CHAPTER 1

Cisco Unified Wireless Network Solution Overview

This chapter summarizes the benefits and characteristics of the Cisco Unified Wireless Network for the enterprise. The Cisco Unified Wireless Network solution offers secure, scalable, cost-effective wireless LANs for business critical mobility. The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the wireless LAN (WLAN) security, deployment, management, and control issues facing enterprises. This powerful indoor and outdoor solution combines the best elements of wired and wireless networking to deliver high performance, manageable, and secure WLANs with a low total cost of ownership.

WLAN Introduction

The mobile user requires the same accessibility, security, quality-of-service (QoS), and high availability currently enjoyed by wired users. Whether you are at work, at home, on the road, locally or internationally, there is a need to connect. The technological challenges are apparent, but to this end, mobility plays a role for everyone. Companies are deriving business value from mobile and wireless solutions. What was once a vertical market technology is now mainstream, and is an essential tool in getting access to voice, real-time information, and critical applications such as e-mail and calendar, enterprise databases, supply chain management, sales force automation, and customer relationship management.

WLAN Solution Benefits

Benefits achieved by WLANs include:

- *Mobility within buildings or campus*—Facilitates implementation of applications that require an always-on network and that tend to involve movement within a campus environment.
- *Convenience*—Simplifies networking of large, open people-areas.
- *Flexibility*—Allows work to be done at the most appropriate or convenient place rather than where a cable drop terminates. Getting the work done is what is important, not where you are.
- *Easier to set-up temporary spaces*—Promotes quick network setup of meeting rooms, war rooms, or brainstorming rooms tailored to variations in the number of participants.
- *Lower cabling costs*—Reduces the requirement for contingency cable plant installation because the WLAN can be employed to fill the gaps.

- *Easier adds, moves, and changes and lower support and maintenance costs*—Temporary networks become much easier to set up, easing migration issues and costly last-minute fixes.
- *Improved efficiency*—Studies show WLAN users are connected to the network 15 percent longer per day than hard-wired users.
- *Productivity gains*—Promotes easier access to network connectivity, resulting in better use of business productivity tools. Productivity studies show a 22 percent increase for WLAN users.
- *Easier to collaborate*—Facilitates access to collaboration tools from any location, such as meeting rooms; files can be shared on the spot and requests for information handled immediately.
- *More efficient use of office space*—Allows greater flexibility for accommodating groups, such as large team meetings.
- *Reduced errors*—Data can be directly entered into systems as it is being collected, rather than when network access is available.
- *Improved efficiency, performance, and security for enterprise partners and guests*—Promoted by implementing guest access networks.
- *Improved business resilience*—Increased mobility of the workforce allows rapid redeployment to other locations with WLANs.

Requirements of WLAN Systems

WLAN systems run either as an adjunct to the existing wired enterprise network or as a free-standing network within a campus or branch. WLANs can also be tied to applications, such as location-based services, in the retail, manufacturing, or health care industries. WLANs must permit secure, encrypted, authorized communication with access to data, communication, and business services as if connected to the resources by wire.

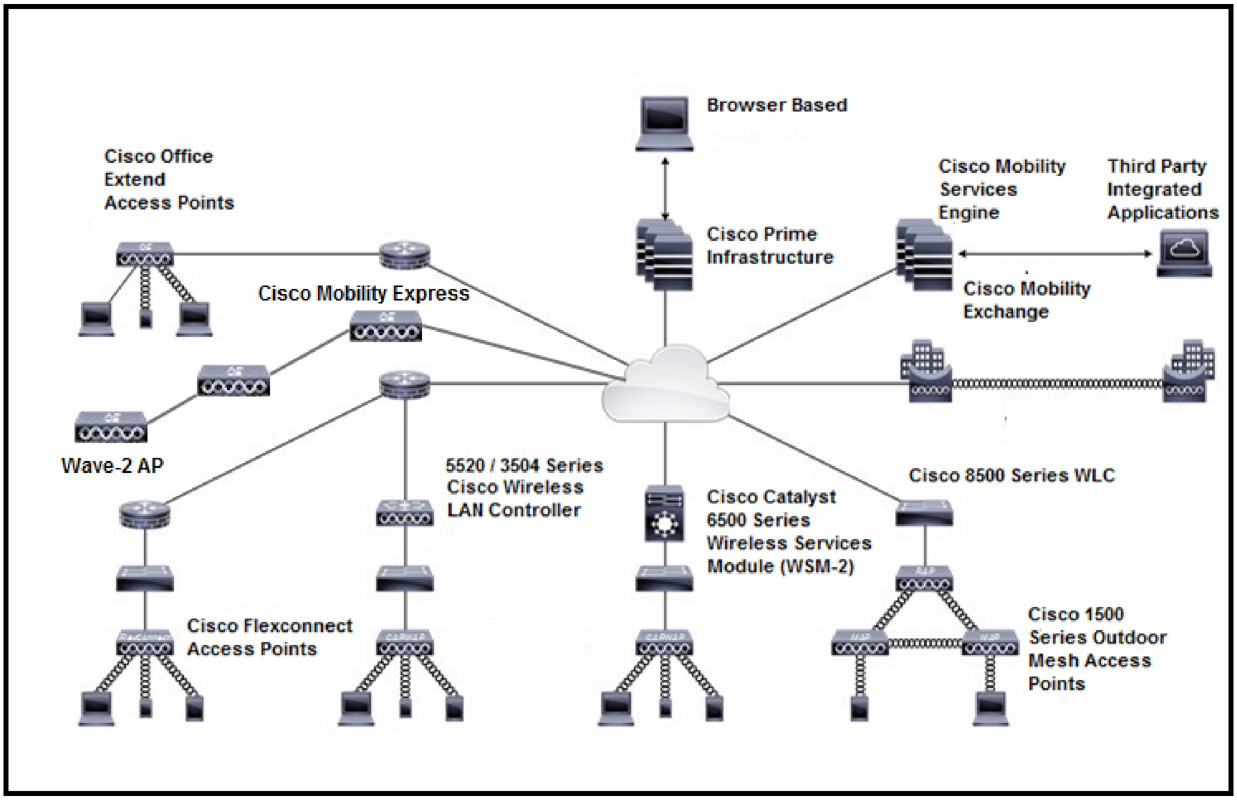
WLANs must be able to do the following:

- *Maintain accessibility to resources while employees are not wired to the network*—This accessibility enables employees to respond more quickly to business needs regardless of whether they are meeting in a conference room with a customer, at lunch with coworkers in the company cafeteria, or collaborating with a teammate in the next building.
- *Secure the enterprise from unauthorized, unsecured, or 'rogue' WLAN access points (APs)*—IT managers must be able to easily and automatically detect and locate rogue APs and the switch ports to which they are connected, active participation of both APs, and client devices that are providing continuous scanning and monitoring of the RF environment.
- *Extend the full benefits of integrated network services to nomadic users*—IP telephony and IP video-conferencing are supported over the WLAN using QoS, which by giving preferential treatment to real-time traffic, helps ensure that the video and audio information arrives on time. Firewall and Intruder Detection that are part of the enterprise framework are extended to the wireless user.
- *Segment authorized users and block unauthorized users*—Services of the wireless network can be safely extended to guests and vendors. The WLAN must be able to configure support for a separate public network—a guest network.
- *Provide easy, secure network access to visiting employees from other sites*—There is no need to search for an empty cubicle or an available Ethernet port. Users should securely access the network from any WLAN location. Employees are authenticated through IEEE 802.1x and Extensible Authentication Protocol (EAP), and all information sent and received on the WLAN is encrypted.

- *Easily manage central or remote APs*—Network managers must be able to easily deploy, operate, and manage hundreds to thousands of APs within the WLAN campus deployments and branch offices or retail, manufacturing, and health care locations. The desired result is one framework that provides medium-sized to large organizations the same level of security, scalability, reliability, ease of deployment, and management that they have come to expect from their wired LANs.
- *Enhanced Security Services*—WLAN Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) control to contain wireless threats, enforce security policy compliance, and safeguard information.
- *Voice Services*—Brings the mobility and flexibility of wireless networking to voice communications via the Cisco Unified Wired and Wireless network and the Cisco Compatible Extensions voice-enabled client devices.
- *Location Services* — Simultaneous tracking of hundreds to thousands of Wi-Fi and active RFID devices from directly within the WLAN infrastructure for critical applications such as high-value asset tracking, IT management, location-based security, and business policy enforcement.
- *Guest Access*— Provides customers, vendors, and partners with easy access to a wired and wireless LANs, helps increase productivity, facilitates real-time collaboration, keeps the company competitive, and maintains full WLAN security.

WLANs in the enterprise have emerged as one of the most effective means for connecting to a larger corporate network or to the internet. Figure 1-1 shows the elements of the Cisco Unified Wireless Network.

Figure 1-1 Cisco Unified Wireless Network Architecture in the Enterprise



The interconnected elements that work together to deliver a unified enterprise-class wireless solution include:

- Client devices
- Access points (APs)
- Network unification through controllers
- World-class network management
- Mobility services

Beginning with a base of client devices, each element adds capabilities as the network needs evolve and grow, interconnecting with the elements above and below it to create a comprehensive, secure WLAN solution.

Cisco Unified Wireless Network

The core components of Cisco Unified Wireless Networks include the:

- Aironet access points (APs)
- Wireless LAN controller (WLC)
- Cisco Prime Infrastructure

For more information about the Cisco Unified Wireless Network, see:

http://www.cisco.com/go/unifiedwireless