This chapter provides the Authentication, Authorization and Accounting (AAA) extensions to the Cisco BTS 10200 Softswitch. These extensions represent modifications to the current scheme of user account management on the system. It includes support for the following two protocols; these protocols are not required to be mutually inclusive.

- Radius Protocol
- Lightweight Directory Access Protocol (LDAP)

Prior to Release 4.4, user account management for the Cisco BTS 10200 Softswitch used the standard Solaris password management facilities without the use of the Authentication Dial-In User Service Network Information Service (NIS). All accounts are stored locally and referenced locally. This security feature begins support for a complete AAA model for user account management. This model impacts several internal subsystems of the Cisco BTS 10200 Softswitch Element Management System (EMS) application. It also impacts the core login support on the other nodes of the Cisco BTS 10200 Softswitch.

Pluggable Authentication Module Support

The Cisco BTS 10200 Softswitch deploys a Secure Shell (SSH) package with Pluggable Authentication Module (PAM) support. The package includes the PAM support required to utilize the Radius and LDAP servers.

The supporting configuration allows local accounts to fall through if the Radius and LDAP servers are not available. These default local accounts for the Cisco BTS 10200 Softswitch are the btsuser, btsadmin and secadmin accounts. These are the standard default accounts provided in the base product and use the native password management.

A UNIX-based user provides access to the operating system on all nodes. The oamp user is defined for package management purposes. The account is locked and no password is available. However, to grant UNIX access to all nodes of the Cisco BTS 10200 Softswitch, a default password is provided.

When PAM support is used, SSH transfers the control of authentication to the PAM library, which then loads the modules specified in the PAM configuration file. Finally, the PAM library tells SSH whether the authentication was successful. SSH is not aware of the details of the actual authentication method employed by PAM. Only the final result is of interest.
User Security Account Management

The Cisco BTS 10200 Softswitch EMS contains an application program known as User Security Management (USM). This program determines if an account is local or off-board. Password management facilities are disabled for all accounts on the Cisco BTS 10200 Softswitch when an AAA deployment is configured. The AAA deployment transfers the responsibility for these existing facilities to the end-user AAA servers. These facilities include the following attributes:

- Password aging, warning, and expiration
- Password reset and automatic account locking
- Local account management (password and shadow files) for new accounts