Sentry Switch Operations

Operations Manual

First Edition, February 2000.

Table of Contents

Introduction and Initial Connection

The Server Technology Inc. Sentry Switch product provides easy, practical, and secure serial connections to a number of connected serial devices. This manual describes the software operation of the Sentry Switch product.

Starting a Session

Once you have installed your Sentry Switch product, it is necessary to establish a connection to the Sentry Switch controller so that you can connect to one of the attached serial devices. You may use any terminal or terminal emulation program you chose to connect to the Sentry Switch.

Sending a carriage return to the Sentry Switch product starts a session.

For Modem access, the user first uses any communication software that supports ANSI or VT100 terminal emulation to dial the phone number of the external modem attached to the Sentry Switch. When the modems connect, the user should see a “CONNECT” message. The user then presses the Enter key to send a carriage return.

Note: When setting up the Sentry Switch product for the first time, the first modem call made to the Sentry Switch product should be made with the dialing modem set to 9600 bits per second (BPS), which is the factory default modem data rate for the Sentry. This should guarantee that the first connection will succeed, after which the Sentry’s modem initialization data rate can be increased with the “SET MODEM RATE” command and the dialing modem’s data rate can be increased in the communication software

For direct RS-232C access, the user starts any serial communication software that supports ANSI or VT100 terminal emulation. The program must configure the serial port to one of the supported data rates (38400, 19200, 9600, 4800, 2400, 1200, and 300 BPS), along with no parity, 8 data bits, and one stop bit, and must assert its Device Ready signal (DTR or DSR). The user then presses the Enter key to send a carriage return.

For Ethernet Network Connections, the user connects to the Sentry Switch product by using a TELNET program and connecting to the TCP/IP address configured for the ServerTech MSS1 installed in the Sentry. Please refer to the Network Access Device Configuration section of this manual for information on configuring the MSS1.

The Sentry Switch product will automatically detect the data rate of the carriage return and send a username login prompt back to the user, starting a session.

Logging In

After the carriage return, the user will receive a banner that consists of the word “Sentry Switch Version” followed by the current Sentry Switch product version string and a blank line and then a “Username:” prompt. (Note the X.Xx in the following illustration is replaced by the current Sentry Switch product version.

```
Sentry Switch Version X.Xx

Username: _
```

The Sentry Switch product Banner will only be displayed after the initial connection or after the LOGIN command. In response to the “Username:” prompt, the user enters a valid username string. The username is a character string up to 16 characters long followed by a carriage return. Usernames may not contain either spaces or the colon ‘:’ character. Usernames are not case sensitive. The user has up to 60 seconds to enter a username string. If data is not entered with in the time limit, the session is ended with the following message: "Sorry your time is up. Try again later!"

After the user responds to the “Username:” prompt, the user will be prompted for an associated password with the “Password:” prompt.

```
Password: _
```

The Sentry Switch product will not echo characters typed in response to the password prompt. Passwords are up to 16 characters and are case sensitive. Alphanumeric and other typeable characters (ASCII 32 to 126 decimal) may be used. The Sentry Switch product will validate the username/password strings against the internal table of usernames/passwords that has been previously defined. If the user enters an invalid username string or password, the Sentry Switch product will send an error message as follows: “Sorry, the Username/Password you have entered is NOT valid!”. The user will then receive the “Username:” prompt again. The user will have three chances to enter a correct username/password. If a valid username/password is not specified on the third attempt, the following message will be sent: “Check your Username/Password and try again later!”. The current user session will then be ended. As with the username, the user has up to 60 seconds to enter a password string. If data is not entered with in the time limit, the session is ended with the following message: “Sorry your time is up. Try again later!”.

The Sentry Switch product allows up to 128 usernames to be defined. The system has three built username/password pairs.

The Sentry Switch product supports a two-level username/password scheme. There is one system-administrative level username (ADMN), and up to 128 general-user level usernames.

A user logged in with the administrative username (ADMN) can make configuration changes as well as make connections to attached serial devices. A user logged in with a general username can only make connections to attached serial devices.

Default Usernames

There are three built in usernames and passwords. The built in username and passwords are:

Username: admn	Password: admn
Username: gen1	Password: gen1
Username: gen2	Password: gen2

These usernames cannot be deleted. The “admn” username is the administrative username. When logging in for the first time, the system administrator should use the default administrative username. This will allow the system administrator to configure all the options, as well as to change the default passwords. Changing the passwords is done using the “SET PASSWORD” command from the command prompt. The command as well as the other administrative commands are described in the next section.

Command Prompt

The command prompt interface is used for both making connections and configuration of some options, including adding/deleting usernames, changing passwords and changing the modem initialization data rate.

All configuration changes made at the command prompt are saved to non-volatile RAM and are effective immediately.

Once a valid username and password has been entered, the Sentry Switch product displays a command prompt:

```
Switch: _
```

To get a display of available commands, press enter at the Sentry prompt, which will show:

```
Sentry commands are:

  CONNECT LOGIN QUIT SET ADD DEL LIST SHOW VERS
```

Note: The SET, ADD, DEL, and LIST commands will only be available when logged in with the administrative-level password.

Command Syntax Rules

`CAPS` Keywords that are entered exactly as shown appear in all uppercase letters. Upper or lowercase can be used when the command is entered.

`Words` Parameters that are replaced with data appear in words that are a combination of uppercase and lowercase letters. The word indicates the type of parameter required. Upper or lowercase can be used when the command is entered.

`{ }` Required parameters appear within curly brackets. Do not include the brackets when the command is entered.

`[ ]` Optional parameters appear within square brackets. Do not include the brackets when the command is entered.

`|` A broken vertical bar indicates the OR function. Enter only one of the options or parameters shown. Do not include the broken vertical bar when the command is entered.

* An asterisk indicates that an entry may be repeated as many times as needed. The entry that may be repeated appears within the preceding curly or square brackets. Do not include the asterisk when the command is entered.

General Commands

CONNECT {1-16|Serial Port Name|IPM Name|CONSOLE|MODEM|LINK|NETWORK}

This command attempts to make a connection to a serial device attached to 1 of 16 possible serial ports that are connected to the Sentry Switch product. If the CONNECT command is entered with a single parameter which is a number from 1 to 16, the connection is attempted to one of the ports attached to the Sentry Switch product.

To ease the use of the CONNECT command, an administrator can configure any of the possible serial ports that are available with names. The CONNECT command can then be used with the assigned name (i.e. the Serial Port Name parameter) to connect to the port associated with the Serial Port Name.

If the CONNECT command is entered with no parameters, a list of possible names is displayed on the screen. The user can then use the CONNECT command with one of the names displayed to attempt a serial port connection. The administrator can use the ADD, DEL , and LIST commands to set up the Serial Port Name configuration. These commands are described later in this manual.

For all CONNECT commands, the Sentry Switch product defaults to requiring that the attached device assert both Data Set Ready (DSR) and Clear To Send (CTS), in order to successfully connect. These requirements can be individually enabled and disabled with the “SET CONNECT” command. When a connection is successful, the message “Connection complete” will be displayed, at which point communication to the attached device will be transparent through the Sentry.

When finished communicating to the serial device, type “!*login<CR>”. The keyword “login” is not case sensitive. This disconnection character sequence returns the user to the login username prompt at which point the user may login normally to the Sentry.

A disconnection will also automatically occur when CD or DSR go inactive (as caused by hanging up a modem or exiting a communications program) or when a Telnet session is disconnected.

LOGIN

Brings up the “Username::” prompt to allow a user to re-login under a different username. No parameters.

VERS

Displays the firmware version of the first Sentry Switch product Commander in the chain. No parameters.

QUIT

Ends the session. No parameters.

SET Commands

Note: Set commands are only available when logged in with the administrative username (i.e. admn).

To get a display of available SET commands, just enter “SET” at the Switch prompt, which will show:

```
SET commands are:

  CONNECT LOCATION MODEM PASSWORD
```

SET CONNECT {SWITCH|CONSOLE|MODEM|NETWORK}
{DSRCHECK|NODSRCHECK|CTSCHECK|NOCTSCHECK}

Turns on or off active signal checking when connecting to a pass-through port when using the CONNECT command. There are two required parameters with the command. The first is one of four possible serial port names.

DSRCHECK requires that DSR be active from the attached device to connect. NODSRCHECK ignores that state of DSR. CTSCHECK requires that CTS be active from the attached device to connect. NOCTSCHECK ignores that state of CTS. The defaults are DSRCHECK and CTSCHECK.

SET LOCATION {Location}

Sets the location value that is displayed as part of a “Welcome to...” message when a session is started. Up to 16 characters, including spaces, can be entered. Extra characters will be truncated from the location field.

SET MODEM {RATE {NONE|300|1200|2400|4800|9600|19200|38400}}
SET MODEM {{INIT1|INIT2|INIT2|ATTENTION|HANGUP} {DEFAULT|NONE}}

SET MODEM RATE sets the initialization data rate for the modem attached to the Sentry. The data rate can be set to any of the listed speeds (300, 1200, 2400, 4800, 9600, 19200, or 38400 Bits Per Second). The NONE parameter is used to disable all modem initialization string support. The default is 9600 BPS. The initialization takes place at the user selectable data rate, with no parity, 8 data bits, and one stop bit.

SET MODEM INIT1, INIT2, INIT3, ATTENTION, or HANGUP allows an individual modem initialization string to be enabled (DEFAULT) or disabled (NONE). All default to enabled (DEFAULT).

The Sentry Switch product initializes the modem when the Sentry Switch product is first turned on, whenever the modem is turned on or connected and after every user session (via modem) with the Sentry. During initialization, the Sentry Switch product sends each of the five-fixed modem initialization strings that is enabled to the modem in the following order:

Attention String:	**@@@**
Hang-up String:	**ATH**<CR>
Initialization String 1:	**AT**<CR>
Initialization String 2:	**AT E0 Q1 S0=3 S2=64 S12=50 &C1 &D2**<CR>
Initialization String 2:	**AT S0=1**<CR>

The Attention String is sent to break from online mode to command mode if a modem is connected. The attention string can be set on most modems to match the @@@ string used by the Sentry.

The Hang-up String is sent to cause the modem to hang up if there is an active connection.

Initialization String 1 is sent to alter the modem and to allow the modem time to prepare for the next command.

Initialization String 2 is sent to initialize the modem to defaults required by the Sentry. The “E0” turns off the echoing of data, the “Q1” turns off result codes and the "S0=3" sets the modem to answer on the 3rd ring.

Initialization String 3 is sent to set the modem to answer on the 1st ring.

The modem initialization features allow a choice for the modem to answer on either ring number 1 or ring number 3. The Initialization String 3 is “AT S0=1<CR>”. Like the other initialization strings, Initialization String 3 defaults to being enabled, and is sent in sequence after Initialization String 2. When this happens the modem answers on ring number 1. To have the modem instead answer on ring number 3, disable Initialization String 3 with the command “SET MODEM INIT3 NONE”.

For most modems, Initialization String 1 or 2 being sent by the Sentry Switch product to the modem at one of the supported data rates is all that is needed for the modem to work with the Sentry. This is because most modems will communicate to the attached serial device (in this case, the Sentry) at the data rate of the last AT command that was sent to it. A modem that operates in this manner is operating in *fixed data rate mode*. Since the Sentry Switch product sends the last AT command at one of its supported data rates, the modem will talk back to the Sentry Switch product at that same data rate when it is on-line with another modem.

Some high-speed modems, however, can be configured to operate in *variable data rate mode*. With a modem set to operate in *variable data rate mode*, when the modems connect, the modem may change from the speed of the last AT command to a different data rate, automatically adjusting to a data rate that is best for the actual modem-to-modem connect speed. If the data rate changes to one of the supported data rates, then the Sentry Switch product will be able to communicate. But, if the data rate changes to a non-supported data rate, such as 14400, 28800, or faster than 38400 BPS, the Sentry Switch product will not be able to communicate. Thus, it is best that the modem be configured to operate in *fixed data rate mode*, NOT *variable data rate mode*.

Configuring the modem to operate in *fixed data rate mode* is not addressed by the modem initialization built into the Sentry Switch product because the command that sets the modem to use *fixed data rate mode* varies significantly with different modem manufacturers.

If the modems are able to connect with each other, but there is not communication with the Sentry Switch product, the modem attached to the Sentry Switch product is probably in *variable data rate mode* and has switched to an unsupported speed. In this case, in the modem’s manual, lookup the appropriate AT command(s) for the modem to operate in *fixed data rate mode*. Then attach the modem to a PC with a terminal program, send the command(s) to the modem, followed by an &W to write the new setting to the modem’s memory and make it the default, and then re-attach the modem to the Sentry.

SET PASSWORD [username]

SET PASSWORD command is used to change the password of any username. The user may specify the username for which the password is to be changed as a parameter to the SET PASSWORD command or he may enter the SET PASSWORD command with no parameters. If a user enters the SET PASSWORD command without specifying a username, the system will prompt the user for a username with the following prompt: “Username:”. If a valid username is not specified either as a parameter on the SET PASSWORD command or in response to the “Username:” prompt, the following message is displayed: “Sorry, the username you have entered is NOT valid!”, and the SET PASSWORD command is terminated. If the user enters a valid username he is prompted for the new password and also for a verification of the new password. The user must specify the current password in order to change the password for the administrator username (i.e. admn). For all other usernames the password is changed without having to first specify the existing password. The password can not contain more than 16 characters or the command is aborted with the following message: “Sorry, the password you have entered is NOT valid!”. The following message is displayed when the password is changed: “Password successfully changed”.

The Sentry Switch product will echo the ‘*’ character for all characters entered by the user for passwords when using the SET PASSWORD command. This includes the new password, the verification of the new password and the verification of the existing password in the case of changing the ADMN password.

Username/Password and Serial Port Name Administration Commands

Note: The username/password and Serial Port Name administration commands are only available when logged in with the administrative username (i.e. admn). These commands are used to add/delete users and to view the current usernames. They are also used to assign names to the various serial ports that can be accessed via the CONNECT command.

ADD {USER|SNAME} [Username|Serial Port ID] [Serial Port Name]

The ADD command is used to add usernames to the system, and to add Serial Port Names. The ADD command takes one required parameter and up to two optional parameters.

The first parameter is required and indicates whether a username is to be added (ADD USER), or whether a Serial Port Name is to be added (ADD SNAME).

The ADD USER command is used to add a new username to the system. The command can be entered with a single parameter (which is the new username) or with no parameters. If a parameter is not specified, the user is prompted for the username with the following prompt: “Username:”. A non-blank username that contains no more than 16 characters, and does not contain the colon ‘:’ character, must be entered at this prompt or the command is aborted with the following message: “Sorry, the username you have entered is NOT valid!”. The username is not case sensitive.

Once the username is specified, the user is prompted for a password via the “Password:” message. The user is prompted for a verification of the newly entered password after entering the password. The verification password must match the first password entered or the command is aborted with the following message: “Sorry, the password you have entered is NOT valid!”. The ‘*’ character is echoed in response to the characters typed for the password and the password verification strings. The password value entered at this prompt and successfully verified is stored as the password for this username and is used to validate this username during normal Sentry Switch product logon processing. The password can not contain more than 16 characters or the command is aborted with the following message: “Sorry, the password you have entered is NOT valid!”. The password is case sensitive.

Once the information has been entered, the user receives the following message: “Username successfully added”. Note that only a value in the Username is required in this command. Blank or empty responses to the password prompt and the password verification prompt are accepted as valid.

The ADD SNAME command is used to add a new name to a serial device connected to a Sentry Switch product. The command can be entered with no parameters, with a single parameter (which is the serial port ID –identifies which port is to be named) or with two parameters (which are the serial port ID followed by the serial port name). If a parameter is not specified, the user is prompted first for the serial port ID with the “Serial Port ID:” message followed by a prompt for the serial port name with the following prompt: “Name:”. If the user does not specify a valid serial port name in response to the “Name:” prompt, the command aborts with the following message: “The serial port name you have entered is NOT valid!”. Valid serial port names are from 1 to 16 characters with blanks not allowed.

In response to the “Serial Port ID:” prompt, the user may enter either a number from 1 to 16 (to specify one of the 16 possible ports connected to the Sentry Switch product). The parameter is verified to ensure the serial port exists and that the serial port is not already named. If the specified serial port is already named, it must first be deleted using the DEL command and then added.

DEL {USER|SNAME} [Username|Serial Port NAME]

The DEL command is used to delete usernames from the system, and to delete Serial Port Names. The DEL command takes one required parameter and one optional parameter.

The first parameter is required and indicates whether a username is to be deleted (DEL USER), or whether a Serial Port Name is to be deleted (DEL SNAME).

The DEL USER command is used to remove a username from the system. The command can be entered with a single parameter (which is the username to remove) or with no parameters. If a parameter is not specified, the user is prompted for the username with the following prompt: “Username:”. A valid system username must be entered at this prompt or the command is aborted with the following message: “Sorry, the username you have entered is NOT valid!”. This command cannot be used to remove any of the three default usernames (i.e. admn, gen1, or gen2).

When the DEL USER command completes successfully, the user receives the following message: “Username successfully deleted”.

The DEL SNAME command is used to remove a serial port name. The command can be entered with no parameters, or with a single parameter (which is the serial port name). If a parameter is not specified, the user is prompted first for the serial port name with the “Name:” message. If the user does not specify a valid serial port name in response to the “Name:” prompt, the command aborts with the following message: “The serial port name you have entered is NOT valid!”.

LIST {USERS|SNAME}

The LIST command is used to list the current usernames active in the Sentry system, and to list the currently defined Serial Port Names.

The LIST USERS command is used to display a list of all the valid users on the system. If the username list fills the screen, the user is prompted to press N for additional names or Q to end the list. The following is an example of the LIST USERS display:

```
        admn    gen1     gen2     sentry1

Press: N)ext, Q)uit
```

When all users have been listed, the following message is displayed: “Username List Complete”.

The LIST SNAM command is used to display the current serial port names and the port associated with the serial port name. The command takes no parameters. The output of the LIST SNAM command is a display of the current serial port names. Each serial port name is followed by the associated serial port device for the name. The names are displayed in groups of 20 ports. After each group of 20 ports is displayed the user is prompted to press N for additional names or Q to end the list. The following is an example of the screen with 20 serial port names displayed (only 3 are listed here for illustration).

```
 TERMINALPORT           5
 NTSYSTEM               12
 LINKPORT               15

Press: N)ext, Q)uit
```

Ending a Session

Ending a session can be done from the command prompt prior to making a connection to a serial device by entering the QUIT command and pressing Enter. If a connection has been made, the “!*login<CR>” string can be used, or by ending the terminal program (which drops the DTR signal).

If there is no active connection to a serial device, the session will automatically be terminated after 5 minutes of inactivity. With a modem connection, the modem will automatically be hung-up by the Sentry Switch product lowering DTR to the modem, as well as sending the attention and Hang-up strings to the modem, if they have not been disabled.

A session will also automatically end when CD or DSR go inactive into the Modem port, which occurs when the modem is hung-up or the communication software is exited.

When a session is ended, the user is notified with the message:

```
Session ended
```

There is then a period of about 15 seconds after a session is ended before another session can be started. This is due to the Sentry Switch product reinitializing the modem after a session is ended. If a modem is not used and the modem initialization strings are turned off, the time between sessions is only about 7 seconds.

Resetting to Factory Defaults

The non-volatile RAM that stores all configurable Sentry Switch product options, including the passwords, can be reset to factory defaults. This resets all the command-line configurable options to defaults, including the passwords.

An administrative-level command reset is performed with the command:

```
SET CNFG ALL FACTORY
```

Please note that this command will not reset any of the unit's Network Access Device (NAD) settings; to reset the NAD, you must gain priviledged-user access—as defined in the following pages—and use the NAD's factory reset command, which is:

```
INIT FACTORY
```

Alternatively, to reset **both** the Sentry Switch product options *and* the Network Access Device options, the Reset switch (located next to the unit's Status LED) can be used in the following manner:

1) Power off the unit using the 0|1 rocker-style switch located at the far right of the unit's main panel

2) Depress and *hold* the Reset switch push-button

3) Power on the unit while keeping the Reset button depressed

4) Release the Reset button only after eight seconds have passed

Allow one minute to pass after releasing the Reset button (to allow time for the Sentry Switch and its NAD to reset, resynchronize, and bootup). The entire unit will be reset to factory defaults.

Network Access Device Configuration

The network option of the Sentry products is implemented by an OEM version of the MSS1 Micro Serial Server manufactured by Lantronix. This device is enclosed within the Sentry case and provides the Telnet-to-asynchronous functionality that allows the Sentry to be accessed over a TCP/IP Ethernet network.

NOTE: For purposes of this document, the MSS1 shall be considered part of the Sentry. References will be made to the Sentry as an Ethernet device, when, in actuality, it is the MSS1 inside the Sentry that provides the network functionality. The MSS1 will generally be referred to as the Sentry "network access device".

Network Access Device TCP/IP Configuration

Before the Sentry Switch product can be accessed over a network, the network access device must first be configured with an IP Address, Subnet Mask, and Default Gateway. These instructions explain how to configure the network parameters through either a Modem or Console connection.

Start a session with the Sentry Switch product through either the Modem or Console port (follow the Operations Manual). Start this session with a data rate of 9600.

At the “Sentry:” prompt, issue the command “CONNECT NETWORK”. This should connect the session to the internal network access device’s serial port and display the message “Connection complete”.

Press enter multiple times. A version message from the network access device inside the Sentry Switch product should be displayed, followed by a ‘Login password>’ prompt:

```
ServerTech MSS1 Version STI3.6/1 (991214)
Type HELP at the ‘Local_1>’ prompt for assistance.
Login password>
```

Enter the following default `Login password`:

```
access  <Enter>
```

The password is case sensitive. A “`Local_1>`” prompt should appear:

At the “`Local_1>`” command prompt of the network access device, issue the command:

```
SET PRIVILEGED  <Enter>
```

This will log you in as a privileged user. A “`Password>`” prompt will be displayed, at which point you must enter the following default `privileged` password:

```
system  <Enter>
```

The password *is* case sensitive. When the valid password is entered the command prompt will change to ‘`Local_1>>`’ (two greater than signs), indicating you are in a privileged user mode.

From the privileged command prompt, enter the command:

```
CHANGE IPADDRESS xxx.xxx.xxx.xxx  <Enter>
```

where `xxx.xxx.xxx.xxx` is the IP address that you want to assign to the Sentry. This command stores the IP address in the memory of the Sentry NAD.
Issue the command:

```
SHOW SERVER  <Enter>
```

On the screen displayed, verify the information entered in the above steps is correct. If the ‘`TCP/IP Gateway:`’ entry is ‘`(undefined)`’, or the ‘`Subnet Mask:`’ is incorrect for your network, you should also issue the following commands:

```
CHANGE GATEWAY xxx.xxx.xxx.xxx  <Enter>
```

and/or

```
CHANGE SUBNET MASK xxx.xxx.xxx.xxx  <Enter>
```

where `xxx.xxx.xxx.xxx` is the appropriate IP address(es). 7) Once you have finished network configuration, issue the commands:

```
SHOW SERVER <enter>
SHOW PORT <enter>
```

to verify the information entered in the above commands.

When finished, issue the command:

```
INIT DELAY 0 <enter>
```

to logout and re-initialize the network access device in the Sentry Switch product with the new settings. Wait one minute for the network access device to re-initialize.

Break the connection to the network access device by typing the disconnect sequence “!*LOGIN” followed by Enter.

```
!*LOGIN <enter>
```

Log back into the Sentry Switch product and QUIT. Additionally the connection will break when the modem is hung up, or the cable is disconnected from the Modem or Console port, or power is cycled to the Sentry.

For other methods of configuring the Network Access Device TCP/IP parameters, refer to the Lantronix web site at www.lantronix.com.

Starting a Session through the Network Access Device:

To start a Sentry Switch product session via the TCP/IP network access device, the user must connect a Telnet session to the IP address of the Sentry Switch product using `Port 2001`. This is done with the command:

```
telnet xxx.xxx.xxx.xxx 2001  <Enter>
```

where `xxx.xxx.xxx.xxx` is the IP address that was assigned to the Sentry.

Once the telnet connection is established, the user will be presented with the standard Sentry Switch product Login prompt as described earlier in this manual. If the "Username" prompt is not presented, press the Enter key for one second and then release. This sends a series of carriage returns that will start the Sentry Switch product session. From this point forward, the Sentry Switch product will respond as described earlier in this manual.

Modifying the Network Access Device Telnet Port

It is possible to change the Telnet port used to connect to the Sentry product via the Network Access Device. By default a Telnet connection to the default Telnet port (23) connects users to the Network Access Device console. This allows users to enter commands to configure and view the settings of the Network Access Device. To connect to the Sentry product, users connect to Telnet port 2001 as described earlier. It is possible to change the Telnet port to cause the default Telnet port of 23 to connect to the Sentry product rather than to the Network Access Device console. To change the connection for the default Telnet port (23), you must connect to the Network Access Device console (i.e. Telnet port 23) and use the CHANGE TELNETDEST command. The command is restricted to privileged users (see the previous section for details on logging on and getting into privileged mode). Details of the command follow.

CHANGE TELNETDEST {Console | Serial}

Parameters – specify either Console or Serial where:

Console causes Telnet Port 23 connections to connect to the Network Access Device console.

Serial causes Telnet Port 23 connections to connect directly to the serial port (just as if they connected to Telnet Port 2001).

If the CHANGE TELNETDEST command is used to change the default Telnet connection to the serial port and then you wish to change the default back to the Network Access Device console you must connect to Telnet Port 7000. This connection results in a '#' prompt from the Network Access Device. Respond to this prompt with the default login password (i.e. access) to begin a session with the Network Access Device console. You can then use the CHANGE TELNETDEST command to change the Telnet default port (23) back to the console.

Disabling the Network Access Device Inactivity Timeout

When connecting to a Sentry Switch product and then using a serial pass through port to connect to another device the normal Sentry Switch product inactivity timeout is not enforced. However, the Network Access Device inactivity timeout remains in effect. If users wish to disable or modify the Network Access Device inactivity timeout, there are two Network Access Device console commands available for this purpose. The first is the CHANGE INACTIVE LOGOUT command. This command is used to enable or disable the inactivity timeout. This command requires privileged user status as described previously. The format of the command is as follows.

```
CHANGE INACTIVE LOGOUT {Enabled | Disabled}
```

Use the Disabled parameter to disable the inactive logout timer. Use the Enabled parameter to enable the inactive logout timer.

To change the length of the inactive timer use the CHANGE INACTIVE TIMER command. This command requires privileged user status as described previously. The format of the command is as follows.

```
CHANGE INACTIVE TIMER {XXs | YYYm}
```

The parameter is specified either in seconds (5 to 60) or in minutes (1 to 120). For seconds add an ‘s’ after the number. For minutes add an ‘m’ after the number. The default value is 30 minutes.

Encrypted Telnet Support

Support for encrypted Telnet connections with the Network Access Device is available. Connections can be made from a Win32 PC to the Network Access Device. Win32 connections are established using a Lantronix supplied Telnet application.

For specific details about the encryption algorithms please contact Lantronix product marketing.

For Win32 to Network Access Device encrypted logins Lantronix provides the TCPSCRAM.EXE utility program. This program allows a user on a Win32 platform to form an encrypted connection to a Sentry Network Access Device.

The target Network Access Device must be configured with the encryption password. Use the command:

```
CRYPT PASSWORD "xxxxxxx"
```

Note that the password can be up to 7 alphanumeric characters and is case sensitive. After entering the encryption password, the unit must be rebooted.

To create a connection run the program TCPSCRAM.EXE. In the fields provided specify the IP address of the Network Access Device, the Telnet port to be used for the connection, (i.e.23 for the local console prompt or 2001 for a connection to the Sentry), and the encryption password. Note that the password specified in the application must match the password (case sensitive) configured on the MSS itself.

The TCPSCRAM program will then form a connection to the Sentry Switch product and all data passed between the PC and the Sentry Switch product will be encrypted. The TCPSCRAM.EXE file is available on the Lantronix FTP server in the ./priv/misc_tools/tcpscram directory.

Units that support encrypted connections support a key size of 56 bits.

For more information on the commands described in this section, and/or to view the complete MSS1 manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Network Access Device TACACS Configuration

If TACACS support is required, the following section describes the commands that must be issued on the Network Access Device (i.e. the MSS1 -- all commands require privileged access).

Login to the MSS1 as described in the previous section or by connecting via Telnet to port 23 rather than port 2001. Once connected enter privileged mode as described in the previous section. The current settings can be viewed with the command: SHOW SENTRY.

The Sentry Switch product TACACS support is enabled and disabled in the MSS1 by setting the TACACS IP address and defining the TACACS key. TACACS support is compatible with TACACS Plus servers only. To set the TACACS Plus server IP address issue the following command:

```
SENTRY TACACS SERVER nnn.nnn.nnn.nnn
```

where nnn.nnn.nnn.nnn is the IP Address of the TACACS PLUS server that will authenticate telenet connection to the Sentry.

The Sentry TACACS Plus key string is defined in the MSS with the command:

```
SENTRY TACACS KEY "string"
```

The key string should be enclosed in double quotes to ensure the case is preserved. Since the key does not echo it is important to be sure the key is specified correctly with case being significant. The key must match the key specified on the TACACS PLUS server.

Setting the TACACS KEY to any value activates TACACS PLUS authentication. Clearing the TACACS KEY by entering a null string in double quotes (i.e. “”) disables TACACS PLUS authentication.

PLEASE NOTE: Once you have enabled TACACS PLUS authentication and rebooted the MSS1 you will not be able to telnet to the Sentry Switch product without successfully completing TACACS PLUS authentication. If you enter an invalid key, you will be unable to access the Sentry Switch product without reloading the MSS1. If your TACACS PLUS server is unavailable you will not be able to access the Sentry Switch product via telnet.

When finished, issue the command:

```
SHOW SENTRY <enter>
```

To verify the settings you have entered are correct, then issue the command:

```
INIT DELAY 0 <enter>
```

To logout and re-initialize the network access device in the Sentry Switch product with the new settings. Wait one minute for the network access device to re-initialize.

For more information on the commands described in this section, and/or to view the complete MSS1 manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Network Access Device SecurID Support

SecurID support is available with the Sentry Network Access Device. The MSS1 with SecurID version string is “STI3.5/5+ (981103)”.

SecurID is not enabled by default. It is enabled and configured by several privileged-level MSS1 commands.

Prior to enabling SecurID, the Sentry Switch product unit should be entirely configured and operational. You must also already be familiar with how to log into the MSS1 and how to set privileged-user mode.

These instructions also assume thorough understanding of the ACE/Server configuration items and processes.

There are six configurable SecurID parameters: the primary ACE/Server IP address, the secondary (backup) ACE/Server IP address, the SecurID authentication request timeout, the maximum number of authentication request retries, the encryption method, and the SecurID port (TCP/IP socket number).

The current SecurID parameter settings can be displayed by the MSS1 privileged-level command:

```
SHOW  SENTRY
```

SecurID is enabled if either the primary or secondary ACE/Server IP Addresses is defined. This is done with the MSS1 privileged-level command:

```
SENTRY  SECURID  { PRIMARY | SECONDARY }  { ipaddress | NONE }
```

Where ipaddress is in decimal numerical form.
NONE removes the ipaddress definition.

Note: changing an ACE/Server IP Address clears the MSS1’s Node Secret.

The other MSS1 SecurID commands are:

```
SENTRY  SECURID  TIMEOUT  n
```

Where n is the number of seconds between authentication request retries. Default = 3.

```
SENTRY  SECURID  MAXRETRY  n
```

Where n is the maximum number of authentication request retries. Default = 5.

```
SENTRY  SECURID  ENCRYPTION  { SID | DES }
```

Where SID or DES selects the encryption method. Default = DES. This must match the client configuration on the ACE/Server. Note: new ACE/Server versions renamed the SID encryption to SDI.

```
SENTRY  SECURID  PORT  nnnnn
```

Where nnnnn is the SecurID authentication socket number. Default = 5500. This must match the port configured on the ACE/Server.

```
SENTRY  SECURID  FACTORY
```

Resets all the SecurID configuration parameters to their factory defaults.

In the ACE/Server Database Administration, create and configure an MSS1 client, selecting “Communication Server” as the Client Type. The MSS1 can perform multiple transactions and therefore can display the Next Tokencode and New PIN prompts.

When SecurID is enabled, the standard MSS1 password protection is redundant, and you will probably want to turn it off. You can leave it on if you want, in which case you will first be prompted for the MSS1 login password, and then, after a successful entry, will be prompted for the SecurID username/passcode. To turn off the standard MSS1 password protection, use the privileged-level MSS1 commands:

```
CHANGE  PASSWORD  PROTECT  DISABLED
CHANGE  INCOMING  NOPASSWORD
CHANGE  PASSWORD  INCOMING  DISABLED
```

For more information on the commands described in this section, and/or to view the complete MSS1 manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Network Access Device Security Options

The Sentry network access device supports two passwords -- a Privileged password and a Login password. The Privileged password is used to become the privileged user (administrator), which is required to change settings of the network access device. This password was used in the previous two procedures with the `SET PRIV` command. The network access device defaults to not using the Login password, but can be configured to require the Login password when logging on (before entering a user name) and/or to establish a Telnet session using Port 2001 to begin a power control session with the Sentry.

The default Privileged password is "system", which is changed with the `CHANGE PRIVPASS` command. The default Login password is "access", which is changed with the `CHANGE LOGINPASS` command.

Both passwords can be made up of up to 6 case-sensitive alphanumeric characters. Changing either password requires privileged user status.

To configure the network access device to require the Login password when logging in, use the `CHANGE INCOMING PASSWORD` command. To not require the Login password when logging in, use the `CHANGE INCOMING NOPASSWORD` command.

To configure the network access device to require the Login password when starting a Telnet session to port 2001, use the `CHANGE PASSWORD INCOMING ENABLED` command. To configure the network access device to not require the Login password when starting a Telnet session to port 2001, use the `CHANGE PASSWORD INCOMING DISABLED` command.

The Sentry network access device also supports an IP Security option that you may wish to implement. IP security allows the system administrator to restrict incoming and outgoing TCP/IP sessions and access to the serial port. Connections are allowed or denied based upon the source IP address for incoming connections and the destination IP address for outgoing connections.

IP security information can be added to the IP local host table using the CHANGE IPSECURITY command. Specify an address in standard numeric format. An address with 0 or 255 in any segment restricts all addresses in that range.

To add an entry, specify an IP address and whether to allow or deny connections. The following command disables connections for all addresses between 192.0.1.1 and 192.0.1.254.

CHANGE IPSECURITY 192.0.1.255 DISABLED

The following example disables the address 192.0.220.77.

CHANGE IPSECURITY 192.0.220.77 DISABLED

The CHANGE IPSECURITY command requires privileged user status.

To view the host table entries, enter the SHOW IPSECURITY command. To remove an entry, use the DELETE IPSECURITY command followed by the IP address that you want to remove.

For more information on the commands described in this section, and/or to view the complete MSS1 manual and support files see the Lantronix WWW page at http://www.lantronix.com.

Support and Warranty

Support

Server Technology, Inc. provides free product support between 9:00AM and 5:00 PM Pacific Time, Monday-Thursday, and between 9:00AM and 5:00PM on Fridays, at the following Reno, NV phone number:

(775) 284-2000

Server Technology, Inc. also has an e-mail address for support issues:

support@servertech.com

Warranty

Server Technology, Inc. extends a one-year limited warranty, from the date of purchase.

This warranty covers defects in material and workmanship for the Sentry Switch product Remote Power Manager under normal use and service, and any failure to perform substantially in accordance with this User's Manual.

This warranty does not cover any failure which results from accident, abuse, misapplication or alternation. Incidental and consequential damages are not covered by this warranty and are not the responsibility of Server Technology, Inc.

For warranty issues, contact the Product Support Department at the number listed above. All repair and return shipments must be approved by Server Technology and must be accompanied by an RMA (return merchandise authorization) number and dated proof of purchase.