



## Security

---

Wireless IP Telephony networks require a carefully planned security implementation to ensure that the telephony network operates properly and that voice traffic is secure. This chapter defines and explains security for the Cisco 7920 Wireless IP Phone and the wireless network infrastructure needed for a highly secure Wireless IP Telephony system in an enterprise environment. This chapter also discusses deployment methods and some of the configuration steps.

The Cisco 7920 Wireless IP Phone is supported in the architecture of the Cisco Wireless Security Suite. This architecture fits into the overall Cisco SAFE security architecture. For a description of the Cisco Wireless Security Suite and design guidelines for Cisco SAFE, refer to the documentation for these topics available at

<http://www.cisco.com>

The following sections describe network security, deployment options, and configuration settings for the Cisco 7920 Wireless IP Phone and WLAN:

- [Security Mechanisms, page 3-1](#)
- [ACS Deployment Options, page 3-2](#)

## Security Mechanisms

The Cisco 7920 Wireless IP Phone supports both Static Wired Equivalent Privacy (WEP) and Cisco LEAP for authentication and data encryption. If either encryption model is used, both the signaling (Skinny Client Control Protocol, or SCCP) and media (RTP) are encrypted between the Cisco 7920 phone and the AP.

### Static WEP

Static WEP requires that a 40-bit or 128-bit key be entered manually on all of the Cisco 7920 phones as well as the APs. It performs AP-based authentication by verifying that the accessing device (in this case, the Cisco 7920 phone) has a matching key.

### LEAP

LEAP allows devices (such as the Cisco 7920 phone and AP) to be authenticated mutually (phone-to-AP and AP-to-phone) based on a user name and password. Upon authentication, a dynamic key is used between the Cisco 7920 phone and the AP to encrypt traffic.

If LEAP is used, a LEAP-compliant RADIUS server, such as the Cisco Access Control Server (ACS), is required to provide access to the user database. The Cisco ACS can either store the user name and password database locally, or it can access that information from an external Microsoft Windows NT directory.

When using LEAP, ensure that strong passwords are used on all wireless devices. Strong passwords are defined as being between 10 and 12 characters long and can include both uppercase and lowercase characters as well as the special characters \* & % \$ # @.

Because most users save their passwords on the phone, Cisco recommends that you use different user names and passwords on data clients and wireless voice clients. This practice helps with tracking and troubleshooting as well as security.

**Note**

Although it is a valid configuration option to use an external (off-ACS) database to store the user names and passwords for the Cisco 7920 phones, Cisco does *not* recommend this practice. Because the ACS must be queried whenever the Cisco 7920 phone roams between APs, the unpredictable delay to access an off-ACS database could cause excessive delay and poor voice quality.

## ACS Deployment Options

When deploying LEAP, give careful consideration to the placement of the Cisco ACS. LEAP authentication is required every time a Cisco 7920 phone roams between APs, and RTP traffic (voice) will not flow until the LEAP authentication is completed. Therefore, reducing the amount of delay between the AP and the ACS is a critical component of engineering proper voice quality into the WLAN network.

You can deploy the Cisco Access Control Servers in one of the following ways:

- Centralized ACS

All users access the ACS in a central location within the network.

- Remote ACS

For remote offices that have slow-speed WAN links or congested WAN links that might delay LEAP processing, an ACS could be deployed locally at each remote office.

- Local and/or fallback RADIUS server functionality in the Cisco AP

Cisco IOS Release 12.2(11)JA introduced support for the Cisco AP to authenticate LEAP users without having to access an external ACS. This functionality supports up to 50 user names and is supported for LEAP only. This functionality does not interact with a centralized or remote ACS for database synchronization. This functionality is designed to be used as the primary RADIUS functionality in a small office, but it could also be used as a backup to a Cisco ACS in case of a WAN link failure. (See [Example Configurations for AP and RADIUS Server, page C-1](#), for a configuration example.)

**Note**

With Cisco Centralized Key Management (Cisco CKM), the phone can perform fast Layer-2 or Layer-3 roaming with a Wireless LAN Services Module (WLSM) in the network because the APs cache credentials and thus do not have to re-authenticate the device with the ACS each time.