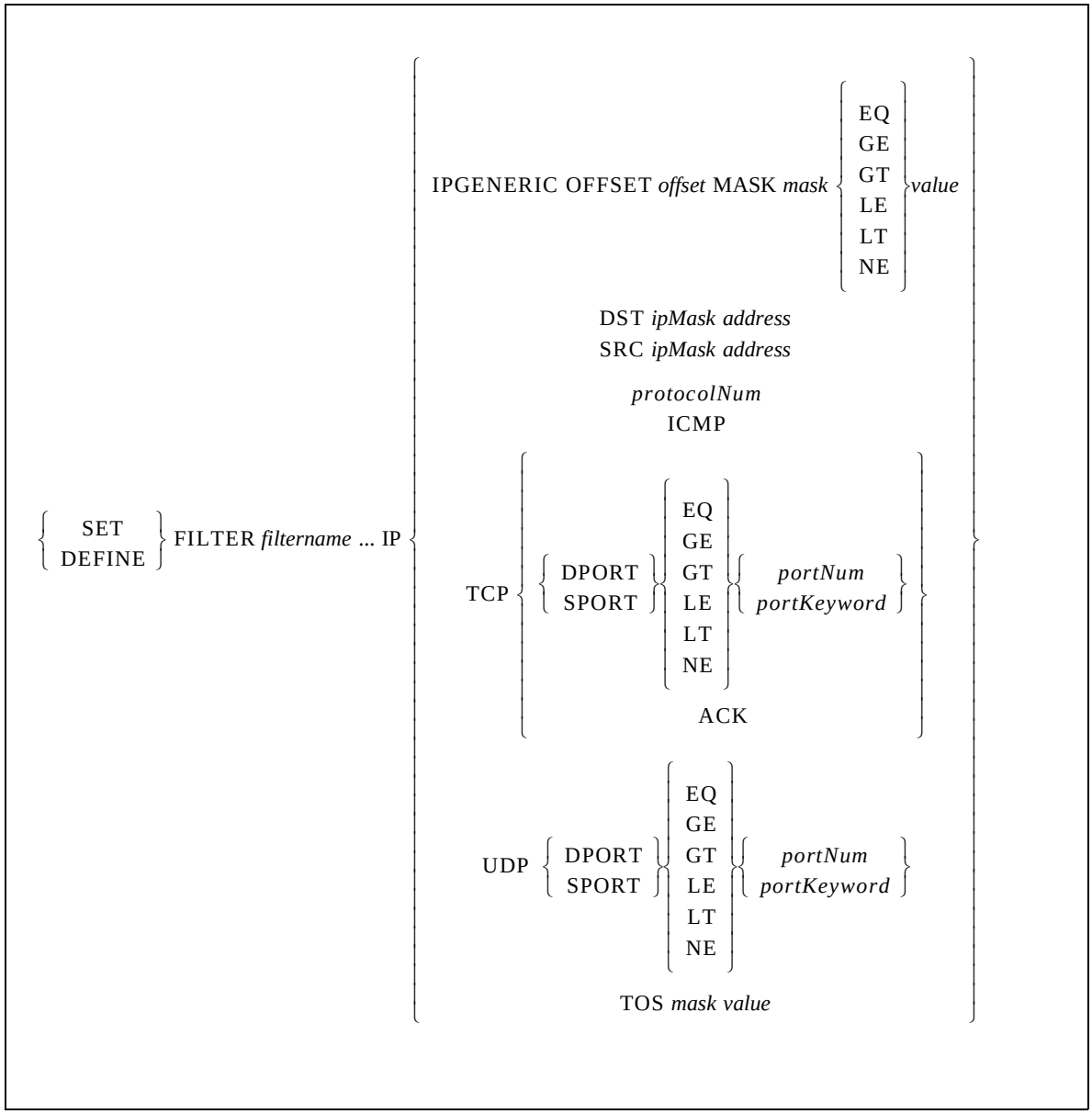
Examples

```
Local>> DEFINE FILTER abc ADD DENY GENERIC OFFSET 0 MASK 0xff000000 GT
0x25000000 OFFSET 8 MASK 0xffffffff EQ 0x12345678
```

(Adds a rule containing two generic segments to filter abc.)

See Also Define Site Filter, page 12-138; Clear/Purge IP Security, page 12-19; Define Ports Dialback, page 12-70; *Packet Filters and Firewalls*, page 11-23

12.10.18 Set/Define Filter IP



Creates a rule which will be applies only to IP protocol packets.

Restrictions Requires privileged user status.

Parameters

IPGeneric
Specifies a general IP rule using one set of offset, mask, operator, and value. Multiple IPGeneric segments can be included in a single rule (in one command), subject to the maximum command line length of 132 characters.

offset
Defines where in the data packet to apply the mask. May be a decimal value from 0 to 1500, where 0 indicates the first data position in the data packet.

mask
A hexadecimal or decimal number. The **mask** is applied to the data using the operator and the result is compared with the **value**. In the case of TOS, the operator EQ is implied.

operator
(EQ, GE, GT, LE, LT, NE)
The available operators are: equal to (EQ), greater than or equal to (GE), greater than (GT), less than or equal to (LE), less than (LT), and not equal to (NE).

value
A hexadecimal or decimal number.

DST
Allows or denies passage of data packets destined for a specific node on the local area network. Must be used in conjunction with the **ipMask** and **address** parameters.

SRC
Allows or denies passage of data packets that originated from a specific node on the local area network. Must be used in conjunction with the **ipMask** and **address** parameters

ipmask
An IP address in standard numeric format (for example, 193.0.1.255).

address
An IP address in standard numeric format (for example, 193.0.1.50).

TOS
Builds a rule using the IP Type of Service field. Must be used in conjunction with the **mask** and **value** parameters. For TOS, the operator EQ is implied.

protocolNum
Allows or denies packets of the protocol specified by an IP protocol identifier number between 0 and 65535.

ICMP
Allows or denies Internet Control Message Protocol packets.

TCP
Allows or denies TCP-based packets which match criteria specified by the subsequent parameters. Applications that use TCP include Telnet, FTP, and SMTP (Simple Mail Transfer Protocol).

UDP
Allows or denies User Datagram Protocol (UDP) based packets which match criteria specified by subsequent parameters. Applications that use UDP include DNS (Domain Name Service), TFTP (a variant of FTP), and BOOTP (used by some computer systems to acquire IP addresses).

DPort
Defines the destination protocol port. Data packets are filtered based on both the protocol and on the protocol port of the data packet.

SPort
Defines the source protocol port. Data packets are filtered based on both the protocol and the protocol port of the data packet.

portNum
A TCP or UDP port number.

portKeyword
A keyword corresponding to the TCP or UDP port number. Available keywords are BOOTP, DNS, FINGER, FTP, FTPDATA, HTTP, NNTP, NTP, POP2, POP3, RIP, SMTP, SNMP, SYSLOG, TELNET, and TFTP.

ACK
Allows or denies TCP-based packets in which the ACK (acknowledge) bit is set.

Examples

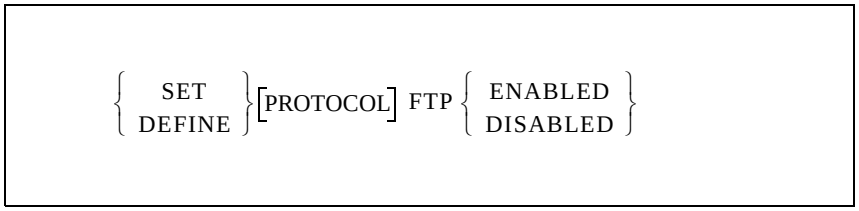
```
Local>> DEFINE FILTER abc ADD DENY IP
```
(Adds a rule for all IP traffic to filter abc.)

```
Local>> DEFINE FILTER abc ADD ALLOW IP IPGENERIC OFFSET 0 MASK 0xff000000
LT 0x34000000 TCP DPORT EQ TELNET
```
(Adds a rule containing an IP generic segment and DPORT to filter abc.)

```
Local>> DEFINE FILTER abc ADD ALLOW IP SRC 255.255.255.0 192.34.87.0 TCP
DSOCK EQ NCP
```
(Adds a rule containing IP SPORT and SRC to filter abc.)

See Also Define Site Filter, page 12-138; Clear/Purge IP Security, page 12-19; Define Ports Dialback, page 12-70; *Packet Filters and Firewalls*, page 11-23

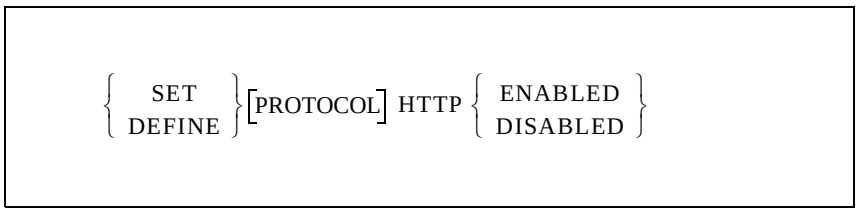
12.10.19 Set/Define FTP



Enables or disables the on-board FTP server.

See Also *Disabling the FTP and HTTP Servers*, page 11-23

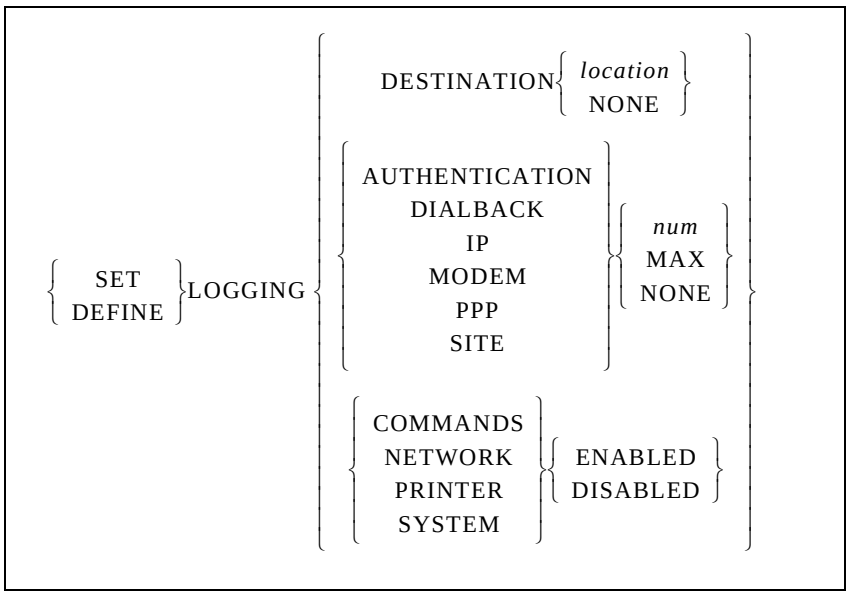
12.10.20 Set/Define HTTP



Enables or disables the on-board HTTP server.

See Also *Disabling the FTP and HTTP Servers*, page 11-23

12.10.21 Set/Define Logging



Controls error and event logging on the SCS. Events can be logged to a network host via TCP/IP or to a terminal connected to the SCS.

The host must be configured to support logging. For a TCP/IP host, the host's syslog facility must be configured; make sure all priorities equal to or higher than *.notice are being logged. The syslog file is typically located in the /etc directory; see your host's documentation or syslogd for more information.

Note: *Logging levels are cumulative; setting logging to level 4 includes levels 1 through 3 as well. See Chapter 11, Security, for a detailed description of the events that can be logged.*

Restrictions Requires privileged user status.

Parameters

Destination
Specifies a destination for the logging messages. Must be used in conjunction with the address parameter or the None parameter.

location
A fileserver name or IP address. This parameter may be specified as one of the following:

String/Form	Action
IP *hostname*:	Specifies a TCP/IP host
CONSOLE	Sends events to the SCS console port
MEMORY	Saves events in SCS memory
FILE *filename*	Saves events in a file *filename*. The default location is the SCS /ram disk, although other SCS disks can be specified (e.g. /flash/syslog.txt).

None
Disables logging.

Authentication
Logs events associated with authentication. Must be used with the num parameter or the None parameter.

Level	Information
1	System Problems
2	Failures and Successes
3	All Logins and Logouts
4	Incorrect Passwords
5	All Passwords, RADIUS Warnings

Dialback
Logs events associated with dialback functionality. Must be used with the num parameter or the None parameter.

Level	Information
1	Dialback Problems
2	Unauthorized Users
3	Dialback Failures
4	Dialback Successes
5	Dialback Attempts
6	Modem Chat

IP
Traces the activities of the IP router. Must be used with the num parameter or the None parameter.

Level	Information
1	Errors
2	Packets triggering remote connections
3	Routing table/interface changes
4	Incoming/outgoing RIP packets
5	Resulting routing table (verbose)
6	Contents of all RIP packets (verbose)
7	Routed packets (verbose)

Note: *Setting the IP logging level to 2 or greater results in a syslog that prints the source/destination IP address, protocol, and TCP/UDP source/destination ports.*

Modem
Logs modem activity, including modem jobs (incoming and outgoing). Must be used with the num parameter or the None parameter.

Level	Information
1	Problems
2	Call Statistics Dump From Modem
3	Setup

PPP
Logs events associated with PPP. Must be used with the num parameter or the None parameter.

Level	Information
1	Local System Problems
2	Remote System Problems
3	Negotiation Failures
4	Negotiation Data
5	State Transitions
6	Full Debugging

Site
Logs events associated with sites. Must be used with the num parameter or the None parameter.

Level	Information
1	Errors
2	State Transitions
3	Chat Scripts
4	Modem Dialing
5	Port Connections
6	Connection Failures
7	Usage Summary

num
An integer that specifies a particular level of logging.

Max
Sets logging to the maximum value.

Commands
When enabled, logs all commands users type.

Network
When enabled, logs network events. This is useful for diagnosing network-related problems.

Printer
When enabled, logs printer related events including online/offline conditions and job status at the end of job.

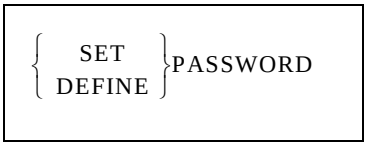
System
When enabled, logs server boots, log file open/closes, and other system related activity.

Defaults
Destination: None
Logging Options: None/Disabled (logging turned off)

Examples
```
Local>> SET LOGGING AUTHENTICATION 5
Local>> SET LOGGING DESTINATION FILE logfile
```

See Also
Show/Monitor/List Logging, page 12-179; *Event Logging*, page 11-25

12.10.22 Set/Define Password



Changes the current user's password in the local authentication database, provided the user is defined in the database and has permission to alter the password. When this command is entered, the user will be prompted for the old password, then prompted to enter and verify a new password.

Note: *The user has three chances to enter the old password before he or she is logged out of the SCS.*

Restrictions
Does **not** require privileged user status. To prevent users from altering their own passwords, enter the **Set/Define Authentication User Alter Disabled** command.

See Also
Set/Define Authentication User, page 12-163; Clear/Purge Authentication, page 12-151; Show/Monitor/List Authentication, page 12-177

12.10.23 Set/Define Server Incoming Secure

See Set/Define Server Incoming on page 12-119.

12.10.24 Set/Define SNMP

Configures a community name and access mode for SNMP access. Each name has an access restriction associated with it; if an SNMP command comes in with an unknown name or an unauthorized command, an SNMP error reply will be sent. Community names are not case-sensitive.

Restrictions You must be the privileged user to use this command.

Parameters

community
A text name, up to 16 characters long.

Access
Specifies the type of SNMP access. Must be used in conjunction with one of the following parameters: Both, None, or Readonly.

Both
Both read and write requests will be permitted.

None
No SNMP requests are permitted.

Read
Read-only access will be permitted.

Examples Local>> SET SNMP COMMUNITY SUNMAN ACCESS BOTH

See Also Clear/Purge SNMP, page 12-153; ,

12.10.25 Show/Monitor/List Authentication

Displays the local authentication database.

Restrictions Requires privileged user status.

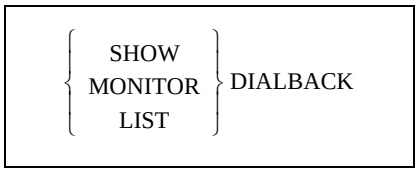
Parameters

username
Displays authentication information for the specified user.

Examples Local>> SHOW AUTHENTICATION USER “bob”

See Also Set/Define Authentication, page 12-153; *Local (NVR) Database*, page 11-9

12.10.26 Show/Monitor/List Dialback

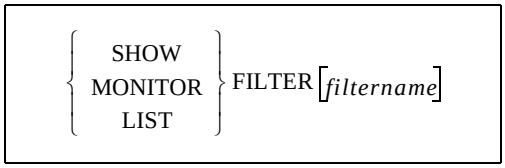


Displays the currently configured dialback strings, as well as the number of connect attempts with that string the number of connect failures.

Restrictions Requires privileged user status.

See Also Clear/Purge Dialback, page 12-152; Define Ports Dialback, page 12-70; Set/Define Dialback, page 12-165; *Dialback*, page 8-12; *Dialback from Character Mode*, page 11-6

12.10.27 Show/Monitor/List Filter

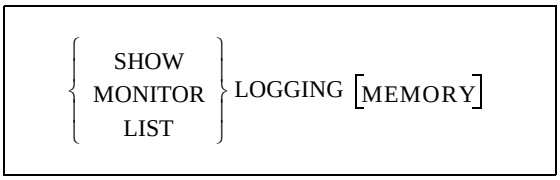


Displays the current packet filters. An individual filter may be specified using the **filtername** parameter.

Restrictions Requires privileged user status.

See Also Set/Define Filter, page 12-166; Clear/Purge Filter, page 12-152; *Filter Lists*, page 5-2

12.10.28 Show/Monitor/List Logging



Displays the current or saved event logging configuration.

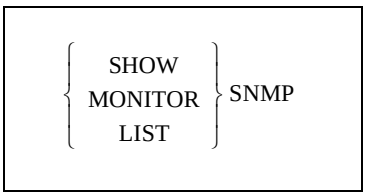
Restrictions You must be the privileged user to use the Monitor command.

Secure users may not use this command.

Parameters **Memory**
Displays the memory log.

See Also Set/Define Logging, page 12-172; *Event Logging*, page 11-25

12.10.29 Show/Monitor/List SNMP



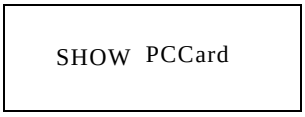
Displays the current or saved SNMP security table entries.

Restrictions Requires privileged user status.

See Also Clear/Purge SNMP, page 12-153; ,

12.10.30 PC Card Commands

12.10.31 Show PCCard



Provides general information about the PC card(s) installed in an SCS200 or SCS400.

12.11 Navigation/Help Commands

12.11.1 Apropos

APROPOS *keyword*

Displays commands containing the specified keyword. If a command containing the keyword cannot be found, the SCS will display “nothing appropriate.”

The SCS will not display all relevant commands. If there are any logout commands, such as Set Ports and Define Ports, only one will be shown (in this case, Set Ports).

Restrictions Privileged commands containing the specified keyword will only be displayed if you are currently the privileged user.

Parameters

keyword
An alphanumeric string. You do not have to type the complete command keyword in order to get a response; partial strings will yield appropriate commands that contain that string.

Examples APROPOS SITE

See Also Help, page 12-187

12.11.2 Backwards

BACKWARDS

Switches sessions from the current session to the most recently started previous session. If there is only one active session, it resumes. Repeating the command will cycle you “backward” through the active sessions. If you search the beginning of the session list, entering this command returns you to the most recent session.

See Also Forwards, page 12-186; Show/Monitor Sessions, page 12-98; *Port-Specific Session Configuration*, page 8-4

12.11.3 Broadcast

BROADCAST { ALL | PORTS *PortNum* | *username* } *message*

Sends a message to another port, all ports, or a specific user on the server. Broadcast may only be used if broadcasts have been enabled on the server using the **Set/Define Server Broadcast** command.

Restrictions You must be the privileged user to use the All parameter.

Secure users may not send broadcasts.

Errors An error will be returned if the port broadcasted to is flow controlled or if the server does not have broadcast enabled. The sender is notified if a message was not received.

Parameters

All
Sends the message to all ports.

Ports
Specifies a particular port as recipient of the message. Must be used with the PortNum parameter.

PortNum
A particular SCS port.

username
A particular user as recipient of this message.

message
One word, or several words, **in quotes**. The message will be sent exactly as typed if enclosed in quotes, or in uppercase if not. The message length is limited only by the length of the command line.

Examples

```
Local>> BROADCAST PORT 7 “ready for lunch?”
Local>> BROADCAST fred “Meeting in 10 minutes.”
```

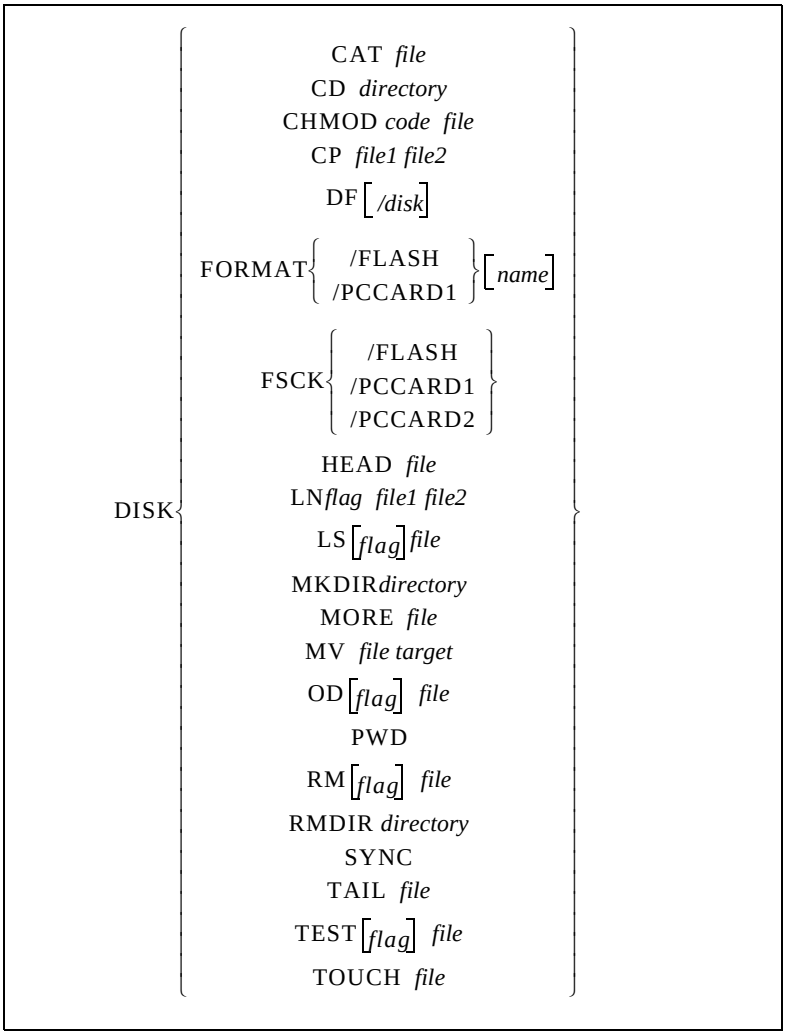
See Also Set/Define Server Broadcast, page 12-116; *Rebooting*, page 2-5

12.11.4 Cls

```
CLS
```

Clears the screen on your terminal device if the port is configured as Type ANSI.

12.11.5 Disk



Performs disk management functions for the SCS and, for models with PC card support, for any installed ATA flash card. The SCS contains two modifiable directories—/ram and /flash—and one read-only directory—/rom. For SCS models with one PC card slot, an ATA card can be accessed as /pccard1; for models with two slots, the card in the top slot can be accessed as /pccard1 and the card in the bottom slot as /pccard2.

The Disk commands are very similar to the file management commands in UNIX environments. Unlike the similar UNIX commands, each disk command must be preceded by the word DISK. The commands are also not case-sensitive.

The Disk commands honor disk permissions. All disks are read only for non-privileged users.

Restrictions

The Format and FSCK parameters requires privileged user status.

The PC card parameters only apply to the SCS200.

The ROM disk is read-only and cannot be modified by users.

Errors

For the /pccard1 and /pccard 2 parameter, you will receive an error if either the specified card is not a storage card or if there is no card in the slot.

Parameters

Cat
Displays an entire file in your terminal window.

Cd
Changes your current working directory.

Chmod
Changes permissions for a file or directory. To assign permissions, enter a 3-digit number. The first digit represents the owner's permissions. The second digit represents the group's permissions. The third digit represents the world's permissions.

Table 12-6:

Digit	Meaning
0	No permissions.
1	Execute permission only.
2	Write permission only.
3	Write and Execute permissions.
4	Read permission only.
5	Read and Execute permissions.
6	Read and Write permissions.
7	All permissions.

Cp
Copies or moves a file. To copy a file, enter the filename for file1 and the new file name as file2. To move a file, specify the filename as file1 and the destination directory as file2.

Df
Displays the blocks of free space on the SCS disks. When you add the -i switch, the display includes in the display the number of inodes used versus the number still available. If no disk name is specified, all disks are displayed.

/disk
Enter the disk name, e.g. /flash.

Format
Formats either the Flash disk or the specified PC card with the Lantronix filesystem.

/Flash
Formats or erases the /flash disk.

/PCCard1
Formats an ATA flash card for use in an SCS PC card slot. An unformatted card can not be used by the SCS.

name
Names the specified disk

Fsck
Checks the SCS filesystem and corrects any problems.

Head
Outputs the beginning of a string.

Ln
Creates a hard or soft link for files, linking a file or set of files to another file. using no flag creates a hard link. Adding the -s flag creates a soft link.

Ls
Displays the contents of a directory. The available flags are:

-l	Returns a list in long form, which includes information about modification date, size, owner, and permissions.
-t	Sorts the list by modification date, with the newest file appearing first.
-r	Reverses the order of the file listing. For example, if -t was also specified, -r would list the oldest file first.

Mkdir
Creates a new directory on the SCS RAM or flash disk.

More
Displays the contents of a file on the terminal, 24 lines of text at a time. Normally the display pauses after each screen and prints "--MORE--" at the bottom of the screen. To access the next screen, press the Space bar. To abort, press Ctrl-C.

Mv
Moves files or directories on the SCS RAM and flash disks. You can also rename files with this command by inserting the new filename for *target*

Od
Displays the contents of the specified file as raw hexadecimal byte values. The possible flags are:

-b	Prints the bytes in octal format.
-ct	Prints the bytes in ASCII format.
-x	Prints the bytes in hexadecimal format.

Pwd
Displays the full pathname of your current directory.

Rm
Removes files and/or directories from the RAM and Flash disks. The possible flags are:

-i	Prompts for a Y (yes) or N (no) before the file is removed.
-r	Removes an entire directory and all of its subdirectories.

Rmdir
Removes a directory from the specified disks. The command can only be used if the directory is empty. If the directory is full, you must add the **DISK RM -rf** command.

Sync
Forces the SCS to write files on all disks (including any PC card disks) immediately. Normally, when the SCS is rewriting files to disk, it will buffer data before initiating a write sequence. Write sequences are automatically written after 5 seconds of disk inactivity.

Tail
Outputs the end of a file.

Test
Evaluates a file (true or false). The possible flags that will be returned are:

-d	True if file exists and is a directory.
-e	True if file exists (regardless of type).
-f	True if file exists and is a regular file.
-l	True if file exists and is a symbolic link.
-r	True if file exists and is readable.
-w	True if file exists and is writable. True indicates only that the write flag is on. The file is not writable on a read-only file system even if this test indicates true.
-x	True if file exists and is executable. True indicates only that the execute flag is on. If the file is a directory, true indicates that the file can be searched.

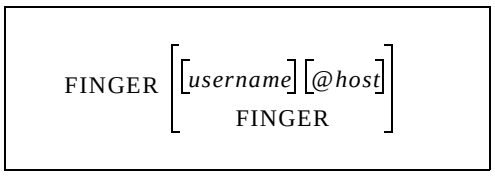
Touch
Creates an empty disk file.

Examples

```
Local>> DISK CHMOD 755 /PCCARD1/index.txt
Local>> DISK FORMAT /PCCARD1
Local>> DISK LS -l /PCCARD1/
Local>> DISK TEST /PCCARD1/add.exe
```

See Also *Disk Management*, page 2-18

12.11.6 Finger



This command is based on the UNIX Finger command that displays local and remote users.

If a **username** is specified, information about that username will be displayed. If the user@hostname parameters are specified, information regarding user **user** on TCP/IP host **host** will be displayed. Using the Finger command without any parameters will display all current logins.

Restrictions Secure users cannot use the finger command.

Errors An error is displayed if the host cannot be accessed.

Parameters

username
A username. If this parameter is omitted, all users on the host will be displayed.

@host
The "at" character, followed by a hostname.

Finger
Displays a list of current processes.

Examples

Local> FINGER BOB
(shows user bob on SCS)

Local> FINGER @HYDRA
(shows users on host hydra)

Local> FINGER bob@hydra
(shows user bob on hydra)

See Also Show/Monitor Users, page 12-131

12.11.7 Forwards

Cycles forward through your sessions in the order displayed by the Show Sessions command. The next session on the list becomes the active session. If there is only one active session, the session will resume. If the bottom of the session list is reached (the most recently started session) and this command is entered, the session at the top of the session list is resumed.

Errors An error is displayed if no sessions are active.

See Also Backwards, page 12-180;Set/Define Ports Forward Switch , page 12-73; Show/Monitor Sessions, page 12-98; *Port-Specific Session Configuration*, page 8-4

12.11.8 Help

HELP [*command*] [*parameter*]

Accesses the SCS Help system. Using the Help command without any parameters displays all available commands. Specifying a command gives information about that command a list of its parameters. Specifying a parameter gives information about the parameter, including any sub-parameters it may have.

Restrictions Requires privileged user status to view help text.

Parameters

command
An SCS command name.

parameter
An SCS parameter name. More than one parameter can be added to the Help command.

Examples

```
Local> HELP
Local> HELP CONNECT
Local> HELP DEFINE SERVER BROADCAST
```

See Also Apropos, page 12-180

12.11.9 Monitor

MONITOR

Displays current operating characteristics. The displayed information is updated every 3 seconds until a key is pressed. Each Monitor command and its parameters are documented together with the corresponding Show command.

Restrictions You must be the privileged user to use this command.

12.11.10 Netstat

NETSTAT

Displays the currently active network connections. This information is primarily meant for debugging network problems.

Restrictions Secure users may not use this command.

12.11.11 Ping

PING *hostname* [*num*]

Sends a TCP/IP request for an echo packet to another network host. This provides an easy way to test network connections to other TCP/IP hosts. In general, any host that supports TCP/IP will respond to the request if it is able, regardless of login restrictions, job load, or operating system.

If there is no reply from the host, this may indicate a network or TCP/IP configuration problem.

Parameters

hostname
Text name or IP address of the network host.

num
Enter the size of the packet you wish to send. The max size is 2000.

Defaults packet size of 50

Examples

```
Local> PING 192.0.1.23
Local> PING HYDRA.LOCAL.NET
```

See Also Your *Installation Guide*

12.11.12 Resolve

RESOLVE *hostname*

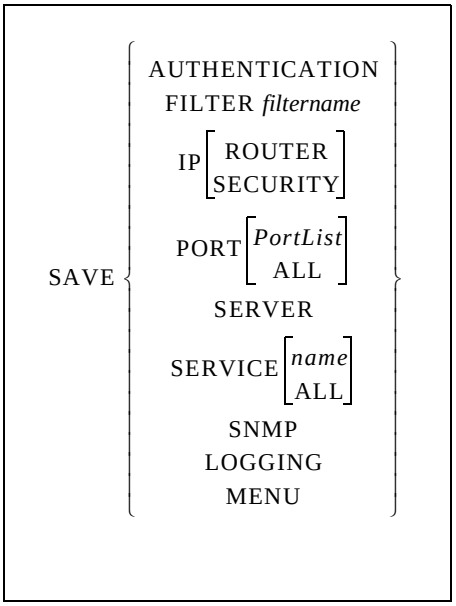
Attempts to resolve a TCP/IP name from the local host table and/or network nameserver.

Errors An error is returned to signal either that the attempted name service failed, or that the specified hostname is invalid.

Parameters

hostname
A TCP/IP hostname. Hostnames are usually limited to 64 characters, so the string is limited to 64 characters.

12.11.13 Save



Saves current configurations (made with the Set command) into the permanent database. This treats configurations as if they were made using the Define command.

To easily make current changes permanent, use the Save command after you have configured the port service, server, or printer. This eliminates the need to issue a corresponding Define command for each Set command.

Restrictions Requires privileged user status.

Errors Save without a parameter is invalid.

Parameters

Authentication
Saves authentication database preferences and the local authentication database.

Filter
Saves the packet filter settings for the specified filter. Must be used in conjunction with the filtername parameter.

IP Router
Saves the state of the IP router.

IP Security
Saves the current IP security table to the permanent database.

Menu
Saves all of the menu items setup using the **Set Menu** command to the permanent database.

Port
Saves the status of particular ports to the permanent database.

PortList
A port number or list of ports. Port numbers should be separated with commands (for lists) or dashes (for ranges).

All
Saves the settings for all ports or services to the permanent database.

Server
Save all the server characteristics to the permanent database.

Service
Save the current characteristics of a local service to the permanent database.

Note: *No more than one service per port can be defined at any time; if more than one service is defined, the Save Service command may fail.*

name
A service name.

SNMP
Saves all parameters associated with SNMP.

Logging
Saves the current logging configuration to the permanent database.

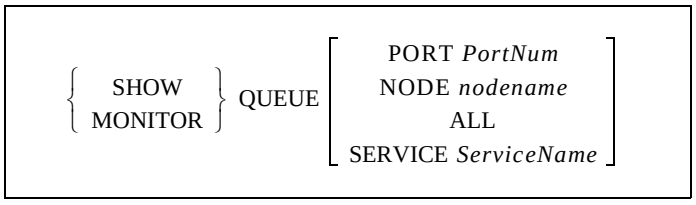
Menu
Saves all menu items setup using the **Set Menu** command (discussed on page 12-112) to the permanent database.

Examples

```
Local>> SAVE PORT 2
Local>> SAVE SERVICE NTX
```

See Also *Command Types*, page 2-3

12.11.14 Show/Monitor Queue



Show Queue will display the entries in a connect queue, if it exists. Particular sets of queues or entries can be selected with the Port, Node, or Service parameters. All can also be specified to show all entries.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Port
Displays information for all queue entries that can be served by the specified port. Must be used in conjunction with the **PortNum** parameter.

PortNum
Specifies a particular SCS port.

Node
Displays information for all queue entries requested from the specified node. Must be used in conjunction with the **nodename** parameter.

nodename
Specifies a particular node.

All
Displays information for all ports and nodes.

Note: *All is the default setting for Show/Monitor Queue.*

Service
Displays information for all queue entries for the local service specified with the **ServiceName** parameter.

ServiceName
Specifies a service name of up to 16 characters.

Examples

```
Local> SHOW QUEUE Port 6
Local> MONITOR QUEUE SERVICE lab5
```

12.11.15 Show Version

```
SHOW VERSION
```

Displays the current version of the SCS software.

See Also *Reloading Operational Software*, page 2-6

12.11.16 Zero Counters

This command is used to reset the counters for errors and other network and server events.

Restrictions You must be the privileged user to zero some other port (or All).

Parameters

All
Zeroes all Ethernet, TCP/IP, SLIP, and serial port counters.

Ethernet
Zeroes only Ethernet counters.

Port
Zeroes only the counters for events associated with a single serial port.

Note: *In the absence of a PortNum or the All or Ethernet parameters, the configuration will affect the current port.*

Examples

```
Local>> ZERO COUNTERS PORT 6
```

A: Environment Strings

A.1 Usage

An environment string is a sequence of key letters, sometimes prefixed by a plus (+) or minus (-). Environment strings can be used with certain commands to configure connections. The keys are added after the hostname (if one is given) and a colon.

Key letters are not case-sensitive, and no white space is allowed in the environment string. In addition, commands that oppose previously-configured settings will overwrite the previous setting, even if they appear on the same command line.

A.1.1 Multiple Strings

More than one string can be entered as part of a single command. Multiple strings do not need to be separated from each other. For example, you can enter a command that specifies both the desired port number and that the connection should in Passall mode.

Figure A-1: Entering Multiple Strings

```
Local>> DEFINE PORTS DEDICATED TELNET 192.0.1.3:2001+P
```

A.2 Available Strings

Note: *In most applications, environment strings are not necessary.*

Environment keys must be separated from the hostname, if one is specified, by a colon. Read the following sections carefully for more details on proper usage of each key.

Table A-1: Environment Strings

nnnn	socket number (SSH and TCP only)	
C	+C = CR to CRLF,	-C = CR to LF
D	+D = Backspace mode	-D = Delete mode
E	+E = Local Echo mode	-E = Remote Echo mode
P	+P = Passall mode	-P = Passthru mode
R	Rlogin protocol (sets port number to 513 if not already set)	
S	SSH protocol (Secure Shell)	
T	TCP mode (raw uninterpreted data stream)	

A.2.1 Usage Examples

These examples should illustrate the proper usage of the above environment strings.

A.2.1.1 nnnn

Sets a socket number. For SSH and TCP connections only. The most common socket numbers are 20*xx* (for Telnet IAC interpretation), 30*xx* (for raw TCP/IP), and 22*xx* (for SSH connections), where *xx* is the number of the desired serial port.

Examples

% telnet 192.0.1.66:3001
(forms a raw TCP/IP connection to the unit's first serial port)

Local> TELNET 192.0.1.45:2003
(forms a connection with Telnet IAC interpretation to the unit's third serial port)

A.2.1.2 +C and -C

+C specifies CR to CRLF. -C specifies CR to LF.

Examples

Local>> DEFINE PORTS PREFERRED TELNET 192.0.1.3:+C

A.2.1.3 +D and -D

+D sets Backspace mode. -D sets Delete mode.

Examples

% telnet 192.0.1.5:-D

A.2.1.4 +E and -E

+E sets Local Echo mode. -E sets Remote Echo mode.

Examples

% telnet 192.0.1.48:+E

A.2.1.5 +P and -P

+P specifies Passall method. -P specifies Passthru mode. Both Passall and Passthru will prevent the proper handling of the Forward and Backward keys.

Examples

Local>> DEFINE DEDICATED TELNET 192.0.1.221:+P

A.2.1.6 R

Specifies that the connection use the Rlogin protocol. Sets the port number to 513 if not already set.

Examples

Local>> DEFINE PORTS DEDICATED TELNET 192.0.1.8:R

A.2.1.7 S

Specifies that the connection use the SSH protocol.

Examples

Local>> DEFINE PORTS DEDICATED TELNET 192.73.220.248:S

A.2.1.8 T

Forms a raw Telnet connection. If no environment string is specified, a Telnet connection is assumed.

Examples

Local> DEFINE PORTS DEDICATED TCP chimaera:2001T

B: Show 802.11 Errors

B.1 Introduction

Note: *This appendix applies only to the SCS200.*

When you enter the **Show 80211** command without any other parameters, the resulting screen includes a field for errors. The "**Errors:**" field displays two eight-digit numbers, separated by a comma. These numbers are a 64-bit wide bitfield of error bits, each one indicating whether or not the given error has occurred at least once.

For example, suppose you're using an SCS200 with a ZoomAir card in Infrastructure mode. After having been running for a long time, your Access Point loses power in the middle of sending a fragmented packet to the SCS. If you entered the **Show 80211** command, you might see a screen resembling the following:

Figure B-1: Example of Error Bits

```
Local>> SHOW 80211
 802.11 Support:         Active
   Network Type:          Infrastructure
   Use MAC address from:    SCS (00-80-a3-30-ee-31)
   ESS ID:                (none set)
   Regulatory Region:      FCC/USA
   DS Channel:            Any
   RTS Threshold:          3000
   Fragmentation Threshold: 2346
   Card Present:          Zoom Air 4000

   Status:                Scanning
   Errors:                08020002,00000920

   Card Firmware Revision:  2.01
```

The Errors bitfield is zeroed each time you issue either a **Zero** command or a **Set 802.11 Reset** command at the Local> prompt.

The Errors bitfield is zeroed each time you issue either a **Zero** command or a **Change 802.11 Reset** command at the Local> prompt.

B.2 Error Bits

B.2.1 Leftmost Number

80000000	An authentication or association sequence timed out. An expected reply from the AP was not received within the required time window.
40000000	Internal error.
20000000	Internal error.

10000000	Internal error.
08000000	Fragment reassembly timed out. Failed to receive all the fragments of a fragmented 802.11 packet before the reassembly window expired. Dropped some correctly received fragments.
04000000	Received an 802.11 packet with invalid subtype code.
02000000	Received an 802.11 packet with invalid type code.
01000000	Received an 802.11 packet with invalid version code.
00800000	Dropped a correctly received 802.11 packet due to lack of a sufficiently sized buffer to hold it. May happen under heavy network load if applications are not processing network data fast enough.
00400000	Internal error.
00200000	Internal error.
00100000	Failed to transmit an 802.11 management packet.
00080000	Failed to transmit an 802.11 data packet.
00040000	Internal error.
00020000	Lost contact with the AP. Unit will attempt to reestablish contact by itself.
00010000	Unit was deauthenticated or disassociated by the AP for attempting to pass data packets before being fully associated. (Indicates confusion of either the unit or the AP.)
00008000	Unit was disassociated by the AP for inactivity.
00004000	Unit was deauthenticated or disassociated by the AP because the AP is going offline or being reconfigured to serve a different network.
00002000	Unit was deauthenticated by the AP because its previous authentication is no longer valid.
00001000	Authentication or association with the AP failed, or the unit was deauthenticated or disassociated by the AP for an unknown reason.
00000800	Association with the AP failed because the unit does not support all of the data rates marked as basic in the AP.
00000400	Association with the AP failed, or the unit was disassociated by the AP because the AP is full, and cannot handle any more stations associating with it.
00000200	Authentication with the AP timed out. The AP did not receive an expected reply from the unit within the required time window.

00000100	Authentication with the AP failed because the WEP key the unit is using is not the same as the key the AP is using.
00000080	Authentication with the AP failed because either the unit or the AP sent an incorrect authentication packet. Some APs will erroneously return this error code when the problem is actually "authentication type not allowed".
00000040	Authentication with the AP failed because the AP does not allow the authentication type requested by the unit.
00000020	Authentication or association with the AP failed for administrative reasons.
00000010	Reassociation with another AP serving the same ESS as the previous one failed because the association could not be confirmed by the previous AP.
00000008	Association with the AP failed because the AP does not support all 802.11 options requested by the unit.
00000004	Authentication or association with the AP failed, or the unit was deauthenticated or disassociated by the AP for a reason explicitly given as "unspecified".
00000002	Could not find any beacons matching the network parameters the unit is configured with. Most likely there is no AP or ad-hoc network within range that satisfies the unit's ESSID, NETWORK-TYPE, and CHANNEL parameters.
00000001	Internal error.

B.2.2 Rightmost Number

80000000	Unassigned.
40000000	Unassigned.
20000000	Unassigned.
10000000	Unassigned.
08000000	Unassigned.
04000000	Unassigned.
02000000	Unassigned.
01000000	Unassigned.
00800000	Unassigned.
00400000	Unassigned.
00200000	Unassigned.

00100000	Unassigned.
00080000	Unassigned.
00040000	Unassigned.
00020000	Internal error. May occur on some cards in conjunction with other described error codes.
00010000	The 802.11 card in use is not compatible with the regulatory region to which the unit has been programmed.
00008000	Internal error.
00004000	Internal error. May occur on some cards in conjunction with authentication or association failures, or other configuration mismatches.
00002000	Received an 802.11 packet that was too large to be handled.
00001000	Internal error.
00000800	Failed to queue a data packet that could not be sent immediately for later transmission. It was dropped.
00000400	Internal error.
00000200	Failed to find, sync to, and associate with an AP or ad-hoc network within a reasonable time. Most likely there is no AP or ad-hoc network within range that satisfies the unit's ESSID, NETWORK-TYPE, and CHANNEL parameters.
00000100	Received an 802.11 data packet that was not encapsulated as per RFC1042 or 802.1h. Unit will still decapsulate and interpret the packet. Some vendors' APs trip this error when they send out "magic packets" containing proprietary extensions not defined by the 802.11 spec.
00000080	Received an 802.11 data packet encapsulated in a completely foreign manner, or not encapsulated at all. Unit will still attempt to interpret the packet, but proper interpretation is not guaranteed. The packet may be dropped as unintelligible.
00000040	Received an encrypted packet that could not properly be decrypted. Packet was dropped.
00000020	Unspecified error during packet reception. At least one packet was dropped. Absence of this error bit does not imply that all packets have been received correctly, however.
00000010	A received packet failed CRC check and was dropped.
00000008	Internal error. May occur in conjunction with "no AP or ad-hoc network within range" errors.
00000004	Internal error.

00000002	Internal error.
00000001	Internal error.

C: SNMP Support

SNMP is an abbreviation for Simple Network Management Protocol. SNMP commands enable users (usually system administrators) to get information from and control other nodes on a local area network.

Information about SNMP can be obtained in RFCs (Request For Comments) which can be obtained via anonymous FTP from nisc.jvnc.net. To obtain a specific RFC, use the pathname pub/RFC/ rfcnnn, where nnn is the name of the desired RFC. To obtain the RFC index, use the pathname pub/RFC/rfc-index.txt.

The extent to which other nodes may be controlled and/or queried for information is documented in Management Information Bases (MIBs). The MIBs and SNMP in general are documented in RFCs 1066, 1067, 1098,1317, 1318, and 1213.

Table C-1: Supported MIBs

MIB	Description
MIB-II (RFC 1213):	System, Interface, Address Translation, IP, ICMP, TCP, and UDP. They do not support the EGP group.
RS-232 MIB (RFC 1317):	All objects (RS-232-style objects).
Character MIB (RFC 1318):	All objects (character-oriented devices).

C.1 Support

- The SCS will respond to queries for unknown MIBs with a “not in MIB” error to the requesting host.
- The SCS has a local SNMP security table to restrict or prevent unauthorized SNMP configuration.
- The SCS will also generate limited forms of 3 of the SNMP traps. Traps are sent to a host when an abnormal event occurs on the SCS.

Currently, the SCS will generate a Coldstart trap when it first boots, and will send a Linkup trap when the startupfile (if any) has been read from a host and normal operation commences. If a startupfile has been configured but the download fails, the SCS will send an Authentication trap. In all 3 cases, the trap will be directed to the IP address of the loadhost for the SCS. If a loadhost has not been specified (Flash ROM based units, for example), the traps will not be sent. The SCS will not generate traps other than the cases listed here.

C.2 Security

Because SNMP can be used to change security settings, the SCS provides a security mechanism for restricting SNMP access to the unit. The security mechanism is linked to the SNMP community name. By default, the only allowed community name is Public, which is given only Read privilege.

To change, add, or delete community names in the table, **Set/Define SNMP** and **Clear/Purge SNMP** are used. Set SNMP requires specification of a community name and an access type. Available access types are Readonly, Both (allows read and write), or None. Clear SNMP requires either a community name to remove a single entry or the **All** parameter to clear the entire table. **Show/Monitor/List SNMP** commands require privileged access to prevent unauthorized users from seeing the allowed community names.

The SCS sends an error message when it receives SNMP queries or Set requests that are not permitted for the current user.

D: Supported RADIUS Attributes

This appendix lists and explains the RADIUS attributes currently supported by the SCS. The SCS transmits these attributes whenever they are appropriate for the given connection.

Users cannot directly specify which attributes the SCS will transmit—this is negotiated for each connection based on the connection type and requirements. For example, CHAP-Challenge packets are only needed for PPP connections that authenticate via CHAP.

D.1 Authentication Attributes

D.1.1 Access-Request

For Access-Request packets, the SCS can transmit the following attributes.

User-Name

User-Password

CHAP-Password Either a User-Password or CHAP-Password will be sent.

CHAP-Challenge

NAS-Identifier The NAS-Identifier is the SCS's name string configured with the **Set/Define Server Name** command.

NAS-Port

NAS-Port-Type

Service-Type The Service-Type will be either **Login** or **Framed** (PPP/SLIP).

Framed-Protocol When the Service-Type is **Framed** or **Callback-Framed**, this value denotes which of the framed protocols (PPP or SLIP) is being used for the connection.

Calling-Station-ID When Caller-ID is enabled on the port and a phone number is found in the modem's response string, the SCS will report this value.

Note: *For more information about Caller-ID, see the Caller-ID section on page 9-12.*

D.1.2 Access-Accept

The SCS interprets reply attributes based on the Service-Type received in the Access-Accept. Supported service types include:

Login The user is connected to a specific host.

Framed A PPP or SLIP connection is started.

Callback-Login The user is disconnected and called back, then connected to a host.

Callback-Framed The user is disconnected and called back, then begins a PPP/SLIP connection.

Prompt The user is provided with a command line prompt on the SCS from which it is possible to enter privileged commands.

Note: *See RADIUS on page 11-14 for the differences between the login and prompt service types and how they are handled by the SCS.*

The table below shows the additional attributes that can be used in Access-Accept packets sent by the RADIUS server. Items marked with plus signs (+) are only valid when the Service-Type is Login or Callback-Login. Items marked with asterisks (*) are only valid when the Service-Type is Framed or Callback-Framed.

Table D-1: Access-Accept Attributes

Attribute	Supported Values (if any)
Framed-Protocol*	PPP SLIP
Framed-IP-Address*	See *Framed-IP-Address* on page D-3
Framed-Routing*	Send Listen Send & Listen None
Filter-ID*	See *Filter-ID*, page -3
Framed-MTU*	
Framed-Compression*	None Van-Jacobson TCP/IP Header Compression
Login-IP-Host+	See *Login-IP-Host* on page D-3
Login-Service+	Telnet Rlogin TCP-Clear (raw TCP connection)
Login-TCP-Port+	
Reply-Message	
Session-Timeout	
Idle-Timeout	

D.1.2.1 Framed-IP-Address

Using this attribute is equivalent to setting the remote address range of a site to “undefined.” Two values are available:

- 255.255.255.255 (0xFFFFFFFF) allows the user to choose and IP address
- 255.255.255.254 (0xFFFFFFFE) assigns the user an address from the SCS IP address pool

If an IP address pool is defined for the SCS and the incoming user asks for an address, one will be assigned from the pool. If the user asks for a specific address, the user will be given the address, provided it is available. In the absence of an address pool, the user will be given any address that he requests.

D.1.2.2 Filter-ID

The SCS renames filters by appending suffixes based on the filter type. For example, a filter named “dallas” configured on the SCS will be renamed “dallas.in” (for an incoming filter), “dallas.out” (for an outgoing filter), “dallas.idl” (for an idle timeout filter), and “dallas.st” (for a startup filter).

Note: *The maximum filter name length is 12 characters, but should be limited to 8 characters to account for the added suffix.*

To understand how the Filter-ID attribute works, imagine that user **irvine** is trying to make a PPP connection using RADIUS authentication. When the connection is initiated, the SCS starts a copy of the default site.

During the authentication phase, RADIUS looks in NVR for a site that has the same name as the user. If RADIUS finds a match, this site becomes the **base site**. If the SCS does not find a match, RADIUS will use a copy of the default site as the base site. RADIUS uses the attributes passed from the RADIUS server during authentication to modify the base site.

If the Filter-ID attribute is present and has the value “irvine,” RADIUS examines NVR for a filter named **irvine.in**. If it finds the filter, it uses that filter as the incoming filter for the site. If it doesn’t find the filter, the incoming filter from the base site, if any, is used. If no incoming filter is defined for the base site, no incoming filter is used. RADIUS then repeats the process for the other three filter types (outgoing, idle, and startup). As long as RADIUS finds at least one filter matching the Filter-ID value, the connection will succeed.

However, if the Filter-ID attribute is present and no filters are found matching the Filter-ID value, the connection is refused. This prevents a potential security hole created when a user is allowed to connect without the intended restrictions being enforced.

Note: *Because startup filters only apply to outgoing sites, which RADIUS doesn’t handle, there is no need to define a startup filter for a RADIUS user.*

D.1.2.3 Login-IP-Host

If the Service-Type is Login or Callback-Login and the Login-Ip-Host value is not set or is set to 0.0.0.0, the preferred Telnet host will be used. If the Service-Type is Login or Callback-Login and this value is set to 255.255.255.255, the user will be prompted to enter the name of the host to use for the connection, including normal SCS environment strings. If present, the Login-TCP-Port value will override the user-entered environment.

If Login-Service is Rlogin and the Login-IP-Host value is not set, the SCS makes an Rlogin connection to the preferred Telnet host.

D.2 Accounting Attributes

For all Accounting packets, the SCS transmits Acct-Status-Type (On, Off, Start, or Stop) and the SCS's NAS-Identifier. For individual Accounting-Start and Accounting-Stop packets, the SCS can also transmit the attributes listed in Table C-2.

Note: *Items marked with* ***** *are only sent when the Service-Type value is Framed or Callback-Framed.*

Table D-2: Accounting Packet Attributes

Accounting-Start	Accounting-Stop
Acct-Session-ID	Acct-Session-ID
Acct-Delay-Time	Acct-Delay-Time
User-Name	User-Name
NAS-Identifier	NAS-Identifier
NAS-Port	NAS-Port
NAS-Port-Type	Class
Calling-Station-ID	Acct-Input-Octets
Class	Acct-Output-Octets
Service-Type	Acct-Input-Packets*
Framed-Protocol*	Acct-Output-Packets*
Framed-IP-Address*	Acct-Session-Time
Framed-Routing*	Acct-Terminate-Cause (if known)
Filter-ID*	
Framed-MTU*	
Framed-Compression*	
Idle-Timeout	
Session-Timeout	

D.3 Examples

The following examples can be used as templates for the public domain Merit RADIUS server available via anonymous FTP at **ftp.merit.edu**. The examples will also work with the public domain Livingston RADIUS server available via anonymous FTP at **ftp.livingston.com**.

If you are using a different server, please note that the file format for the Merit and Livingston RADIUS servers are of following form:

```
username        check-item1, check-item2, ..., check-itemN
                reply-item1,
                reply-item2,
                ...,
                reply-itemN
```

Check-items are attribute/value pairs that must be received from the authentication client (for example, the SCS) for authentication to occur. Reply-items are attribute/value pairs that will be returned to the client upon authentication. Note that the Merit and Livingston Password attribute may be used to match either User-Password or CHAP-Password.

Note: *Please read your RADIUS server's documentation for more information about how to configure your RADIUS server.*

D.3.1 Configuring Authenticated PPP Connections

The following entry allows user **april** to gain access to a LAN via PPP using the IP address 192.0.1.58:

```
april           Password = "fools"
                Service-Type = Framed,
                Framed-Protocol = PPP,
                Framed-IP-Address = 192.0.1.58
```

This user may be authenticated via PPP PAP, PPP CHAP, or via the local mode username and password prompts. If authenticated by the latter, the user will automatically be forced to execute the command **Set PPP** *sitename;* **Logout** where *sitename* is the name of the site dynamically created by the SCS for this user.

Note: *All settings in the default site other than the IP address will apply for this user.*

Here is a more complicated example for a dialback PPP user who is not allowed to perform a local mode login:

```
april           Password = "fools", Service-Type = Framed, Framed-Protocol = PPP
                Service-Type = Callback-Framed,
                Framed-Protocol = PPP,
                Framed-IP-Address = 192.0.1.233,
                Callback-Number = "555 1234"
```

D.3.2 Forcing a Telnet Connection to Preferred Host

The following example shows a local mode user that is forced to Telnet to the SCS's preferred Telnet host:

```
froggy      Password = “ribbit”
            Service-Type = Login
```

The **Telnet; Logout** command is forced as soon as authentication is complete. To force the user to make an Rlogin to connect to the preferred Telnet host, add “Login-IP-Service = Rlogin” to the reply-item list.

D.3.3 Forcing a Telnet Connection to a Specific Port

To force the user to Telnet to a particular port on the specified host, add the Login-IP-Port attribute:

```
froggy      Password = “ribbit”
            Service-Type = Login,
            Login-IP-Host = 192.0.1.155,
            Login-IP-Service = Telnet,
            Login-IP-Port = 1000
```

The **Connect Telnet 192.0.1.155:1000** command is forced as soon as authentication is complete. Remember that if a user connects via PPP and is authenticated by the RADIUS server with Service-Type set to Login or Prompt, the SCS RADIUS client code will reject the user because a user cannot be made to fall out of PPP mode into local (character) mode.

D.3.4 Preventing RADIUS Authentication

You may wish to prevent the user from being authenticated by the RADIUS server in the first place. If so, enter the following:

```
froggy      Password = “ribbit”
            Service-Type = Login,
            Login-IP-Host = 192.0.1.88,
            Login-IP-Service = Telnet,
            Login-IP-Port = 1000
```

In this case, if the SCS sends an authentication request for the user froggy with the Service-Type set to Framed, the authentication request will be rejected by the RADIUS server.

Index

Numerics

A

B

S

U

V

W

X

Z