Chapter 4: Wireless LANs

Scaling Networks

Chapter 4

Chapter 4: Objectives

- Describe wireless LAN technology and standards.

- Describe the components of a wireless LAN infrastructure.

- Describe wireless topologies.

- Describe the 802.11 frame structure.

- Describe the media contention method used by wireless technology.

- Describe channel management in a WLAN.

- Describe threats to wireless LANs.

- Describe wireless LAN security mechanisms.

- Configure a wireless router to support a remote site.

- Configure wireless clients to connect to a wireless router.

- Troubleshoot common wireless configuration issues.

4.1 Wireless Concepts

Supporting Mobility

- Productivity is no longer restricted to a fixed work location or a defined time period.

- People now expect to be connected at any time and place, from the office to the airport or the home.

- Users now expect to be able to roam wirelessly.

- Roaming enables a wireless device to maintain Internet access without losing a connection.

Benefits of Wireless

- Increased flexibility

- Increased productivity

- Reduced costs

- Ability to grow and adapt to changing requirements

Wireless Technologies

Wireless networks can be classified broadly as:

- **Wireless personal-area network (WPAN)** – Operates in the range of a few feet (Bluetooth).

- **Wireless LAN (WLAN)** – Operates in the range of a few hundred feet.

- **Wireless wide-area network (WWAN)** – Operates in the range of miles.

- **Bluetooth** – An IEEE 802.15 WPAN standard; uses a device-pairing process to communicate over distances up to .05 mile (100m).

- **Wi-Fi (wireless fidelity)** – An IEEE 802.11 WLAN standard; provides network access to home and corporate users, to include data, voice and video traffic, to distances up to 0.18 mile (300m).

Wireless Technologies (cont.)

- **Worldwide Interoperability for Microwave Access (WiMAX)** – An IEEE 802.16 WWAN standard that provides wireless broadband access of up to 30 mi (50 km).

- **Cellular broadband** – Consists of various corporate, national, and international organizations using service provider cellular access to provide mobile broadband network connectivity.

- **Satellite Broadband** – Provides network access to remote sites through the use of a directional satellite dish.

Radio Frequencies

Radio Waves of the Electromagnetic Spectrum
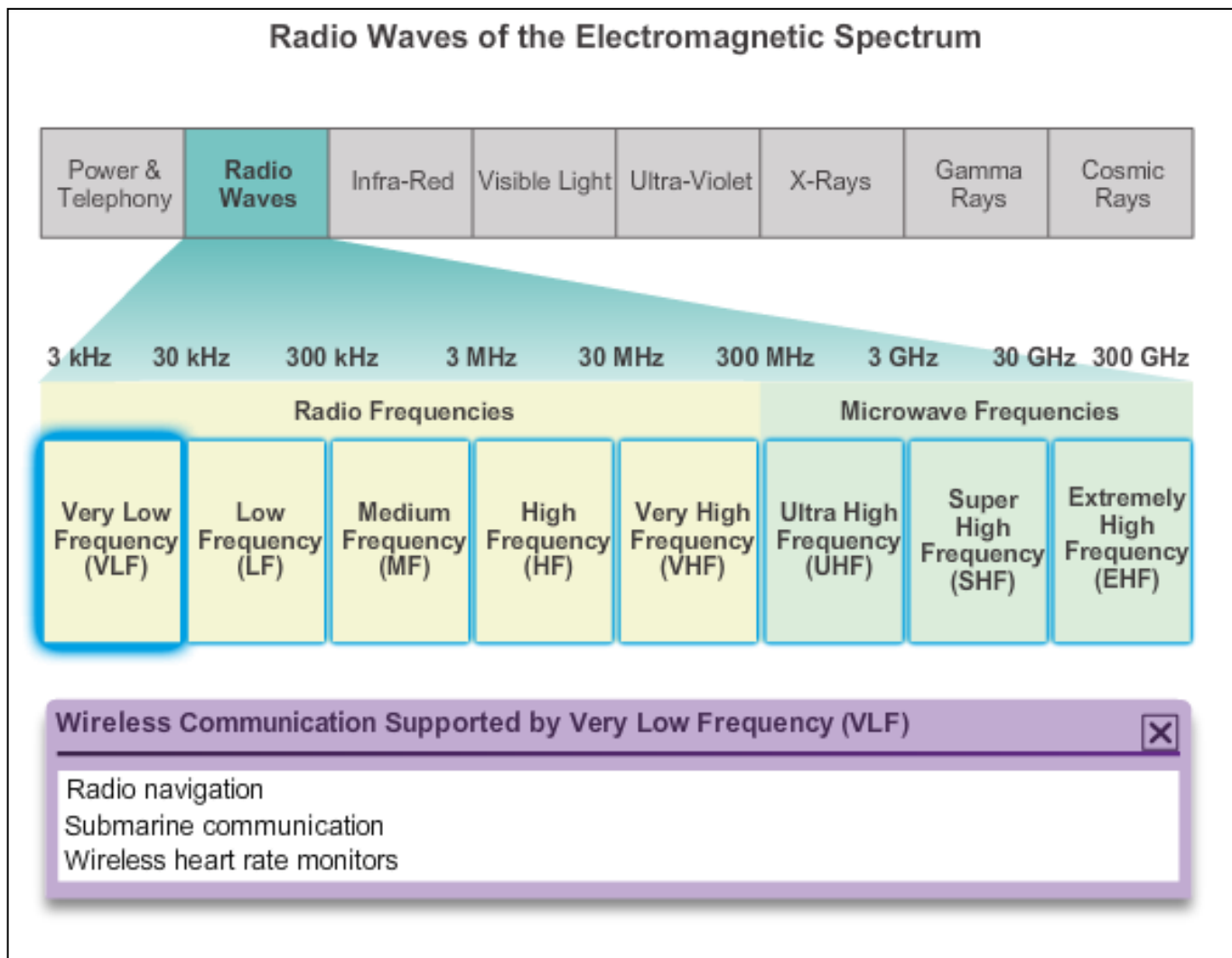
802.11 Standards

IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

Wi-Fi Certification

The Wi-Fi Alliance certifies Wi-Fi and the following product compatibility:

- IEEE 802.11a/b/g/n/ac/ad-compatible.

- IEEE 802.11i secure using WPA2™ and Extensible Authentication Protocol (EAP)

- Wi-Fi Protected Setup (WPS) to simplify device connections.

- Wi-Fi Direct to share media between devices

- Wi-Fi Passpoint to simplify securely connecting to Wi-Fi hotspot networks

- Wi-Fi Miracast to seamlessly display video between devices

Comparing WLANs to LANs

Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

Wireless NICs

Wireless deployment requires:

- End devices with wireless NICs

- Infrastructure device, such as a wireless router or wireless AP

Wireless USB Adapters

Linksys AE6000 Mini USB Wi-Fi Wireless-AC Dual-Band Adapter 2.4 or 5 GHz 802.11ac

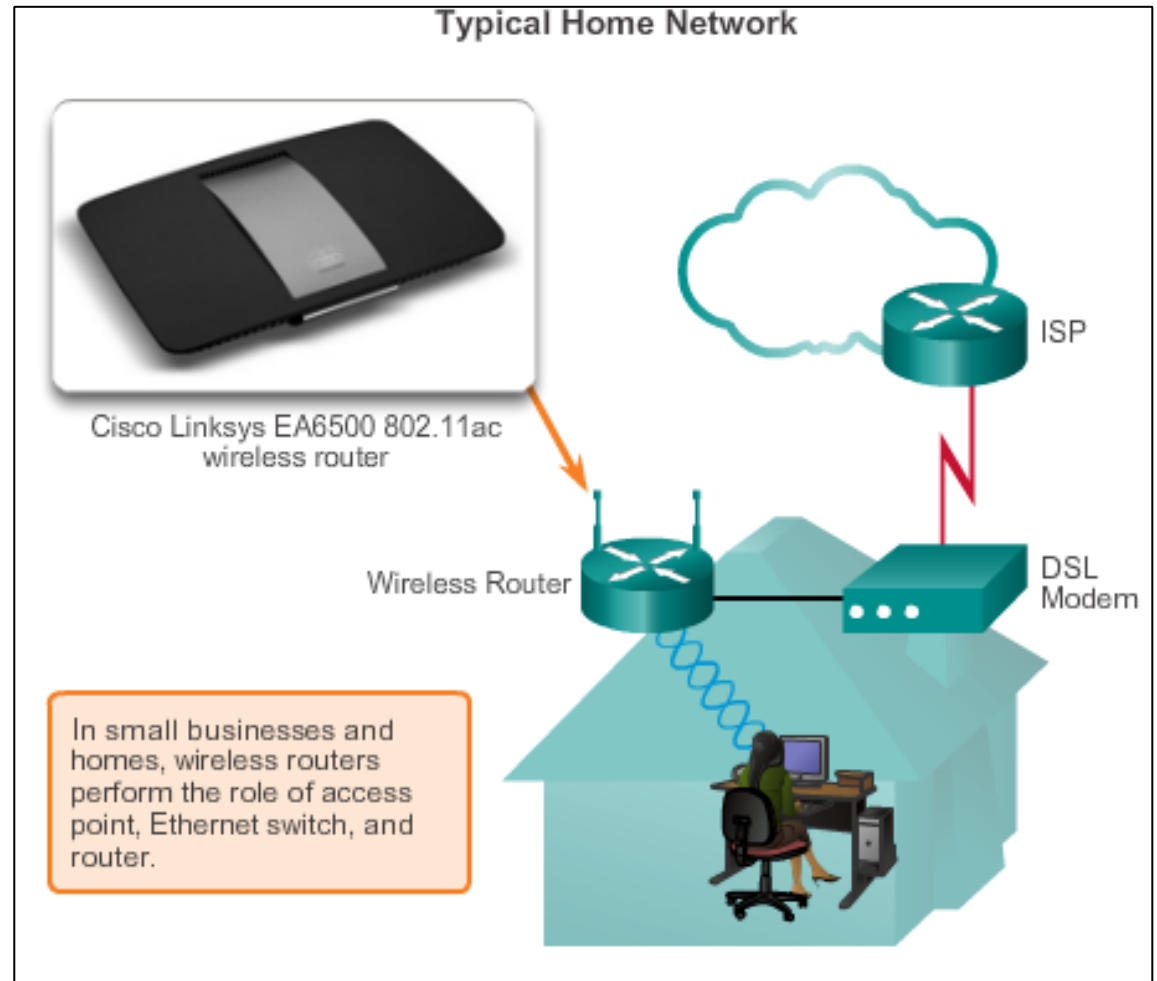Linksys AE3000 High Performance Dual-Band N USB Adapter

Wireless Home Router

A home user typically interconnects wireless devices using a small, integrated wireless router.
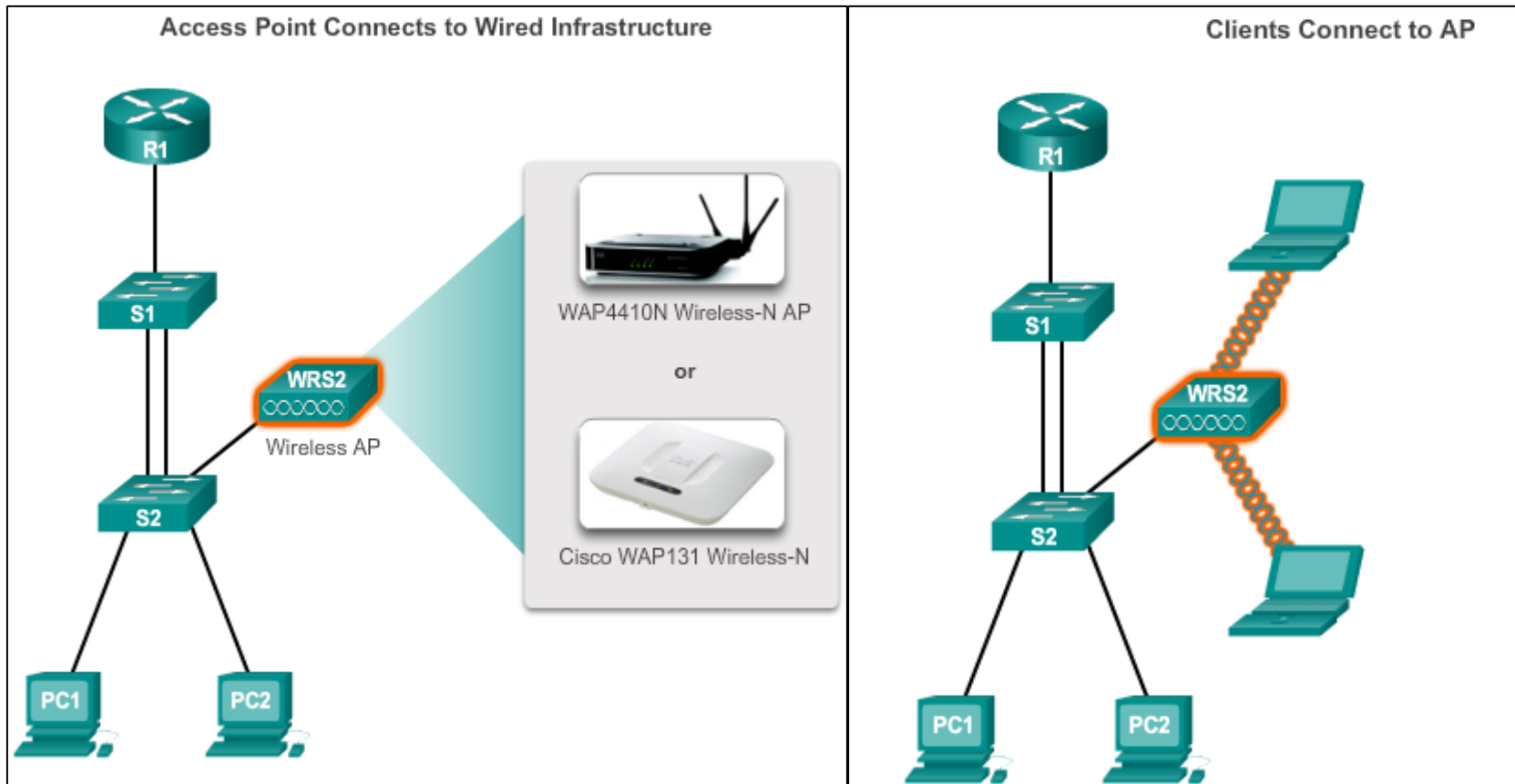
These serve as:
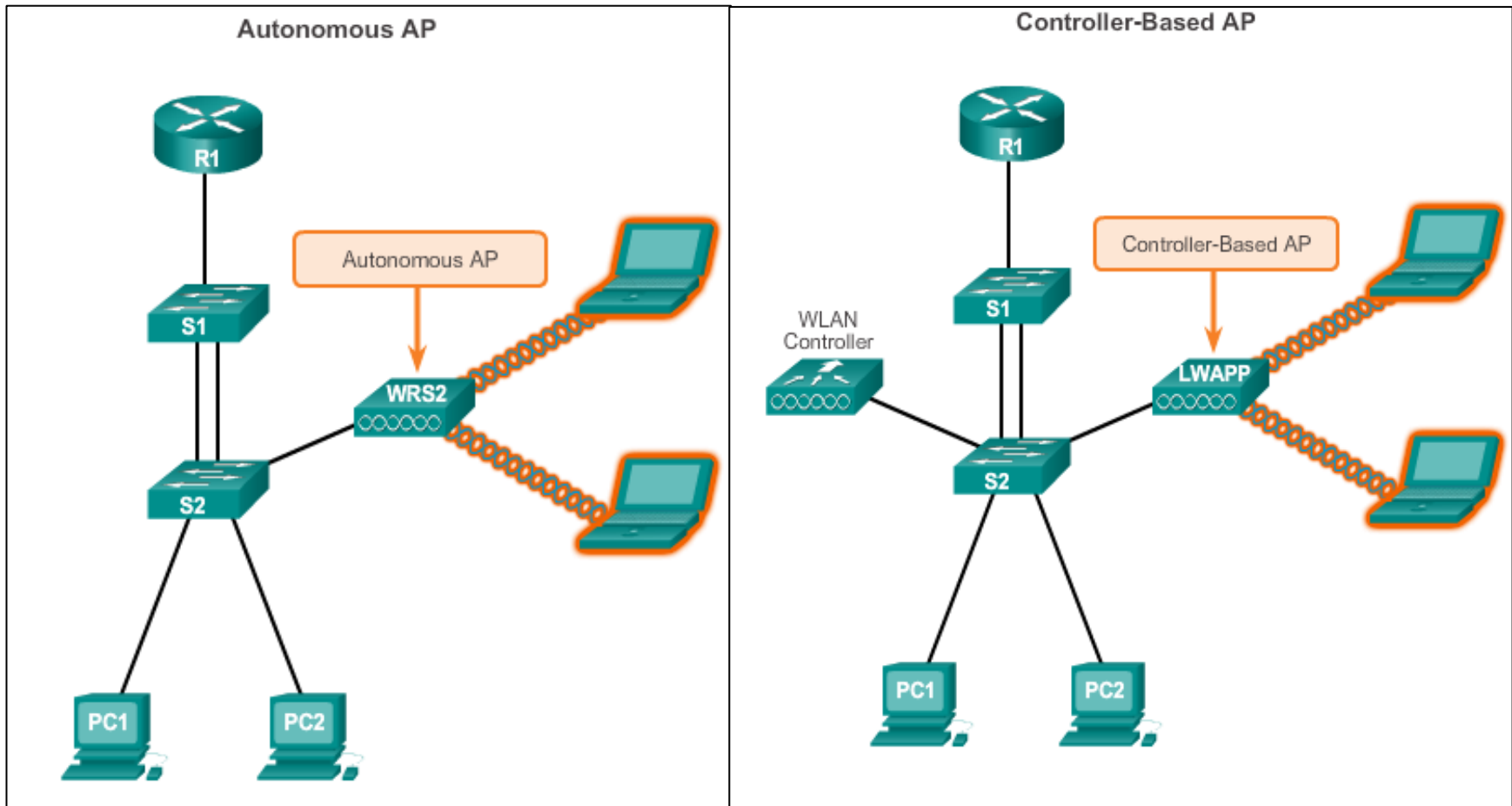
- access point

- Ethernet switch

- router

Typical Home Network

Cisco Linksys EA6500 802.11ac wireless router

ISP

DSL Modem

Wireless Router

In small businesses and homes, wireless routers perform the role of access point, Ethernet switch, and router.

Business Wireless Solutions

Wireless Access Points

Small Wireless Deployment Solutions

Cisco Small Business Autonomous APs

Cisco WAP4410N
- Intro-level small business AP
- Configured using a GUI
- Powered using AC or PoE

Cisco WAP121 and WAP321
- Mid-level small business APs
- Configured and managed using a GUI or CLI
- Supports clustering with Single PointSetup
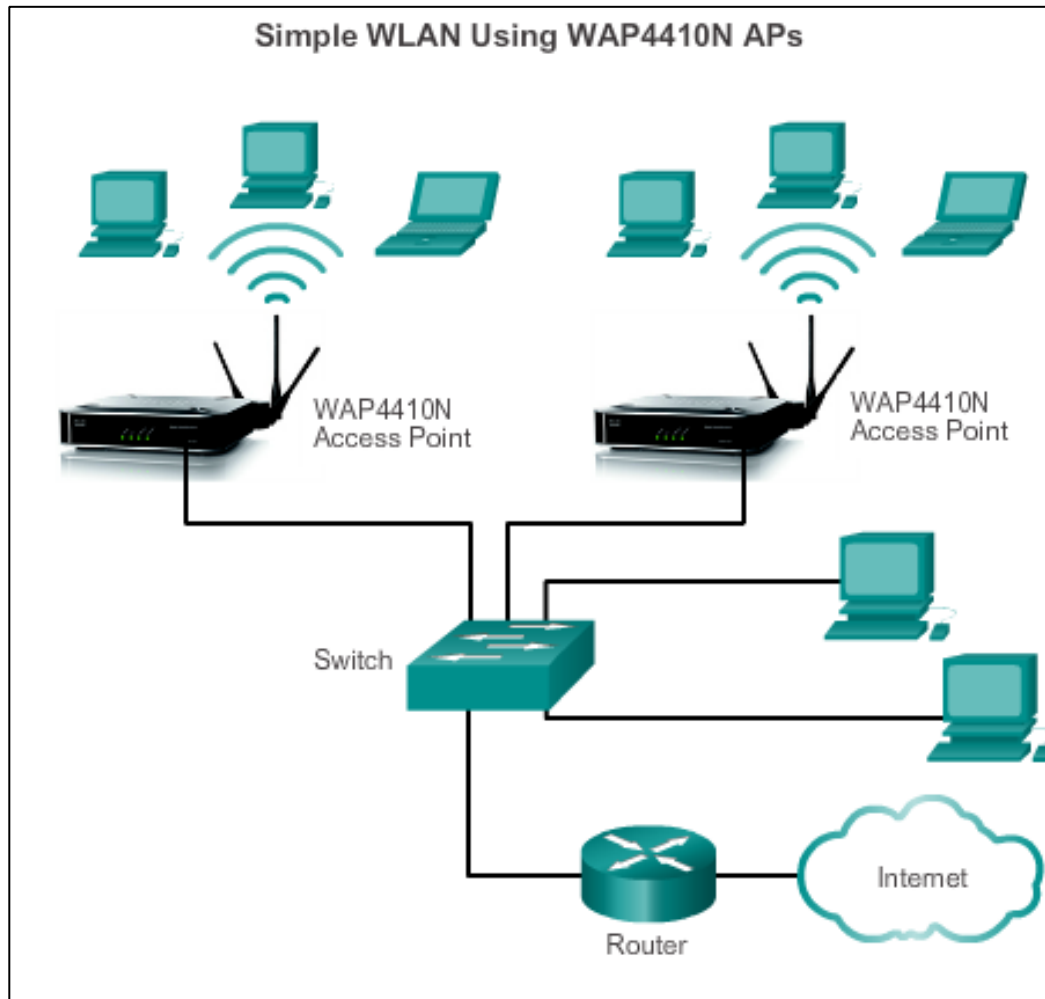- Powered using AC or PoE

Cisco AP541N
- Mid-level small business APs
- Configured using a GUI
- Supports controller-less clustering technology
- Powered using AC or PoE

Components of WLANs
Small Wireless Deployment Solutions (cont.)
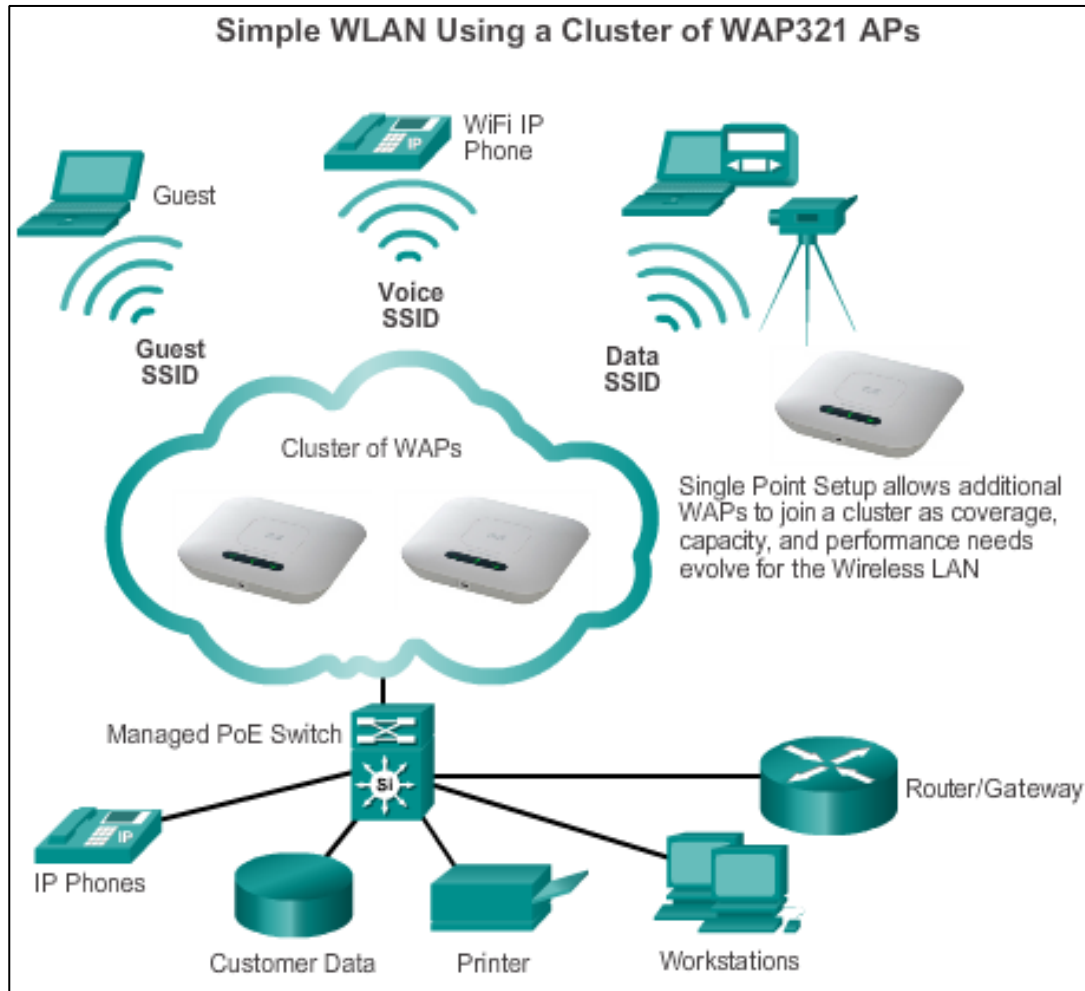
Simple WLAN Using WAP4410N APs

- Each AP is configured and managed individually.

- This can become a problem when several APs are required.

Components of WLANs
Small Wireless Deployment Solutions

Simple WLAN Using a Cluster of WAP321 APs

Guest

WiFi IP Phone

Voice SSID

Data SSID

Guest SSID

Cluster of WAPs

Single Point Setup allows additional WAPs to join a cluster as coverage, capacity, and performance needs evolve for the Wireless LAN

Managed PoE Switch

Router/Gateway

IP Phones

Customer Data   Printer   Workstations

- Support the clustering of APs without the use of a controller.

- Multiple APs can be deployed and pushed to a single configuration to all devices within the cluster, managing the wireless network as a single system without worrying about interference between APs, and without configuring each AP as a separate device.

Large Wireless Deployment Solutions

- For larger organizations with many APs, Cisco provides controller-based managed solutions, including the Cisco Meraki Cloud Managed Architecture and the Cisco Unified Wireless Network Architecture.

- Cisco Meraki cloud architecture is a management solution used to simplify the wireless deployment. Using this architecture, APs are centrally managed from a controller in the cloud.

Meraki Cloud Controller
(MCC)

Large Wireless Deployment Solutions (cont.)

Controller-Based Wireless APs

Cisco Aironet 1600, 2600, and 3600 Series
Robust controller-based APs

Cisco Aironet 600 Series OfficeExtend
Used to extend 802.11n wireless coverage to the home teleworking environment

Cisco 1552 Series Outdoor Rugged APs
Robust outdoor controller-based AP

Large Wireless Deployment Solutions (cont.)

Controllers for Small and Medium-Sized Businesses

Cisco Virtual Controller

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Wireless Antennas

Cisco Aironet APs can use:

- **Omnidirectional Wi-Fi Antennas** – Factory Wi-Fi gear often uses basic dipole antennas, also referred to as "rubber duck" design, similar to those used on walkie-talkie radios. Omnidirectional antennas provide 360-degree coverage.

- **Directional Wi-Fi Antennas** – Directional antennas focus the radio signal in a given direction, which enhances the signal to and from the AP in the direction the antenna is pointing.

- **Yagi antennas** – Type of directional radio antenna that can be used for long-distance Wi-Fi networking.

802.11 Wireless Topology Modes

Ad Hoc Mode

Devices interconnect directly without the use an AP or wireless router.

802.11 Wireless Topology Modes (cont.)

Infrastructure Mode

Distribution System

Devices interconnect using the services of an AP or wireless router.
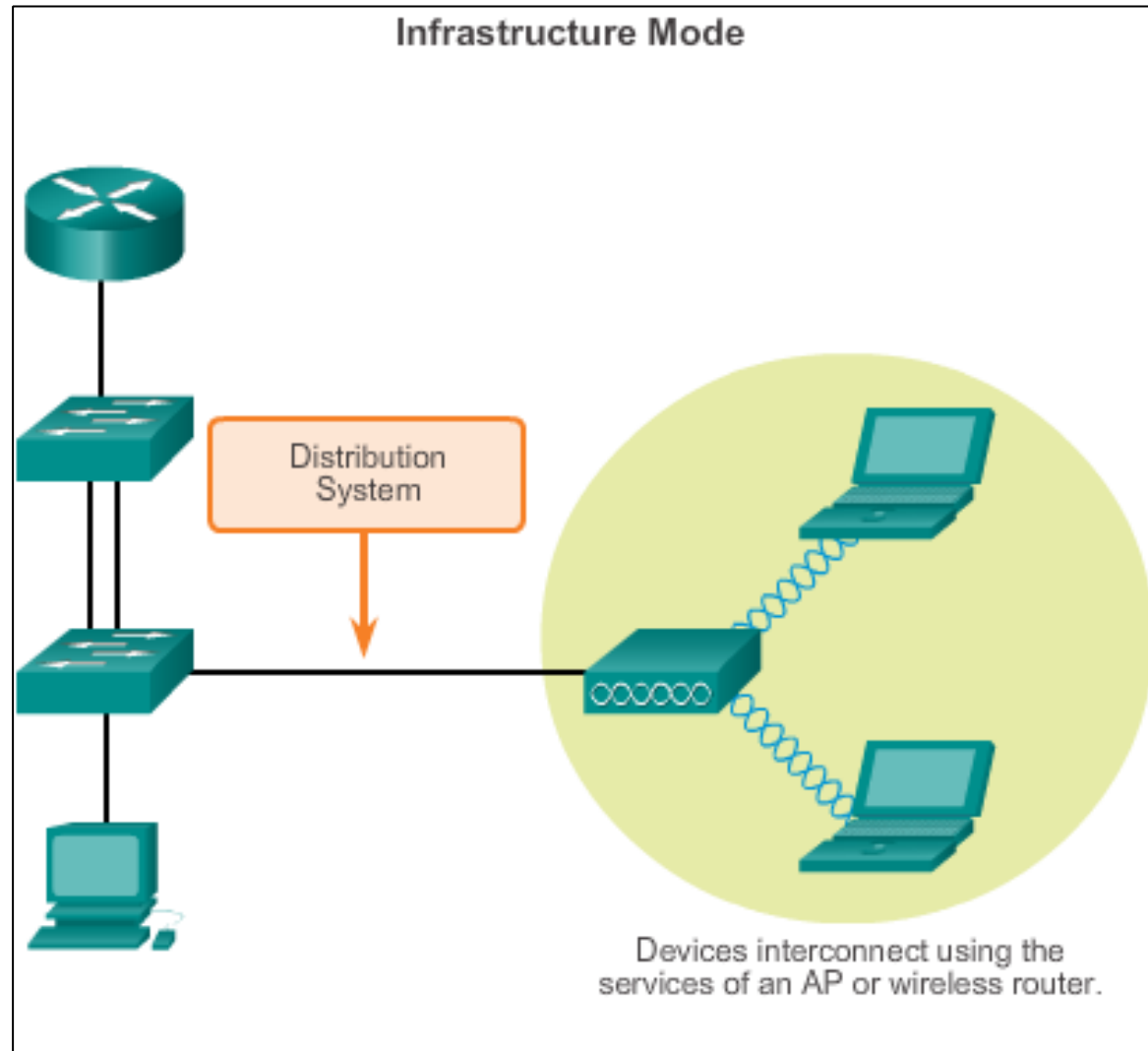
Ad Hoc Mode

Tethering (personal hotspot) – Variation of the Ad Hoc topology when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.
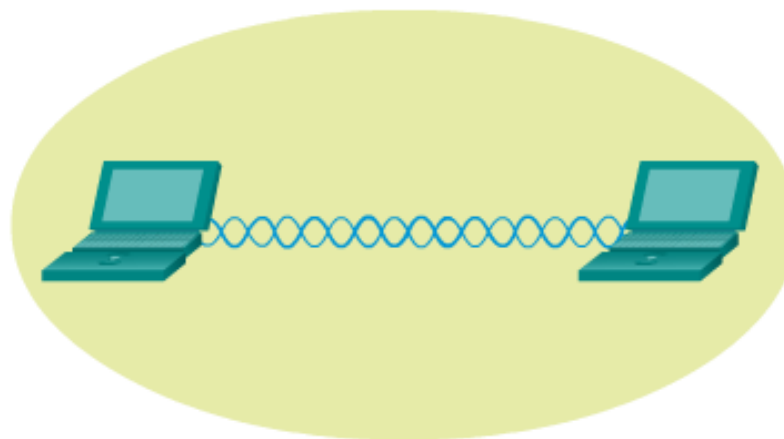
IBSS Summary	
WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)

Infrastructure Mode

Basic Service Set Summary

BSS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Basic Service Set (BSS)
Number of APs	1
802.11 Coverage Area	Basic Service Area (BSA)

Infrastructure Mode (cont.)
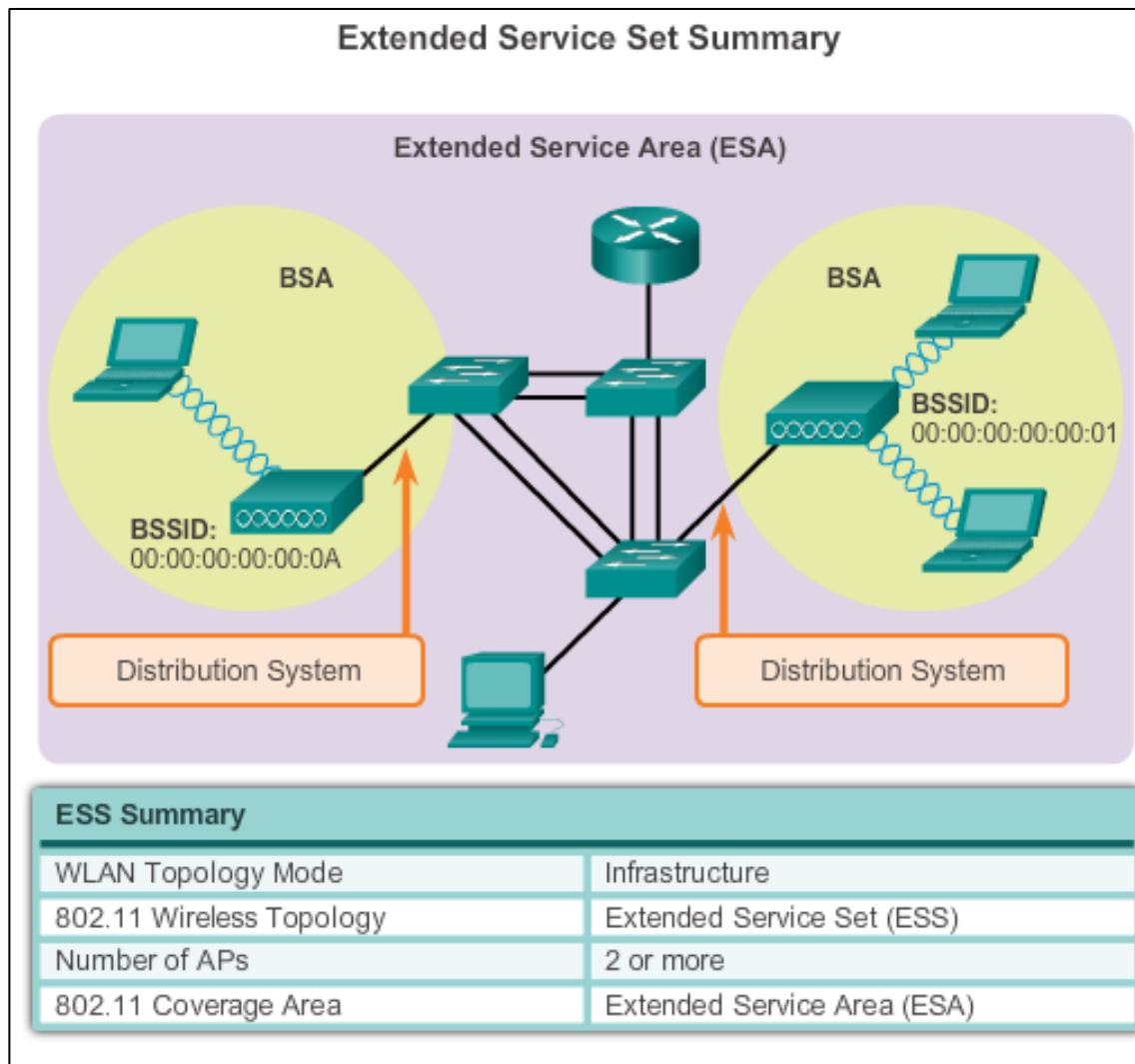
4.2 Wireless LAN Operations

Wireless 802.11 Frame

Content of Wireless 802.11 Frame Header

Wireless 802.11 Frame

Frame Control Field
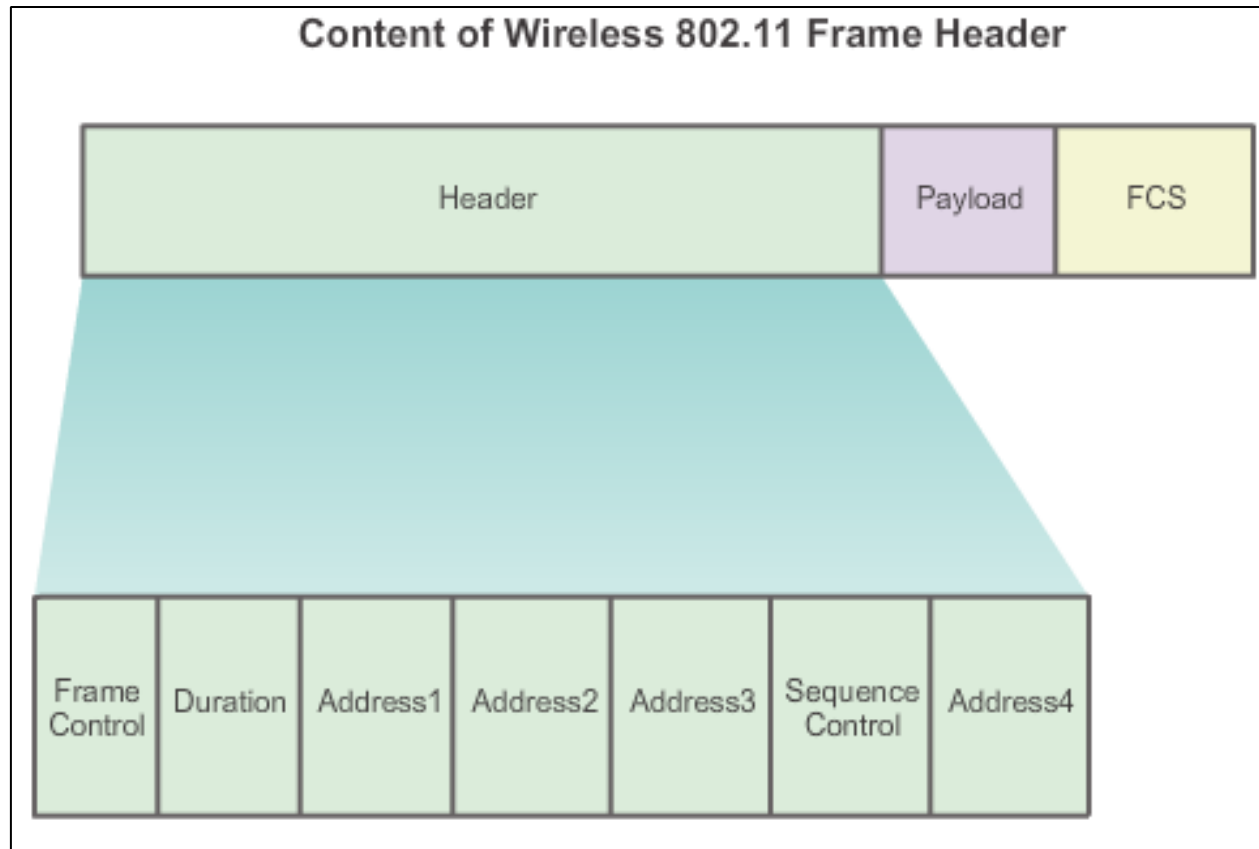
Remainder of 802.11 Frame Fields

Frame Control Field

Frame Control Subfields

Wireless Frame Type
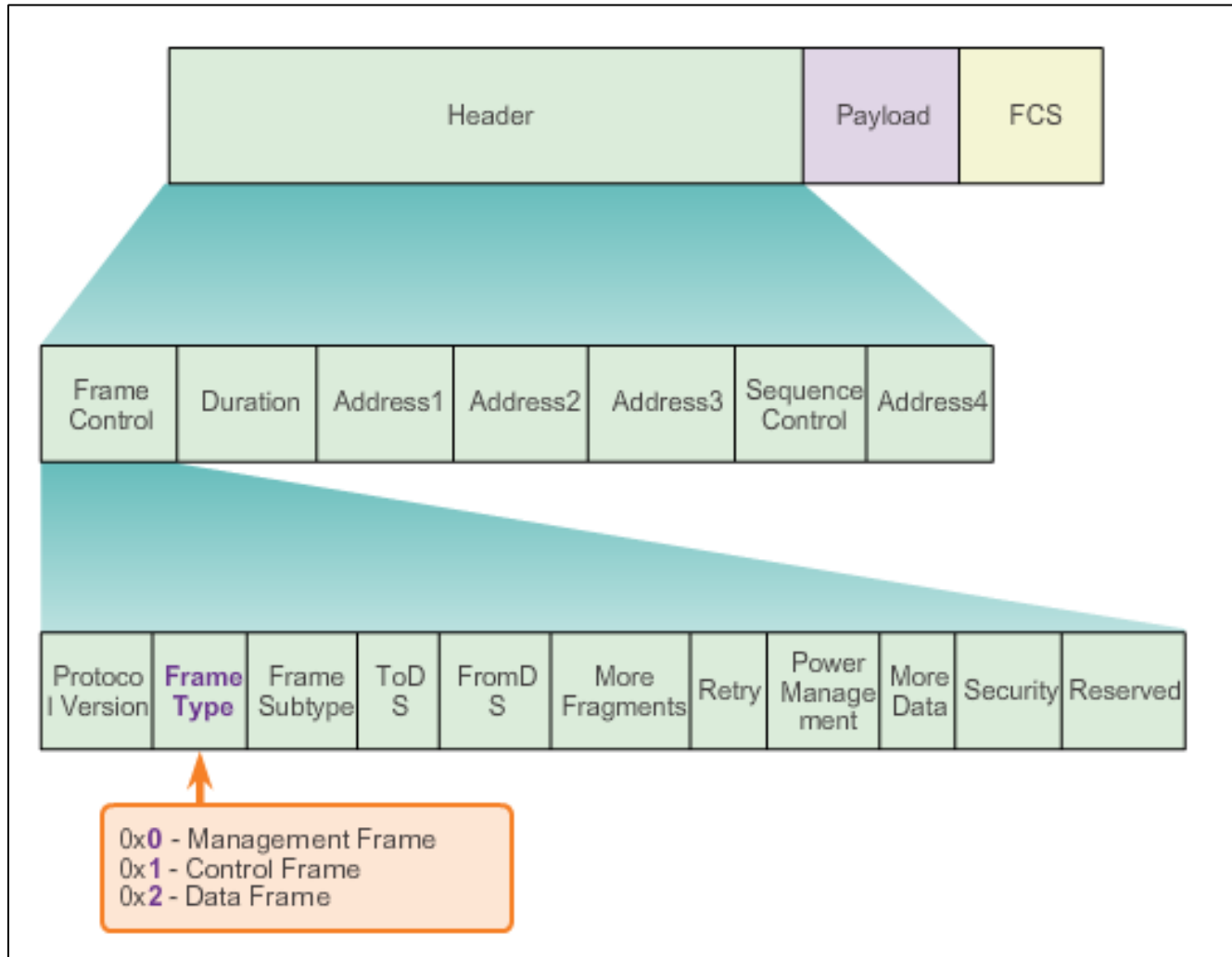
© 2008 Cisco Systems, Inc. All rights reserved.   Cisco Confidential   33

Management Frames

Content of the Management Fields

Control Frames

Content of the Frame Control Field

Header	Payload	FCS

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4

Protocol Version	Frame Type	Frame Subtype	ToDS	FromDS	More Fragments	Retry	Power Management	More Data	Security	Reserved

0x**1B** - Request to Send (RTS)
0x**1C** - Clear to Send (CTS)
0x**1D** - Acknowledge (ACK)
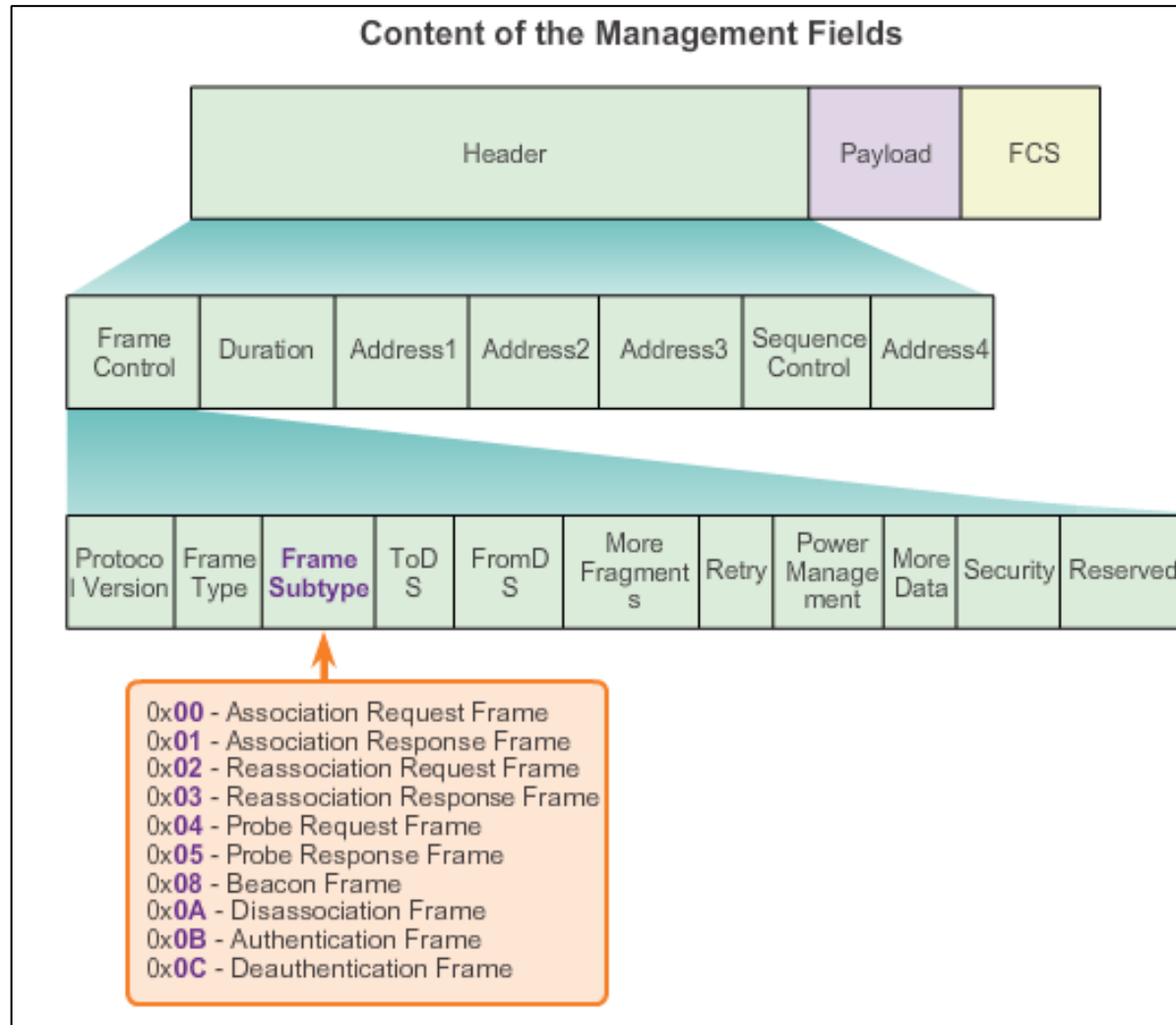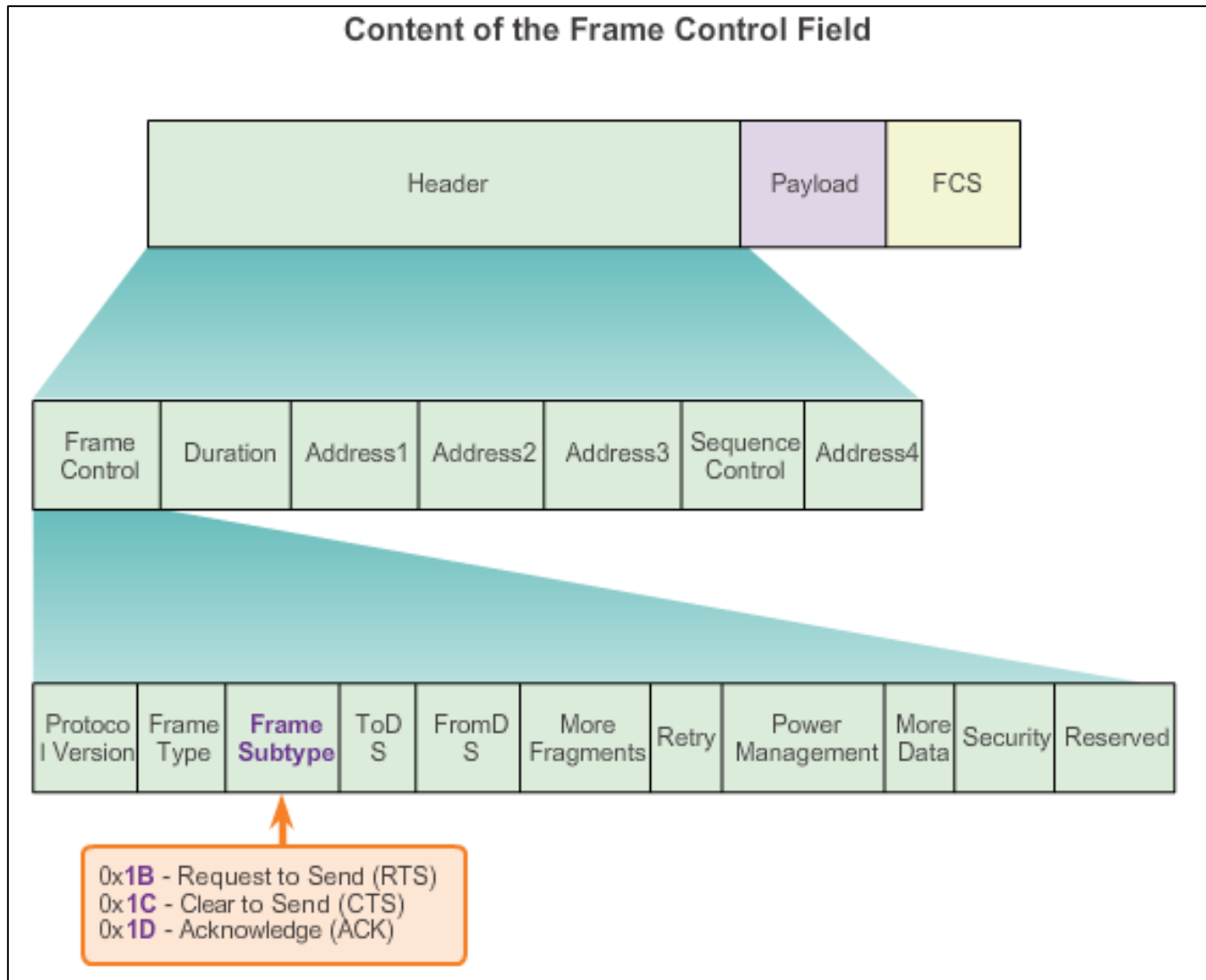
CSMA/CA

CSMA/CA Flowchart
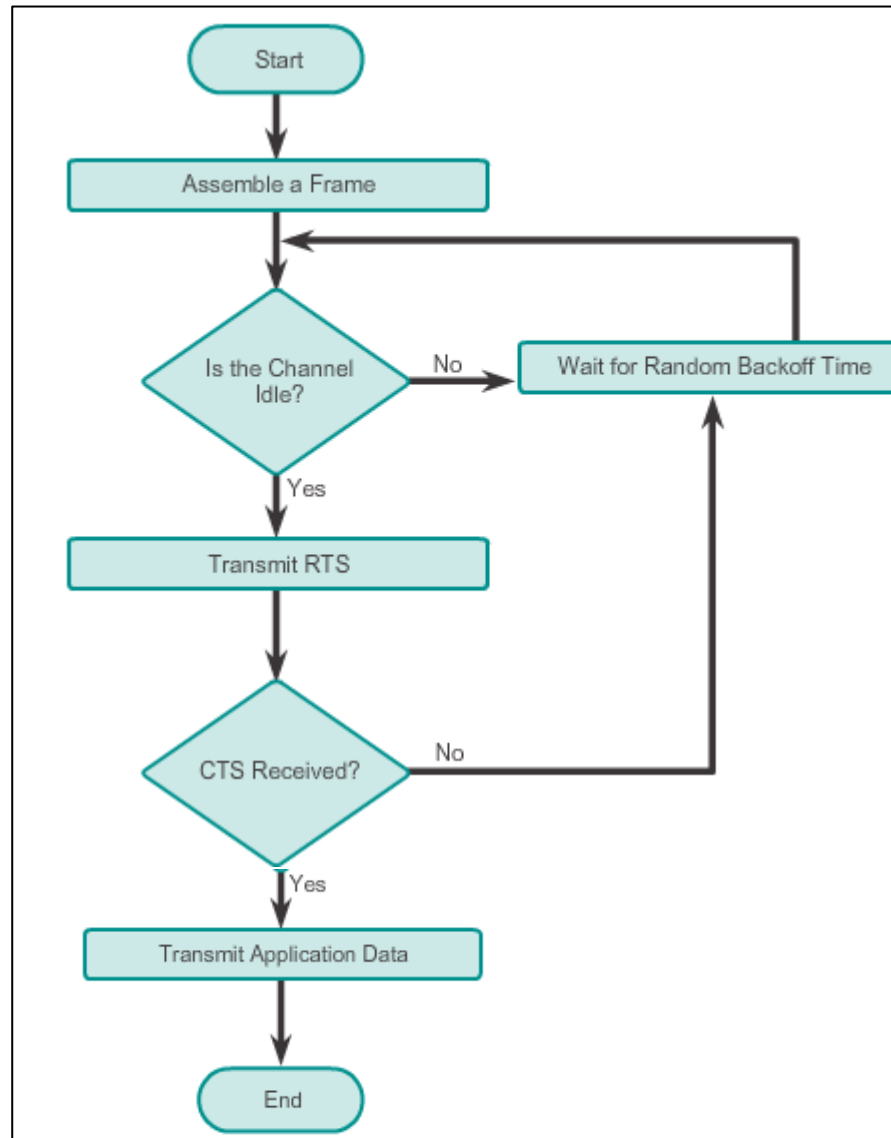
Wireless Clients and Access Point Association

Three-Stage Process

Sender — Receiver

Discover AP

Authenticate
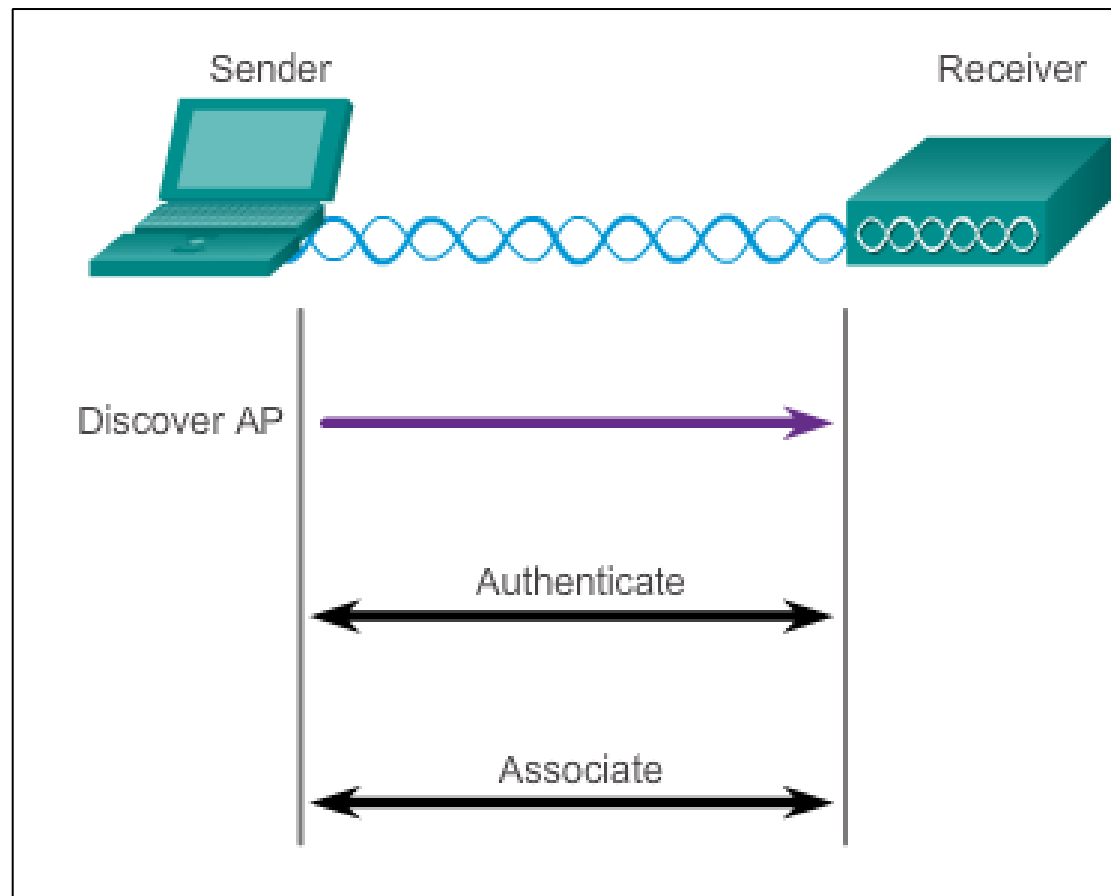
Associate

Wireless Operation
Association Parameters

- **SSID** – Unique identifier that wireless clients use to distinguish between multiple wireless networks in the same vicinity.

- **Password** – Required from the wireless client to authenticate to the AP. Sometimes called the security key.

- **Network mode** – Refers to the 802.11a/b/g/n/ac/ad WLAN standards. APs and wireless routers can operate in a mixed mode; i.e., it can simultaneously use multiple standards.

- **Security mode** – Refers to the security parameter settings, such as WEP, WPA, or WPA2.

- **Channel settings** – Refers to the frequency bands used to transmit wireless data. Wireless routers and AP can choose the channel setting or it can be manually set.

Discovering APs

Passive mode

- AP advertises its service by sending broadcast beacon frames containing the SSID, supported standards, and security settings.

- The beacon's primary purpose is to allow wireless clients to learn which networks and APs are available in a given area.

Active mode

- Wireless clients must know the name of the SSID.

- Wireless client initiates the process by broadcasting a probe request frame on multiple channels.

- Probe request includes the SSID name and standards supported.

- May be required if an AP or wireless router is configured to not broadcast beacon frames.

Authentication

Client and AP Authenticate

Sender   Receiver

Authentication Frame (0x0B)
- Type (open or shared key)
- Key (if shared)

Authentication Frame (0x0B)
- Type
- Key
- Successful or unsuccessful
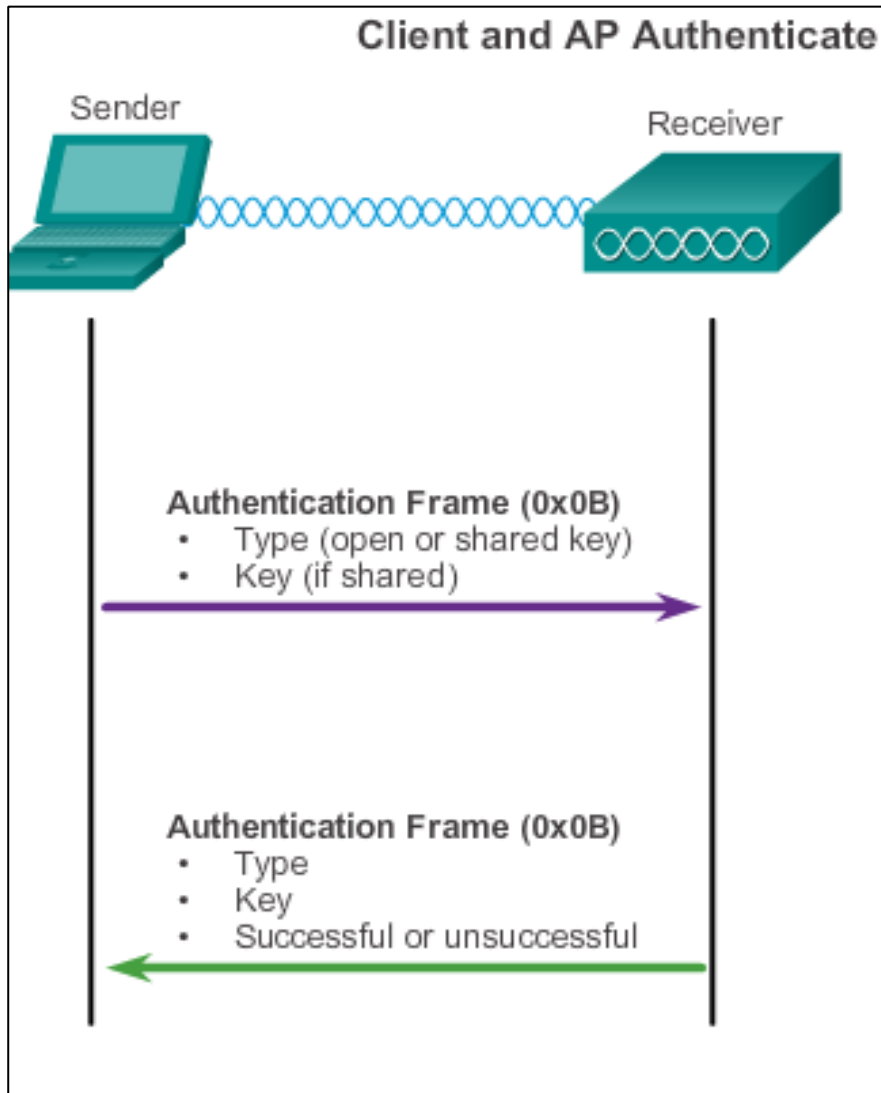
- **Open authentication** – A NULL authentication where the wireless client says "authenticate me" and the AP responds with "yes." Used where security is of no concern.

- **Shared key authentication** – Technique is based on a key that is pre-shared between the client and the AP.

Frequency Channel Saturation

Direct-sequence spread spectrum (DSSS)

- Uses spread-spectrum modulation technique; designed to spread a signal over a larger frequency band making it more resistant to interference.
- Used by 802.11b.

Frequency-hopping spread spectrum (FHSS)

- Relies on spread-spectrum methods to communicate.
- Transmits radio signals by rapidly switching a carrier signal among many frequency channels.
- This channel-hopping process allows for a more efficient usage of the channels, decreasing channel congestion.
- Used by the original 802.11 standard.

Frequency Channel Saturation (cont.)

Orthogonal Frequency-Division Multiplexing (OFDM)

- Subset of frequency division multiplexing in which a single channel utilizes multiple subchannels on adjacent frequencies.

- Because OFDM uses subchannels, channel usage is very efficient.

- Used by a number of communication systems, including 802.11a/g/n/ac.
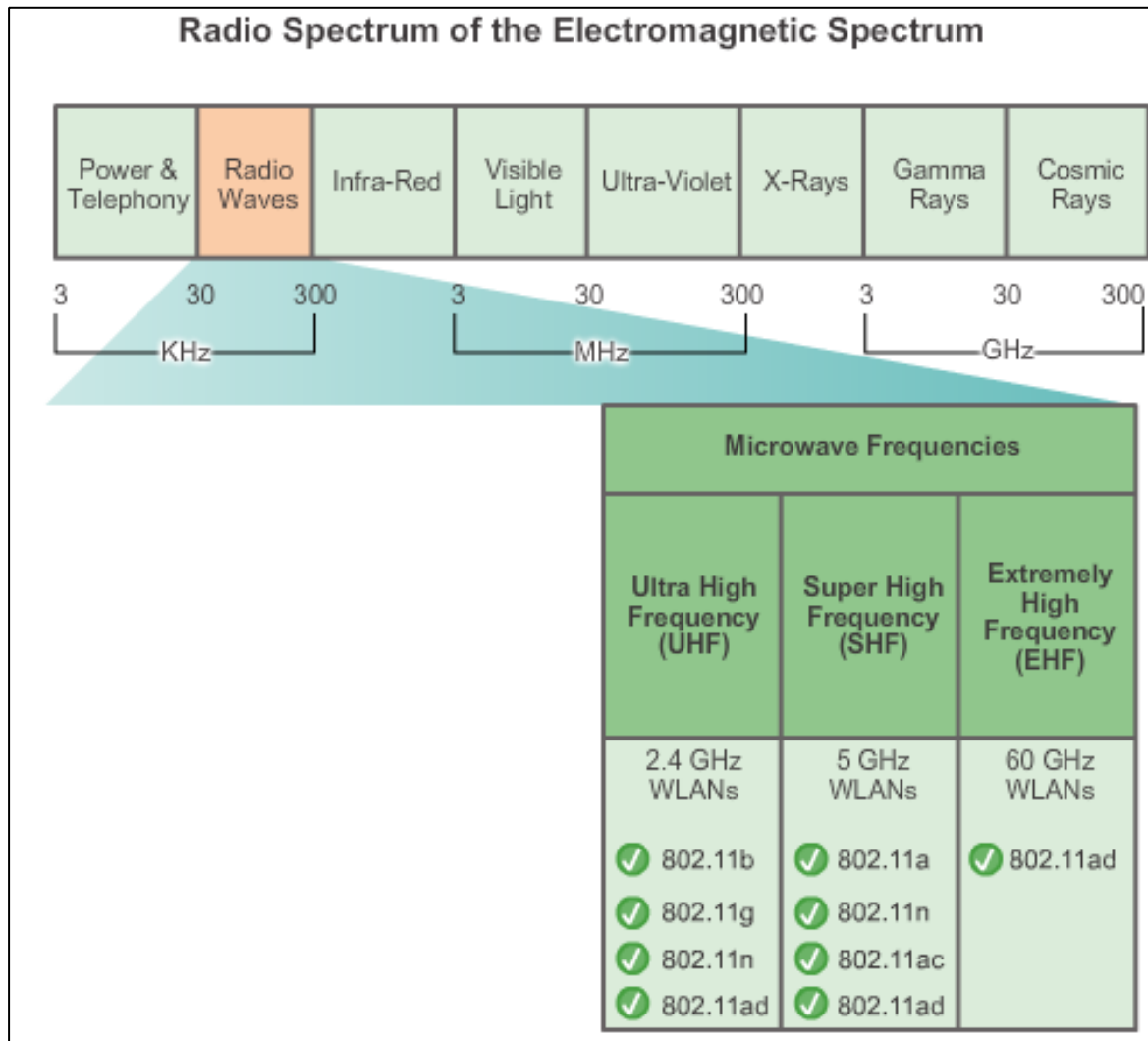
Selecting Channels

Selecting Channels (cont.)
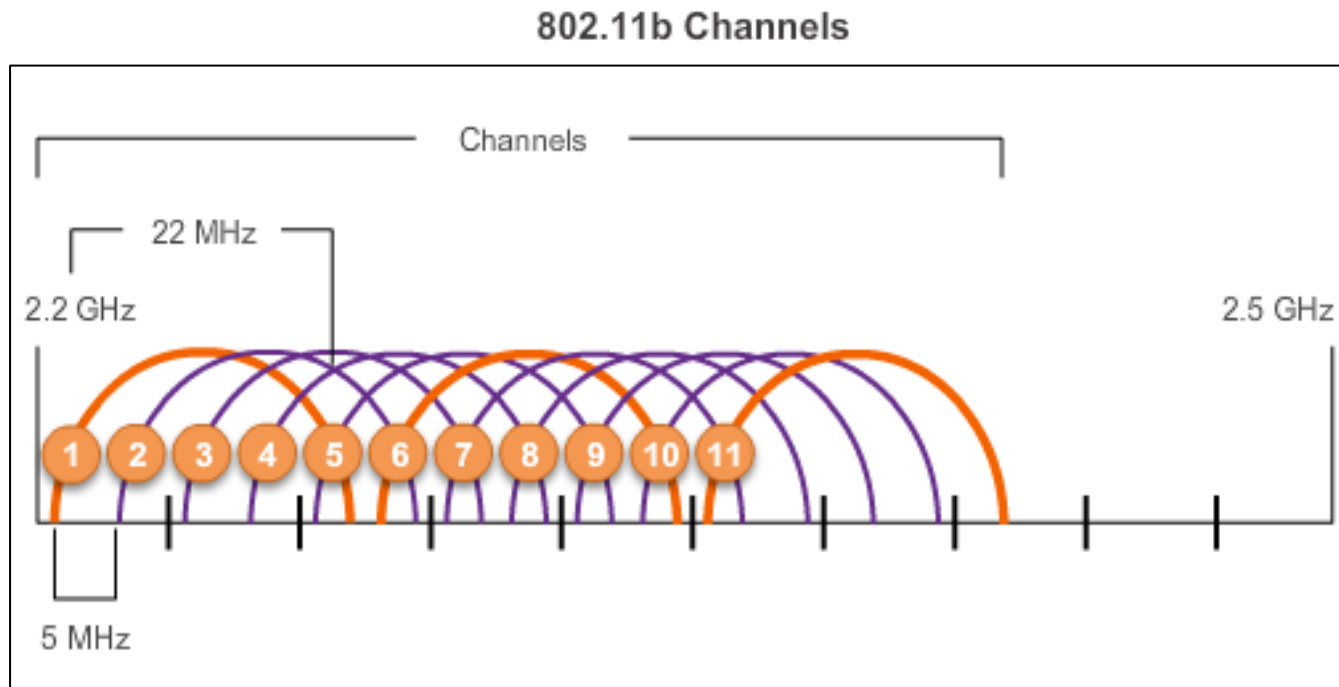
802.11b Channels

The solution to 802.11b interference is to use nonoverlapping channels 1, 6, and 11.

Selecting Channels (cont.)

802.11g/n (OFDM) Channel Width 20 MHz
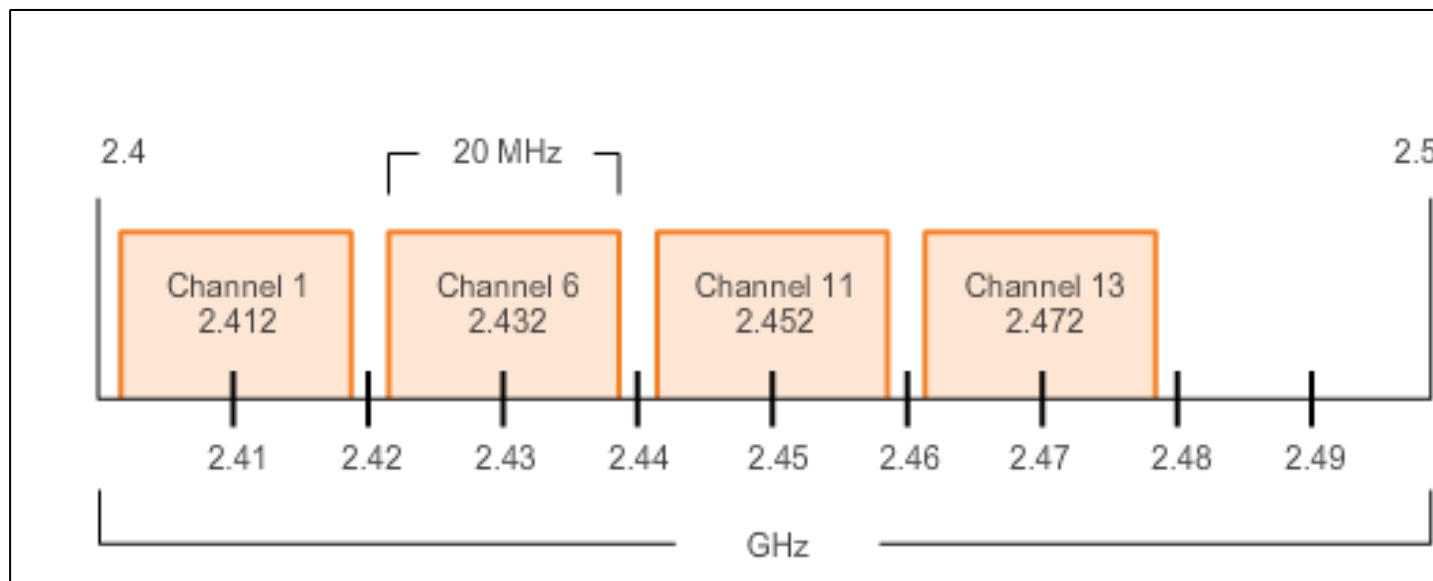
Use channels in the larger, less-crowded 5 GHz band, reducing "accidental denial of service (DoS)," this band can support four non-overlapping channels.

Selecting Channels (cont.)

802.11n (OFDM) Channel Width 40 MHz
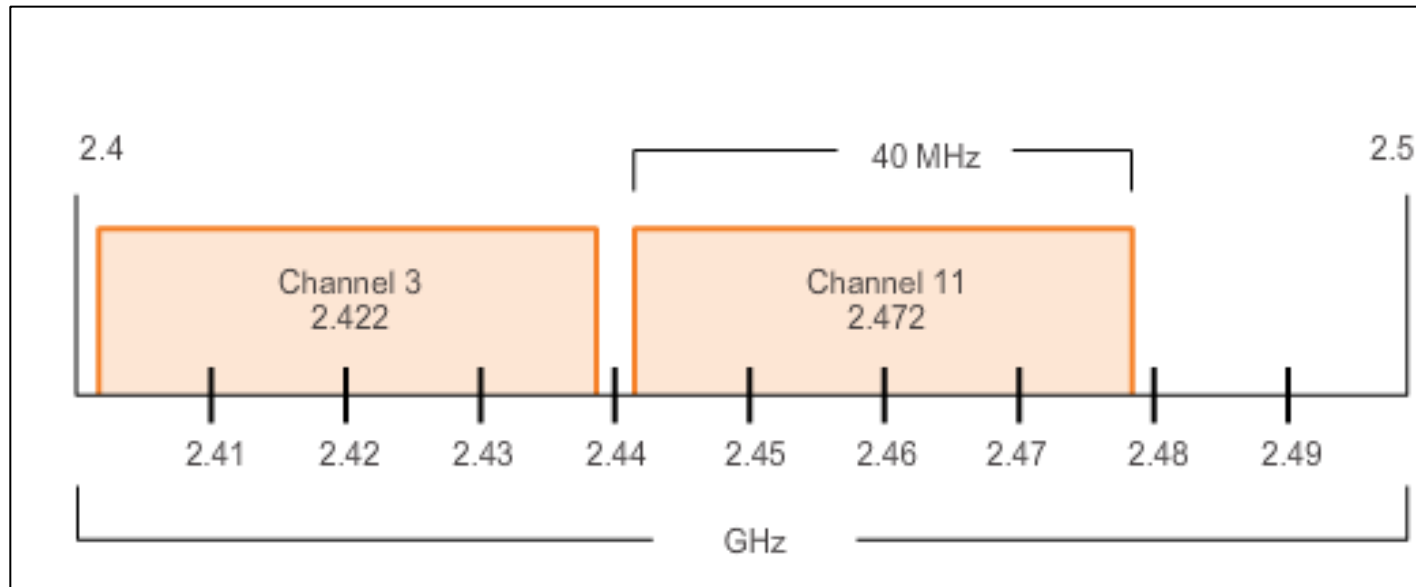
Channel bonding combines two 20-MHz channels into one 40-MHz channel.

Channel Management
Planning a WLAN Deployment
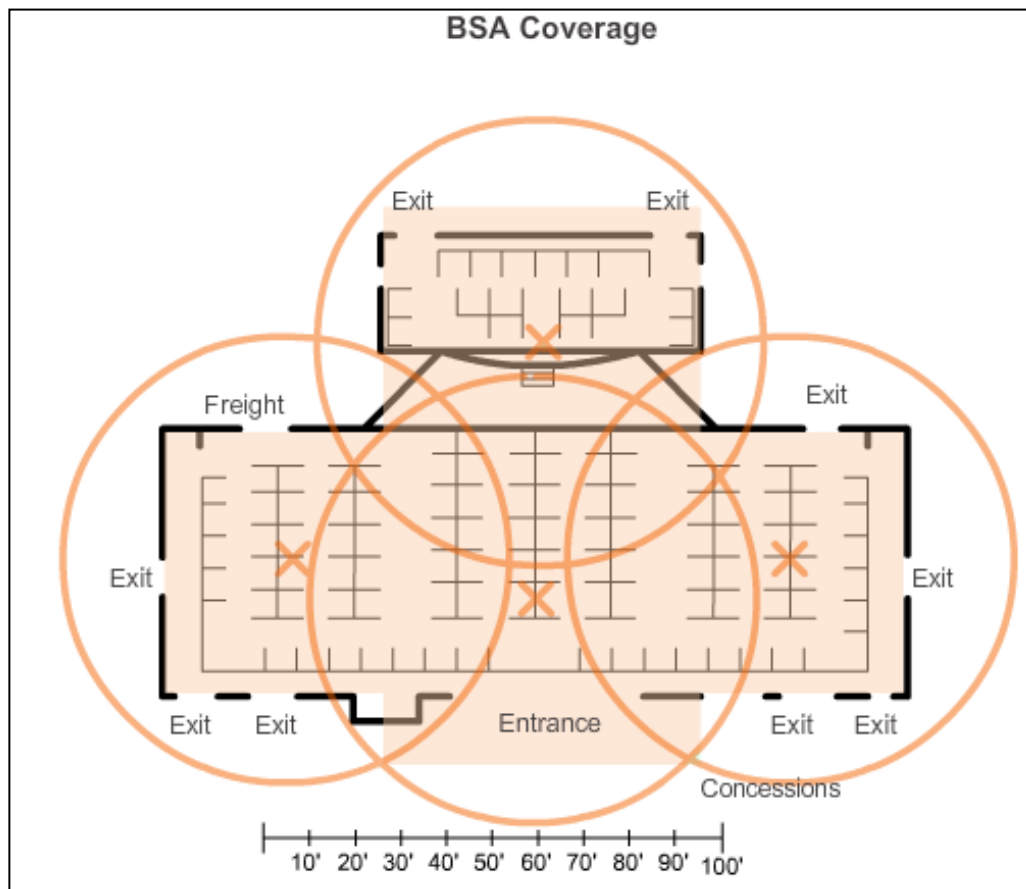
BSA Coverage

- If APs are to use existing wiring, or if there are locations where APs cannot be placed, note these locations on the map.

- Position APs above obstructions.

- Position APs vertically near the ceiling in the center of each coverage area, if possible.

- Position APs in locations where users are expected to be.

4.3 Wireless LAN Security

Securing Wireless

Common Wireless Threats

Wireless Intruders

Rogue APs

Wireless Threats

Interception of Data

Denial of Service Attacks

Rogue APs
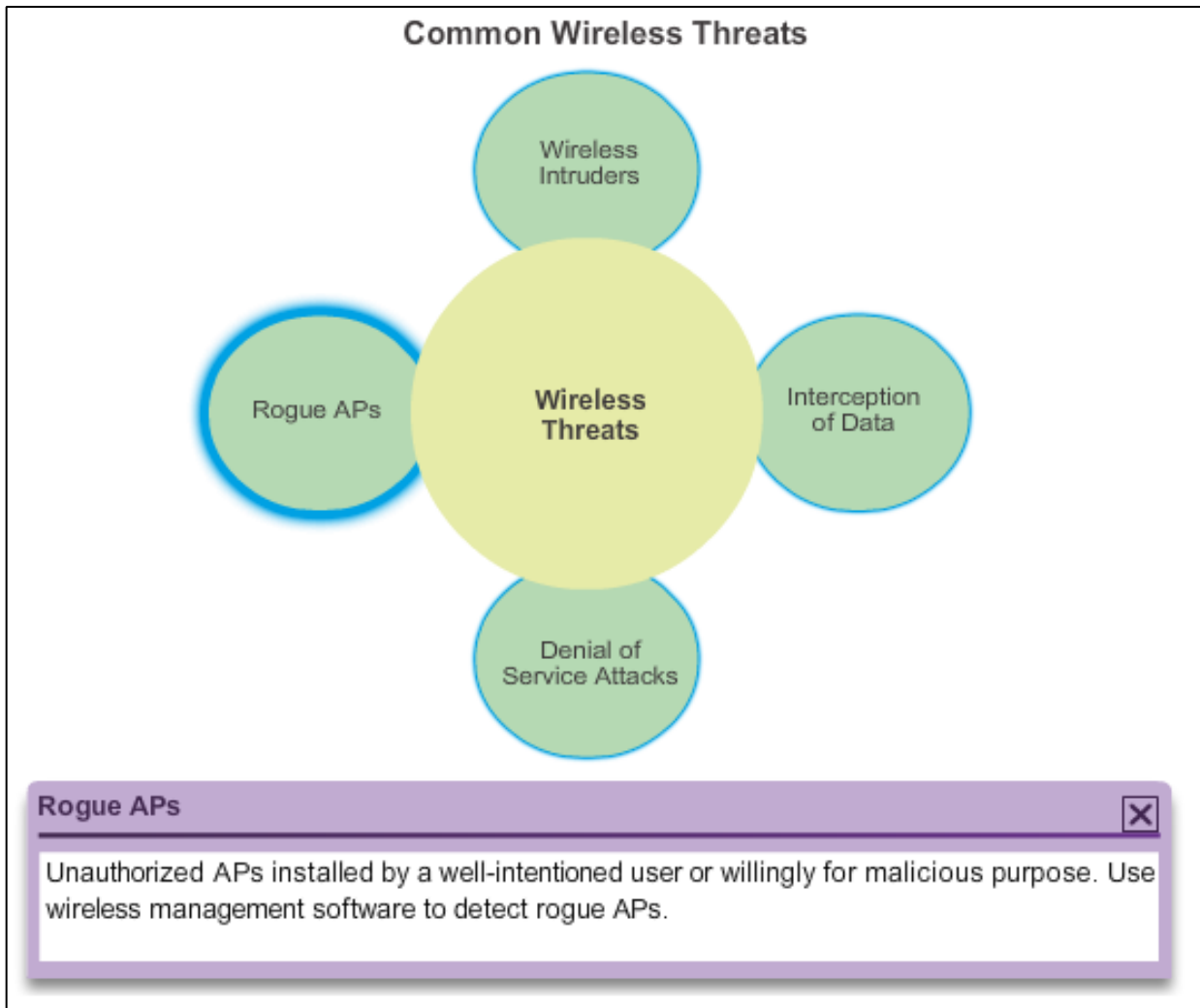
Unauthorized APs installed by a well-intentioned user or willingly for malicious purpose. Use wireless management software to detect rogue APs.

DoS Attack

Wireless DoS attacks can be the result of:

- Improperly configured devices.

- Configuration errors can disable the WLAN.

- A malicious user intentionally interfering with the wireless communication. Disable the wireless network where no legitimate device can access the medium.

Accidental interference

- WLANs operate in the unlicensed frequency bands and are prone to interference from other wireless devices.

- May occur from such devices as microwave ovens, cordless phones, baby monitors, and more.

- 2.4 GHz band is more prone to interference than the 5 GHz band.

Management Frame DoS Attacks

A spoofed disconnect attack

- Occurs when an attacker sends a series of "disassociate" commands to all wireless clients.

- Cause all clients to disconnect.

- The wireless clients immediately try to re-associate, which creates a burst of traffic.

A CTS flood

- An attacker takes advantage of the CSMA/CA contention method to monopolize the bandwidth.

- The attacker repeatedly floods Clear to Send (CTS) frames to a bogus STA.

- All wireless clients sharing the RF medium receive the CTS and withhold transmissions until the attacker stops transmitting the CTS frames.

Rogue Access Points

A rogue AP is an AP or wireless router that has been:

- Connected to a corporate network without explicit authorization and against corporate policy.

- Connected or enabled by an attacker to capture client data, such as the MAC addresses of clients (both wireless and wired), or to capture and disguise data packets, to gain access to network resources, or to launch man-in-the-middle (MITM) attacks.

- To prevent the installation of rogue APs, organizations must use monitoring software to actively monitor the radio spectrum for unauthorized APs.
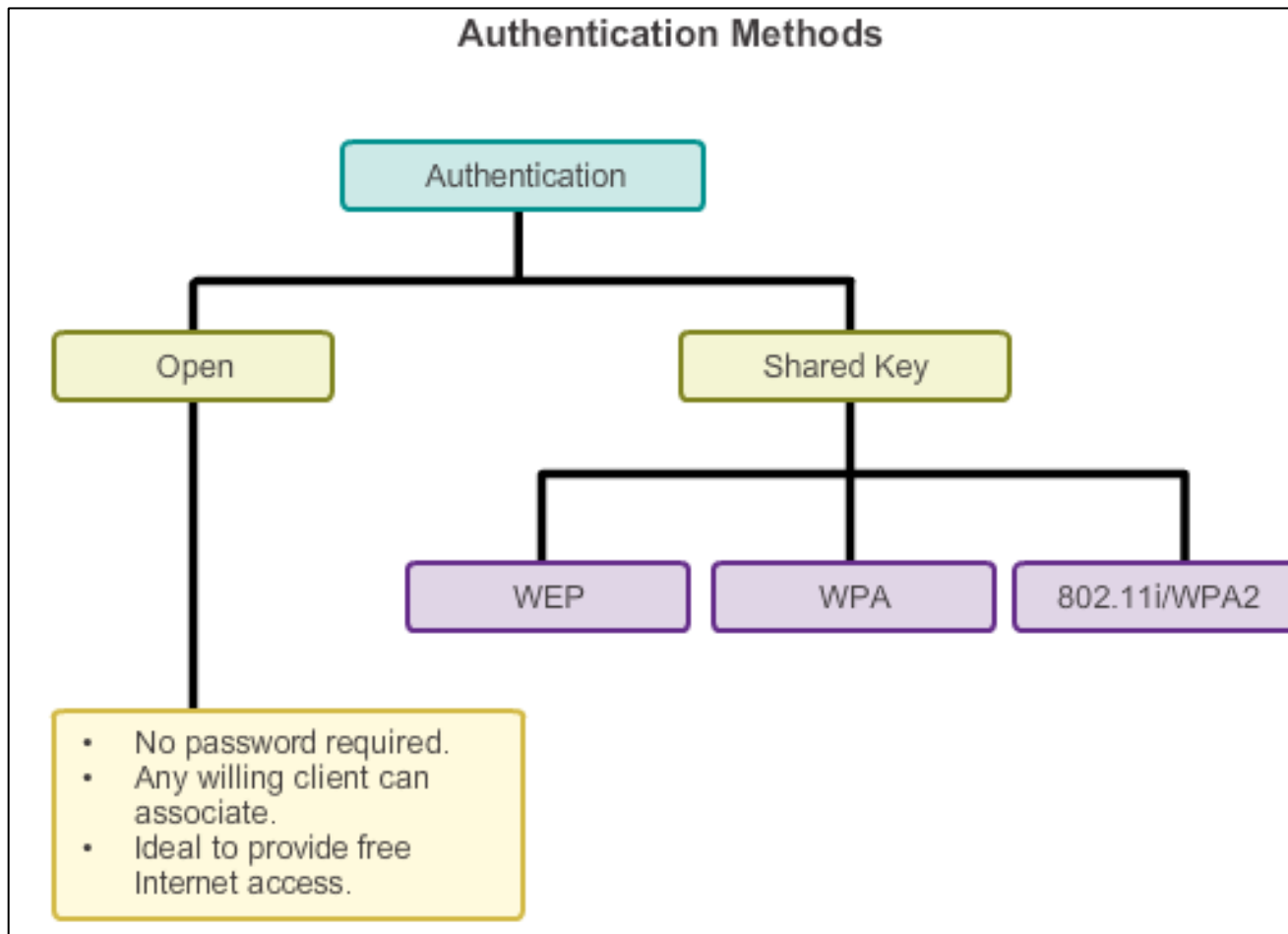
Man-in-the-Middle Attack

"Evil twin AP" attack:

- A popular wireless MITM attack where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.

- Locations offering free Wi-Fi, such as airports, cafes, and restaurants, are hotbeds for this type of attack due to the open authentication.

- Connecting wireless clients would see two APs offering wireless access. Those near the rogue AP find the stronger signal and most likely associate with the evil twin AP. User traffic is now sent to the rogue AP, which in turn captures the data and forwards it to the legitimate AP.

- Return traffic from the legitimate AP is sent to the rogue AP, captured, and then forwarded to the unsuspecting STA.

Wireless Security Overview

Use authentication and encryption to secure a wireless network.

Authentication Methods

- Authentication
  - Open
    - No password required.
    - Any willing client can associate.
    - Ideal to provide free Internet access.
  - Shared Key
    - WEP
    - WPA
    - 802.11i/WPA2

Shared Key Authentication Methods
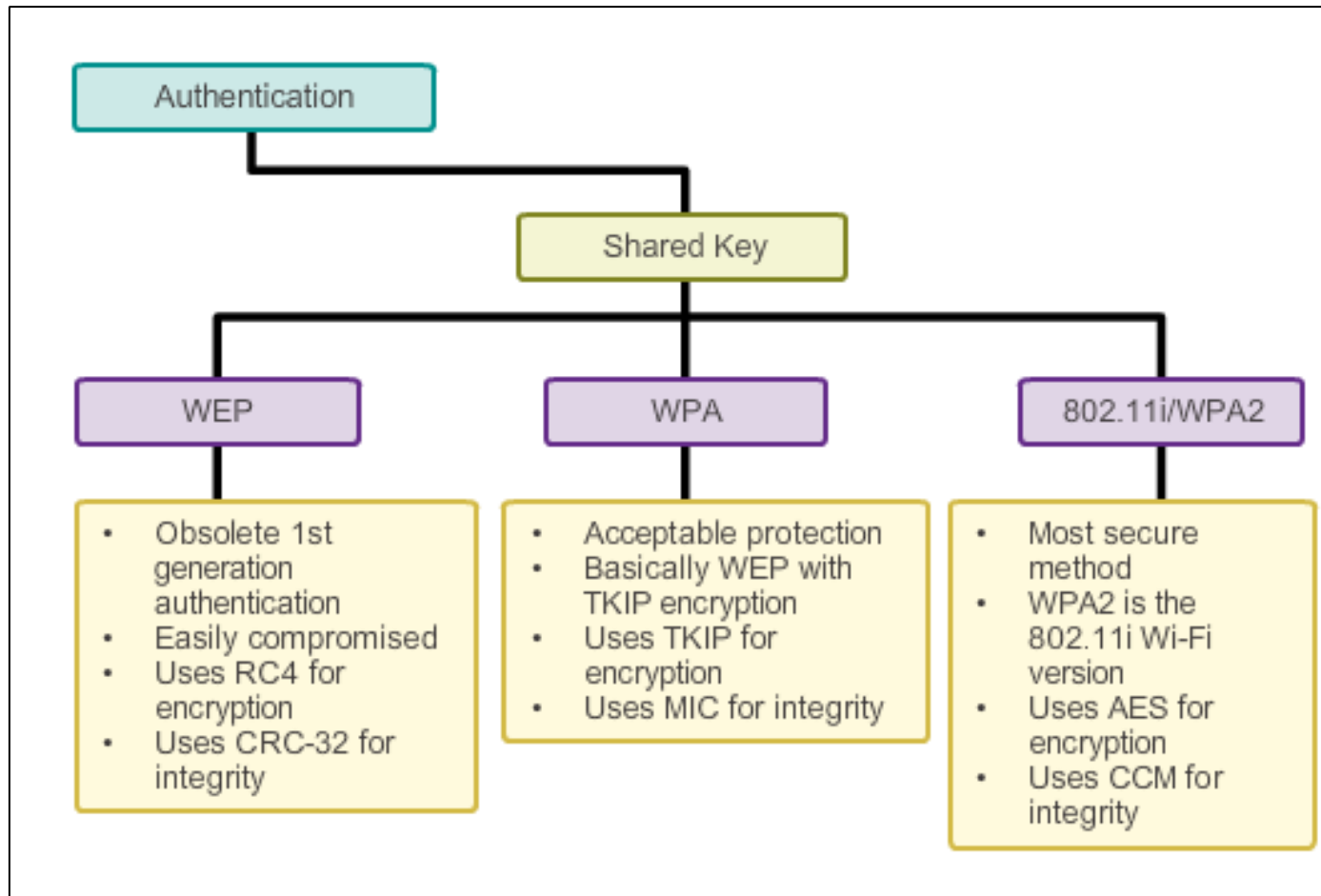
Encryption Methods

IEEE 802.11i and the Wi-Fi Alliance WPA and WPA2 standards use the following encryption protocols:

- **Temporal Key Integrity Protocol (TKIP)**
    - Used by WPA.
    - Makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Cisco Message Integrity Check (MIC).
- **Advanced Encryption Standard (AES)**
    - Encryption method used by WPA2.
    - Preferred method because it aligns with the industry standard IEEE 802.11iA.
    - Stronger method of encryption.
    - Uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP).
    - Always choose WPA2 with AES when possible.

Authenticating a Home User

WPA and WPA2 support two types of authentication:

- **Personal**

  - Intended for home or small office networks, or authenticated users who use a pre-shared key (PSK).

  - No special authentication server is required.

- **Enterprise**

  - Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server.

  - Provides additional security.

  - Users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

Authentication in the Enterprise

Enterprise security mode choices require an Authentication, Authorization, and Accounting (AAA) RADIUS server.

Entering the RADIUS Server Specifics

8.4 Wireless LAN Configuration

Configuring a Wireless Router

Before installing a wireless router, consider the following settings:

Management Parameters	Settings
Network Name (SSID)	Home-Net
Network Password	cisco123
Router Password	class123
Guest Network Name	Home-Net-Guest
Guest Network Password	cisco
Linksys Smart Wi-Fi Username	My-Name
Linksys Smart Wi-Fi Password	class12345

Configuring a Wireless Router

An Implementation Plan consists of the following steps:

Step 1. Start the WLAN implementation process with a single AP and a single wireless client, without enabling wireless security.

Step 2. Verify that the client has received a DHCP IP address and can ping the local, wired default router, and then browse to the external Internet.

Step 3. Configure wireless security using WPA2/WPA Mixed Personal. Never use WEP unless no other options exist.

Step 4. Back up the configuration.

Configure a Wireless Router
Set Up and Install the Linksys EAS6500

Configuring a Linksys Smart Wi-Fi Homepage

Smart Wi-Fi Router Settings
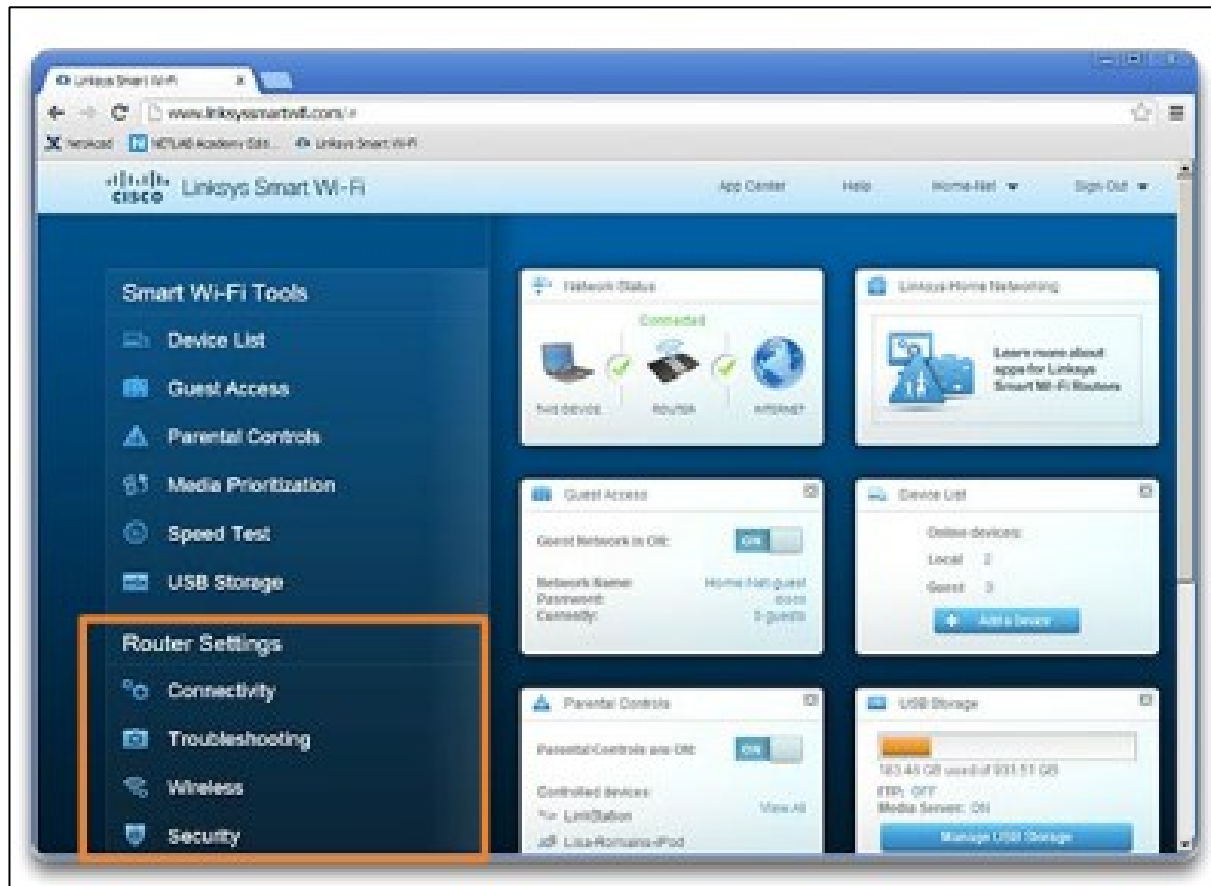
Configure a Wireless Router
Smart Wi-Fi Settings

Smart Wi-Fi settings enable you to:

- Configure the router's basic settings for the local network.

- Diagnose and troubleshoot connectivity issues on the network.

- Secure and personalize the wireless network.

- Configure the DMZ feature, view connected computers and devices on the network, and set up port forwarding.

Smart Wi-Fi Tools

- **Device List** – Lists who is connected to the WLAN. Personalize device names and icons. Connect devices.

- **Guest Access** – Creates a separate network for up to 50 guests at home while keeping network files safe with the Guest Access Tool.

- **Parental Controls** – Protects kids and family members by restricting access to potentially harmful websites

- **Media Prioritization** – Prioritizes bandwidth to specific devices and applications.

- **Speed Test** – Tests the upload and download speed of the Internet link. Useful for baselining.

- **USB Storage** – Controls access to shared files.

Configure a Wireless Router
Backing Up a Configuration

To back up the configuration with the Linksys EA6500 wireless router, perform the following steps:

Step 1. Log in to the **Smart Wi-Fi Home** page. Click the **Troubleshooting** icon to display the Troubleshooting Status window.

Step 2. Click the **Diagnostic** tab to open the Diagnostic Troubleshooting window.

Step 3. Under the Router configuration title, click **Backup** and save the file to an appropriate folder.

Connecting Wireless Clients

- After the AP or wireless router has been configured, the wireless NIC on the client must be altered to allow it to connect to the WLAN.

- The user should verify that the client has successfully connected to the correct wireless network, because there may be many WLANs available with which to connect.

Troubleshooting Approaches

Three main troubleshooting approaches used to resolve network problems:

- **Bottom-up** – Start at Layer 1 and work up.

- **Top-down** – Start at the top layer and work down.

- **Divide-and-conquer** – Ping the destination. If the pings fail, verify the lower layers. If the pings are successful, verify the upper layers.
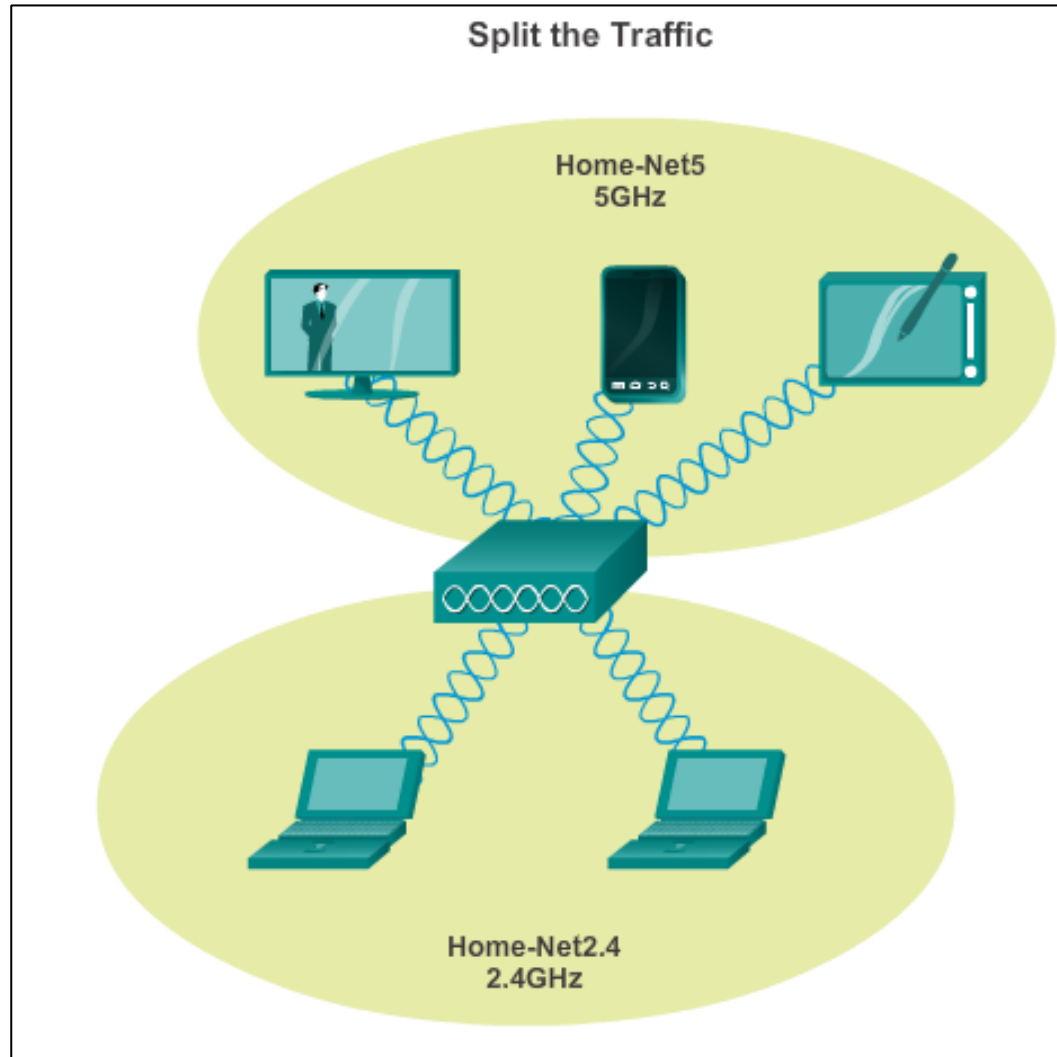
Wireless Client Not Connecting
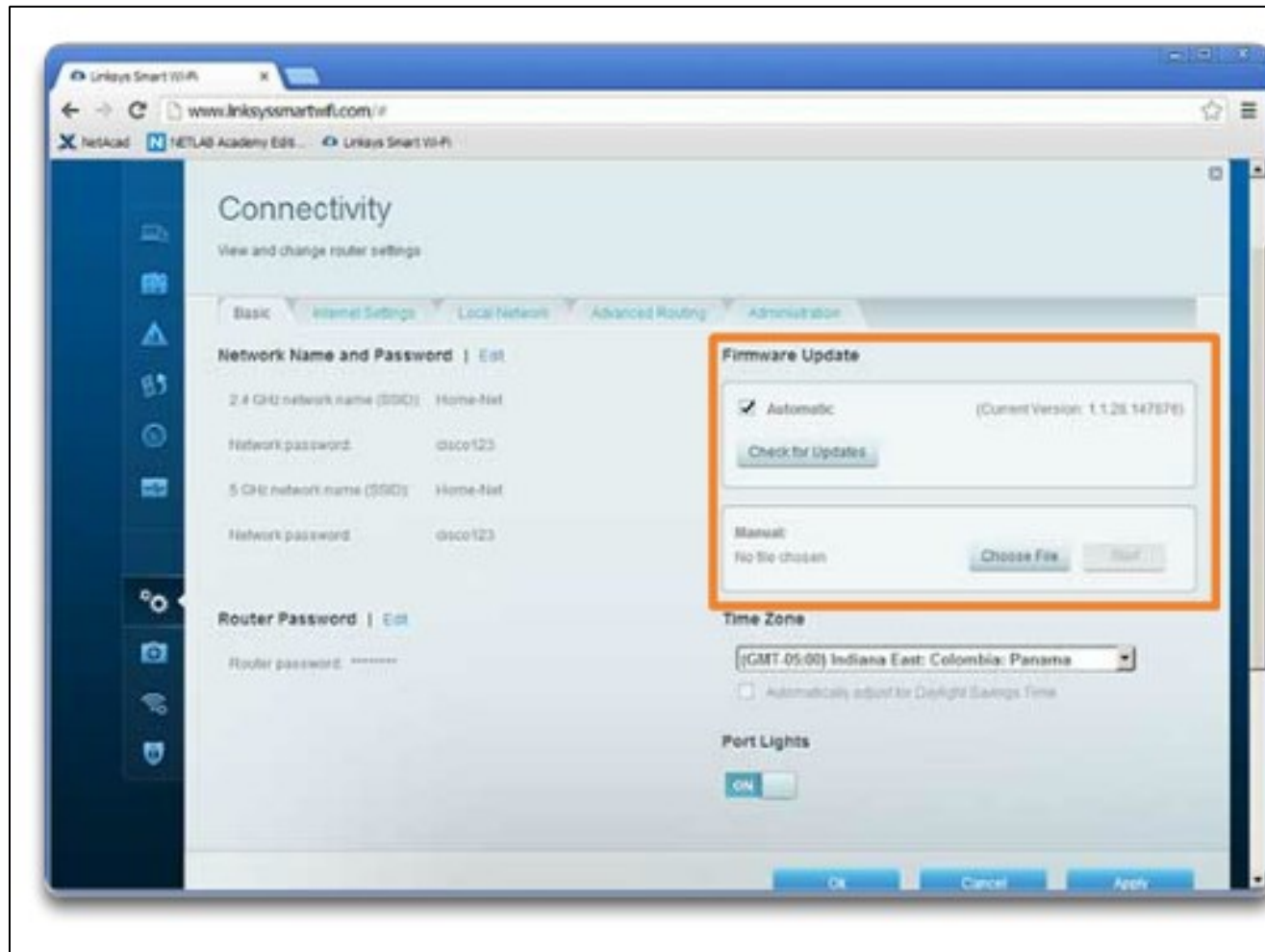

This laptop does not have connectivity.
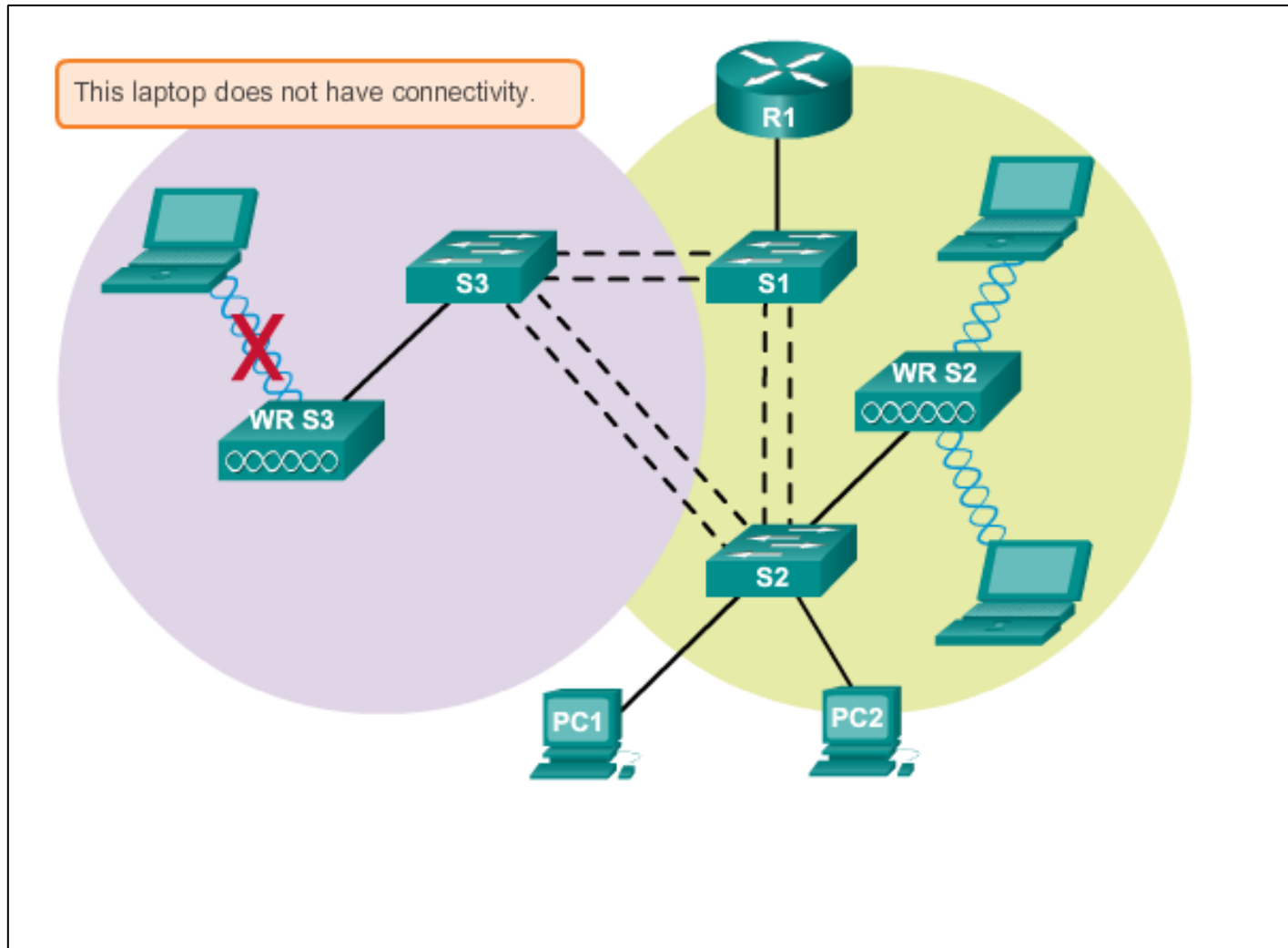
Troubleshooting When the Network Is Slow

Split the Traffic

Updating Firmware

Chapter 4: Summary

- WLANs are often implemented in homes, offices, and campus environments.

- Only the 2.4, GHz, 5.0 GHz, and 60 GHz frequencies are used for 802.11 WLANs.

- The ITU-R regulates the allocation of the RF spectrum, while IEEE provides the 802.11 standards to define how these frequencies are used for the physical and MAC sub-layer of wireless networks.

- The Wi-Fi Alliance certifies that vendor products conform to industry standards and norms.

- A STA uses a wireless NIC to connect to an infrastructure device such as a wireless router or wireless AP.

- STAs connect using an SSID.

- APs can be implemented as standalone devices, in small clusters, or in a larger controller-based network.

Chapter 4: Summary (cont.)

- A Cisco Aironet AP can use an onmidirectional antenna, a directional antenna, or a yagi antenna to direct signals.

- IEEE 802.11n/ac/ad use MIMO technology to improve throughput and support up to four antennas, simultaneously.

- In ad-hoc mode or IBSS, two wireless devices connect to each other in a P2P manner.

- In infrastructure mode, APs connect to network infrastructure using the wired DS.

- Each AP defines a BSS and is uniquely identified by its BSSID.

- Multiple BSSs can be joined into an ESS.

- Using a particular SSID in an ESS provides seamless roaming capabilities among the BSSs in the ESS.

Chapter 4: Summary (cont.)

- Additional SSIDs can be used to segregate the level of network access defined by which SSID is in use.

- An STA first authenticates with an AP, and then associates with that AP.

- The 802.11i/WPA2 authentication standard should be used. Use the AES encryption method with WPA2.

- When planning a wireless network, nonoverlapping channels should be used when deploying multiple APs to cover a particular area. There should be a 10–15 percent overlap between BSAs in an ESS.

- Cisco APs support PoE to simplify installation.

- Wireless networks are specifically susceptible to threats such as wireless intruders, rogue APs, data interception, and DoS attacks. Cisco has developed a range of solutions to mitigate against these types of threats.

Cisco Confidential