TUT Systems
SMS2000 User Guide

Printed in the United States of America
SMS2000 Firmware Version: 2.3.6 and OCS software version 2.0.0
June 14, 2003
SMS2000 User's Guide
Text part number: P/N 220-06288-20

SMS™ User's Guide

SMS Software Release 2.3.6

Contents

List of Tables

List of Figures

Preface

This guides in this series provide detailed information and procedures that will allow you to communicate and interface with your SMS2000 and OCS products, complete basic system and network configuration, and manage your systems using system administration tools.

For further information, use the release notes, frequently asked questions (FAQs), product and technology overviews, and troubleshooting tips in the support area of Tut Systems' website **http://www.tutsystems.com**, or you can reach us at 1-800-998-4888.

Audience

The audience includes:

- Network architects who design Internet services
- Network administrators who manage networks
- Network operations center (NOC) operators who handle subscriber calls and manage customer service related calls

Documentation available for this Release

The following documentation is available for the SMS2000 and OCS systems

- *SMS2000 Command Reference*
- *SMS2000 User's Guide*
- *OCS User's Guide*
- *OCS Quick Start Guide*
- *SMS2000 Release Notes*
- *OCS Release Notes*

Related Documentation

The following documentation is available from www.tutsystems.com

- *Expresso GS/MDU Installation and Operation Manual*
- *Expresso MDU Lite Multiplexing Switch*
- *IntelliPOP 5000 Hardware Manual*
- *IntelliPOP 5000 User's Guide*
- *IntelliPOP 5000 Command Reference*
- *IntelliPOP 5000 Tutorials*

Chapter1 - Introduction

Tut Systems' Expresso Subscriber Management System (SMS2000)and Operation Center Software (OCS) offer a complete solution for delivering and controlling Internet Protocol (IP) based services to subscribers. The SMS2000 delivers powerful subscriber management features to service providers.

The SMS2000 allows almost any type of in-building network infrastructure to be transformed into a robust public network, dramatically reducing configuration headaches, minimizing undesirable interactions between subscribers, and allowing the service provider to deliver a flexible suite of IP services over a common infrastructure.

Authentication, authorization, accounting, provisioning, and a wide range of billing options complete the package, which allows service providers to get subscribers up and running quickly.

Subscriber Management Features

The features supported by Tut Systems' Expresso Subscriber Management System are briefly described below:

- **Plug-and-play networking**—Clients that are misconfigured or have configurations from other networks can connect to the SMS2000 without any reconfiguration of IP address, netmask, or gateway address required. That means, for example, laptops hooked up in hotel rooms by guests need not be reconfigured prior to use.
- **Firewall protection**—Clients attached to the SMS2000 can be protected from many types of Internet hacking by making them invisible from the outside using Network Address Translation (NAT).
- **Authentication, authorization, accounting**—Using the SMS2000 with traditional RADIUS servers or Tut Systems' included OCS server software, service providers are able to authenticate individual users, authorize particular services, and track usage.
- **Provisioning and billing**—OCS adds a number of functions that allow simple provisioning by the service provider or the subscriber. Billing can be applied to credit cards or to hospitality PMS interfaces for direct room billing on a guest's folio.
- **Bandwidth management**—Each individual client can have a separate maximum bandwidth allowance as part of the "user policies."
- **IP address management**—Individual clients can use one of the following:

— A fixed (static) IP address suitable for operating servers visible to the Internet.

— DHCP to retrieve an IP address suitable for using protocols unfriendly to NAT.

— An invisible shared address through the use of NAT.

— IP type 1 to 1 for subscriber accountability with plug and play networking.

— IP type 1 to 1 unique for maximum subscriber accountability with plug and play networking.

- **Portal redirection**—Clients can be directed to a “forced portal” for authentication or to deliver dynamic content. The service provider is able to control and differentiate network service better.
- **IP multicast**—Multimedia content can be delivered to subscribers. By using IGMP snooping, the SMS2000 facilitates multicast delivery.
- **PPTP passthrough**—Point-to-point tunneling protocol can be used by subscribers even if the subscriber’s IP address is shared via NAT.
- **Service management**—Service providers can use the OCS to offer multiple custom service levels to entice customers with a diverse set of connectivity needs and demands, targeted specifically to individual users and/or time periods.
- **Reports**—OCS is equipped with many useful reports designed to assist users in managing their networks.
- **Self provisioning**—Using the OCS, subscribers can choose their own level of service, including bandwidth and IP type (NAT, static, DHCP).

Subscriber Management Components

The SMS2000 can interact with a number of external software and hardware components. Figure 1-1 shows the subscriber management components, which are described in *SMS2000 Tutorials*.

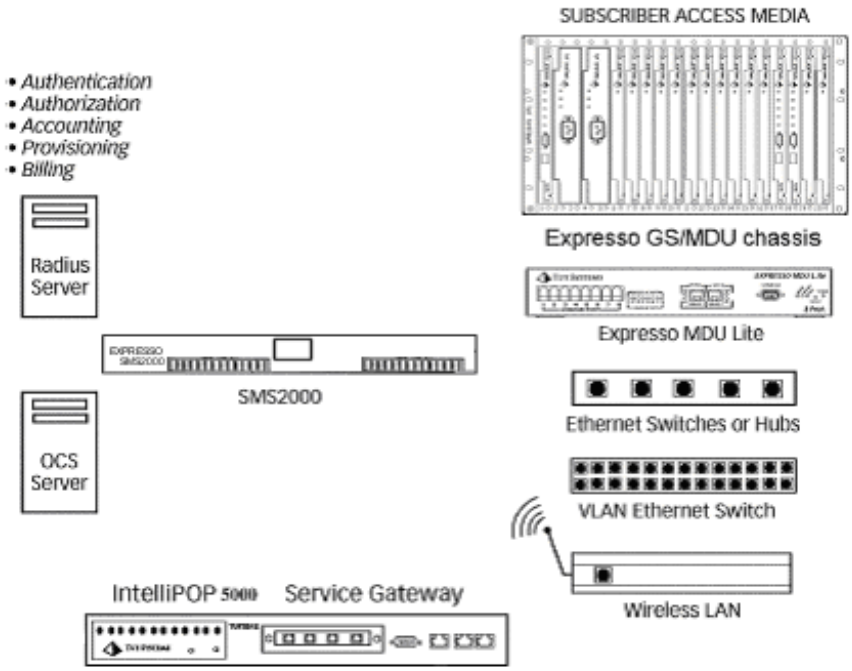

Figure 1-1 Subscriber Management Components

SMS2000

The SMS2000 consists of hardware and embedded software generally placed on a property to control public network access. The SMS2000 handles packet switching functions, traffic shaping, and address translations for a single property. The SMS2000 has a very small internal configuration database and stores no permanent data about users, policies, or billing information. However, it can conduct "machine authentication" using groups and rules including the MAC address, location (with SNMP or VLAN ID), and/or IP address of the subscriber.

- The SMS2000 hardware and embedded software perform the following functions:
- Physically connects via two 10/100Base-T ports to the subscriber network and the Internet.
- Routes IP unicast and multicast traffic.
- Optionally translates addresses of IP packets between the network and clients.
- Monitors and controls the bandwidth utilization for each client.
- Authenticates and authorizes clients (with RADIUS or through OCS).
- Directs Web requests to a service provider-specified Web server.
- Connects to a local Property Management System (PMS) via asynchronous serial interface.

OCS

The OCS software runs on either a Microsoft Windows 2000 Server or on a Linux server. It handles authorization, authentication, accounting, provisioning, and billing for up to 300 SMS2000s simultaneously.

OCS is normally deployed in a service provider's data center, although it can be placed directly on a property. OCS can be configured and managed entirely from any location through its advanced HTML interface using any browser.

OCS is implemented as a Web server running active PHP 4 pages. Microsoft SQL Standard or MySQL Win32 is used as the back-end database on Microsoft Windows 2000. PostgreSQL is used as the back-end database on Linux.

The Linux based solution requires no additional software licenses.

The Windows based solution requires that the system administrator obtain a copy of Microsoft Windows 2000 Server as well as a copy of MS SQL Server. If MySQL Win32 is used on a Microsoft Windows operating system, no additional licensing is required for the MySQL database.

The SMS2000 and OCS communicate using an HTML-based protocol. OCS can "push" policy information about an entire network configuration, telling the SMS2000 how to handle addressing and bandwidth management for a particular property, and how to provide individual policy for subscribers as they gain access to the network. These methods correspond to the evolving IETF standards for policy-based networks known as

"provisioning" and "outsourcing." OCS can perform numerous billing functions. It can bill a subscriber's credit card periodically (such as, monthly fixed service charges from an apartment dweller) or as services are delivered (such as a daily charge in a hotel room once a guest requests Internet service). OCS can handle billing through a credit card service bureau, or it can send its billing information to an SMS2000 connected via a serial interface to a hotel Property Management System (PMS).

The OCS software performs various functions:

- Authenticates and authorizes individual users.
- Manages specific policies for users and properties.
- Handles self-subscription, allowing users to choose their own service levels.
- Handles credit card billing.
- Stores accounting information.
- Delivers Web content.
- Sends billing information to a hotel PMS connected to an SMS2000.
- Offers subscribers multiple service levels as configured by the service provider.
- Provides service offerings that are configurable by properties, room types, and rooms.
- Is completely service provider customizable and brandable.

The SMS2000 and OCS do not have to be connected to the same network. They can communicate with each other over the Internet.

Chapter 2 - Getting Started

Before beginning this chapter, you must have already installed your hardware, completed your cable and power connections, and successfully powered up your system following the instructions in the *SMS2000 Quick Start Guide*.

This chapter presents information and procedures to help you:

- Communicate and interface with your system
- Use the online help system
- Use the CLI to navigate through the system
- Become familiar with the CLI conventions used in this guide

The User Interface

The command line interface (CLI) allows you configure your SMS2000 system. The interface looks the same whether you are communicating with the SMS2000 through the console port, a modem, or a telnet connection. Listed below are other things to consider when using the SMS2000 CLI:

- The Command Line Interface (CLI) is not case-sensitive.
- Commands can be truncated so that only the first few unique characters need to be entered.

For example, the command **show configuration** may be entered as **show conf**, **sho conf**, or **show configuration**.

Style Conventions

To facilitate the proper interpretation of command syntax and parameters as you read this guide, we've applied style conventions to distinguish various elements of the commands, as well as to show how to use the commands. The style conventions used throughout this document are described in Table 2-1.

Table 2-1 Documentation Conventions

Convention	Description
boldbase	Boldface treatment show the actual text that you must enter For example: **show logins** Press Enter to accept the completed command string
italic	Italic treatment indicates that the text is a variable. You must supply the actual value. For example: **show status dhcp** *poolname*
[ ]	Square brackets delimit optional keywords or arguments. For example: [**file** *file*]
{x | y}	Curly braces delimit two or more required keywords. For example: **restore** {**config** | **web**} | **original-config** You must use one of the keywords inside the braces. The vertical bar separates the choices. **Note**: In the above case, the keywords are the actual values that you type. If they were in italic, the words are variables for which you supply the actual values.
`Courier`	Courier plain shows an example of information displayed on the screen.
`boldface Courier`	Boldface courier shows an example of information you must type. For example: `sms2000%` **`port-definition tut`**
Ranges	Ranges of numbers are separated by a dash (**1 — 7**).
/	Slash separators, with no spaces are used in some commands, typically with the variable *masklen*, for example: **ifconfig** *port_number ip_address/masklen* `sms2000%` **`ifconfig 192.168.254.224/31`**

Accessing Help for Commands

There are three ways to access help for commands when you are configuring the SMS2000:

- At the command line, enter the command and press **<Enter>**. If parameters are required, the command and listed parameters are described.
- For definitions of the commands, enter **help** at the prompt.
- Enter *command-name* **help** for additional help.

Note: The **?** character can be used interchangeably with the **help** command.

Cursor Movement

To save time, you can use the arrow keys on your keyboard to navigate between levels. The command keystrokes are used to move the cursor around on the command line and within the command history buffer. The arrow keys can also be used for cursor movement.

Navigation and cursor movement for the SMS2000 system is described in Table 2-2.

Table 2-2 Cursor Motion Keystrokes

Keystroke	Operation
Backspace	Deletes the character behind the cursor
Delete	Deletes the character under the cursor
Left arrow	Moves the cursor back one character
Right arrow	Moves the cursor forward one character
Up arrow	Recalls the previous command in the command history
Down arrow	Recalls the next command in the command history
Control+A	Moves cursor to the first character at the beginning of the line.
Control+B	Moves cursor backward to the beginning of the previous word to the first character at the beginning of the line.
Control+C	Interrupts the currently executing command
Control+E	Moves the cursor to end of line
Control+K	Deletes the characters from the cursor to the end of the line.
Control+R	Reprint the current line to the screen
Control+W	Moves cursor forward to the end of the next word
Control+X	Deletes from the current cursor position to the beginning

.

Chapter 3 - Initial Configuration

You may configure the SMS2000 via a serial interface or a Telnet connection as described in the following sections.

Establishing a Connection with the SMS2000

Establishing a Connection Via a Serial Interface

> **Note:** Verify you have installed the SMS2000 on a rack or shelf with air circulating above and below the SMS2000.

Perform the following steps to configure the SMS2000 via a serial interface connection:

1. If you have not already done so, connect a PC to the DB-9 RS-232 console port connector on the SMS2000 using the DB-9 RS-232 null modem cable supplied.
2. Using Microsoft Windows 95 or later, from the Windows task bar, click **Start**.
3. From the **Start** menu, select **Programs**.
4. From the **Programs** menu, select the **Accessories/Communication** menu and then select the **HyperTerminal** folder.
5. Click the **HyperTerminal** icon.

The **Connection Description** dialog box displays.

6. Enter a name (for example, SMS2000) and select an icon for the connection, then click **OK**.

   The **Connect To** dialog box displays.
7. Select **Connect Using Direct to COM 1 or 2** (the COM port on this PC).
8. Click **OK**.
9. Click **Configure**.
10. Set the following parameters in the **Connection** tab:
    - Set **Bits per second** to **9600**.
    - Set **Data bits** to **8**.
    - Set **Parity** to **None**.
    - Set **Stop bits** to **1**.
    - Set **Flow control** to **None**.

11. Click **OK**.
12. Set the following parameters in the **Settings** tab:
    - Select **Terminal keys**.
    - From the **Emulation pull-down** menu, select **Auto Detect**.
    - Set **Backscroll buffer lines** to **500**.
13. Click **OK** to close the dialog box.

    Note: To avoid cutting off a section of the display, set the window to full screen size.
14. To save this configuration for the future, select **File/Save As** and enter the name of the file for this configuration.

Perform the following steps to log on to the SMS2000:

1. Power up the SMS2000 when the system is finished rebooting (1 to 5 minutes). You will hear three consecutive beeps when ready.
2. From the **Hyperterm Call** menu, select **Connect**.
3. To verify that you have correctly configured your console port, press **<Enter>**.

    - If the Login Display screen does not appear:
    - Make sure that you entered the correct settings.
    - Verify that you are using the correct cable and that the cable is not damaged.
    - Check that you have good cable connections and connector.

    If you are still unable to view the Login Display screen, call your Tut Systems Customer Service representative.
4. Log on using the username “manager” and the password “manager.”

    Note: The password “manager” is the factory default password for the SMS2000. You are strongly encouraged to change your initial logon password as soon as possible to ensure security. For instructions on changing your password, see the *Changing Your Password* section of this chapter.

Warning Security is a critical component of this system. As the system administrator, it is *your* responsibility to manage the security of this system.

Establishing a Connection Via Telnet

Perform the following steps to gain Telnet access to an unconfigured SMS2000 from the subscriber port:

To connect directly to the subscriber port:

If you have not already done so, connect the PC to the SMS2000 subscriber port, by plugging one end of a cross-over Ethernet cable into the Ethernet port on the PC and the other end into the subscriber port on the back of the SMS2000.

> **Note:** If you are not using a hub to connect to the subscriber port, you must use a crossover cable.

To connect using a hub:

5. Plug one end of a straight-through Ethernet cable into the PC's Ethernet port and the other into the hub.
6. Plug one end of another Ethernet cable into the subscriber port on the back of the SMS2000 and the other into the hub.
7. Ensure the hub is not connected to any other network.

> **Note:** Do not plug the subscriber port of the SMS2000 into your network. Isolate the PC and SMS2000 from the rest of your network.

Perform the following steps to gain access to an unconfigured SMS2000:

1. From the Windows task bar, click **Start**.
2. From the **Start** menu, select **Run**.
3. In the Run dialog box, enter **Telnet**.
4. Click **OK**.
5. Click **Connect** and select Remote System.

   The Connect dialog box displays.
6. Enter **35.42.42.42** for the host name.

> **Note:** 35.42.42.42 is the internal factory default IP address for the SMS2000. Once you configure the IP address on your SMS2000, use the IP address that you have assigned instead.

7. Enter **4242** for the port number.
8. Select **vt100** for the TermType.
9. Click **Connect**.

   At this point you will be presented with the logon prompt.
10. Log on using the login name "manager" and password "manager."

> **Note:** The password "manager" is the default password for the SMS2000. You are strongly encouraged to change your initial logon password as soon as possible to ensure security.

Once you have successfully logged on to the SMS2000, you can proceed with the basic configuration of your system.

Initial Configuration

There are five steps required for the initial configuration of the SMS2000:

1. Step 1 Change the password for security purposes.
2. Step 2 Set the Quick Configuration.
3. Step 3 Change the system hostname to identify the system on the network.
4. Step 4 Disable authentication.
5. Step 5 Save the configuration.
6. Step 6 Reboot the system.
7. Step 7 Verify connectivity.

For advanced configuration information, see the *SMS2000 User's Guide*.
For information on using OCS with the SMS2000, see the *OCS User's Guide*.

Changing Your Password

You are encouraged to change the initial configuration password, "manager," after your initial login to the SMS2000. Perform the following steps to change your password:

1. At the system prompt enter:

   `sms2000% passwd`

2. Press **<Enter>**.
3. Enter your new password.
4. Press **<Enter>**.

   The system asks you to verify your password.

5. Reenter your password.
6. Press **<Enter>**.

> **Note:** If you forget your password at any time, please call your Tut Systems Customer Service representative to assist you in logging on again.

You must have access to the serial port and have a phone nearby when contacting Customer Service to bypass your password.

Setting the Quick Configuration

To reset the entire system configuration, using the IP address, network mask, default gateway, and DNS servers specified in the basic system configuration, use this command:

> **set quick-config** {*ip_address/masklen* | *ip_address* **netmask** *ip_mask*} *gateway dns*[*dns*] [*dns*]

This example resets the system configuration, setting the local IP address to 192.168.1.244 with a 24-bit subnet mask (255.255.255.0) and the default gateway is 192.168.1.1.

There are two DNS servers; the first is 192.168.1.42, and the second is 192.168.1.1.

```
sms2000% set quick-config 192.168.1.244/24 192.168.1.1
192.168.1.42 192.168.1.1
```

Setting the Hostname

Use the **set hostname** command to immediately change the host name at the command prompt. SMS2000 uses the specified host name when communicating with the OCS and as the SMS2000 command prompt. Each SMS2000 in a network should have a unique host name.

> **Note:** Host names cannot contain spaces, unprintable characters, quotation marks (“ ”), or apostrophes (’).

To set the system hostname, use this command:

set hostname *hostname*

For example, to set the host name of the local system to ParkPlace,type:

```
sms2000% set hostname ParkPlace
```

Disabling Authentication

The command **auth off** disables authentication.

> **Note:** Additional options for forced web pages are available in the *SMS2000 Command Reference.*

To disable authentication for the current group and remove the server IP, use this command:

auth off

For example, to disable authentication for the current group, type:

```
sms2000% auth off
```

Saving the Configuration

To save the configuration, use this command.

Save

for example, to save the current configuration, type:

```
sms2000% save
```

Rebooting the System

In order for saved configuration changes to take effect, you must **reboot** the system. To force the system to shut down completely and then restart, use this command:

reboot

For example, to reboot the system, type:

```
sms2000% reboot
```

Verifying the Configuration

1. Login to the system.
2. Ping a known site.

   ```
   sms2000% ping www.yahoo.com
   ```
3. Press CTRL-C to stop the pinging.
4. Ping another known site.

   ```
   sms2000% ping www.apple.com
   ```
5. Press CTRL-C to stop the pinging.

If the SMS2000 cannot ping these sites, try to ping a known external IP Address, check your configuration and the local network to verify that you have connectivity to the Internet.

Chapter4 - System Administration

This chapter describes the system administration activities and commands, including:

- Configuration E-Mail Settings
- Configuration and System File Tools
- Configuring SMTP
- Configuring NTP
- Configuring SNMP Polling
- Connectivity and Testing
- System Tools
- Event Tracking
- System Administration Tools
- Troubleshooting Tools
- Subscriber Connectivity Commands
- Upgrades

Configuration E-Mail Settings

Setting the Default Configuration E-mail

Each time you save a new configuration, the SMS2000 can automatically send an e-mail with the new configuration to a specified recipient. The **set config-mail** command allows you to specify the recipient.

> **Note:** The SMTP server must be the DNS name or IP address of the destination mail server. If the IP address is not provided, the server name in the e-mail address is used, which is normally not the desired behavior.

To configure the SMS2000 to send its configuration file to a specified e-mail address each time the configuration is saved, use this command:

> **set config-mail** *recipient@SMTPserver* [*SMTPserver*]

For example, to configure the SMS2000 to send an e-mail with the new configuration file attached to ted@smith.com, using smith.com as the e-mail server, type:

```
sms2000% set config-mail ted@smith.com mail.smith.com
```

Mailing the Current Configuration

The **config-mail** command mails the current configuration to the address specified. The SMS2000 uses the SMTP (Simple Mail Transfer Protocol) server specified by the e-mail address or SMTP-server command line parameter. If you enter **config-mail** with no parameters, the SMS2000 uses the server last configured with **set config-mail**.

Once connected, the SMS2000 sends an e-mail message to the specified (or default - if none is entered) recipient. The message includes a brief explanation of why it was sent with the SMS2000 configuration file attached.

The manager can store the configuration file on an FTP or HTTP server, and later recover it using the **load config** command.

To temporarily override the default e-mail configuration settings and mail the SMS2000 configuration to the specified e-mail address using the given local email server, use this command:

config-mail [*recipient_e-mail* [*SMTP_server*]]

For example, to override the default configuration e-mail settings and send the config e-mail to billy@chung.com, using chung.com as a valid e-mail server that accepts e-mail directly from the SMS2000, type:

```
sms2000% config-mail billy@chung.com mail.chung.com
```

Deleting the Configuration E-mail

To delete the configured e-mail address and mail server to be notified when saving the system configuration, use this command:

delete config-mail

For example, to disable e-mail notification of configuration changes, use this command:

```
sms2000% delete config-mail
```

Configuration and System File Tools

Committing Configuration Changes

To immediately commit configuration changes to the running system and synchronize the running system with the state of the configuration, use this command:

commit

For example, to immediately commit a configuration change, type:

```
sms2000% commit
```

Note: Some types of changes, including adding a static port with the **set port** command or resetting the system configuration with the **set quick config** command require that you reboot the SMS2000 before continuing.

Automatically Committing Configuration Changes

To commit configuration changes to the running system immediately after they are entered without having to enter the **commit** command, use this command:

commit auto

For example to force all configuration changes to be executed immediately, type:

```
sms2000% commit auto
```

Note: Some commands cannot be committed without saving and rebooting. When one of these commands is issued, the SMS2000 displays a warning to the system administrator and disables the automatic commitment of commands.

Note: You can determine the state of the autocommit feature by checking its value at the bottom of the **show config** screen.

Disabling Automatic Configuration Changes

Use the **commit noauto** command to disable the **commit auto** command and revert to using **commit** manually. This allows commands that are not already dynamic/instantaneous to be queued for batch mode execution.

For example, some of the commands that are *not* dynamic are:

delete dns	**load sys**	**set quick-config**
dump-info	**set default**	**set time**
system	**set dns**	**set timezone**
load config	**set port**	

To disable the automatic commitment of configuration commands, use this command:

commit noauto

For example, to set the systemto not commit changes until the **commit** command is issued, type:

```
sms2000% commit noauto
```

Note: Changes to the running system will be lost upon reboot, unless you enter the **save** command.

Saving a Configuration

After committing configuration changes to the running system, the **save** command is used to store the current configuration to a startup script, which is executed the next time the system boots.

To save the current configuration for use on the next reboot, use this command:

save

For example, to save configuration changes made in the current session to permanent storage and for use on the next reboot, type:

```
sms2000% save
```

Note: You must reboot the system for the saved configuration changes to take effect.

Loading a Configuration File

The command **load config** can be used for system recovery. If a SMS2000 fails and you have saved the old configuration file to an external server, you can use the **set quick-config** command to get the SMS2000 up and running and **load config** to restore the complete old configuration file. This minimizes the risk associated with missing a minor configuration parameter when you replace a SMS2000.

Note: No integrity checking is performed besides checking the file header. A corrupt configuration file can be loaded and hang the system. To troubleshoot possible system failure, use the **show startup** command.

To load a configuration file from a remote FTP or HTTP server, use this command:.

load config *url*

Note: Once the file is loaded, you must reboot the SMS2000 so that the new configuration takes effect.

For example, to load the configuration file previously saved for the Connie Hotel from an FTP server, type:

```
sms2000% load config
ftp://ftp.local.com/Connie_Hotel/config_file
```

Restoring a Previous Configuration

To restore the SMS2000 configuration to the last one that was active before you saved the image, use this command:

restore {**config** | **web** | **original-config**}

For example, to restore the last configuration you saved with the **save** command, type:

```
sms2000% restore config
```

Note: You must reboot the SMS2000 for the restored configuration to take effect.

Restoring the Default Configuration

To restore the SMS2000 to the default configuration (with no functions configured), use this command:

set default

For example, to reset the SMS2000 configuration to default, type:

```
sms2000% set default
```

Note: This command does not change the password.

Configuring SMTP

Setting the SMTP Server

The command **set smtp-server** starts proxying SMTP sends to the specified SMTP server. Many mail (SMTP) servers reject mail sent from users who are behind a NAT device. To compensate for this, an ISP can install a mail server that accepts mail from each SMS2000. When a subscriber wants to send mail, the SMS2000 can automatically proxy the mail to the ISP's mail server, which can then cleanly forward it to its final destination. Many SMTP servers do not forward e-mail from hosts outside the local network. It is recommended that you use a local SMTP server. For example, if you have a computer with an IP address in the same subnet as the SMS2000 that can send e-mail, use the SMTP server configured for your e-mail program.

To redirect Simple Mail Transfer Protocol (SMTP) sends to a specified SMTP server, use this command:

set smtp-server {*server_name* | *ip_address*}

For example, to route all outgoing mail messages through an SMTP server with the IP address 1.2.3.4, type:

```
sms2000% set smtp-server 1.2.3.4
```

Deleting the SMTP Server

To stop SMTP proxy sends to the specified SMTP server, use this command:

delete smtp-server {*server_name* | *ip_address*}

For example, to stop forwarding mail to the mail server 1.2.3.4, type:

```
sms2000% delete smtp-server 1.2.3.4
```

Setting the SMTP ID

To configure the SMS2000 to modify the header of outbound e-mail messages from subscribers to ensure that the configured SMTP server will accept their messages when they are connected behind SMS2000, use this command:

set smtpid {**on** | **off**}

For example, to enable SNMP messages to be sent to the SMTP server, type:

```
sms2000% set smtpid on
```

Note: The commands **set smtpid** and **set smtp-server** are each independently configurable mechanisms to help subscribers send e-mail messages without changing any configuration items on their PCs.

Configuring NTP

The Network Time Protocol (NTP) server is used to synchronize the clock on the SMS2000 with the true time. Using an NTP server ensures that the SMS2000 accurately time stamps data to other servers, such as syslog. If an NTP server is not configured, the SMS2000 (like many other devices) may experience clock drift and you may later need to reset the time.

Setting the Timezone

Use the **set timezone** command to configure the timezone. You must configure a timezone before you can synchronize system time using NTP.

To set the local time to a specified time zone, use this command:

set timezone *timezone_name*

For example, to set the time zone to Michigan time, type:

```
sms2000% set timezone US/Michigan
```

Note: To list the valid time zones, enter **set timezone** with no arguments

Configuring the NTP server

To configure a network time protocol server for the SMS2000 to use when synchronizing its clock use the **set ntp-server** command. This command requires that you have already configured a time zone for the SMS2000 using the **set timezone** command.

To configure an NTP (time) server using its hostname or IP address, use this command:

set ntp-server {*hostname* | *ip_address* | **off**}

For example, to set the network time server to 192.168.254.42, type:

```
sms2000% set ntp-server 192.168.254.42
```

Setting the Time

The command **set time** changes the hardware clock on the SMS2000. Unlike other commands, **set time** changes the SMS2000 clock immediately. However, this change takes effect on the SMS2000 only after you reboot the system. This means that the **set time** function cannot be undone by exiting without saving.

> **Note:** If a time zone is not set, time can be specified based on the local time. If a time zone is set, the time must be specified in terms of GMT (Greenwich Mean Time).

To set a new time and date, use this command:

set time [*mm/dd/[cc]yy hh:mm:ss* | *month day hh:mm:ss year*]

For example, to set the time to 9:39:43 PM, April 12, 2002, type:

```
sms2000% set time 04/12/2002 21:39:43
```

> **Note:** Time changes will not affect the running SMS2000 until it reboots.

Configuring SNMP Polling

SNMP polling is required when using an SMS2000 with one or more Expresso GS/MDU Chassis and/or MDU Lites in a hotel environment with PMS billing to isolate subscribers to a specific room. It is optional in other environments such as apartments with Expresso GS/MDU Chassis and/or MDU Lites. With the IntelliPOP 5000 and VLAN switches, an SMS2000 uses a unique VLAN ID for each room to determine the room from which a specific subscriber is connecting.

Enabling SNMP Polling

The **set snmp-poll** command starts polling the specified Expresso GS/MDU Chassis or

MDU Lite (LongRun or HomeRun) for addressing information on new subscribers. The SMS2000 may use polling data from Expresso GS/MDU Chassis equipment to determine the room from which a subscriber is generating traffic. This data can then be used by the OCS or another server to tailor its response to the room and to determine the room number for hotel PMS billing. For example, the OCS can charge a different price for conference rooms than for suites at a hotel. This command allows you to configure the different devices.

To poll a Tut Systems product, use this command:

set snmp-poll *ip_address* [**expresso** | **mduLite**]

For example, to configure the SMS2000 to first poll the Expresso GS/MDU Chassis at 192.168.254.211 to determine the line card and port ID from which the subscriber is connecting, type:

```
sms2000% set snmp-poll 192.168.254.211 expresso
```

Testing to See if SNMP Polling will Work

Use a MAC address (sequence of 12 hexadecimal digits, such as 00A28C94FEB8) to poll the configured SNMP server(s) for the location of a device with the specified MAC address.

To test if the SMS2000 can perform an SNMP poll of the Expresso GS/MDU Chassis and MDU Lites that were last configured and saved, use this command:

snmp-poll *mac_address*

This example polls for a subscriber with the specified MAC address. If the subscriber is connected to a configured Expresso GS/MDU Chassis orMDULite and **snmp-poll** quickly returns the correct IP, slot, and port towhich the subscriber is connected, and SNMP polling is correctly configured.

```
sms2000% snmp-poll 00E0922609FB
```

This example polls for a non-existent MAC address. If the command returns quickly, indicating that the device cannot be found, SNMP polling is correctly configured. If there are long delays, verify that the configured Expresso GS/MDU Chassis or MDU Lite is reachable via IP using the **ping** command, and that it is configured to accept SNMP queries from the SMS2000.

```
sms2000% snmp-poll 000000000000
```

Disabling SNMP Polling

To stop polling the specified Expresso GS/MDU chassis or MDU Lite (LongRun or HomeRun) for addressing information on new subscribers, use this command:

delete snmp-poll *ip_address*

For example, to stop SNMP polling the server whose IP address is 192.168.254.211, type:

```
sms2000% delete snmp-poll 192.168.254.211
```

Connectivity and Testing

Traceroute

To use a standard network application that tracks the path a packet follows to arrive at a specified network destination, use this command:

traceroute {*ip_address*|*hostname*}

This example shows how **traceroute** is used for internal network verification.

```
sms2000% traceroute 208.226.86.252
```

This example shows how **traceroute** is used to verify throughput of an external network (with active DNS).

```
sms2000% traceroute apple.com
```

Testing Connectivity

The ping command is used to test connectivity with a remote computer. By using a host name instead of an IP address, **ping** also verifies that your DNS server is working and properly configured by doing a DNS lookup on the specified host name. The ping can be interrupted by pressing CTRL+C.

To test connectivity with a remote computer, use this command:

ping {*ip_address* | *hostname*}

For example, to test connectivity with a computer with an IP address of 123.2.2.2, type:

```
sms2000% ping 123.2.2.2
```

Note: Some major Web sites do not allow pings for security reasons. However, **rtfm.mit.edu** is a consistently stable site that allows remote pings.

System Tools

Setting Specialized System Options

To set specialized system options, use the following command:

system {**checksig** {**on**|**off**} | **dhcparch** {**on**|**off**} | **linetest** {**on**|**off**} | **lprtest** | **maxusers** *n* | **multicast** {**on**|**off**} | **nonvlandev** {**left**|**right**} | **tut** | **vlandev**

{**left**|**right**}}[**help** | **?**]

For example, with **system linetest on** and the SMS2000 rebooted, the SMS2000 generates a broadcast to the subscriber Ethernet interface once per second. Installers should check for a blinking LED on a Long Run or Home Run adapter if they do not have diagnostic equipment.

```
sms2000% system linetest on
```

For example, to cause a test print page to be sent to the configured LPR printer, use:

```
sms2000% system lprtest
```

Note: Some of the **system** command options will disrupt elements of the current configuration. For more information on the use of the **system** command and its' options, see the *SMS2000 Command Reference*.

Defining Ports

Note: Altering this setting is normally not necessary, even when using VLAN switches in conjunction with Expresso GS/MDU Chassis or MDU Lites.

To configure the type of addressing information used by the SMS2000 to identify unique subscriber ports, use this command:

port-definition {**mixed** | **tut** | **vlan**}

For example, to configure SMS2000 to ignore VLAN tags and focus exclusively on SNMP information, which is useful in error situations where addressing information fails when a subscriber is connected bymeans of an Expresso GS/MDU Chassis behind a VLAN switch, type:

```
sms2000% port-definition tut
```

Setting and Deleting Static Ports

Use the **set port** command to specify port types for all ports, and to set a port or a range of ports as static, dynamic, or disabled or to delete ports.

For static ports, this command can also configure an IP address, local route, and default VLAN ID. When you configure a single static port, you can use an optional IP address and subnet mask to automatically configure the interface and add a local route. If a subnet mask is not specified, the default 255.255.255.255 is used.

Note: When using multiple MDU Lites behind a VLAN switch, such as a Cisco Catalyst switch where most ports can have only one non-default VLAN ID, make sure to specify the VLAN ID of each MDU Lite when configuring its static port. After configuration is complete, verify that it is working. First, reboot the SMS2000, VLAN Switch, and MDU Lites. Then, "snmp-poll 000000000000". If the SMS2000 should correctly ARP for each MDU Lite on its configured default VLAN, and immediately SNMP poll it, the command will return promptly. If this test fails, check the VLAN configuration.

To activate a port or range of ports as static or dynamic, or to deactivate one or more ports, use this command:

> **set port** *port* {[**static** [*ip_address* | *ip_address* **netmask** *ip_mask* | *ip_address*/*masklen*] [**vlan** *vlan_id*]] | **dynamic** | **disable**]}

For example, to set port 800 to a static port with IP address 192.168.254.244 and subnet mask 255.255.255.255, type:

```
sms2000% set port 800 static 192.168.254.224
```

Disconnecting a Session on a Port

To disconnect a session on a port, use this command:

> **disc** {*session_id* | **active** | **group** *groupname* | **mac** *mac_address* | **snmp** *tut_address* | **user** *username* | **vlan** *vlan_id*}

For example, to disconnect the subscriber using slot 4, line 1 of the Expresso GS/MDU Chassis, at 192.168.254.211, type:

```
sms2000% disc snmp 192.168.254.211-004-001
```

Event Tracking

Setting the Syslog Server

To specify the host to which system log messages are sent or to disable this function, use the following command:

> **set syslog** {*hostname facility*| **off**}

For example, to send diagnostic syslog messages to the server 192.168.254.249, type:

```
sms2000% set syslog 192.168.254.249 1
```

For example, to disable the syslog server, type

```
sms2000% set syslog off
```

> **Note:** For more information on the set syslog command, including a list of valid facilities, see the *SMS2000 Command Reference*.

Displaying Log Messages

To enable the display of log messages in the current telnet session on a local console or to disable this function, use the following command:

displog {**on** | **off**}

For example, to enable the display of log messages in current telnet session window, type:

```
sms2000% displog on
```

For example, to disable the display of log messages in current telnet session window, type:

```
sms2000% displog off
```

System Administration Tools

Displaying Version Information

To display the release number, reboot count, system images, active system images, and port information, use the following command:

version

For example, to see version information, type:

```
sms2000% version
```

Exiting the Management Session

Use the **exit** command to exit a management session. If you are using telnet, SMS2000 terminates the connection. If you have made configuration changes during the session, SMS2000 prompts you to save the unsaved changes, if you do not save them, the changes are lost. To exit the management session, use this command

exit

For example, to exit the management session, type:

```
sms2000% exit
```

Rebooting the System

In order for saved configuration changes to take effect, you must use the **reboot** command to restart the system.
To force the system to shut down completely and then restart, use this command:

reboot

For example, to reboot the system, type:

```
sms2000% reboot
```

Changing a Password

Use the **password** command to prevent unauthorized users from accessing the SMS2000.

> **Note:** A bad password can dramatically reduce the system security of the SMS2000. Please follow general password guidelines by including alpha, numeric, and other printable characters in a password that is at least seven characters long.

The default password is “manager”. You should change the default as soon as possible in order to secure the SMS2000.

To change the SMS2000 password, use this command:

passwd

For example, to set a new password, type:

```
sms2000% passwd
```

> **Note:** No characters are displayed when entering the new password.

Displaying Control Keys

To display a summary of the valid control keys for the system, use this command:

keys

For example, to display the on-line key mapping, type:

```
SMS2000% keys
```

> **Note:** For a complete list of all available control keys see *Chapter 2*, “*Getting Started”*.

SNMP Management

Beginning with SMS2.3.6, the SMS supports remote SNMP management. SNMP System Contact and System Location will be reported in the SNMP system OID. All SMS OIDs are read-only. An SNMP trap is sent to the trap-recipient when the SMS boots or reboots. By default, the SNMP agent is disabled.

SNMP Agent

To enable the SNMP agent, type:

snmp enable

To disable the SNMP agent, type:

snmp disable

To view the SNMP agent status, type:

show snmp status

SNMP System Contact

To specify the SNMP System Contact, type:

snmp system-contact *system-contact-string*

For example,

```
SMS2000% snmp system-contact "Some Person"
```

Note: Place the system contact in quotes if it includes spaces

To view SNMP System Contact information, type:

SMS000$ **show snmp system-contact**

SNMP System Location

To specify the SNMP System Location, type:

snmp system-location *system-location-string*

For example,

SMS2000% **snmp system-location "Basement 123 Any St, New York, NY 10001 USA"**

Note: Place the system location in quotes if it includes spaces

To view SNMP System location information, type:

SMS000$ **show snmp system-location**

SNMP Community

You can define up to five SNMP Communities with unique IP Addresses for access to MIB objects.

To add an SNMP Community and Management IP, type:

snmp add community *community-name mgmt-address* {**rw** | **ro**}

For example, to create a public community without restrictions:

SMS2000% **snmp add community public 0.0.0.0**

Or, to limit the access to a particular Management IP address:

SMS2000% **snmp add community donttell 10.240.1.50**

To delete an SNMP community, type:

snmp delete community *community-name*

For example,

SMS2000% **snmp delete community donttell**

To view the SNMP Community configuration, type:

show snmp community

To support a community with more than one configured management station, add it twice:

SMS2000% **snmp add community donttell 10.240.1.50**
SMS2000% **snmp add community donttell 10.240.1.51**

SNMP Trap Recipient

A maximum of one SNMP trap recipient may be configured.

To configure an SNMP trap recipient, type:

snmp add trap-recipient *community-name ip-address*

For example,

SMS2000% **snmp add trap-recipient donttell 10.240.1.50**

To delete the SNMP trap recipient, type:

SMS2000% **snmp delete trap-recipient**

To view the SNMP trap recipient configuration, type:

show snmp trap-recipient

Troubleshooting Tools

System Information Tools

Setting the System Information Dump

Use the **dump-info** command to e-mail the status of the system to a specified address when the SMS2000 has a fatal error.

An e-mail address of the network administrator can be entered, along with an SMTP server, or the diagnostic information can be mailed directly to the Tut Systems' Customer Support e-mail address: **support@tutsys.com**.

To e-mail the status of the system to a specified address when SMS2000 has a fatal error, use this command:

dump-info {*recipient_@_server* [*recipient_server*] | **off**}

For example, to configure the e-mail address of Tut Systems' Technical Support to receive notification of system failures, type:

```
sms2000% dump-info support@tutsys.com itsmail.tutsys.com
```

Setting a Software Watchdog

Use the **set soft-watchdog** command to enable or disable the software watchdog in order to get diagnostic builds from the SMS2000. The software watchdog is disabled by default.

Note: The software watchdog should only be enabled if you have configured a recipient for diagnostic information with **dump-info** and are experiencing problems with the SMS2000.

set soft-watchdog [**on** | **off**]

For example, to enable the software watchdog, force a fault condition, and reboot the SMS2000 to test e-mail sending, type:

```
sms2000% set soft-watchdog on
```

Subscriber Connectivity Commands

Setting the ARP Failure Limit

The SMS2000 periodically sends an unsolicited ARP request to clients from whom it has not received network traffic for a certain period of time. If a device does not respond to the specified number of requests, the SMS2000 assumes that it has been disconnected and closes the session with the device. The set **arp-fails** command allows you to set the number of allowed failures.

To set the maximum number of ARP failures allowed before a device is assumed to be down or disconnected, use this command:

set arp-fails *fail_count*

For example, to configure the SMS2000 to end subscriber sessions, if no response is received from a subscriber after 10 ARP requests are sent, type:

```
sms2000% set arp-fails 10
```

Setting the ARP Polling Period

The SMS2000 uses unsolicited ARP requests to verify client connectivity. This allows you to select theminimum polling period and response time in seconds for client ARP requests.
To set the ARP polling period, in seconds, type:

set arp-time *seconds*

For example, to configure the SMS2000 to wait 10 seconds between intervals when using ARP to test the connection status of subscribers, type:

```
sms2000% set arp-time 10
```

Upgrades

The following sections provide detailed steps for installing or upgrading SMS2000 images.
For information on installing and upgrading the OCS software, see the *OCS User's Guide*.
You can load new firmware using an http or ftp server. The SMS2000 supports authentication via username and password. You can load the firmware directly from Tut Systems' website. Alternatively, you can locally cache firmware on another ftp or http server, and load the SMS2000 firmware from that server.

Upgrading from Tut Systems' Website

1. Go to the Tut Systems website at http://www.tutsystems.com.
2. On the Support pull-down menu, click "SMS/OCS".
3. Click Downloads.
4. Enter your Company's name and product serial number (as printed on your invoice) where required. If you purchased the product before 1-September-2000, or have purchased the product through a third party, please contact Customer Support.
5. Click Login.
6. Obtain the URL required for the SMS2000 **load sys** command, which is located at the bottom of the *Latest SMS/OCS Software and Documentation* section of the website. The **load sys** command will be in this format: `sms2000% load sys url` Where the *url* is listed on the Tut Systems Web site.

   Note: The complete URL for the latest build is on the Tut Systems web site.
7. Log in to the SMS2000 and type in the **load sys** command that you obtained from the Tut Systems website.

Downloading the SMS2000 Firmware from the Tut Systems' Website

1. Go to the Tut Systems website at http://www.tutsys.com.
2. On the Support pull-down menu, click "SMS/OCS".
3. Click Downloads.
4. Enter your Company's name and product serial number (as printed on your invoice) where required. If you purchased the product before 1-September-2000, or if you purchased the product through a third party, please contact Customer Support.
5. Click Login.
6. Click SMS2000 Version 2.3.2 Firmware.

Archiving SMS2000 Firmware and distributing it from a Server

1. Download the firmware using a browser utility from the source server at Tut Systems.
2. Place the firmware on the local ftp or http server.
3. To load the firmware, use this command, where *your url* is the URL to the file: sms2000% **load sys** *your url*

   Note: The OCS server is an http server and can be used to archive SMS2000 firmware builds.

Verifying a Successful Upgrade

1. After the SMS2000 reboots, telnet to the SMS2000.

   Note If the new firmware fails to boot, the SMS2000 reloads the older firmware.

2. Login. Use the **version** command to verify that the release matches the upgrade version and the SMS2000 booted from the same location from which the new firmware was loaded.

   This example shows that the SMS2000 booted from hda2.

```
sms2000% version

Release: SMS/2.3.2b4 30Sept01
server: SMS/2.3.2b4 30Sept01
config: SMS/2.3.2b4 30Sept01
kernel: SMS/2.1.2b4 30Sept01
Ports: 800/800
Reboot #657 - Booted from hda2 on Thur Sept 30 11:36:53 2001
vlan device: tulip; non-vlan: eepro100
hda1 - System http://www.tutsys.com/sms/sms-2-3-2b4.bin Loaded
Fri May 6 10:30:10 2001
hda2 - System http://www.tutsys.com/sms/sms-2-3-2b4.bin Loaded
Thur Sept 30 11:35:17 2001

sms2000%
```

3. Use the **show status** command to verify that the system is operating normally.

```
sms2000% show status
```

   If you see: connect (/var/run/ppctl): Connection refused, the SMS2000 is not operating normally and the upgrade has failed. If for any reason the upgrade is unsuccessful, contact your support Representative.

Returning to an Older Firmware Version

The SMS2000 stores two firmware images. If the newer firmware image fails to start, the SMS2000 automatically boots from the older image. You can force the SMS2000 to boot the older image using the **load sys** command.

Loading Another Image

1. Use the **version** command to determine the image from which you want to boot.
2. Enter **load sys 1** to load the image for hda1, or **load sys 2** to load the image for hda2.
3. Reboot your SMS2000 system.

   Note: If you download new firmware that fails to boot, the SMS2000 will boot from the older firmware. Do not manually instruct the SMS2000 to reload the

new firmware because the SMS2000 will not boot the older firmware, it will continue to fail to boot the newer firmware upon each subsequent boot attempt. Always download the newer firmware again in the event of upgrade problems.

Chapter 5 - Authentication

Authentication is the process of verifying the identity of a subscriber.

Authentication

The SMS2000 is capable of performing authentication by using an external server (OCS or RADIUS). For more information on using the OCS for authentication, see the *OCS User's Guide*. For more information on RADIUS, see *Chapter 13*, "*Using SMS2000 with a RADIUS Server."* Scenarios for performing these functions in various configurations are described below.

> **Note:** The SMS2000 can authorize machines based on source MAC address (sometimes called "machine authentication", VLAN ID, SNMP information, IP address, or any combination of these using groups and rules.

Table 5-1 shows how authentication is performed with no external server, with RADIUS, and with the OCS.

Table 5-1 Authentication

Server	Functionality
With No External Server	The SMS2000 has no database capable of authentication, however it can be used to authorize machines based on source MAC address (sometimes called "machine authentication"), VLAN ID, SNMP information, IP address, or any combination of these using groups and rules. For more information on using groups and rules, see Chapter 10, "*Groups and Rules."*
With RADIUS	The SMS2000 behaves like a standard network access server (that is, a dial-in network server) and supports RADIUS authentication. The client enters a user name and password on a Web page generated locally by the SMS2000.
With OCS	The OCS can be configured to authenticate clients. The OCS can also be configured to allow some subscribers (such as servers) network access without authentication.

Configuring the Command Server

Setting the Command Server for OCS Interaction

To set the command server for the OCS interaction, use this command:

set cmd-serv *ip_address*

For example, to set the command server to 10.228.10.251, type:

```
sms2000% set cmd-serv 10.228.10.251
```

Note: This is normally not necessary if you use the **auth add web** command with the **cmd-serv** option when adding the OCS.

Deleting the Command Server

To delete the command server, use this command:

delete cmd-serv *ip_address*

For example, to delete the command server with the IP address 10.228.10.251, use this command:

```
sms2000% delete cmd-serv 10.228.10.251
```

Note: This is normally not necessary if you use the **auth delete web** command.

Authentication

Adding the OCS as the Authentication Server

Use the **auth add web** command to configure a Web-based authentication server (OCS). When subscribers connect, they are redirected to the specified page on the server. The server then authenticates and redirects the subscriber to the specified URL in the SMS2000 for network access. You can also configure the authentication server as a command server by entering the **cmd-serv** option of **auth add web**. This is required for the OCS.

The **auth add web** command automatically adds an allow-net to the specified server so that subscribers can be redirected to the allow-net without being intercepted. For more information on allow-nets, see "*Allow-Nets" on page 49*.

To add a Web server as the authentication server for the current group, use this command:

auth add web *url* **secret** *secret* [**cmd-serv**]

For this example, the SMS2000 will be configured to authenticate using the OCS server at 192.168.254.249. The shared secret **donttell** will be used for mutual authentication between the SMS2000 and the OCS. The OCS is treated as a command server by periodically sending it requests for commands. Type:

```
sms2000% auth add web
http://192.168.254.249/pp/welcome.php3
secret donttell cmd-serv
```

Note: This feature can be used to create an allow-net of sites that are accessable without authentication.

Note: A shared secret is similar to a password.

Deleting an Authentication Server

Use the **auth delete** command to automatically remove an allow-net for the IP address of the Web server with a 32-bit subnet mask. If the same server is used as theWeb server and the cmd-server, **auth delete** deletes the cmd-server also.

To delete an authentication server from the current group, use this command:

auth delete {**radius** *server*|**web** *url*}

For example, to stop authentication using the Web server with the IP address 192.168.254.249, type:

```
sms2000% auth delete web 192.168.254.249
```

Note: If no other servers are configured, authentication for the current group is disabled.

Testing Authentication

To test authentication for the current group without using any specific server, use this command:

auth on

For example, to enable authentication for the current group, type:

```
sms2000% auth on
```

A warning will appear.

> **Note:** You do not have to specifically enable authentication. Simply adding a Web or RADIUS server is sufficient.

Disabling Authentication

Use the **auth off** command to disable authentication for the current group.
If you use the **auth off** command with the **forcedweb** option, when an unauthenticated subscriber first trys to access the Internet, the subscriber is automatically redirected to the specified Web page; for example, an ISP's portal page. If the **blockall** option is also specified, subscribers cannot use network services, such as FTP and telnet, until this Web page has been viewed, otherwise only web services are blocked. To disable authentication for the current group use this command:

auth off [**forcedweb** *authok_url* [**blockall**]]

For example, to disable authentication for the current group, but send subscribers to the tutsys.com page, type:

```
sms2000% auth off forcedweb http://www.tutsys.com
```

Setting the Authentication Interval

> **Note:** This is only used when authentication is turned off for the group and **forced web** is enabled.

To set the interval used for recurring authentication (in minutes), use this command:

auth interval {*minutes* | **off**}

For example, to set the interval between recurring authentications to one hour (60 minutes), type:

```
sms2000% auth interval 60
```

> **Note:** When authentication is off and a forced web page is enabled, the forced web page will be presented to the subscriber at the end of every **auth interval**.

Bypassing Authentication

To manually connect a client and bypass authentication, use this command:

connect *session_id*

For example, to manually connect the user associated with port 3, type:

```
sms2000% connect 3
```

> **Note:** This command requires a session id and that authentication is enabled.

HTTP Request Throttle

Setting the HTTP Request Throttle

Use the **set http-request throttle** command to configure a per-session throttle on the rate at which HTTP requests from that session are handled before authentication. A new session begins with *max_requests* requests enabled. Every request uses one from a pool of available requests until there are no requests available in the pool. Requests are allocated to the session at *request_rate* requests per second.

> **Note:** This command has no effect on authenticated subscribers.

To configure a per session throttle on the rate at which HTTP requests from that session are handled before authentication, use this command:

> **set http-request-throttle** *max_requests* [*request_rate*]

For example, to enable an HTTP request throttle for each unauthenticated session, starting with 10 requests, and with requests available to that session at one request per second, use:

```
sms2000% set http-request-throttle 10 1
```

If the subscriber generates 11 HTTP requests in less than one second, it is ignored. After using all available requests, only 1 request per second is handled and additional requests are ignored.

Deleting the HTTP Request Throttle

To disable the HTTP request throttle for sessions not yet authenticated, use this command:

> **delete http-request-throttle**

For example to turn off the HTTP throttle request setting, type:

```
sms2000% delete http-request-throttle
```

Allow-Nets

Allow-nets provide single IP addresses or subnets to which subscribers can send IP data without authentication, the **set allow-net** command supports up to 1000 allow-nets. Beginning with the release of SMS2.3.6, Allow-Nets support DNS names as well as IP addresses.

Setting an Allow-Net

> **Note:** When adding the OCS using the **auth add web** command an allow-net is automatically configured for you. An OCS server will always be added as an allow-net entry when you use an OCS authentication server. This allows the SMS2000 to redirect subscribers to the server before authentication. Other servers may also be required in your allow-net, such as **www.authorize.net** (for credit card authentication) and/or the address of any portal page that you want to present for Web authentication.

To allow subscribers to access a specific subnet before they are authenticated, use the following command:

set allow-net *{ip_address* [*netmask*] | *dns-name}*

For example, if an Internet service provider placed a page for a hotel called "Central Park Hotel" at the following URL:

http://www.notarealserver.com/CentralParkHotel/index.html

And this embedded remote content directly in the page:

<script language="JavaScript"
src="http://dynamic.notasyndicate.com/newsphoto/photo.js">

With the following DNS entries:
www.notarealserver.com 192.168.1.1
dynamic.notasyndicate.com 192.168.254.254

The Internet service provider would then configure the SMS2000 as follows:

1. Set an allow-net for the first DNS server.

   ```
   sms2000% set allow-net 192.168.1.1
   ```

   or

   ```
   sms2000% set allow-net notarealserver.com
   ```

2. Set an allow-net for the second DNS server.

   ```
   sms2000% set allow-net 192.168.254.254
   ```

   or

   ```
   sms2000% set allow-net notasyndicate.com
   ```

3. Set the redirection URL.

   ```
   sms2000% set authok
   http://www.notarealserver.com/CentralParkHotel/index.html
   ```

> **Note:** You can specify multiple allow-nets by entering the **set allow-net** command for each allow-net.

Deleting an Allow-Net

To remove allow-net entries, use this command:

delete allow-net [*ip_address netmask* | *ip_address*/*masklen* | *dns-name* | *dns-name/masklen*]

For example, to delete an allow-net starting at 192.168.254.128 with a 32-bit network mask, type:

```
sms2000% delete allow-net 192.168.254.128/32
```

For example, to delete an allow-net for a dns name, type:

```
sms2000% delete allow-net notarealserver.com
```

Automatic Redirection URLs

Setting the Automatic Redirection URL

The command **set authok** specifies the URL to which a subscriber is automatically redirected when authentication completes, or to which the subscriber connects if authentication is off. The page specified here is also the forcedweb page specified when authentication is off.

> **Note:** The authok URL can include replaceable parameters such as the port id, subscriber MAC address, and VLAN ID. It can include a sequence number and be optionally signed using the sig parameter and either the secret on this command or the secret used previously when adding the OCS.
>
> **Note:** When using RADIUS authentication with an authok page, the authok server should also be added to your allow-nets.

For example, when tutsys.com is 123.123.123.123, type:

> sms2000% **set authok http://www.tutsys.com**
> sms2000% **set allow-net 123.123.123.123**

To set the URL used for network access after successful authentication, use this command:

> **set authok** *url*

For example, to redirect subscribers to the Tut Systems home page after successful authentication or when subscribers use theirWeb browser for the first time if authentication
is off, type:

```
sms2000% set authok http://www.tutsys.com
```

SMS2000 can substitute subscriber information for replaceable parameters in the URL. For example, here the **set authok** command is shown using the **secret** as well as the **blockall** parameters, and a URL with parameters embedded in it which are handled during the redirect.

```
sms2000% set authok
http://www.myserver.com/mypath/myscript.cgi?port=$port&host=$host&
mac=$mac&group=$group&origurl=$origurl&seq=$seq&sig=$sig secret
mysecret blockall
```

> **Note:** This can be used in conjunction with an OCS to create a free service at slower speeds, selling higher speed services through the SMS2000.

Deleting the authok Page

To delete the URL (forcedweb page) to which a subscriber is automatically redirected when authentication is complete or to which a subscriber connects if authentication is off, use this command:

delete authok

For example, To delete the URL for subscriber access, type:

```
sms2000% delete authok
```

Authentication with RADIUS

Note: A RADIUS accounting server must be separately configured if RADIUS accounting is desired.

Adding a RADIUS Server

Use the **auth add radius** command to configure a RADIUS server as the authentication server for the current group. When a subscriber connects to the SMS2000, he is automatically redirected to a login page, which requires a user name and password. This information is sent to the configured RADIUS server. If the server approves, the subscriber is granted access, and accounting information is automatically sent to the RADIUS accounting server.

Beginning with the 2.3.6 release of SMS software, many RADIUS attributes and additional features have been added.

For example:

- Add multiple RADIUS servers for fault-tolerance
- Add Alias IP addresses for clustered RADIUS Servers
- Configure retransmission, deadtime, and timeout timers

- Support RADIUS ports 1812 and 1813 for RADIUS request and accounting ports (per official RADIUS assigned ports)
- Support Session-Timeout attribute
- Support Idle-Timeout attribute
- Set the NAS type parameter

Note: RADIUS packages are available for all major Linux distributions.

When you communicate with the RADIUS server, use a shared secret of your choosing to:

- Authenticate the SMS2000 with the RADIUS server.
- Verify responses returned from the RADIUS server to the SMS2000.

Note: The **auth add radius** command does not automatically assume that the same RADIUS server (with the same name and secret) is used for accounting, you must configure it with these settings using the **acct add** command.

Command:

auth add radius *server[:auth_port[:acct_port]]* **secret** *secret* [**retrans=***times*] [**retrans-primary-only=***times*] [**timeout=***seconds*] [**deadtime=***minutes*] [**alias**]

Syntax Description

Syntax	Description
Server	IP address or hostname of the RADIUS server
Secret	Password to authenticate the SMS2000 with a RADIUS server
Auth_port	Optional TCP/UDP UDP port on which to contact the RADIUS server for RADIUS authentication requests. Default is 1812
Acct_port	Optional TCP/UDP port on which to contact the RADIUS server for RADIUS accounting requests. Default is 1813
Retrans=*times*	Optional parameter indicating the number of retransmissions to a RADIUS server with no response. The total number of transmissions is **retrans** plus one.
retrans-primary-only=*times*	Optional parameter indicating the number of retransmissions to the primary RADIUS server before simultaneously trying backup and primary servers. Must be less than **retrans**. The total number of transmissions is the to the primary only before contacting backup servers is **retrans-primary-only** plus one
timeout=*seconds*	Optional parameter indicating the total number of seconds to wait after transmitting a request to this RADIUS server without a response.
deadtime=*minutes*	Optional parameter indicating the number of minutes after a RADIUS server fails to respond to an initial RADIUS request and **retrans** retries before attempting to use that server again. After failing to respond, a RADIUS server will be DEAD this number of minutes.

Syntax	Description
Alias	Adding the **alias** parameter to the end of the **auth add radius** command will configure the SMS to receive RADIUS response packets from an IP address other that the IP address configured as the RADIUS server.

Multiple RADIUS Servers

Default

Older versions of SMS used UDP port 1645 for RADIUS authentication requests and 1646 for RADIUS accounting requests by default.

New versions of SMS will continue to use those same ports for previously configured RADIUS servers when upgraded from previous versions.

However, new RADIUS servers will be configured with port 1812 for RADIUS authentication and port 1813 for RADIUS accounting by default.

The default **retrans** is 5.

The default **retrans-primary-only** is 2.

The default **timeout** is 30 seconds.

The default **deadtime** is 0 minutes (disabled)

Usage Guidelines
Note Select a shared secret as you would a password.

Example
This example configures the SMS2000 to authenticate subscribers in the current group using the RADIUS server at 192.168.254.249.

```
sms2000% auth add radius 192.168.254.249 secret donttell
retrans=3 retrans-primary-only=1 timeout=10 deadtime=5
```

Alias IP address

If the RADIUS servers are configured with a virtual interface, the RADIUS response packets will be transmitted to the SMS on a different interface than the request packet was received. The SMS will reject the packets since it did not arrive with the expected source IP address. Setting an alias IP address allows the SMS to receive the RADIUS response from a different source IP. You must configure the alias IP parameter *after* configuring the RADIUS server.

For example;

auth add radius 192.168.1.249 secret donttell
auth add radius 10.1.1.50 alias

The above two commands will cause the SMS to send the RADIUS request to 192.168.1.249 and receive the RADIUS response from both 192.168.1.249 and 10.1.1.50.

The **alias** parameter can be combined with the multiple RADIUS servers to provide fault-tolerant clustered RADIUS servers. RADIUS server configuration to support this is not covered by this documentation as server configurations can vary widely.

Set NAS port type parameter

Beginning with SMS2.3.6, the system administrator can set the NAS type parameter to any supported NAS type. If the NAS type parameter is not set, the default value of 5 will be used.

To set the NAS type parameter, type:

Set nas-port-type <integer>

For example, to set the NAS port type to be used for a Wireless network, you will enter the following command:

Set nas-port-type 19

NAS port type values are specified in RFC2865 section 5.1. They are:

0 Async
1 Sync
2 ISDN Sync
3 ISDN Async V.120
4 ISDN Async V.110
5 Virtual
6 PIAFS
7 HDLC Clear Channel
8 X.25
9 X.75
10 G.3 Fax
11 SDSL - Symmetric DSL
12 ADSL-CAP - Asymmetric DSL, Carrier less Amplitude Phase Modulation
13 ADSL-DMT - Asymmetric DSL, Discrete Multi-Tone
14 IDSL - ISDN Digital Subscriber Line
15 Ethernet
16 xDSL - Digital Subscriber Line of unknown type
17 Cable
18 Wireless - Other
19 Wireless - IEEE 802.11

show status radius

Shows the status of and configuration of RADIUS servers in the running system, including whether they are DEAD or ALIVE. If the RADIUS server is DEAD, the command will also indicate the number of minutes until it is alive again.

show status radius

Example
This example displays the status of RADIUS servers on the system:

```
sms2000% show status radius
```

Testing Authentication on the RADIUS Server

To test a RADIUS authentication server by querying the currently configured server, use this command:

auth test

For example, to test the currently active RADIUS authentication server by attempting to authenticate the user **bob** with the password **bob**, type:

```
sms2000% auth test

User Name: bob
Password:
```

> **Note:** A RADIUS authentication server must already be active for this command to work.

Configuring a RADIUS SSL Back Channel

To configure a RADIUS SSL back channel so that passwords from subscribers are encrypted when transferred to SMS, obtain the `tutsystems-ssl-auth.tar.gz` file and install it and configure it on an SSL capable web server following the instructions in the documentation directory of the archive file.

Configure and verify RADIUS authentication on SMS as normal. Then enter the following command:

auth radius-back-channel-url https://MyServerName/sslonly/authform.php

Verify that you can enter your username and password in the authentication form over HTTPS and that authentication works as before.

> **Note:** It is necessary to obtain a certificate from a registered Certificate Authority recognized by your web browser (e.g. Verisign) to eliminate warnings that subscribers may see when connecting to your secure site.

Chapter 6 - Authorization

Authorization entails determining if a particular user has permission to use a service.

Authorization

The SMS2000 is capable of performing authorization by using an external server (OCS or RADIUS) or by using onboard groups and rules. For details about using the OCS for Authorization, see the *OCS User's Guide*. For more information on RADIUS, see Chapter 13, "*Using SMS2000 with a RADIUS Server*." Scenarios for performing these functions in various configurations are described below.

Authorization

Table 6-1 shows how authorization is performed with no external server, with RADIUS, and with the OCS.

Table 6-1 Authorization

Server	Functionality
With No External Server	No user authentication is possible. Groups and rules can be used to authorize subscribers based on their MAC address, VLAN ID, SNMP information, IP address, or any combination of these. For more information on using groups and rules, see Chapter 10, "*Service Creation using Groups and Rules."*
With RADIUS	Authorization follows authentication as it does on a standard network access server (NAS). Parameters include static IP and bandwidth.
With OCS	The OCS provides enhanced authorization functions based on user name, physical port, MAC address, and more. Parameters include Stat IP, auth required, and bandwidth.

Chapter 7 - Accounting

Accounting entails the reporting of network resource usage.

Accounting

The SMS2000 is capable of performing accounting by using an external server (OCS, RADIUS, or Syslog). For more information on using the OCS for accounting, see the O*CS User's Guide*. For more information on RADIUS, see Chapter 13, "*Using SMS2000 with a RADIUS Server*." Scenarios for performing these functions in various configurations are described below.

Accounting

Table 7-1 shows how accounting is performed with no external server, with RADIUS, and with the OCS.

Table 7-1 Accounting

Server	Functionality
With syslog	Only syslog session information is available. This information is sent using unreliable UDP transport and, depending on network conditions, may not be delivered in every case. Syslog messages are sent in a similar fashion as standard RADIUS START and STOP messages
With RADIUS	The SMS2000 sends session information with standard START and STOP records. START records are sent upon authorization. STOP records are sent when a client is no longer responsive to periodic ARPs sent by the SMS2000, usually because it is disconnected or shut down.
With OCS	The OCS offers enhanced resource accounting.

RADIUS accounting is available with the OCS authentication.

Sending Accounting Messages to a Syslog Server

Note: This command is ignored if no syslog server has been configured.

To enable and disable transmission of RADIUS-style accounting messages to the configured syslog server, use this command:

acct syslog {**on** | **off**}

For example, to send usage information to the configured syslog server instead of to a RADIUS server.

```
sms2000% acct syslog on
```

Radius Accounting Configuration

Sending Accounting Messages to a RADIUS Server

> **Note:** This command does not require that you have configured RADIUS authentication.

When subscribers connect or disconnect, usage data can be sent to a RADIUS accounting server. RADIUS accounting can be configured to track the usage of subscribers, including time on, time off, and bandwidth used.

To configure SMS2000 to send accounting messages to the specified RADIUS server, use this command:

acct add radius *radius_server* **secret** *secret*

For example, to add 192.168.254.249 as a RADIUS accounting server, type:

```
sms2000% acct add radius 192.168.254.249 secret donttell
```

Deleting a RADIUS Accounting Server

To delete a previously configured RADIUS accounting, or syslog server, use this command:

acct delete *server*

For example, to delete the previously configured RADIUS accounting server, type:

```
sms2000% acct delete 192.168.254.249
```

Configuring Accounting Parameters

To configure the number of transmit attempts for accounting and system server logs on a RADIUS server, use this command:

acct retransmit *pos_integer*

For example, to set the number of transmit attempts to 4, type:

```
sms2000% acct retransmit 4
```

> **Note:** Use **acct retransmit** only for a RADIUS accounting server.

Chapter 8 - Provisioning

The SMS2000 is capable of performing provisioning by using an external server (OCS or RADIUS) or internally using groups and rules. For more information on using the OCS to provision the SMS2000, see the *OCS User's Guide*. For more information on RADIUS, see Chapter 13, "*Using SMS2000 with a RADIUS Server*." Scenarios for performing these functions in various configurations are described below.

Table 8-1 shows how provisioning is performed with no external server, with RADIUS, with the OCS, and internally.

Table 8-1 Provisioning

Server	Functionality
With No External Server	SMS2000 based rules and groups allow you to target services at sets of subscribers. For more information on using groups and rules, see Chapter 10, "*Groups and Rules."*
With RADIUS	RADIUS may set a user's IP address and traffic shaping parameters. The provisioning of user names and services must be done either manually or by a separate provisioning server supplied for ISPs by a number of software vendors.
With OCS	The OCS can handle provisioning of new users by either network administrators or users themselves (self-provisioning). A number of user attributes can be controlled, including addressing and traffic shaping.

Chapter 9 - Billing

Billing is charging the subscriber money for using the service.

Billing

The SMS2000 is capable of performing billing by using an external server (OCS or RADIUS). For more information on using the OCS for billing, see the *OCS User's Guide*.

For more information on RADIUS, see Chapter 13, "*Using SMS2000 with a RADIUS Server*." Scenarios for performing these functions in various configurations are described below.

Table 9-1 shows how billing is performed with no external server, with RADIUS, and with the OCS.

Table 9-1 Billing

Server	Functionality
With No External Server	Billing must be handled independently
With RADIUS	The SMS2000 sends RADIUS messages to drive third party billing systems.
With OCS	Manual, credit card (one time or periodic), pre-paid time card, or property management system (PMS).

Chapter 10 - Service Creation Using Groups and Rules

Groups are created on the SMS2000 in order to provide an easier way to manage multiple subscribers. Subscribers are placed into groups according to a set of rules. Rules may be configured directly on the SMS2000 through the command line interface or, more typically, are generated automatically by the OCS and downloaded to the SMS2000. Rules are a set of Boolean operators that compare a subscriber's MACaddress, IP address, VLAN tag, and SNMP-reported origin (for Tut Systems' Expresso GS/MDU Chassis media).

When a rule is matched, the subscriber is placed in the appropriate group. Rules also specify attributes such as IP addressing or traffic shaping parameters, which override the group defaults.

The SMS2000 can treat subscribers differently, depending on the group into which they are placed. By default, a single group is used for all subscribers, but additional groups can be added. Group membership controls the following attributes:

- DHCP pool selection
- Authentication and accounting server selection
- DNS server for queries
- Default traffic shaping parameters

Groups

Many configuration items, including authentication type, IP type, and shaping can be tied to groups. For example, if a manager had previously configured an SMS2000 to use RADIUS to authenticate users, but had a particular subscriber who wanted to use a NAT box which could not conduct RADIUS authentication, the manager might use a rule to place that particular box in a special group which did not require authentication.

Adding a Group

To add groups with specific characteristics, use this command:

group add *groupname* [**noinherit | inherit** *groupname*]

For example, to add a group named custnat, type:

```
SMS2000% group add custnat
```

> **Note:** The new group automatically becomes the new group context. Group specific commands affect the new group.

Deleting a Group

To delete groups with specific characteristics, use this command:

group delete *groupname*

For example, to delete the group library, type:

```
sms2000% group delete library
```

Setting the Active Group Context

Most configuration items are tied to the current group. To set the active group context, use this command:

group [*groupname*]

For example, to set the active/current group to the group buildingA, type:

```
sms2000% group buildingA
```

Subscribers that Cannot Support Authentication

Subscribers who must never be authenticated (such as Web servers) can be configured in one of the following ways:

- Statically in the SMS2000 using the **set port** command.
- Dynamically in the OCS using a static IP address service.

All dynamic ports belong to group ***** by default. To set the group on a given dynamic port or range of ports, use the **set port** command.

Setting Maximum Users Per Port

To set the maximum number of users, per port, for the active group, use this command:

group maxusers *number*

For example, to set the maximum number of users, per port, allowed in the active group to 1, type:

```
sms2000% group maxusers 1
```

Note: This command only has an effect when port information is known through VLAN tags or SNMP.

SMS2000 Rules

The SMS2000 includes a mechanism called rules. Managers can use the rules directly to create configurations which are specific to their environment.

Most configuration attributes for the SMS2000, including traffic shaping and subscriber ID information, are applied to groups. Subscribers are assigned to these groups through rules.

> **Note:** The OCS sends dynamically created rules to the SMS2000 in order to implement configurations specified using services at a given property. The OCS in general provides the simplest mechanism to make and manage rules on the SMS2000.

Adding a Rule

Rules assign a subscriber to a given group.

> **Note:** he OCS also uses these rules to download service offering configurations to the MS2000.

To add a rule, use this command:

set rule *rule_name* [*groupname*] *priority rule_string*

For example, to provide a user called “mary” with an address from a DHCP pool, type:

```
sms2000% group add custdhcp

Active group is "custdhcp"

sms2000% auth off
sms2000% dhcp-pool custnatdhcp 123.123.123.10 123.123.123.20
255.255.255.0
sms2000% iptype DHCP
sms2000% set rule mary 1 mac=00:11:22:33:44:55
```

When “mary” connects, she is automatically placed in the “custdhcp” group based on her source MAC address and assigned a DHCP address from the specified group pool.

Deleting a Rule

To delete a configured rule, use this command:

delete rule

For example, to delete the rule named test, type:

```
sms2000% delete rule test
```

> **Note:** his command does not delete OCS created rules.

Rule Expression Components

A rule expression tells when to apply a rule. The action for the rule is always to place the ession in a group. This group is specified either by **group add** *groupname*, or **group** *goupname* for an existing group, or by including the optional group name parameter on the ommand line.
Expressions include IP addresses, subnets, MAC addresses, VLAN IDs, and SNMP nformation. These can be combined using operators such as NOT, AND, OR, and arentheses " ( )".

IP Address

Rules can include an IP address as well as an optional network mask.

`ip=`*ip_address* [,*netmask*]

Where

ip_address is a valid IP.
netmask is a valid network mask (e.g., 255.255.255.0).

For example:

ip=123.123.123.123 matches the single IP address 123.123.123.123
ip=123.123.123.0,255.255.255.0 matches any IP address from 123.123.123.1 to 123.123.123.254.

MAC Address

Rules can include a single MAC address or a MAC address with some wildcard bytes. Every Ethernet card or embedded Ethernet device has a unique MAC address. This is normally printed on the material accompanying the device. It is also available through the configuration interface in most common desktop operating systems.

`mac=`*mac_addr*|*mac_pattern*

Where
mac_addr is a MAC address written with 6 hexidecimal digits separated by colons.
mac_pattern is a partial MAC address written as 6 hexidecimal digits separated by colons, but with some hex values replaced by the "*" character.

For example:

mac=00:11:22:33:44:55 matches a unique computer/card with the MAC address 00:11:22:33:44:55.
mac=00:11:22:*:*:* matches any unique computer/card with a MAC address whose first 3 digits are 00:11:22. For example, 00:11:22:33:44:55, or 00:11:22:FF:3D:09, or 00:11:22:DE:AD:BF.

VLAN

When using a VLAN switch as a wiring solution, each VLAN effectively is treated as a "room," similar to the "snmp-info" used with Tut Systems equipment (e.g., an MDU Lite or Expresso GS/MDU Chassis).

Managers can write rules that affect one or many VLANs:

`vlan=`*vlanida*`[-`*vlanidb*`]`

Where
vlanida is a VLAN ID expressed as an integer greater than 1.
vlanidb is an optional VLAN ID expressed as an integer greater than *vlanida.*

For example:

vlan=42 matches any computer connected through a VLAN switch on a port assigned to VLAN id 42.

vlan=293-400 matches any computer connected through one or more VLAN switches on any port assigned to VLAN id 293, 294, 295 ... 398, 399, 400.

SNMP-INFO

When using an Expresso GS/MDU Chassis or MDU Lite (LR or HR) as a wiring solution, managers can write rules that apply to users based on their port, or to a set of users on a set of ports.

`tut=`*ip_address*`-`*linenum*`|*`*`-`*portnum*`|*`*`

For example:

"tut=123.123.123.123-001-001" affects any user on slot 1 line 1 of an Expresso GS/MDU Chassis or MDU Lite at IP 123.123.123.123. That device must be in the snmp-poll configuration of the SMS2000.

"tut=123.123.123.123-002-*" affects all users on slot 2 (any line) of an Expresso GS/MDU Chassis or MDU Lite at IP 123.123.123.123.

"tut=123.123.123.124-*-*" affects all users on all slots on all lines of an Expresso GS/MDU Chassis at IP 123.123.123.124.

The NOT Operator

The "NOT" operator is used to negate the subsequent expression. In other words, the rule applies if the subsequent expression is *not* true. `not` *expression*

For example:

"not mac=00:11:22:33:44:55" applies the rule so long as the MAC address of the unit is not the given address. In other words, it applies to every computer in the world but one.

The AND Operator

The "AND" operator is used to group two or more expressions of any type so that the rule applies if both the expression on the left of the "AND" and the expression on the right of the "AND" are true.

expression `AND` *expression*

For example:
"tut=123.123.123.123-001-001 AND mac=00:11:22:33:44:55" applies if a device with a MAC address of 00:11:22:33:44:55 connects on slot 1 and line 1 of the Expresso GS/MDU Chassis or MDU Lite at IP 123.123.123.123. If that device is in a different place (with the same MAC), then the rule does not apply. If a device with a different MAC connects on the given port, the rule also does not apply.

"tut=123.123.123.123-001-001 AND mac=00:11:22:33:44:55 AND ip=123.123.123.5" applies only if a device connects to slot 1, line 1 of an Expresso GS/MDU Chassis or MDU Lite at 123.123.123.123, and that device has a MAC of 00:11:22:33:44:55, and that device has an IP of 123.123.123.5. If any one of these is not true, then the rule does not apply.

The OR Operator

The "OR" operator is used to group two or more expressions so that a rule will apply if any of those expressions is true.

expression `OR` *expression*

For example:

"mac=00:11:22:33:44:55 OR ip=123.123.123.5" applies either if a device has the given MAC address or its IP address is 123.123.123.5.

Parenthesis

Managers can use parenthesis to logically group expressions to ensure the precedence of operators.
`(`*expression*`)`
`(`*expression* `OR` *expression*`)`
`(`*expression* `AND` *expression*`)`

For example:

"(tut=123.123.123.123-001-001 AND mac=00:11:22:33:44:55) OR ip=123.123.123.5" means that this rule applies if the computer is connected at the given tut location using the given MAC, or if the user is connecting (with any mac and from any location) using the given IP address.

Using Rule Priorities

Each rule has a numeric priority; the smaller the number, the greater the priority. When assigning a group to a new session, the SMS2000 first looks at all rules with priority 1. If it finds any matching rule, it stops and uses the group for that rule. If it does not find any matching rule, it goes on to rules with priority 2, and so on.

Managers can use multiple rules in conjunction with one another to provide unique service offerings. For example, a manager has a client named Geraldo in an MCU setting. He is connected through an MDU Lite on port 1. He has a web server at ip 123.123.123.5, and an e-mail server at 123.123.123.6, both of which require a static IP address with no authentication. He also has 13 employees, each of whom is running a PC with DHCP, and would like to have them receive a real IP address.

The manager can enter the following commands:

```
SMS2000% group add gerstat
Active group is "gerstat"
SMS2000% auth off
SMS2000% iptype static
SMS2000% set rule gerstat5 1 ip=123.123.123.5 and
snmp-info=123.123.123.123-001-001
SMS2000% set rule gerstat6 1 ip=123.123.123.6 and
snmp-info=123.123.123.123-001-001
SMS2000% group *
Active group is "*"
SMS2000% group add gerdhcp
Active group is "gerdhcp"
SMS2000% auth off
SMS2000% dhcp-pool gerpool 123.123.123.7 123.123.123.20
255.255.255.0
SMS2000% iptype DHCP
SMS2000% set rule gerdhcp 2 snmp-info=123.123.123.123-001-001
```

Any device that connected through 123.123.123.123-001-001 matches the "gerdhcp" rule.
However, since that rule has a priority 2, which is lower than both "gerstat5" and "gerstat6," those other rules will be checked first. Since both Geraldo's web server and e-mail server have an IP in one of those rules, they will be placed in the "gerstat" group, which has a more restrictive membership, but allows devices to have a static IP.

Chapter 11 - IP Addressing

Tut Systems' Expresso Subscriber Management System (SMS2000) and Operation Center Software (OCS) offer a complete solution for delivering and controlling Internet Protocol (IP) based services to subscribers.

The SMS2000 allows almost any type of in-building network infrastructure to be transformed into a robust public network, dramatically reducing configuration headaches, minimizing undesirable interactions between subscribers, and allowing the service provider to deliver a flexible suite of IP services over a common infrastructure.

IP Addressing

The SMS2000 operates differently from legacy networks. This section describes some of the differences.
The SMS2000 combines several functions of a router, DHCP server, firewall, and network access server, as well as new functions into an integrated platform. As a result, it is possible to create flexible and efficient configurations to deliver networking services.

The SMS2000, unlike most network devices, can treat every client attached to the subscriber side of the network as if it were on a separate LAN. The SMS2000 can do this for all types of subscriber media, including Expresso GS/MDU Chassis and associated HomeRun, LongRun or EoVDSL line cards, MDU Lite, Ethernet, VLAN Ethernet, and wireless. In fact, the SMS2000 automatically adjusts its internal routing system to accommodate clients that have a network configuration on a foreign network or a configuration that has been arbitrarily set.

Plug and Play With NAT

Figure 11-1 shows a sample configuration of plug and play with NAT; client A and client B are two separate configurations.

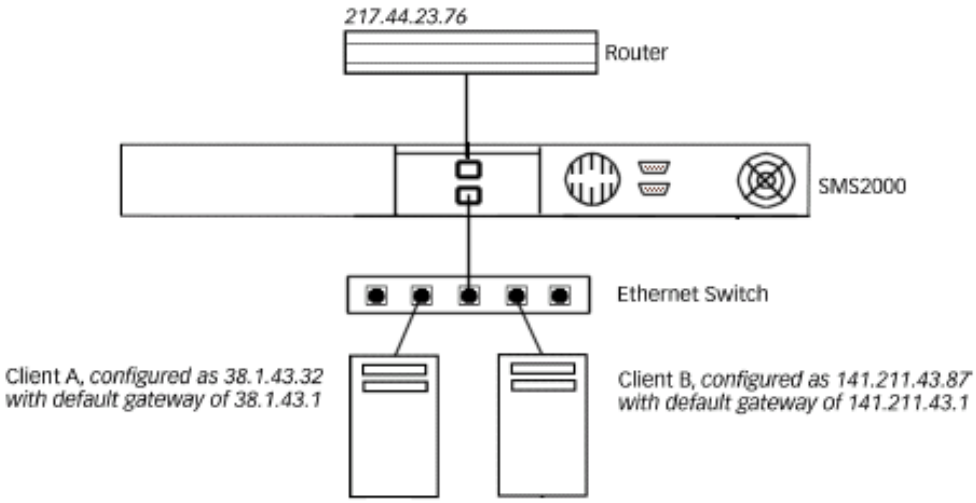

Figure 11-1 Plug and Play with NAT

Client A believes that it's IP address is 38.1.43.32 and client B believes it's IP address is 141.211.43.87. The SMS2000 will respond to each of these clients as their respective gateways, 38.1.43.1 and 141.211.43.1. By using Network Address Translation (NAT), each of these clients is actually sharing the SMS2000's network-side address of 217.44.23.76.

This capability is called "plug and play" since the SMS2000 is automatically adjusting to the client.

In the simplest configuration without RADIUS or the OCS, if a client attempts to learn its address with DHCP, the SMS2000 can respond with an arbitrary IP address. This address can be remembered and may not be given to other clients to prevent address collisions on the subscriber Ethernet side, if the subscriber media pass broadcasts between clients. The

SMS2000 always responds to client DHCP requests.
The SMS2000 can also respond with an IP address from a configured DHCP pool. If that pool is out of IP addresses, the SMS2000 will revert to using NATed addresses.

Static Routable Addresses

It is not always desirable to treat each host on the subscriber network as a client. For example, an Ethernet switch of an Expresso MDU Lite has an SNMP management agent that must be accessed outside of the subscriber network by a static routable IP address. In this case, the SMS2000 allows an administrator to set up static configurations for given IP addresses. No address translation or authentication is performed on static addresses.

> **Note:** Subscribers can get static IP address via RADIUS, SMS2000 rules, or OCS-based service provisioning.
>
> **Note:** The Static routable addresses must be in the same subnet as the SMS2000 or in a control-net.

For example,

sms2000% **group add specials**
sms2000% **iptype static**
sms2000% **set rule ip101 1 ip=192.168.0.101,255.255.255.255**

DHCP Pools

With DHCP a subscriber gets the same IP address as often as possible. The DHCP archiving feature archives past IP address assignments to track previous IP address allocations between reboots of the SMS2000.

The SMS2000 allows the network provider to specify multiple-named DHCP pools that must correspond to real addresses (i.e., not NATed). The SMS2000 then applies policies to determine which clients get addresses from which pools. The OCS can load the policy information such that, for example, a subscriber paying a lower rate gets an arbitrary address that goes through NAT while a subscriber paying a higher rate gets an address

through DHCP that corresponds to a real address from one of the SMS2000's DHCP pools.

> **Note:** Addresses in the DHCP pool must be in the same subnet as the SMS2000 or in a control-net.

For example,

sms2000% **group add dhcpers**
sms2000% **dhcp-pool mypool 192.168.0.100 192.168.0.110 255.255.255.0 lease 80**
sms2000% **iptype dhcp**
sms2000% **set rule bob 1 mac=00:01:02:03:04:05**

Static Non-Routable Addresses

A fixed address can be assigned to a subscriber. Static non-routable addresses with SMS2000 rules are configured in RADIUS or OCS. Subscribers who want to use their assigned static non-routable addresses must set their client TCP/IP configurations with the assigned addresses. If they use any other address or DHCP, they will still receive service but their traffic will go through NAT.

Table 11-1 Static Non-routable Addresses

Address Policy	NAT?	Gets Consistent IP Address?	Policy can be sent via RADIUS?	Policy can be sent via OCS?
Plug-n-Play	Yes	No	No	Yes
Static	No	Yes	No	Yes
DHCP Pools	No	Yes	No	Yes
Fixed	No	Yes	Yes	Yes
1to1	Yes	No	No	No
1to1 Unique	Yes	No	No	No

IP Multicasting

Ethernet multicast packets are translated by the SMS2000 before being sent to the subscriber ports. The SMS2000 snoops IGMP between a multicast querier, such as a multicast router or a content server, and hosts. The SMS2000 translates Ethernet multicast MAC addresses to unicast MAC addresses; multicast packets received on the network side of the SMS2000 are translated to unicast traffic on the subscriber side. Only clients participating in IGMP receive multicast content.

A querier, such as a full feature multicast router or a content server, sends IGMP queries on its local network. The SMS2000 forwards these queries (which are Ethernet broadcasts) to each of the subscribers. If the subscribers are on VLAN switches, the SMS2000 sends the query as a broadcast to each of the active VLANs. By snooping the response from subscribers, the SMS2000 tracks whether each individual client is requesting a multicast stream. If a subscriber fails to respond to three consecutive queries for a particular multicast group or if the subscriber sends an IGMP"leave," the SMS2000 stops sending the multicast content.

Configuring a Control Network for Additional Client IP Addresses

> **Note:** This command is only required when using DHCP or static IP addresses on a physical network with multiple IP subnets, and the administrator wants subscribers to be allocated DHCP or static addresses from these additional IP subnets.

To configure a control network for additional client IP addresses, use this command:

control-net [**delete**] {*ip_address* **netmask** *ip_mask* | *ip_address/masklen* |

start-address end-address ip_mask}

For example, to set a control-net network, type:

```
sms2000% control-net 192.168.20.100 192.168.20.100
255.255.255.255
```

For example, to delete a control-net network, type:

```
sms2000% control-net delete 192.168.20.100 192.168.20.100
255.255.255.255
```

Understanding 1to1 and 1to1 Unique IP Types

> **Note:** Ip types 1to1 and 1to1 unique are helpful in responding to Digital Millennium Copyright Act (DMCA) complaints regarding subscribers sharing copyrighted material illegally because they allow you to quickly isolate the specific subscriber illegally sharing the copyrighted material. However, because complaints may be filed well after a subscriber has disconnected, accounting records indicating which subscriber used which IP address at which time must be kept using either Syslog accounting, RADIUS accounting, or both.

When you configure group members for 1to1, unique addresses are assigned for each session from a pool of source-net addresses. These addresses are used to determine which session incoming packets (from the WAN) belong. The source port number of a 1to1 session is sent without port mapping to the destination.

Every subscriber uses a unique source-net address. When all of the addresses in a source-net pool are in use and additional subscribers try to connect:

- 1to1 reverts to normal NAT (port mapped).
- 1to1 unique does not allow a new session.

Configuring IP Types

To configure the IP type for members of the active/current group, use the following command:

iptype {**default** | **NAT** | **static** | **DHCP** | **1to1** | **1to1Unique**}

For example, to set the IP type to DHCP, type:

```
sms2000% iptype DHCP
```

Source-Nets

Setting a Source-Net

Note: Source nets are only used with IP types **1 to 1** and **1 to 1 unique**.

The command **set source-net** configures a source-net. A source-net is a SMS2000 configured subnet to which subscriber connections are mapped when using the 1 to 1 and 1 to 1 unique IP types. For IP types 1to1 and 1to1Unique subscribers are each given one of the available IP addresses. If there are enough source-net addresses, each subscriber is given a real address.

Note: There can be only one source-net configured for a given group.

Note: The start address must be less than or equal to the end address and should not overlap a DHCP pool address range.

Note: The OCS and SMS2000 can work together to provide non-NATed service to subscribers who are either assigned a permanent real IP address or given an address from an OCS-defined DHCP pool. This is NOT the same as the source-net feature. Use non-NATed addresses in cases where the subscriber wants to run a server (such as a Web server) or use a protocol (such as a gaming server) that is not NAT-friendly. For information on DHCP, see *"DHCP Pools" on page 70, Chapter 11.*

To add a source-net or IP address range in the real network to which client addresses are translated, use this command:

set source-net *start_address end_address subnet-mask*

For example, to have all subscribers now appear with IP addresses from the configured source-net, type:

```
sms2000% set source-net 123.123.123.10 123.123.123.100
255.255.255.128
```

Deleting a Configured Source-Net

To delete a configured source-net, use this command:

delete source-net

For example, to delete a configured source-net, type:

```
sms2000% delete source-net
```

DHCP

Creating DHCP Pools

Subscribers who use protocols that are not NAT-friendly (including some gaming servers) or who use a dynamic DNS service to act as a Web server may want to have a non-NATed real DHCP address.
Subscribers who want this service must have DHCP enabled on their local PCs. If they do not have DHCP enabled, they receive the normal NATed service and do not benefit from having a real IP address.

To create a DHCP pool, use the following command:

dhcp-pool *poolname* {*start_ip end_ip netmask*} [**lease** *mins* | **lease spec** | **delete**]

For example, to create a dhcp-pool called swim starting at 123.123.123.99 and ending at 123.123.123.136, with a subnet mask 255.255.255.0 and a duration of one day, type:

```
sms2000% dhcp-pool swim 123.123.123.99 123.123.123.136
255.255.255.0 lease 1440
```

Removing a DHCP Assignment

To remove a DHCP assignment with a specified hexadecimal MAC address, use the following command:

dhcp-server release *mac_address*

For example, to release a DHCP entry with MAC address 0001030465DB, type:

```
sms2000% dhcp-server release 0001030465DB
```

> **Note:** The MAC address is presented in the format 0001030465DB (with no separators).

DNS

Setting the DNS Server Address

DNS servers allow the SMS2000 to convert a name such as **www.tutsystems.com** to an IP address such as 208.186.133.55. You can configure multiple DNS servers by entering this command once for each server.

To specify the IP address of a DNS server and (optionally) add it for use in the active/current group, use this command:

set dns [**add**] *ip_address*

For example, to configure the SMS2000 to use 192.168.254.254 as a DNS server.

```
sms2000% set dns 192.168.254.254
```

> **Note:** Changing the DNS server(s) requires a reboot.

Deleting the DNS Server Address

To delete the DNS address for the current group, use this command:

delete dns *ip_address*

For example, to delete the DNS server with the IP address 192.168.254.42, type:

```
sms2000% delete dns 192.168.254.42
```

> **Note:** Because multiple DNS servers can be configured, you must delete each server individually.

Static Routes

Adding Routes

The SMS2000 requires local routes for locally configured interfaces. Use **set port** to add these routes.
The **set port** command can add a route while configuring the interface and setting up the port. Use the **set port** command to specify port types for all ports, set a port or a range of ports as static, dynamic, or disabled. For static ports, this command can also configure an IP address, local route, and default VLAN ID. For more information on using the **set port** command see *"Setting and Deleting Static Ports" on page 37, Chapter 4.*

Chapter 12 - Printing

The Expresso Subscriber Management System (SMS2000) offers printing capabilities.

Setting up the LPR Host

To define the printing parameters, including the name of the LPR host and the maximum number of pages and bytes allowed per job, use this command:

set lpr {*hostname* | **off**} [*queuename maxpages maxbytes*]

For example, to set the printer host to the IP address 10.228.10.233, send all printing jobs to the default queue **lp**, set the maximum number of pages to 5 and set the maximum number of bytes per job to 20,000,000, type:

```
sms2000% set lpr 10.228.10.233 5 20000000
```

Chapter 13 - Using SMS2000 with a RADIUS Server

SMS2000 can authenticate subscribers and send accounting messages using RADIUS.

Beginning with the 2.3.6 release of SMS software, many RADIUS attributes and additional features have been added.

For example:

- Add multiple RADIUS servers for fault-tolerance
- Add Alias IP addresses for clustered RADIUS Servers
- Configure retransmission, deadtime, and timeout timers
- Support RADIUS ports 1812 and 1813 for RADIUS request and accounting ports (per official RADIUS assigned ports)
- Support Session-Timeout attribute
- Support Idle-Timeout attribute
- Set the NAS type parameter

See Chapter 5 for details on using the **auth add radius** and **set nas-port-type** commands.

Configuring RADIUS

SMS2000 is designed to operate with standard RADIUS authorization and accounting services. SMS2000 contains a RADIUS client that functions as if the SMS2000 were a dial-in network access server. RADIUS authentication is an option instead of the OCS for network providers that already have RADIUS servers and databases. The RADIUS server is free software available for UNIX systems.

Obtaining the RADIUS Server Software

A variety of RADIUS servers are available. Once such server is FreeRADIUS, a RADIUS sever for the Linux operating system. More information on FreeRADIUS is available at:

http://www.freeradius.org/

Adding the SMS2000 as a Client on the RADIUS Server

For the SMS2000 to be a RADIUS client, it must have an entry in your RADIUS server's clients list. The location and format of this list is different for different RADIUS servers.

Adding Users to the RADIUS Server

RADIUS servers may include a list of specific users in a file, in a database, in an LDAP server, a remote RADIUS server, on the local system, or any combination of these. Please consult your RADIUS server documentation.

While users may have many attributes, none are required for the SMS2000. However, SMS2000 understands several optional attributes.

Configuring Service Parameters

While not required, one feature that can be configured on a per subscriber basis from the RADIUS server is service parameters. Service providers can use service parameters to limit bandwidth utilization based on the subscriber, allowing the ISP to charge different rates for different maximum bandwidths.

The SMS2000 uses "Connect-Info" (id #77) to specify the service parameters for the subscriber connection.

The format of the Connect-Info field is identical to the format of the shape command in the console interface (excluding "shape" as the first word).

```
{<xbps>[/<rbps>]
```

For example, the following RADIUS entry defines a user named "pokey" and limits his throughput to 64000 bits per second both upstream and downstream.

```
Pokey   Password = "pokey"
       Connect-Info = "64000"
```

The following example limits a user named "modemlike" to the best known speed for a 56K modem. That is 56kbps downstream and 33kbps upstream.

```
modemlike     Password = "modemlike"
       Connect-Info = "56000/33000"
```

The following user is limited to 3Mbps downstream and 1Mbps upstream:

```
Zippy          Password = "zoomzoom"
       Connect-Info = "3000000/1000000"
```

If no connect information is provided, connect information defaults to that specified for the default group (called "*" or "star"). This information can be specified at the SMS2000. If no bandwidth management is specified at the SMS2000, then users without "Connect-Info" parameters have no bandwidth limits.

Using Real IP Addresses

Subscribers can use real Internet routable IP addresses when connected to the SMS2000 and authenticated via RADIUS. The easiest way to do this is to configure the default group with the static IP type in SMS, providing an optional DHCP pool of real IP addresses available via DHCP.

If only a few users are going to connect using static IP addresses which are not configured via DHCP, while the rest of your users will be NATed, use the "Framed-IP-Addr" attribute to indicate the expected address in the user's entry.

If the subscriber's PC is configured with the given address, the SMS2000 passes traffic through directly to the subscriber once the subscriber is authenticated without using NAT. If the subscriber's PC is configured for DHCP or is configured with the wrong IP address, the SMS2000 will NAT the subscriber as normal.

For example:

```
Postel Password = "Postel"
       Framed-IP-Address = "18.181.0.29"
       Connect-Info = "3000000/1000000"
```

When Postel connects to the SMS2000, he will initially be NAT-ed and redirected to the SMS2000's RADIUS login page. After properly authenticating himself with his user name and password, the SMS2000 will check his PC's IP address against the one returned via RADIUS. If they match, the SMS2000 will pass traffic from Postel directly through itself, without using NAT. If they don't, Postel will be NATed. Also note that Postel is limited to 3Mbps upstream and 1Mbps downstream. The use of static IP addressing is independent of the quality of service parameters. They may or may not be included together in any subscriber's entry.

RADIUS Ports

The official assigned RADIUS ports are 1812 for authentication and 1813 for accounting. A typical /etc/services file shows the RADIUS ports this way:

```
radius 1812/tcp                 # radius
radius 1812/udp                 # radius

radius-acct 1813/tcp  radacct   # radius Accounting
radius-acct 1813/udp  radacct   # radius Accounting
```

SMS2.3.5 and earlier used ports 1645 and 1646. Any SMS that currently has a RADIUS server configured will retain ports 1645 and 1646 when upgrading to SMS2.3.6.

By default, any new RADIUS configuration with SMS2.3.6 will use ports 1812 and 1813, unless the systems administrator specifies another set of ports.

Any port combination can be specified when configuring RADIUS servers. See page 53, Chapter 5, for details on using the **auth add radius** command.

Check the /etc/services files on the RADIUS server and verify that the RADIUS server is set to use the same ports as the SMS.

SMS2000 NAS File

While it is not required, a NAS file is available that allows your RADIUS server to decode some custom RADIUS accounting attributes from SMS2000. Please contact your Tut Systems representative for this file.

SMS2000 Status Attributes and Statistics

RADIUS Attributes Sent in Accounting Messages

The SMS2000 sends the following attributes in Accounting-Start and Accounting-Stop records (as noted). The RADIUS server may choose to ignore any or all of these.

```
User-Name(1)
NAS-IP-Address(4)
NAS-Identifier(32)
NAS-Port-Type(61)
Tut:Client-IP-Address (1748:5) - ipaddr
Framed-IP-Address(8)
Connect-Info(77)
If unique source ports are enabled:
       Tut:Port-Low (1748:1) – ipaddr
       Tut:Port-Hi (1748:2) - ipaddr
NAS-Identifier (32)
NAS-Port(5)
Service-Type(6)
Framed-Protocol(7)
If received in Access-Accept
       Class(25)
Acct-Session-Id(44)
Acct-Status-Type(40)
Tut:Mac-Address (1780:3) - string

If an Accounting-Stop Message:
       Acct-Input-Octets(42)
       Acct-Output-Octets(43)
       Acct-Input-Packets(47)
       Acct-Output-Packets(48)
       Acct-Session-Time(46)
```

RADIUS Attributes Sent In Access-Request Packets

The SMS2000 sends the following attributes in Access-Request packets. The RADIUS server may choose to ignore any or all of these. The RADIUS server may make its access response based on any or all of these.

```
User-Name(1)
User-Password(2)
NAS-IP-Address(4)
NAS-Identifier(32)
NAS-Port(5)
Service-Type(6)
Framed-Protocol(7)
Tut:Mac-Address(1748:3)
NAS-Port-Type(61)
Tut :Client-IP-Address(1748 :5)
Framed-IP-Address(8)
```

RADIUS Attributes Received in Access-Accept Packets

See *Appendix A*, *"Radius Access-Accept Dictionary File"* for an example of how the SMS2000 uses the attributes defined in a dictionary file.

Using Both RADIUS and OCS Authentication

Because the OCS in some ways manages the SMS2000, there can be only one OCS server configured on the SMS2000, and it must be for the default group. However, a RADIUS authentication server can be added to any group, and the OCS may be on or off for various groups.

To configure both RADIUS and the OCS on one SMS2000, enter the following commands:

```
sms2000% auth off
sms2000% group add radgroup
sms2000% group *
Active group is now "*"
sms2000% auth add web http://web_ip/pp/welcome.php3 secret
web_secret cmd-serv
sms2000% acct add radius radius_ip secret radius_secret
sms2000% group radgroup
Active group is now "radgroup."
sms2000% auth add radius radius_ip secret radius_secret
sms2000% acct add radius radius_ip secret radius_secret
sms2000% set rule israd 1 rule_expression
```

Note: If your OCS is configured, you need not turn authentication off. Simply use **group add radgroup noinherit** to prevent the new group from inheriting the OCS server configuration.

Setting Traffic Shaping

The SMS2000 provides traffic shaping to limit the maximum bandwidth for a group of subscribers or a static port. The configuration parameters for traffic shaping that you set with the **shape** command apply to the active group. **xbs** is the maximum transmit rate (bits per second) from the SMS2000 to the subscriber. **rbs** is the maximum receive rate (bits per second) allowed for the subscriber.
To set traffic shaping for a group/port, use this command:

shape {*xbps*[/*rbps*]
For example, port 801 has previously been set to static. This example limits devices on port 801 to 300Kb/s downstream and 200Kb/s upstream.

```
sms2000% shape 300000/200000 port 801
```

Unless otherwise specified, all subscribers are limited to 400Kb/s both upstream and downstream.

```
sms2000% shape 400000
```

> **Note:** For more information on the shape command, including descriptions of the advanced shaping options, see the *SMS2000 Command Reference*.

Deleting Traffic Shaping

To delete traffic shaping, use this command:

shape {*xbps*[/*rbps*]} **delete**

Chapter 14 - SMS2000 and Property Management Systems (PMS)

For hotels desiring PMS billing, the SMS2000 and the OCS can be configured to send billing records to the PMS. Both SMS2000 and the OCS are involved in PMS billing. The SMS2000 is physically connected to the PMS and handles the serial port line protocol to the PMS. The OCS builds the PMS messages and forwards changes to the SMS2000 for transfer to the PMS. Only one PMS can be configured per property.
To configure the OCS for PMS billing, see the *OCS User's Guide*.

Setting the PMS Server

> **Note:** The OCS is required for PMS billing. The SMS2000 requires the OCS to store the information for mapping room name to location and to ensure accurate billing in case of PMS failures.
>
> **Note:** This command is normally not required because the OCS automatically configures the PMS server interface on the SMS2000.

While the PMS server can be fully configured through both the SMS2000 and the OCS, the OCS overwrites the SMS2000 configuration when it connects to the SMS2000. All parameters are optional since the OCS sets the parameters, but there are two circumstances that require setting one or more parameters at the SMS2000:

• When configured for PMS, the SMS2000 uses its second com port to send billing information to the PMS. To test the second SMS2000 com port without using other equipment, enter the **set pms-server** command with **mode=tty** and **tty_debug=on**. Then reboot the SMS2000. A message is printed using the serial mode you specified.

> **Note:** Before using the SMS2000 with a PMS server attached, be sure to set **tty_debug=off**.

• The **strict_timers** option is not set by the OCS. When disabled (the default), the **strict-timers** option allows the SMS2000 to ignore the responses from the PMS that are too quick based on ACK-NAK or ENQ-ACK-NAK timing requirements. If you configure **strict-timers** to **on**, the SMS2000 rejects all messages that are too quick.
However, the default selection of **Off** should be fine in all cases.

To configure the serial interface to the hotel Property Management System (PMS) server, use this command:

set pms-server
[**baud_rate**=*baud_rate*] [**data_bits**={**7** | **8**}] [**stop_bits**={**1** | **2**}] [**parity**=*value*] [**delay**=*value*] [**message_buffer_size**=*value*] [**protocol**=*value*] [**tty_debug**={**off** | **on**}] [**bcc_count**={**1** | **2**}] [**strict_timers**={**true** | **false**}] [**tty_prefix="***chars***"**] [**tty_suffix="***chars***"**] [**ack_val**=*value*] [**nak_val**=*value*] [**enq_val**=*value*] [**check_bcc**={**true** | **false**}] [**hw_flow_control**={**0** | **1**}]
For example, to disable the **tty_debug** mechanism type:

```
sms2000% set pms-server tty_debug=off
```

Note: For more information on using the **set pms-server** command, see the *SMS2000 Command Reference.*

Protocol Modes

All PMS protocols (except Micros-Fidelio) work in one of three modes:

- TTY
- ACK-NAK
- ENQ-ACK-NAK

TTY provides best effort delivery, while ACK-NAK and ENQ-ACK-NAK provide reliable message delivery.

TTY MODE

In TTY mode, message delivery is best effort only. The SMS2000 sends the message to the PMS and does not look for any response. The message contents are sent followed by a newline character.

SMS -> This is the first message\r\nThis is the second message\r\n

PMS does not reply.

- **\r** is the C program escape for CR (Carriage Return), which is ASCII code 13 (0x0D).
- **\n** is the C program escape for LR (Line Feed), which is ASCII code 10 (0x0A).
- **SMS ->** indicates that the SMS2000 sends this message. It is not a part of the message.

The message format is based on the interface type. The format is slightly different for standard HOBIC as compared to GEAC.

ACK-NAK MODE

In ACK-NAK mode, message delivery is reliable and the PMS must acknowledge receipt of the message within a specific time frame (or the SMS2000 sends it again).

SMS -> <STX>This is the first message<ETX><bcc>
PMS -> <ACK>
SMS -> <STX>This is the second message<ETX><bcc>
PMS -> <ACK>

- **<STX>** is the ASCII character STX, which is ASCII code 2 (0x02).
- **<ETX>** is the ASCII code ETX, which is ASCII code 3 (0x03).
- **<ACK>** is the ASCII code ACK, which is ASCII code 6 (0x06).
- **<bcc>** is a binary checksum character.

That character is used to validate that the message was transmitted without errors. It is calculated by adding up all of the characters in the message proceeding it (except the STX and modulo the sum by 256).
The PMS has a limited time frame in which to respond with an ACK. The PMS may also NAK the message for any reason. It is treated as a transmission error and the message is sent again. After many tries, the SMS2000 gives up on this message and log it as an error in the OCS.

Note: There is an optional second <bcc> character.

ENQ-ACK-NAK MODE

ENQ-ACK-NAK mode provides reliable message delivery. It is similar to ACK-NAK mode, but there is one additional interaction between the SMS2000 and PMS.

SMS -> <ENQ>
PMS -> <ACK>
SMS -> <STX>This is the first message<ETX><bcc>
PMS -> <ACK>
SMS -> <ENQ>
PMS -> <ACK>
SMS -> <STX>This is the second message<ETX><bcc>
PMS -> <ACK>

• <ENQ> stands for the ASCII ENQ character, ASCII code 5 (Ox05).
Again the PMS must respond in a limited time frame to the ENQ as well as the message to avoid retransmission. The PMS may NAK either the ENQ or the message.

Note: There is an optional second <bcc> character.

Chapter 15 - Customizing SMS2000 Web Authentication with RADIUS

This chapter describes how to work with and customize web pages on the SMS2000 when using RADIUS authentication. You can obtain the original web pages, for use in customizing, by contacting your Tut Systems representative, or you may extract them using a web browser.
By default, a set of web pages are created on the SMS2000 and presented to the user during authentication. These default pages can be left as is, or they can be customized for a particular property or group. The customized pages can be loaded to the SMS2000 and are presented in place of the default pages. This chapter describes:

- How to load customized pages to the SMS2000
- How to delete customized pages on the SMS2000
- How to customize pages for the SMS2000

> **Note:** When using the OCS, the entire user experience is customized through the OCS, so you should not need to customize SMS2000 web pages. Instead, all subscriber-visible web pages can be customized through the OCS administrator interface–itself a web based application. SMS2000 web pages are customized only when using the SMS2000 with a RADIUS server.

Loading and Deleting Customized Web Pages

Initially, a default directory is created which stores the default set of web pages used by the SMS2000 for authentication, as well as images and other files that make up the default web pages. The default group (*) and any other group added to the SMS2000 will use the same default set of pages for authentication. Customized pages can be loaded and used in place of the default files. New files, such as image files, new web pages, and subdirectories can also be loaded for a group.

Files For Groups

By default, the files you load are active for the default group, also called "*" (pronounced "star"). If you are using a VLAN switch and would like to present different customized web pages to different groups, you must associate ports with groups, and change the default group using the **set group** command before loading the web pages. For more information on groups, please see *Chapter 10, "Service Creation using Groups and Rules."*

Loading Web Pages or Files

After customizing the authentication files, they must be loaded to the SMS2000 using the **load web** command. This loads a specific web page (html file) or image (.gif, .jpg, or .png) file from an external web or ftp server which you specify.

If the modified page you are loading is the first customized page for a group, a new directory is created to store this and other modified files. This directory is automatically given the same name as the active group. There is no need to reboot the SMS2000. When a new subscriber connects, the subscriber sees the new web page.

> **Note:** SMS2000-based web page customization can only be done using SMS2000 with a RADIUS authentication server.

To load a specified web page from a remote server, specifying a local or remote server name, use this command:

load web {*url* | **defaults**}

For example, to load the customized version of the authentication file for the active group from the server 192.168.254.249, type:

```
sms2000% load web http://192.168.254.249/authfile.html
```

> **Note:** The command **load web** immediately changes the web pages for the active group.

Path Components

Path components are important when specifying the URL for use with the **load web** command. On most web servers there exists a DOCUMENT_ROOT directory where web page(s) are normally stored. If you are attempting to load a web page that exists in the DOCUMENT_ROOT directory, include the IP address of the server and the name of the file you want to load.
For example, to load a modified version of the authfile.html file which resides in the DOCUMENT_ROOT directory of a server with the IP address 192.168.254.249, type:

```
sms2000% load web http://192.168.254.249/authfile.html
```

If the page you are attempting to load is in a directory other than the root directory you must include the full path to the directory and also the name of the local file.

For example, to load a modified version of the authfile.html file which resides in the /somedir directory of a server with the IP address 192.168.254.249, type:

```
sms2000% load web http://192.168.254.249/somedir/authfile.html
authfile.html
```

> **Note:** Loading pages from a directory other that the DOCUMENT_ROOT directory is not recommended.

> **Note:** Apache is a free web server available for all versions of Windows 95 or later, Mac OS-X, and Linux. It can be downloaded from http://www.apache.org/

Image Links

The default web pages contain links to the images that make up the pages. These links specify a relative path to the images, for example <img src="myfile.gif">, meaning that

the location of the image is relative towhere the file is located. Since the default pages and their images reside in the same directory, the default pages load with no problem.

When customizing web pages absolute paths to images such as <img src="http://www.tutsys.com/logo.gif"> can also be specified in the customized pages. These absolute paths contain the full path to the image.

For example, given the absolute image path above, the SMS2000 would look for the logo.gif file at the www.tutsys.com site. In that instance, an allow-net must be added to that site, so that the unauthenticated subscriber can view the image.

It is important to remember how the image links are specified when customizing web pages, since the pages will not be placed into the default directory when they are reloaded. Instead they are placed in a separate directory which is created when the first customized page is loaded for the active group.

For example, if a group called CUSTNAT is added to the SMS2000, and a customized web page is loaded for this group, a directory named CUSTNAT will be automatically created to hold customized web pages and images for this group.

If any of the original links to the images are left in the customized pages they will be broken since they are relative links and the images they link to are still located in the default directory. To fix this, the images specified by the links must also be reloaded.

> **Note:** To avoid broken links it is important to keep IMG and HREF tags consistent on the SMS2000

Upgrading

Customized web pages are kept in a separate location from Tut Systems' original web pages, so your web pages are not affected by upgrades. However, major upgrades may include new web pages which you may wish to modify.

Deleting Web Pages or Files

To delete non-default web pages for the active group, use this command:

delete web *local_name*

For example, to remove the modified version of the authfile.html file so that subscribers view the default authfile.html page, type:

```
sms2000% delete web authfile.html
```

Customizing Web Pages

Preserving the Web Form

The default "authfile.html" contains a web form including:

```
<FORM NAME="PPAuth" ACTION="PP-Authenticate" METHOD=POST>
<INPUT TYPE=TEXT NAME="userid" SIZE=20 MAXSIZE=255 VALUE="">
<INPUT TYPE=PASSWORD NAME="pw" SIZE=20 MAXSIZE=255 VALUE="">
<INPUT TYPE="Submit" NAME="Login" VALUE="Login">
</FORM>
```

While these elements can be presented in any manner you choose, they must exist for the SMS2000 to properly parse the login form.

> **Note:** It is possible to prevent unauthorized subscribers from gaining network access without an authentication server. Configure the authfile.html without the form for the default group and point the SMS2000 to a bogus RADIUS server. Then use groups and rules to assign authorized subscribers to the other groups without authentication.

Size For Web Pages and External Links

Tut Systems recommends that you use no more than 500K for all of customized web pages, including text, graphics, javascript, and Java. However, if this is too restrictive, you can place images on an external server. You must include an allow-net for that server.

For example, given a web server 192.168.254.249 on which the file corplogo.jpg exists in the DOCUMENT_ROOT directory, you can use the following URL in all of your customized web pages:

```
<IMG SRC="http://192.168.254.249/corplogo.jpg">
```

Use the following if you run the allow-net command:

```
sms2000% set allow-net 192.168.254.249 255.255.255.255
```

Warning This allows unauthenticated users full access to the web server specified.

You can also provide limited access to any other servers using the allow-net feature, including your corporate server and affiliates such as local merchants. By providing links on the authfile.html page to those servers, subscribers can access them without paying.

Web Page Redirection

If you would like subscribers to be redirected to your corporate page or portal after authenticating, you can replace “authok.html” with a web page using META HTTP-EQUIV in the header.

The following page redirects a subscriber to the Tut Systems home page after authenticating:

```
<HTML>
<HEAD>
<TITLE>URL Redirection</TITLE>
<META HTTP-EQUIV="refresh"
content="1;URL=http://www.tutsys.com/">
</HEAD>
<BODY>
```

```
<!-- Netscape "HTML Tag Reference" at the URL: >
<!--
http://developer.netscape.com/docs/manuals/htmlguid/index.htm >
<!-- contains information on the META tag, and its use for
redirection >
<!-- Click on "META" in the index for more information. >
You will now be redirected to the URL <B><A
HREF="http://www.tutsys.com/">
www.tutsys.com</A>
</BODY>
</HTML>
```

You are welcome to use this page when customizing your SMS2000.

Active Page Components

The SMS2000 has support for some limited active HTML components which are parsed and replaced before your web page is served. Some components should be used in pairs.

For example, a page component “foo” should be used in the following way:

```
<$ foo> This text and link may not appear! <a
href="www.this.modified.by.active.com">may not be here</a><$
/foo>
```

These include:

- ppauth - Include text between tags only if user is authenticated.
- ppnoauth - Include text between tags only if user is not authenticated.

Some components should be used by themselves. For example, a page component “bar” should be used in the following way:

```
The server will update the next word: <$ bar><br>
Did you see it?<br>
```

These include:

- ppalias - Replace with device alias (address information)
- ppport - Replace with device index
- ppgroupname - Replace with group name
- pporigurl - Replace with subscribers original URL
- pptimeleft - Replace with subscribers time left

Viewing Customizations

The **show web** command shows the customized web pages for each group:

```
sms2000% show web
```

For more information on the show web command, see the *SMS2000 Command Reference*.

Chapter 16 - Configuring Web Proxy Settings

This chapter describes how to configure web proxy settings.

Web Proxy Settings

Setting the WPAD CURL

The SMS2000 supports DNS based web proxy auto discovery. The wpad.dat file must ensure that the subscriber does not use the proxy when communicating with the SMS2000 or the OCS.

> **Note:** The proxy server must not be in any allow-net, or the subscriber will have access to every server to which the proxy server will proxy (normally most of the Internet).

Servers for which an allow-net entry exists, but which can only be contacted through the proxy server, will be unreachable unless subscribers have total access to the proxy server. To implement a "wall garden" or "allow-nets" for a network requires that the subscribers connect to those locations via the proxy server, it is possible to supply a different wpad.dat proxy configuration file for each group, pointing the "walled" group to a more restrictive proxy server. Contact Tut Systems for more information.

To configure the web proxy auto discovery configuration URL (CURL) for subscribers in the current group, use this command:

set wpad-curl [**off** | **on** | **on** *curl*]

This example loads the wpad.dat file onto the SMS2000 from the OCS server at IP address 10.228.10.233, then enables the wpad support.

```
sms2000% load web http://10.228.10.233/wpad.dat
sms2000% set wpad-curl on
```

Setting the WPAD Timeout

Internet Explorer will not refresh the wpad.dat file while running. Once closed and opened, it will correctly refresh a wpad.dat file if the previously cached file was timed out.

Note: Subscribers can manually remove a wpad.dat when using Windows 2000/NT by removing the following file:
C:\WINNT\Temporary Internet Files\wpad.dat

The file all versions of Windows should be named similarly.

To configure the time period for which a wpad.dat file sent to a subscriber is valid, use this command:

set wpad-timeout *seconds*

For example, to set the timeout to 800 seconds, type:

```
sms2000% set wpad-timeout 800
```

Web Proxy Server

Enable Proxy Server Support

When enabled, the SMS2000 will autodetect proxy servers configured on subscribers. A subscriber may have a proxy server configured with any IP address, but the TCP port on which her proxy server is configured must be included in the set of ports configured on the SMS by the **set proxy-ports** command.

To enable proxy server support, use this command:

set proxy-server on

For example to enable proxy server support, type:

```
sms2000% set proxy-server on
```

Note: Changing the proxy server status requires a reboot.

Disable Proxy Server Support

To disable proxy server support, use this command:

set proxy-server off

For example to disable proxy server support, type:

```
sms2000% set proxy-server off
```

Note: Changing the proxy server status requires a reboot.

Viewing Proxy Server Support Status

To view proxy server support status, use this command:

show proxy-server

For example to show the status of proxy server support, type:

```
sms2000% show proxy-server
```

Adding TCP Proxy Ports

The SMS2000 automatically listens for proxy server connections on port 80 when the proxy server is enabled. The **set proxy-ports** command will add the ports specified to the set of ports already configured, but will not delete members of the set of ports previously configured.

To add TCP ports to the set of TCP ports on which the SMS2000 listens for subscriber proxy connections, use this command:

set proxy-ports [port]*

For example, to add two ports to the set of TCP ports on which the SMS2000 listens for proxy server connections, type:

```
sms2000% set proxy-ports 8080 3129
```

Deleting TCP Proxy Ports

To delete TCP ports from the set of TCP ports on which the SMS2000 listens for subscriber proxy connections, use this command:

delete proxy-ports [port]*

For example, to delete two ports from the set of TCP ports on which the SMS2000 listens for proxy server connections, type:

```
sms2000% set proxy-ports 8080 3129
```

Viewing TCP Proxy Ports

To display the set of TCP ports on which the SMS2000 listens for subscriber proxy connections, use this command:

show proxy-ports

For example, to display the TCP proxy ports, type:

```
sms2000% show proxy-ports
```

Chapter 17 - SMS2000 Troubleshooting

SMS2000 Troubleshooting Procedures

Table 17-3 provides valuable information for troubleshooting the SMS2000.

Table 17-3 SMS2000 Troubleshooting Procedures

Problem Area	Commands	What to Look for
Network Connection: If communication problems exist between SMS2000 and the outside world (through the on-site router), verify the cabling is correct between the SMS2000 and the router. Afterwards, diagnose the physical layer, IP configuration, and routing tables.	**ping** *router address*	Look for any packets returned.
	show status ifconfig	Check for non-zero packets being sent or received on eth0 (network port).
	Verify that physical connectivity is good	Look for green lights on intermediate switch. Swap Ethernet cables with known good cable.
	ping *external address*	Verify that the routing table in the router is good
	traceroute *external address*	Determine location of the bad route
Subscriber Connection: If subscribers cannot get IP addresses or Web pages, first verify a physical connection exists. Can any other subscriber get access? Is the SMS2000 receiving packets on the subscriber port? Verify that the physical cabling is correct. Bypass the wiring system by attaching a PC directly to the SMS2000 subscriber port (use x-cable) and seeing if it works		When a subscriber PC is directly connected via x-over Ethernet cable to the subscriber interface of the SMS2000, the front panel LEDs will light on the Subscriber side of the LED panel.
	Show status ifconfig	Check for non-zero packets being sent or received on eth1 (subscriber port).
	From the PC, type **arp a**	. See if there are any entries in the ARP cache for the PC. There should be “35.x.x.x” if physical connectivity is good.

Problem Area	Commands	What to Look for
	From connecting equipment (such as Tut Expresso GS/MDU Chassis), verify that packets are being sent and received.	Check the **W** (mux statistics) or the **S** from the Expresso Management. Look for packets and bytes on a line. Received packets on a line card are packets from the subscriber. Transmit packets on the line card are packets sent to the PC from the router.
	Connect a PC directly to the subscriber port on the SMS2000 using a crossover cable.	See if any packets are received by the SMS2000 or PC. Type "arp a" on the PC.
	If using RADIUS, you can verify that it is operational by using the **auth test** command.	Verify that the connection to the RADIUS server is accurately configured on both ends (there is an entry in the RADIUS database for the SMS2000 client).
SNMP Polling When you **show status** for a user with Tut wiring, there should be a line for `snmp-info=`*nnn.nnn.nnn.nnn-xxx-xxx*. If this is missing, you must configure snmp-poll in the SMS2000. If it is there but the value is "unknown," the Tut system is not responding to the SMS2000 for the device's MAC address.	Verify in Expresso that SNMP is enabled and there is a community name of "public" with read access of 0.0.0.0.	
Multiple frames opened in browser Each IP address a subscriber can access before they are authorized for Internet access must be configured in the allow-net in the SMS2000. Otherwise, they are redirected to the OCS Welcome page in each sub-frame	Verify that `allow-net` for information page and the OCS are configured okay.	
Unable to do credit card billing If using credit card billing with WebLink, you must make sure that the server at authorize.net is in the allow-net since the subscriber gets redirected there. Enter the IP Address and the DNS Name of authorize.net in the allow-net	Verify that `allow-net` for secure.authorize.net is configured. Verify that a DNS allow-net for authorize.net is configured	

Problem Area	Commands	What to Look for
Verify OCS screens off-line It is possible to reproduce the subscriber experience from any Web browser. This allows the custom screens from the OCS to be tested prior to deploying at a hotel	Open browser with URL: http:<ocsipaddress>/pp/welcome.php3?host=<smshostname>&port=<portid>&seq=1234&sig=1234	Verify that the screens are good.

Appendix A - RADIUS Access-Accept Dictionary File

RADIUS Attributes in Access-Accept Packets

The SMS2000 uses the attributes defined in the following dictionary file:

```
#
#
#RADIUS
#Remote Authentication Dial In User Service
#
#Livingston Enterprises, Inc.
#6920 Koll Center Parkway
#Pleasanton, CA 94566
#
#Copyright 1992 Livingston Enterprises, Inc.
#
#Permission to use, copy, modify, and distribute this
#software for any purpose and without fee is hereby
#granted, provided that this copyright and permission
#notice appear on all copies and supporting documentation,
#the name of Livingston Enterprises, Inc. not be used in
#advertising or publicity pertaining to distribution of the
#program without specific prior permission, and notice be
#given in supporting documentation that copying and
#distribution is by permission of Livingston Enterprises,
#Inc.
#
#Livingston Enterprises, Inc. makes no representations
#about the suitability of this software for any purpose. It
#is provided "as is" without express or implied warranty.
#
#
#This file contains dictionary translations for parsing
#requests and generating responses. All transactions are
#composed of Attribute/Value Pairs. The value of each
#attribute is specified as one of four data types. Valid
#data types are:
#
#string - 0-253 octets
#ipaddr - 4 octets in network byte order
#integer - 32 bit value in big endian order (high byte
#first)
#date - 32 bit value in big endian order - seconds since
#00:00:00 GMT, Jan. 1, 1970
#
#Enumerated values are stored in the users file with
#dictionary
#VALUE translations for easy administration.
#
#Example:
#
#ATTRIBUTE VALUE
#--------------- -----
#Framed-Protocol = PPP
```

```
#7= 1(integer encoding)
#
ATTRIBUTEUser-Name1string # comment
ATTRIBUTEUser-Password2string
ATTRIBUTECHAP-Password3string
ATTRIBUTENAS-IP-Address4ipaddr
ATTRIBUTENAS-Port5integer
ATTRIBUTEService-Type6integer
ATTRIBUTEFramed-Protocol7integer
ATTRIBUTEFramed-IP-Address8ipaddr
ATTRIBUTEFramed-IP-Netmask9ipaddr
ATTRIBUTEFramed-Routing10integer
ATTRIBUTEFilter-Id11string
ATTRIBUTEFramed-MTU12integer
ATTRIBUTEFramed-Compression13integer
ATTRIBUTELogin-IP-Host14ipaddr
ATTRIBUTELogin-Service15integer
ATTRIBUTELogin-TCP-Port16integer
ATTRIBUTEReply-Message18string
ATTRIBUTECallback-Number19string
ATTRIBUTECallback-Id20string
ATTRIBUTEFramed-Route22string
ATTRIBUTEFramed-IPX-Network23integer
ATTRIBUTEState24string
ATTRIBUTEClass25string
ATTRIBUTEVendor-Specific26string ### Send as needed
ATTRIBUTESession-Timeout27integer
ATTRIBUTEIdle-Timeout28integer
ATTRIBUTETermination-Action29integer
ATTRIBUTECalled-Station-Id30string
ATTRIBUTECalling-Station-Id31string
ATTRIBUTENAS-Identifier32string
ATTRIBUTEProxy-State33string
ATTRIBUTELogin-LAT-Service34string
ATTRIBUTELogin-LAT-Node 35string
ATTRIBUTELogin-LAT-Group36string
ATTRIBUTEFramed-AppleTalk-Link37integer
ATTRIBUTEFramed-AppleTalk-Network38integer
ATTRIBUTEFramed-AppleTalk-Zone39string
ATTRIBUTECHAP-Challenge60string
ATTRIBUTENAS-Port-Type61integer
ATTRIBUTEPort-Limit62integer
ATTRIBUTELogin-LAT-Port63string
ATTRIBUTEPrompt64integer
ATTRIBUTEConnect-Info77string
#
#Accounting Extensions
#
ATTRIBUTEAcct-Status-Type40integer
ATTRIBUTEAcct-Delay-Time41integer
ATTRIBUTEAcct-Input-Octets42integer
ATTRIBUTEAcct-Output-Octets43integer
ATTRIBUTEAcct-Session-Id44string
ATTRIBUTEAcct-Authentic45integer
ATTRIBUTEAcct-Session-Time46integer
ATTRIBUTEAcct-Input-Packets47integer
ATTRIBUTEAcct-Output-Packets48integer
ATTRIBUTEAcct-Terminate-Cause49integer
ATTRIBUTEAcct-Multi-Session-Id50string
ATTRIBUTEAcct-Link-Count51integer
#
#Integer Translations
#
#Service Types
```

```
VALUEService-TypeLogin1
VALUEService-TypeFramed2
VALUEService-TypeCallback-Login3
VALUEService-TypeCallback-Framed4
VALUEService-TypeOutbound5
VALUEService-TypeAdministrative6
VALUEService-TypeNAS-Prompt7
VALUEService-TypeAuthenticate-Only8
VALUEService-TypeCallback-NAS-Prompt9
#Framed Protocols
VALUEFramed-ProtocolPPP1
VALUEFramed-ProtocolSLIP2
VALUEFramed-ProtocolARA3
VALUEFramed-ProtocolGandalf4
VALUEFramed-ProtocolXylogics5
#Framed Routing Values
VALUEFramed-RoutingNone0
VALUEFramed-RoutingBroadcast1
VALUEFramed-RoutingListen2
VALUEFramed-RoutingBroadcast-Listen3
#Framed Compression Types
VALUEFramed-CompressionNone0
VALUEFramed-CompressionVan-Jacobson-TCP-IP1
VALUEFramed-CompressionIPX-Header-Compression2
#Login Services
VALUELogin-ServiceTelnet0
VALUELogin-ServiceRlogin1
VALUELogin-ServiceTCP-Clear2
VALUELogin-ServicePortMaster3
VALUELogin-ServiceLAT4
#Accounting Status Types
VALUEAcct-Status-TypeStart1
VALUEAcct-Status-TypeStop2
VALUEAcct-Status-TypeAccounting-On7
VALUEAcct-Status-TypeAccounting-Off8
#Accounting Termination Cause
VALUEAcct-Terminate-CauseUser-Request1
VALUEAcct-Terminate-CauseLost-Carrier2
VALUEAcct-Terminate-CauseLost-Service3
VALUEAcct-Terminate-CauseIdle-Timeout4
VALUEAcct-Terminate-CauseSession-Timeout5
VALUEAcct-Terminate-CauseAdmin-Reset6
VALUEAcct-Terminate-CauseAdmin-Reboot7
VALUEAcct-Terminate-CausePort-Error8
VALUEAcct-Terminate-CauseNAS-Error9
VALUEAcct-Terminate-CauseNAS-Request10
VALUEAcct-Terminate-CauseNAS-Reboot11
VALUEAcct-Terminate-CausePort-Unneeded12
VALUEAcct-Terminate-CausePort-Preempted13
VALUEAcct-Terminate-CausePort-Suspended14
VALUEAcct-Terminate-CauseService-Unavailable15
VALUEAcct-Terminate-CauseCallback16
VALUEAcct-Terminate-CauseUser-Error17
VALUEAcct-Terminate-CauseHost-Request18
#NAS Port Types
VALUENAS-Port-TypeAsync0
VALUENAS-Port-TypeSync1
VALUENAS-Port-TypeISDN-Sync2
VALUENAS-Port-TypeISDN-Async-v1203
VALUENAS-Port-TypeISDN-Async-v1104
VALUENAS-Port-TypeVirtual5
#Accounting Authentic Values
VALUEAcct-AuthenticNone0
VALUEAcct-AuthenticRADIUS1
```

```
VALUEAcct-AuthenticLocal2
#Framed-IP-Address
VALUEFramed-IP-AddressAssigned255.255.255.255
#Prompt Values
VALUEPromptNo-Echo0
VALUEPromptEcho1
#
#Tut Vendor Specific Attrs.   (Vendor ID 1748)
ATTRIBUTE Tut:Port-Range-Lo       1 integer
ATTRIBUTE Tut:Port-Range-Hi       2 integer
ATTRIBUTE Tut:Mac-Address         3 string
ATTRIBUTE Tut:Configuration-Group 4 string
ATTRIBUTE Tut:Client-IP-Address   5 ipaddr
```

Appendix B - Technical Assistance and Customer Support

Technical Support

Tut Systems offers a comprehensive range of customer support services, including training, technical assistance, installation, and maintenance agreements. For further information and pricing on Tut Systems' service products, see your sales representative.

Internet

You can find answers to the most common functionality, installation, and configuration questions on the Tut Systems website at http://www.tutsystems.com.

Telephone

If you are unable to resolve a question or problem or believe you have defective equipment, contact Tut Systems for customer support, as described in your warranty/support agreement.

United States and **Canada**:
Toll-free: (800) 998-4888, press 2.

International Customers:
Toll based: (925) 460-3900, press 2.

Equipment Return and Repair

If Customer Support instructs you to return a unit for further testing or repair, they will give you directions on how and where to return the equipment.

To return a unit to Tut Systems for testing or repair:

- Call Customer Support and request a return merchandise authorization (RMA) number.

- Write the RMA number on the shipping box.
- Ship the equipment to the address given you by Customer Support.

Note: Do not return products to Tut Systems without first obtaining an RMA number. Units received without proper authorization will be returned to the sender.

Appendix C - SMS2000 Limited Warranty

Hardware Limited Warranty

This Tut Systems product is warranted against defects in material and workmanship and will substantially conform to Tut Systems product documentation for a period of one (1) year from the date of shipment.

Tut Systems will, at its option, either repair or replace products that prove to be defective. For warranty or repair, return this product to a service facility designated by the reseller in accordance with reseller instructions, which such instructions shall be in accordance with those set forth in Tut Systems Standard Terms and Conditions of Sale.

Limitations of Warranty

The foregoing warranty shall not apply to defects resulting from abuse, neglect by Buyer, improper installation or application by Buyer, Buyer-supplied software or interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, acts of God, or improper site preparation or maintenance.

Note: No other warranty is expressed or implied by statute or otherwise, regarding the product, including their fitness for any purpose, their quality, their merchantability, non-infringement or otherwise.

Exclusive Remedies

The remedies provided herein are the buyer's sole and exclusive remedies. Tut Systems shall not be liable for any direct, indirect, special, incidental, or consequential damages, whether based upon contract, tort, or any other legal theory.Warranties apply only to original purchaser or end-user and cannot be assigned or transferred to subsequent parties.

Assistance

For assistance, contact your nearest representative.

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a computing device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- The equipment and the receiver should be connected to outlets on separate circuits.
- Consult the dealer or an experienced radio/television technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Electrical Safety Advisory

We recommend the installation of an AC surge arrestor in the AC outlet to which this equipment is connected. Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources.

Tut Systems, Inc., Customer Service Department

Tut Systems, Inc.
5200 Franklin Drive Suite 100
Pleasanton, CA 94588

United States and Canada:
Toll Free: (800) 998-4888. Press option 2.

International Customers:
Toll based: (925) 460-3900, press 2.

The information contained in this publication is the latest available. However, Tut Systems reserves the right to change specifications of hardware and software without

prior notice. Purchasers of Tut Systems' products should make their own evaluation to determine the suitability of each product for their specific application. Tut Systems' obligations regarding the use or application of its products shall be limited to those commitments to the purchaser set forth in its Standard Terms and Conditions of Sale for a delivered product.