CHAPTER 2

# Managing Access and Users

**Revised: July 21, 2009, OL-4495-10**

## Introduction

This chapter describes the operator interfaces used for communication with the Cisco BTS 10200 Softswitch, and the procedures for managing access and users.

**Note** After entering any of the commands in this chapter, press the Return or Enter key.

Figure 2-1 illustrates the Cisco BTS 10200 Softswitch operator interfaces of the Element Management System (EMS). These interfaces support several types of communications:

- Local Operations Console—the following options are available:
  - Interactive CLI session—operator connects to the EMS using Secure Shell (SSH) and uses the command line interface (CLI) in an interactive session
  - Bulk Provisioning—operator connects to the EMS using FTP for batch-mode provisioning (requires highest privilege levels)

  SFTP is used as of Release 4.1. The /opt/ems/ftp/deposit directory checks for files every 7 seconds and then deletes them. A report is generated and can be viewed at *https://<ems ip>* (see the HTML file listed in the reports index). You can move the files to a deposit directory. The file must be owned by a valid Cisco BTS 10200 user (such as optiuser or btsadmin). If you are logged in as root, you must use the command **unix -p** when putting the file in the deposit directory.

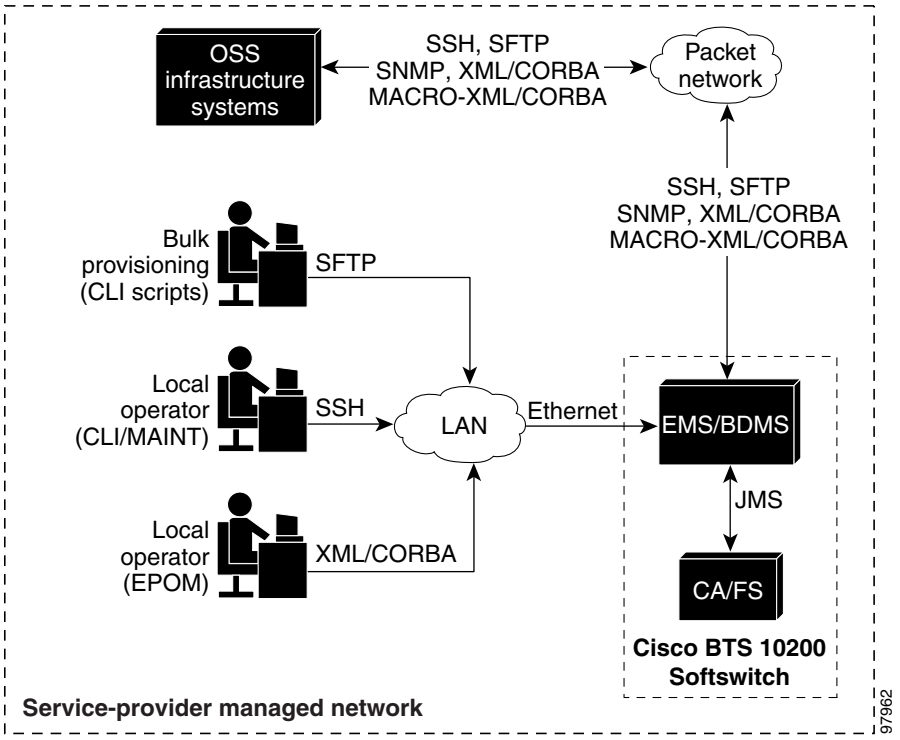
  **Note** See the *Cisco BTS 10200 Softswitch Provisioning Guide* for Bulk Provisioning information.

- Network Management System—provides events, alarms, thresholds and traffic monitoring management commands into the EMS using SNMP
- CORBA Client—provides events, alarms, thresholds and traffic monitoring management commands into the EMS via Common Object Request Broker Architecture (CORBA)

The EMS database holds up to 100 operator logins, and up to 50 user sessions can be active at any time.

The EMS interfaces internally with the Call Agent (CA) and Feature Server (FS) using the Java Message Service (JMS) protocol over IP Protocol.

*Figure 2-1 Operator Interfaces (Billing interfaces also shown)*




# System Administrator Access

When logging in for the first time, log in as **btsadmin** (the default password is **btsadmin**). You must change the password when you take possession of the system.

## Logging into the EMS Using CLI

SSH is a way to access the BTS CLI or maintenance (MAINT) modes. SSH provides encrypted communication between a remote machine and the EMS/CA for executing CLI or MAINT commands. The SSH server runs on EMSs and CAs. To connect the client and server sides run the secure shell daemon (SSHD). With SSH, new users must enter a new password and reenter that password during the first login. In future logins they are prompted once for a password only.

When logging in for the first time, system administrators log in as **`btsadmin`** (the default password is **`btsadmin`**). Change the password.

**Step 1** To log in from the client side for the first time: **`ssh btsadmin@<ipaddress>`**.

**Note** If you are logged in to the system as **`root`**, enter: **`btsadmin@0`**

On the first SSH login from the client side, expect a message like this:

```
The authenticity of host [hostname] can't be established.
Key fingerprint is 1024 5f:a0:0b:65:d3:82:df:ab:42:62:6d:98:9c:fe:e9:52.
Are you sure you want to continue connecting (yes/no)?
```

**Step 2** Enter **yes**.

The password prompt appears, now all communications are encrypted.

**Step 3** Enter your password.

The system responds with a CLI> prompt. You can now send commands to the EMS.

**Step 4** Enter provisioning commands.

**Step 5** To log off, enter **exit** .

# Managing Users

You must have a user privilege level of 9 or higher to add, show, change, or delete a user.

**Caution** Do not add, change, or delete username ***root***, this prevents proper EMS access.

*Table 2-1 Managing Users*

| Task | Sample Command |
|---|---|
| Adding a user | 1. **add user name=UserABC; command-level=9; warn=10; days-valid=30; workgroups=somegroup;**<br>2. Supply a default password: **reset password name=<user name>; new-password=<user password>;** |
| Viewing a user | **show user name=UserABC;** |
| Viewing user activity | **show ems;** |
| Changing a user | **change user name=UserABC; command-level=1; workgroups=some-group;** |
| Deleting a user | **delete user name=UserABC;**<br>You cannot delete ***optiuser***. |

*Table 2-1 Managing Users (continued)*

| Task | Sample Command |
|---|---|
| Changing a user's password | **reset password name=username; days-valid=<number of days the new password will be valid>; warn=<number of days before password expiration to warn user>;**<br><br>**reset password name=username; days-valid=30; warn=4;**<br><br>A password must:<br>• Have 6-8 characters<br>• Have at least two alphabetic characters<br>• Have at least one numeric or special character<br>• Differ from the user's login name and any combination of the login name<br>• Differ from the old password by at least three characters<br>Change the password for user ***optiuser*** on each BTS. |
| Adding a new work-group | **change command-table noun=mgw; verb=add; work-groups=latex;** |
| Adding a user to a work-group | **change user name=trs80nut; work-groups=+rubber;** |
| Removing a user from a work-group | **change user name=trs80nut; work-groups=-latex;** |
| Viewing all currently active users | **show session** |
| Viewing an active user | **show session terminal** |

*Table 2-1 Managing Users (continued)*

| Task | Sample Command |
|---|---|
| Blocking an active user | 1. Select operation mode:<br>• MAINTENANCE—(default) for regular maintenance<br>• UPGRADE—for upgrades<br>2. **`block session terminal=USR16;`**<br>**Note** You cannot block the session of a user with higher privileges than yours.<br>Prevent BTS provisioning during an upgrade or maintenance window from the following interfaces:<br>• CLI<br>• FTP<br>• CORBA<br>• SNMP<br>**Note** The software will support blocking HTTP interfaces in a future release.<br>If you block provisioning before performing an SMG restart or EMS reboot, blocking is still enforced when these applications return to in-service state.<br>There are two levels of blocking:<br>• PROVISION—Prevents all provisioning commands from executing<br>• COMPLETE—Prevents all commands from executing<br>Only terminal type MNT users can use these blocking and unblocking commands. MNT users are never blocked. MNT users issue these commands from either active or standby EMS.<br>A blocking command applies to all non-MNT users on terminals on either active or standby EMS. Commands do not execute for:<br>• Logged-in users<br>• Users who login after the block command<br>Commands are not queued for execution after unblock. The CLI user prompt changes when blocked, notifying the user their commands will not execute. |
| Unblocking a user | **`unblock session terminal=USR16;`**<br>**Note** You cannot unblock the session of a user with higher privileges. |
| Resetting a user's idle time | Idle time is how many minutes (1-30) a user can be idle before being logged off the BTS.<br>**`change session idle-time=30;`** |
| Stopping a user's session | **`stop session terminal=USR16;`** |

# Managing Commands

Each command (verb-noun combination) has a security class of 1-10; 1 is lowest, 10 is highest. Each time a user enters a command, the system compares the user's privilege level to the command's security class. EMS denies the command if the user level is less than the command level.

The Command Level (command-level) table shows the 10 command security classes. BTS has the following presets:

- 1 (lowest level)
- 5 (mid-level)
- 10 (highest level)—These commands require a system administrator with a security level of 10 to execute.

*Table 2-2 Managing Commands*

| Task | Sample Command |
|---|---|
| Viewing a command's security class | `show command-level id=10;` |
| Adding a description to a command's security class | `change command-level id=10; description=This is the highest level administration access;` |
| Changing a command's privilege level | `change command-table noun=mgw; verb=add; sec-lev-el=9;` |
| Resetting a command's privilege level | `reset command-table noun=mgw; verb=add;` |
| Viewing all executed commands | `show history;` |
| Sending all executed commands to a report file | `report history;` |
| Viewing the report of all executed commands | 1. In a web browser enter http://server name.<br>2. Click Reports.<br>3. Click *history.html*. |
| Viewing a security summary | `report security-summary start-time=2002-09-26 00:00:00; end-time=2002-09-27 00:00:00; source=all;` |
| Viewing security summary reports | In a web browser enter https:// <ems ip addr>. |