

# Local Versus Remote Server Authentication

---

This chapter describes the differences between local and remote security databases and the basic authentication process for each. Remote security databases described in this chapter include Terminal Access Controller Access Control System (TACACS+) with Cisco proprietary enhancements and Remote Access Dial-In User Service (RADIUS).

Generally the size of the network and type of corporate security policies and control determines whether you use a local or remote security database.



**Caution** This chapter does not provide an exhaustive security overview. For example, it does not describe how to configure TACACS, Extended TACACS, Kerberos, or access lists. It presents the most commonly used security mechanisms to prevent unauthenticated and unauthorized access to network resources through Cisco access servers. For a comprehensive overview of Cisco security mechanisms, refer to the *Security Configuration Guide*.

Specifically, this chapter describes the following:

- Assumptions
- Local Security Database
- Remote Security Database

## Assumptions

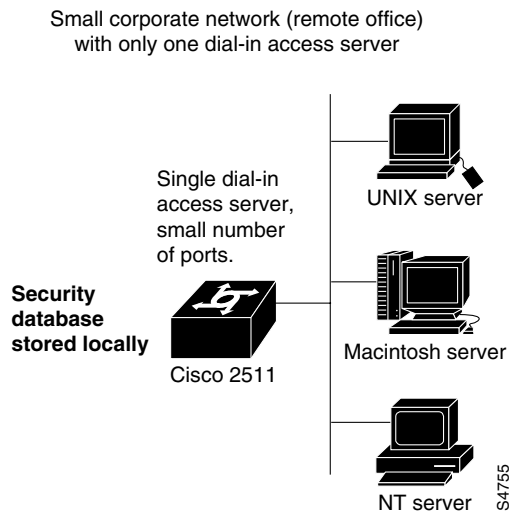
This chapter assumes the following:

- You know which network protocols you will allow access to your network. For example, you know if you will be allowing clients to dial in using modems to access IP, IPX, or AppleTalk networks, or whether clients will be using ISDN to access any of these networks.
- You are not an advanced user of the Cisco authentication, authorization, and accounting (AAA) security facility.

## Local Security Database

If you have one or two access servers providing access to your network, you probably want to store username and password security information on the Cisco access server itself. This is referred to as local authentication. A remote security server is not used. (See Figure 103.)

**Figure 103 Local Security Database**



A local security database configured on the access server is useful if you have very few access servers providing network access. A local security database does not require a separate (and costly) security server.

## Remote Security Database

As your network or demand for dial access grows, you need a centralized security database that provides username and password information to each of the access servers on the network. This centralized security database resides in a security server, which allows you to more easily manage your security solution. (See Figure 104.)

An example of a remote security database server is the CiscoSecure product from Cisco Systems, Inc. CiscoSecure is a UNIX security daemon solution, with which the administrator creates a database that defines the network users and their privileges. CiscoSecure uses a central database that stores user and group profiles with authentication and authorization information.

The Cisco access server exchanges user authentication information with a TACACS+ or RADIUS database on the security server by transmitting encrypted TACACS+ or RADIUS packets across the network.

For specific information about the interaction between the security server and the access server, refer to the *Security Configuration Guide*.



