



## Chapter 4: Wireless LANs



## Scaling Networks

Cisco | Networking Academy®  
Mind Wide Open™



# Chapter 4

## 4.0 Introduction

## 4.1 Wireless LAN Concepts

## 4.2 Wireless LAN Operations

## 4.3 Wireless LAN Security

## 4.4 Wireless LAN Configuration

## 4.5 Summary



# 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



Cisco | Networking Academy®  
Mind Wide Open™



## WLAN Components

# 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.



## WLAN Components

# Benefits of Wireless

- Increased flexibility
- Increased productivity
- Reduced costs
- Ability to grow and adapt to changing requirements





## WLAN Components

# 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).



## WLAN Components

# Wireless Technologies (cont.)

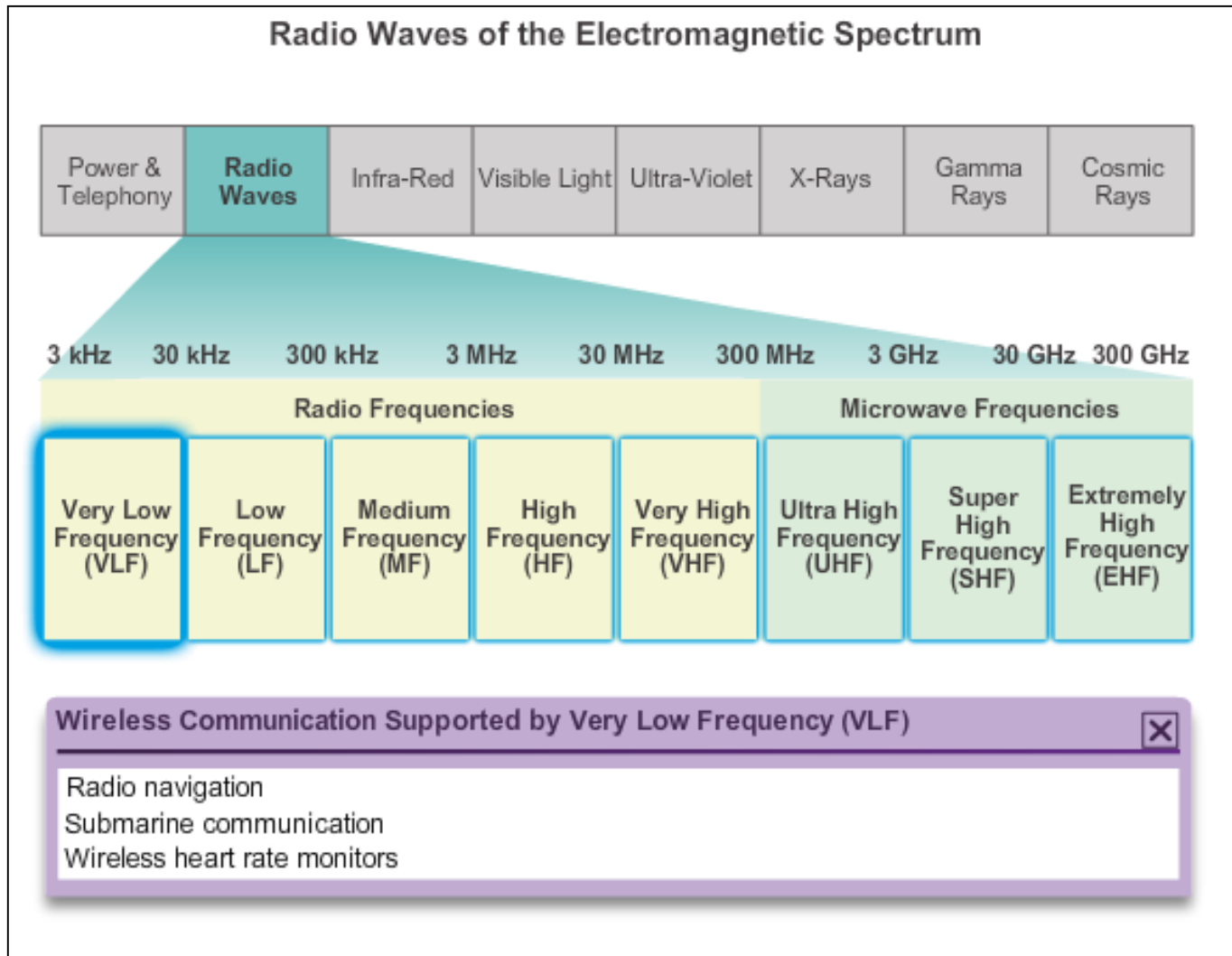
- **Worldwide Interoperability for Microwave Access (WiMAX)** – An IEEE 802.16 WWAN standard that provides wireless broadband access of up to 30 mi (50 km).
- **Cellular broadband** – Consists of various corporate, national, and international organizations using service provider cellular access to provide mobile broadband network connectivity.
- **Satellite Broadband** – Provides network access to remote sites through the use of a directional satellite dish.





# WLAN Components

## Radio Frequencies





# WLAN Components

## 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



## WLAN Components

# 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



## WLAN Components

# 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



## Components of WLANs

# 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



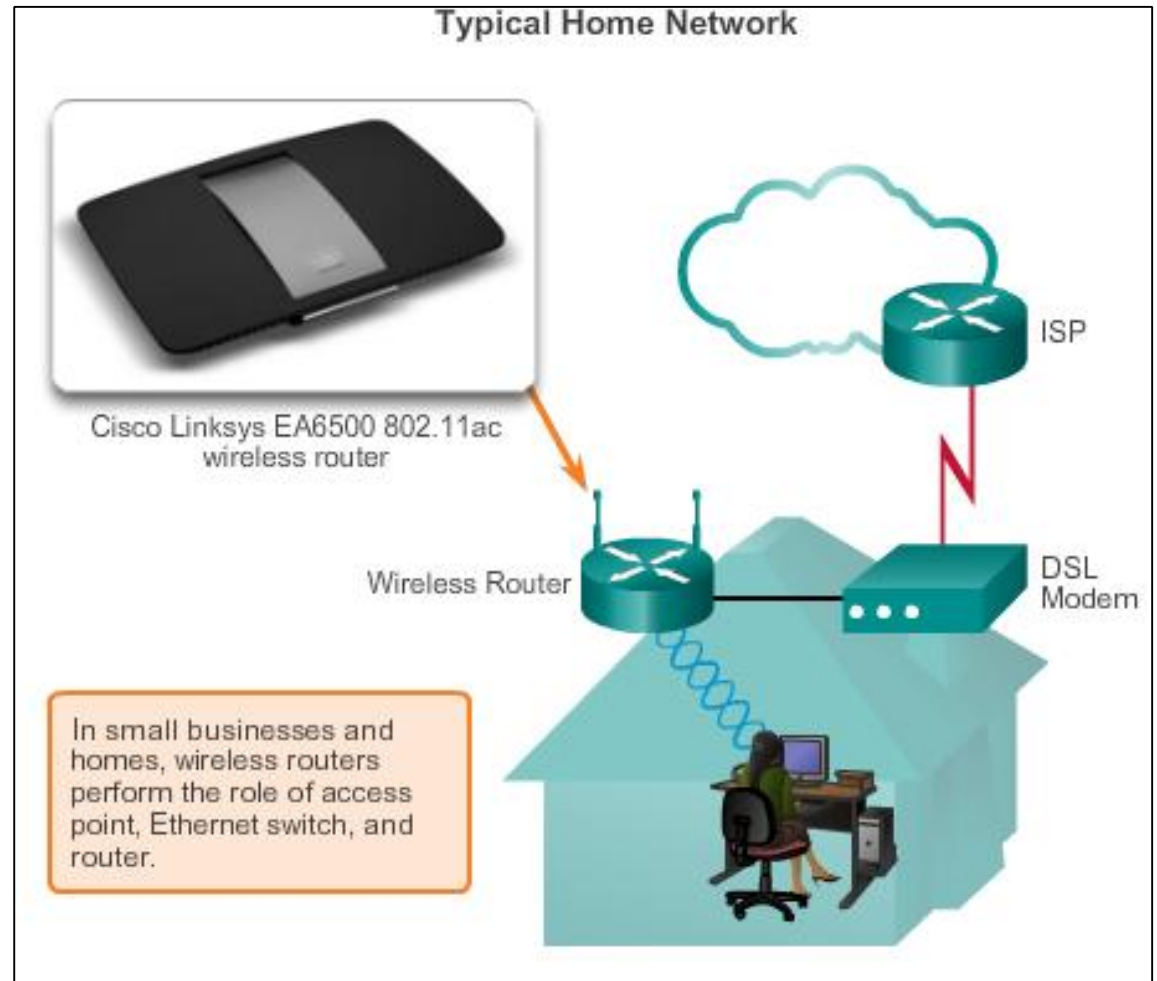
## Components of WLANs

# Wireless Home Router

A home user typically interconnects wireless devices using a small, integrated wireless router.

These serve as:

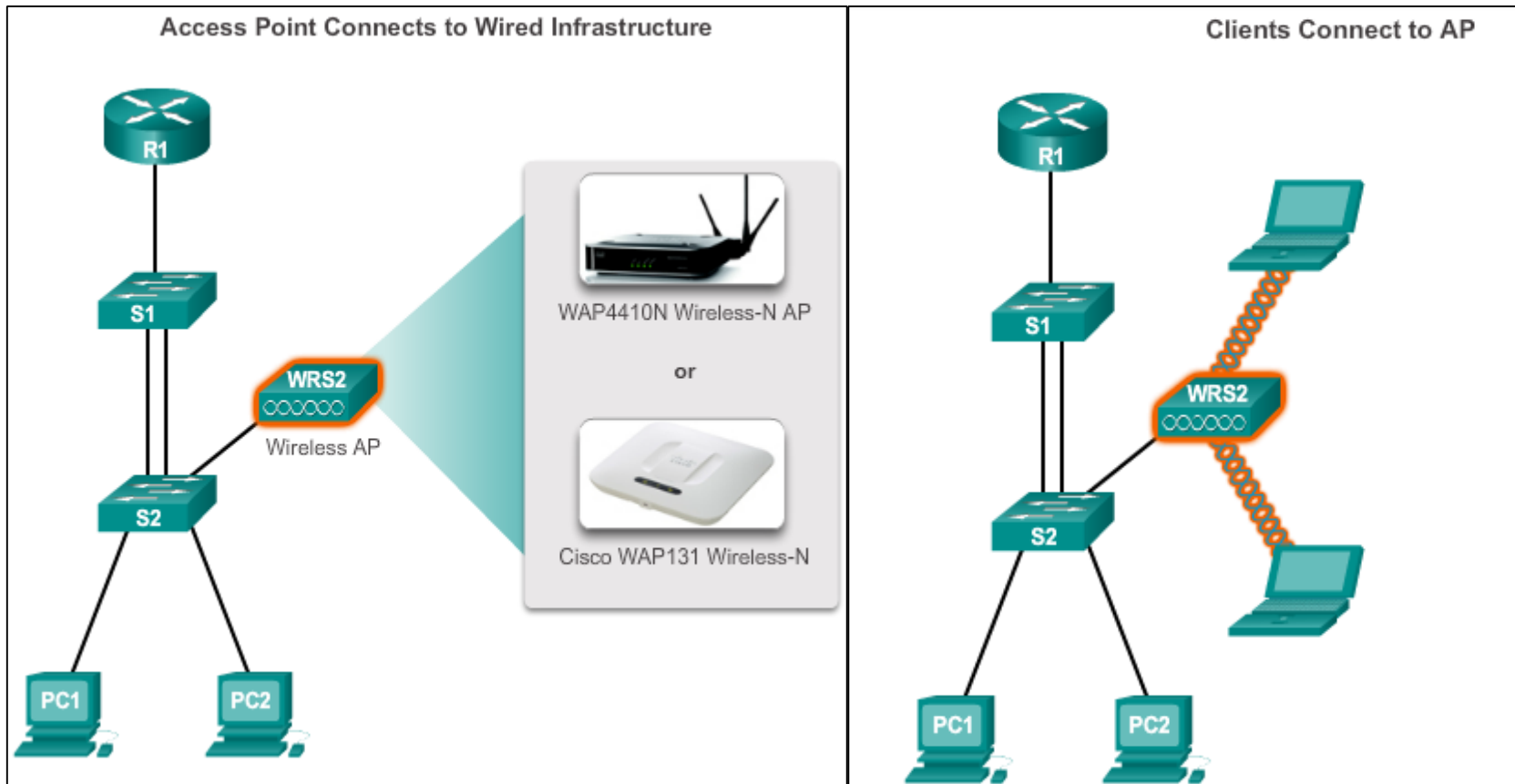
- access point
- Ethernet switch
- router





# Components of WLANs

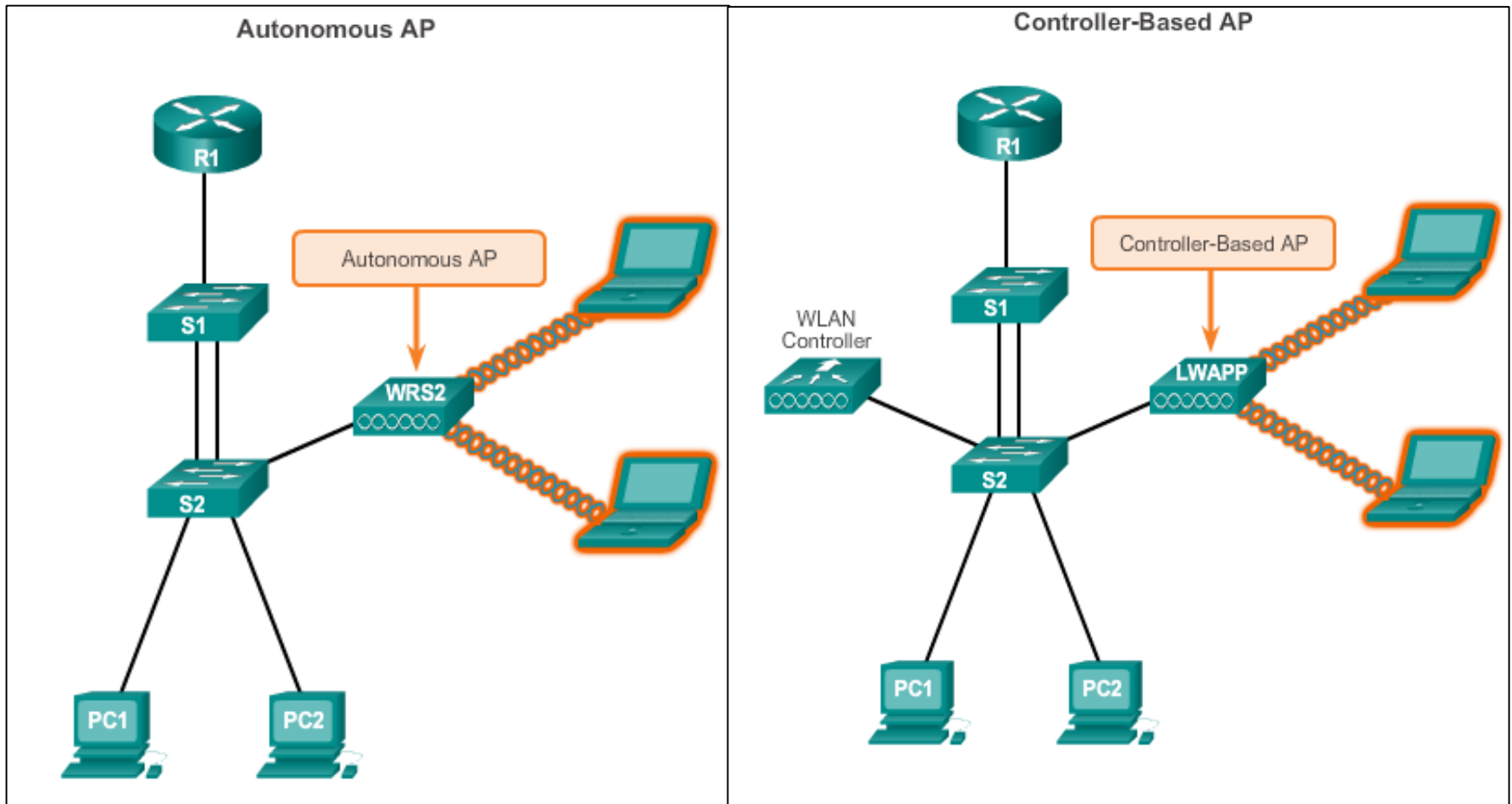
## Business Wireless Solutions





# Components of WLANs

## Wireless Access Points







## Components of WLANs

# 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



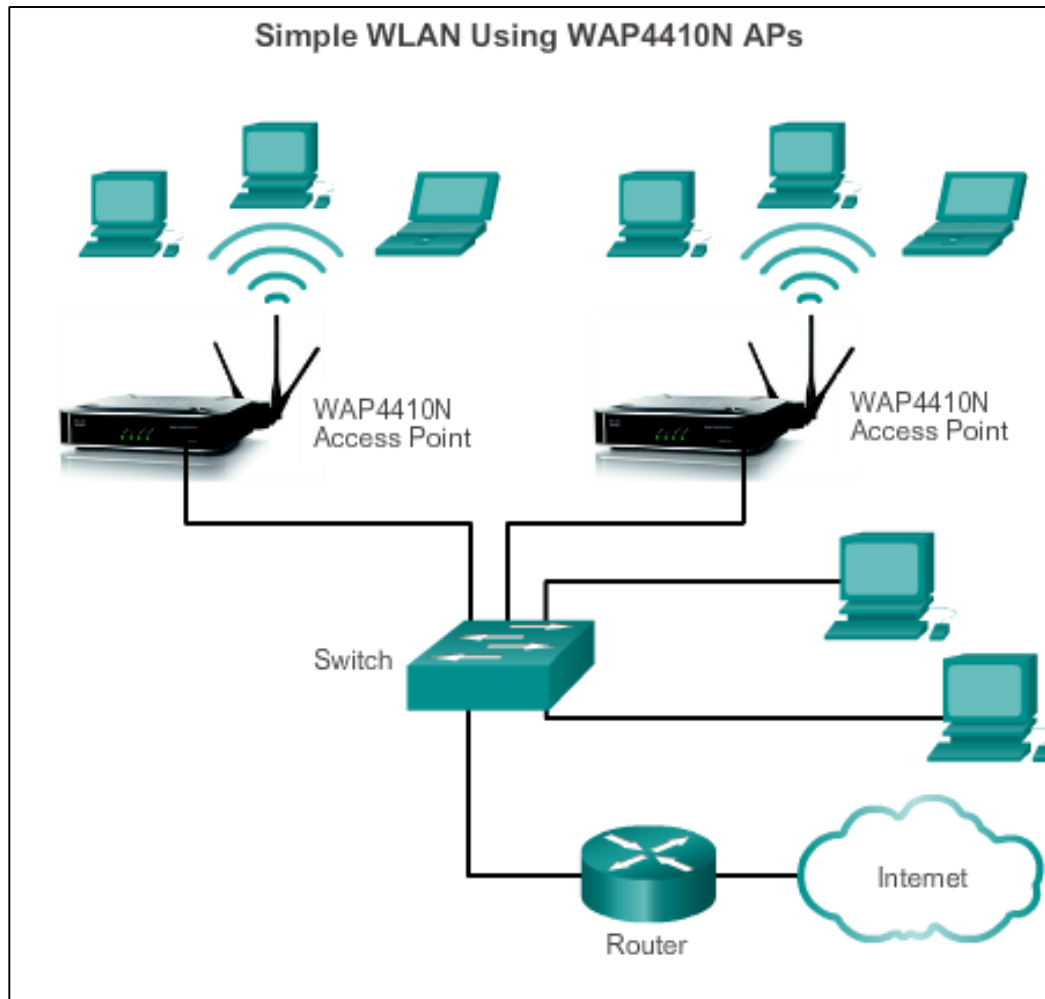
#### Cisco AP541N

- 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.)

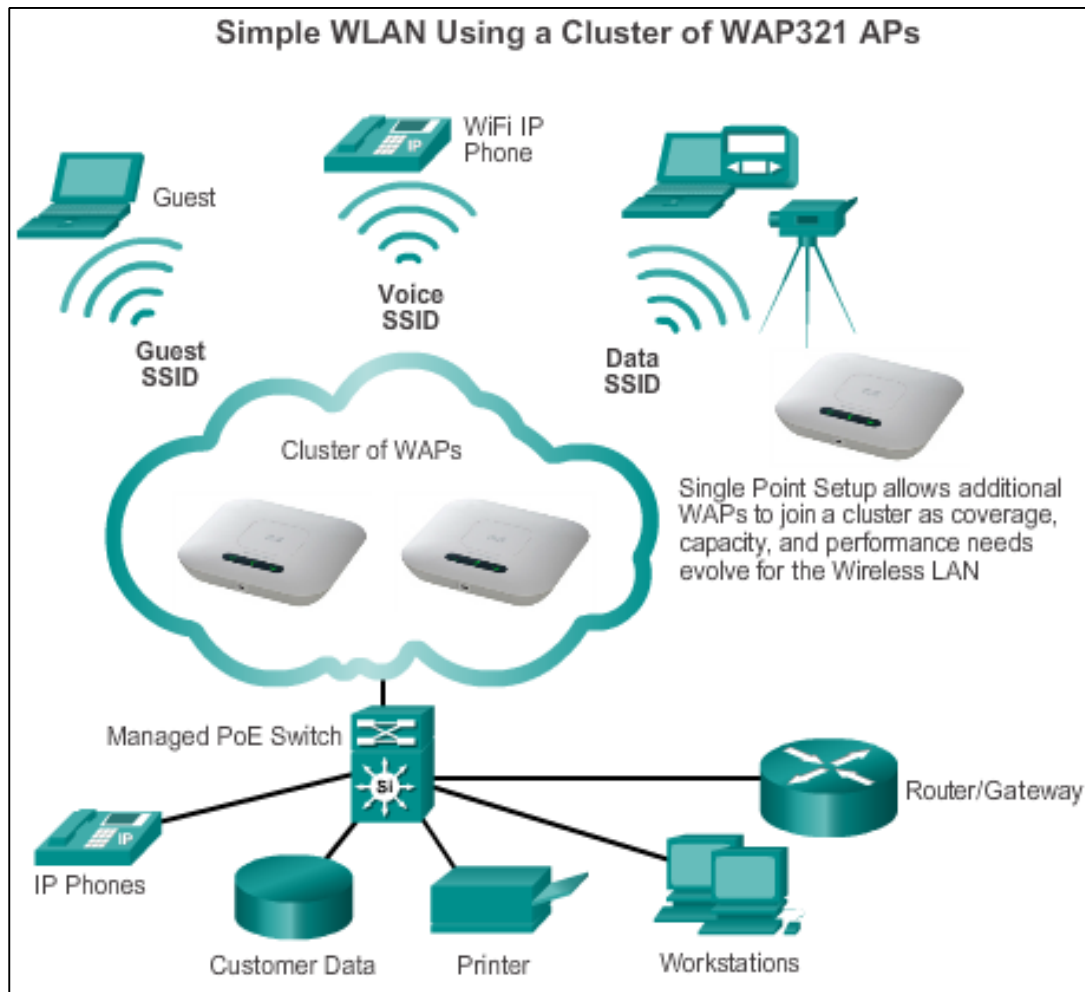


- Each AP is configured and managed individually.
- This can become a problem when several APs are required.



## Components of WLANs

# Small Wireless Deployment Solutions



- 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.



## Components of WLANs

# 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.





## Components of WLANs

# 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



## Components of WLANs

# 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)



## Components of WLANs

# Wireless Antennas

Cisco Aironet APs can use:

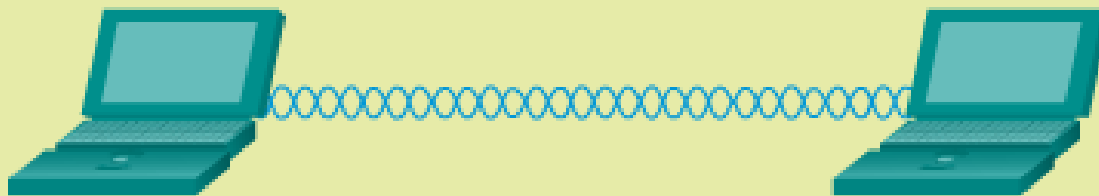
- **Omnidirectional Wi-Fi Antennas** – Factory Wi-Fi gear often uses basic dipole antennas, also referred to as “rubber duck” design, similar to those used on walkie-talkie radios. Omnidirectional antennas provide 360-degree coverage.
- **Directional Wi-Fi Antennas** – Directional antennas focus the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

# 802.11 Wireless Topology Modes

### Ad Hoc Mode



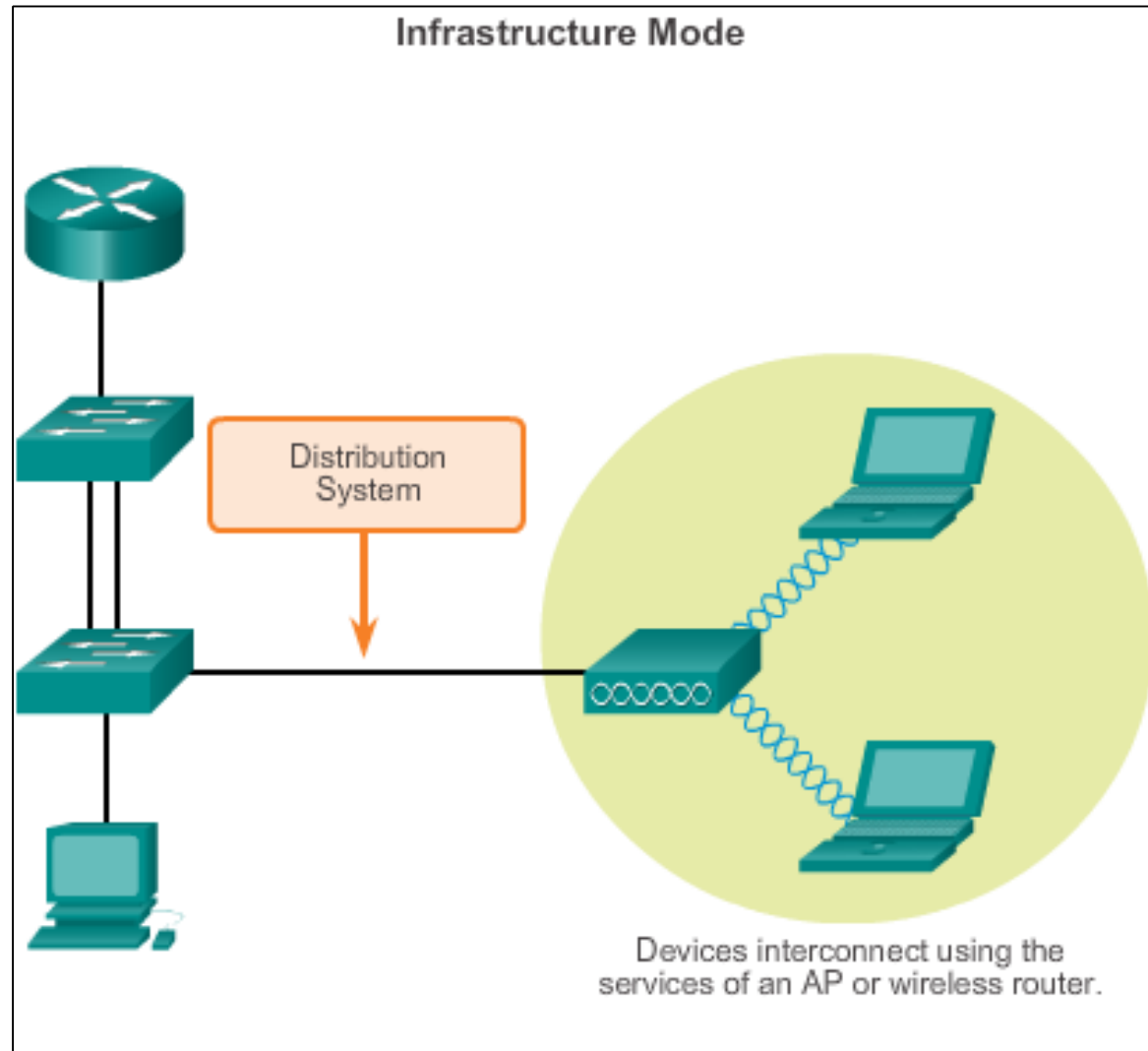
Devices interconnect directly without the use an AP or wireless router.





## 802.11 WLAN Topologies

# 802.11 Wireless Topology Modes (cont.)

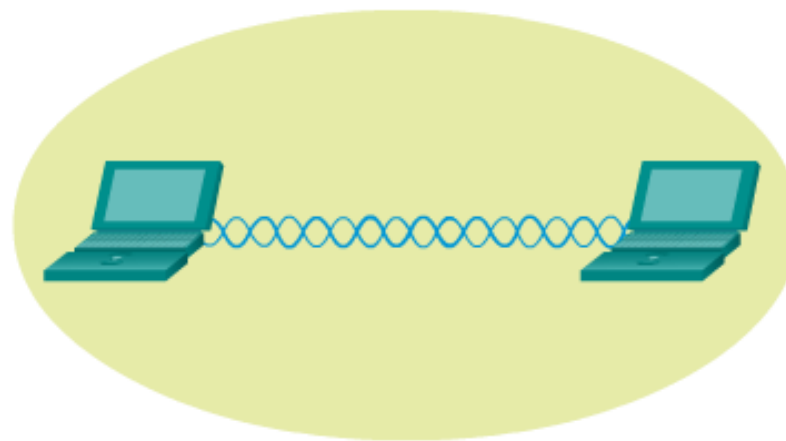




## 802.11 WLAN Topologies

# 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

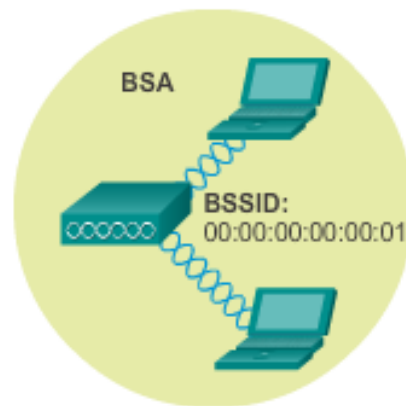
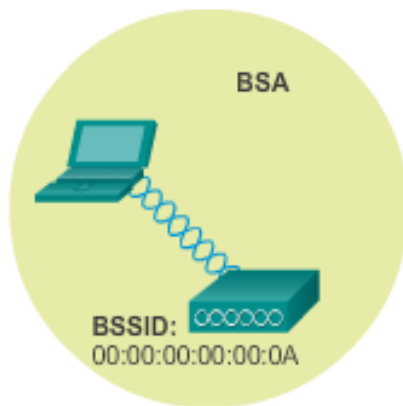
WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)



# 802.11 WLAN Topologies

## Infrastructure Mode

Basic Service Set Summary



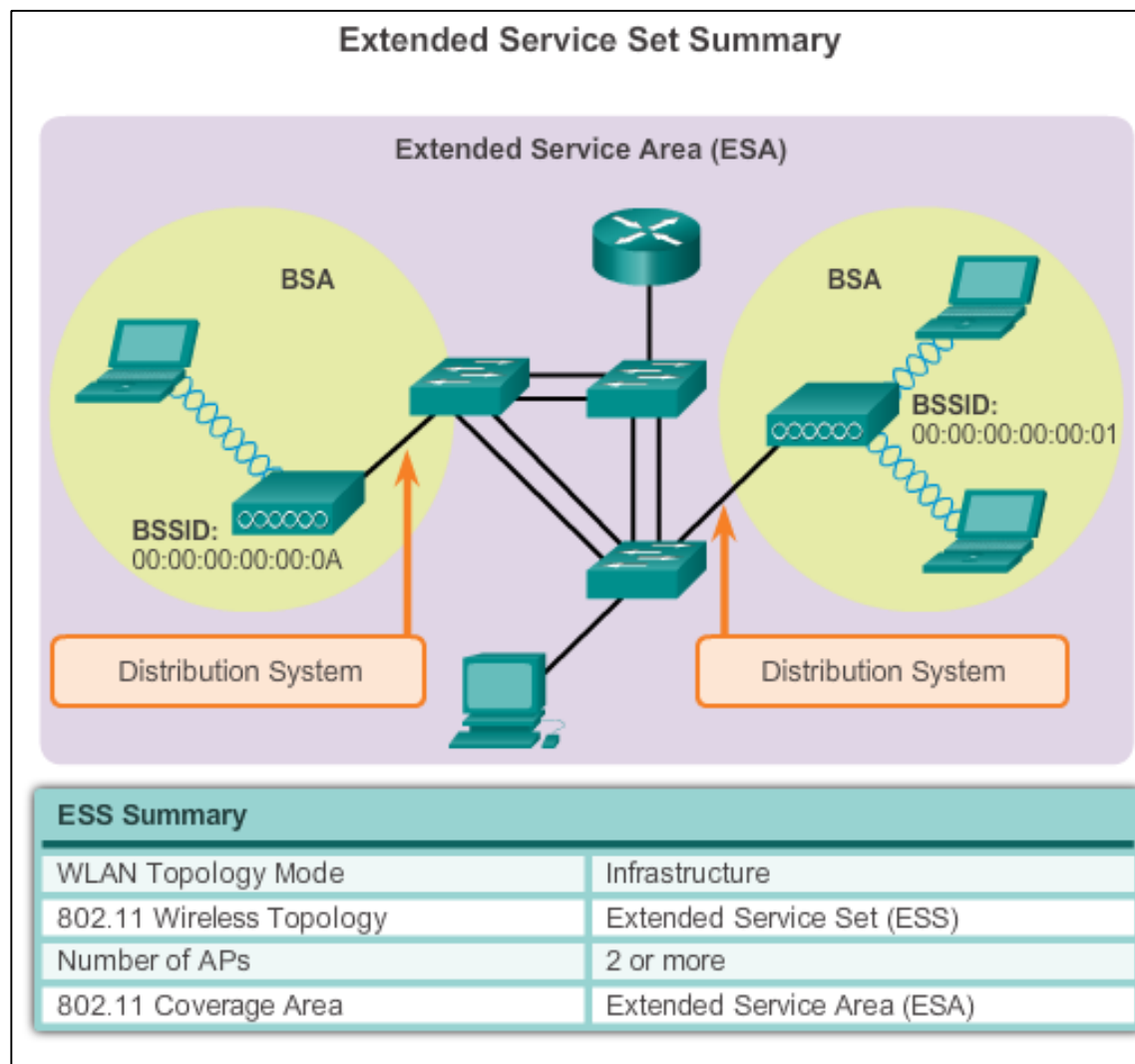
BSS Summary

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



# 802.11 WLAN Topologies

## Infrastructure Mode (cont.)





## 4.2 Wireless LAN Operations

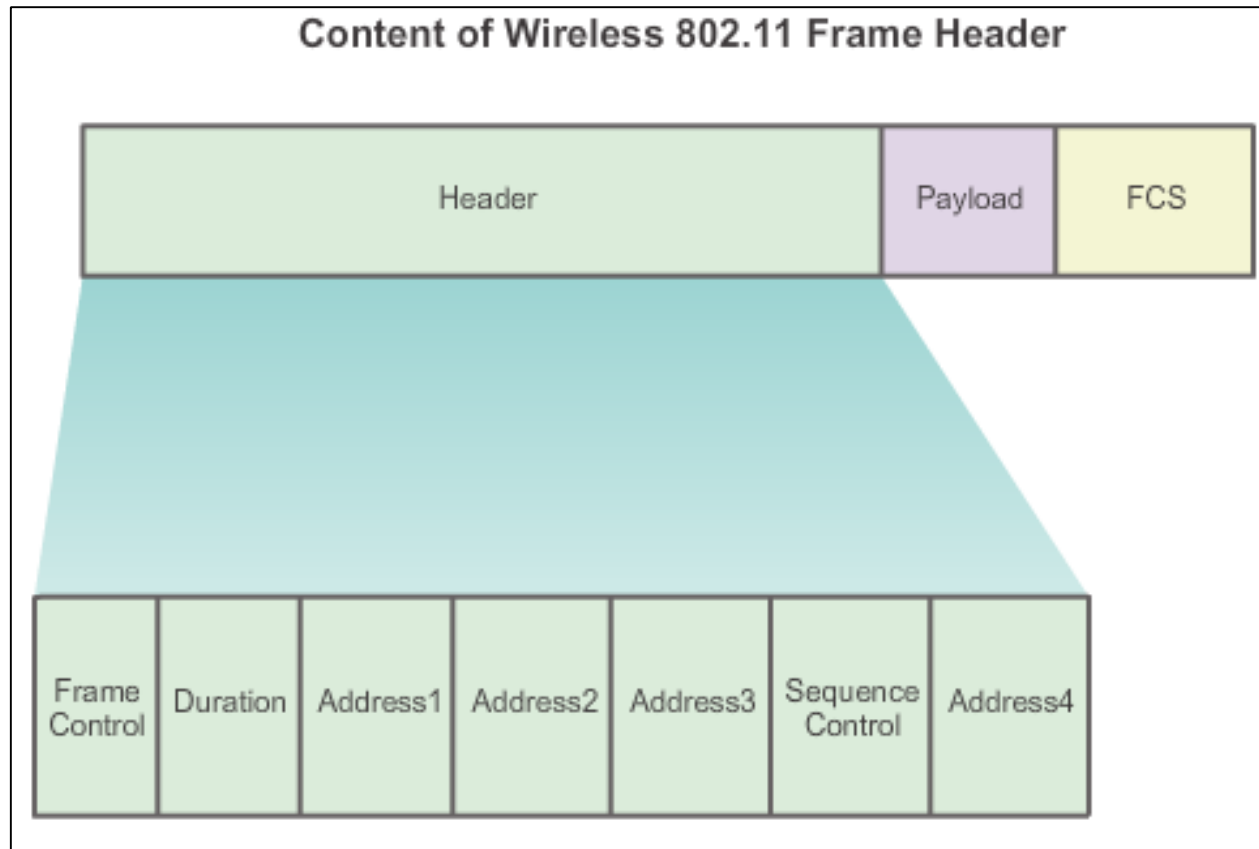


Cisco | Networking Academy®  
Mind Wide Open™



## 802.11 Frame Structure

# Wireless 802.11 Frame





## 802.11 Frame Structure

# Wireless 802.11 Frame

The image shows a Wireshark capture of 802.11 frames. The packet list at the top shows four packets, all of type 'Broadcast' and '802.11 Beacon frame'. The packet details pane for the first packet (Frame 1) is expanded, showing the 'IEEE 802.11 Beacon frame' structure. Two orange boxes with arrows point to specific fields:

- Frame Control Field:** Points to the 'Type/Subtype: Beacon frame (0x08)' and 'Frame Control: 0x0000 (Normal)' fields.
- Remainder of 802.11 Frame Fields:** Points to the 'Duration: 0', 'Destination address: Broadcast (ff:ff:ff:ff:ff:ff)', 'Source address: Siemens\_A1:bd:6e (00:01:e3:41:bd:6e)', 'BSS ID: Siemens\_A1:bd:6e (00:01:e3:41:bd:6e)', 'Fragment number: 0', and 'Sequence number: 1841' fields.

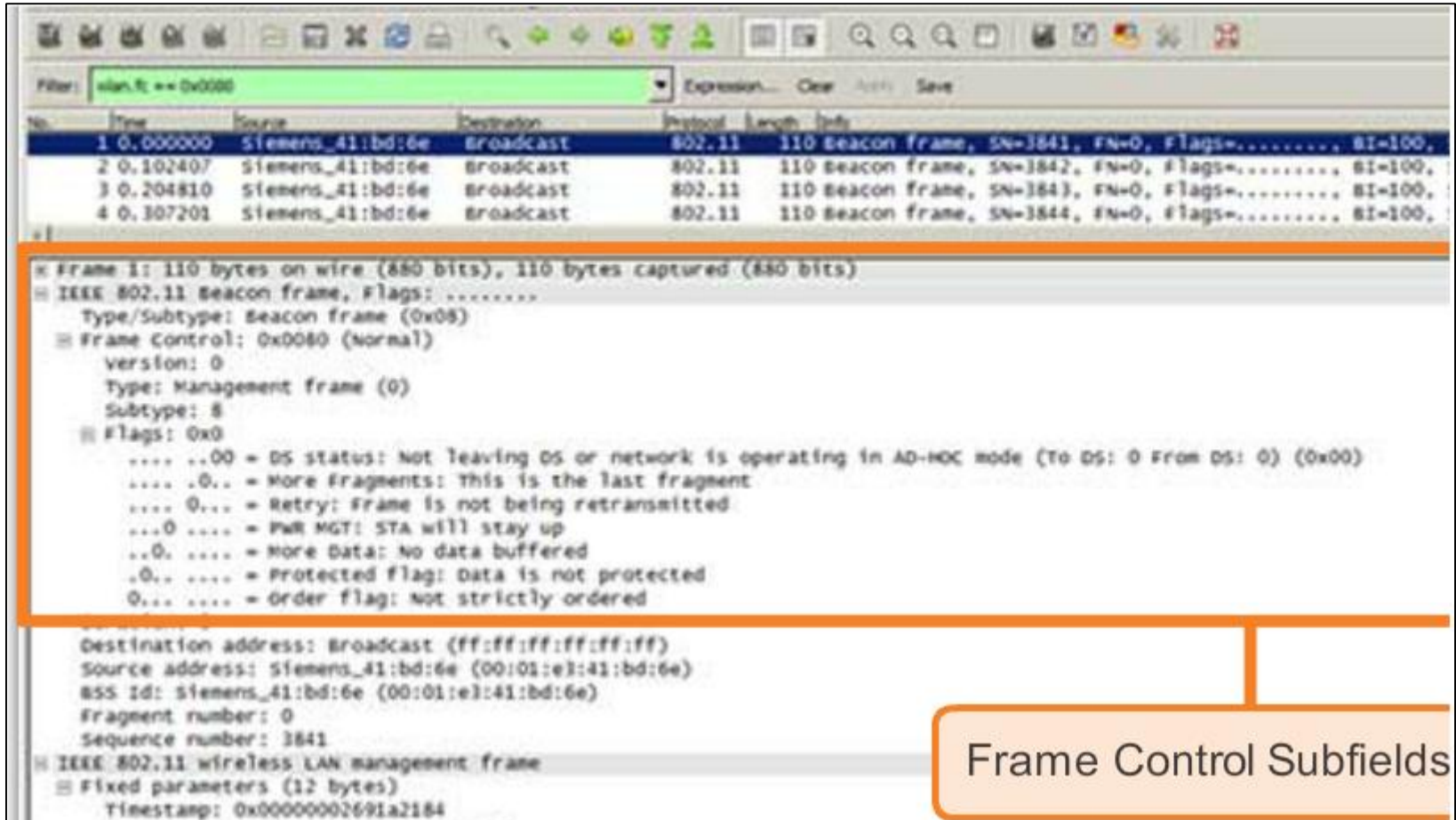
The packet bytes pane at the bottom shows the raw data of the frame, including the frame control field and the remainder of the frame fields.





# 802.11 Frame Structure

## Frame Control Field



Filter: wlan.fc == 0x0000

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3841, FN=0, Flags=....., BI=100.
2	0.102407	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3842, FN=0, Flags=....., BI=100.
3	0.204810	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3843, FN=0, Flags=....., BI=100.
4	0.307201	Siemens_41:bd:6e	Broadcast	802.11	110	Beacon frame, SN=3844, FN=0, Flags=....., BI=100.

Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

- IEEE 802.11 Beacon frame, Flags: .....
  - Type/Subtype: Beacon frame (0x08)
  - Frame Control: 0x0080 (Normal)
    - Version: 0
    - Type: Management frame (0)
    - Subtype: 8
  - Flags: 0x0
    - .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
    - .... .0.. = More Fragments: This is the last fragment
    - .... 0... = Retry: Frame is not being retransmitted
    - ...0 .... = PWR MGT: STA will stay up
    - ..0. .... = More Data: No data buffered
    - ..0.. .... = Protected flag: Data is not protected
    - 0... .... = Order flag: Not strictly ordered

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)  
 Source address: Siemens\_41:bd:6e (00:01:e3:41:bd:6e)  
 BSS Id: Siemens\_41:bd:6e (00:01:e3:41:bd:6e)  
 Fragment number: 0  
 Sequence number: 3841

IEEE 802.11 wireless LAN management frame

- Fixed parameters (12 bytes)
  - Timestamp: 0x000000002691a2184

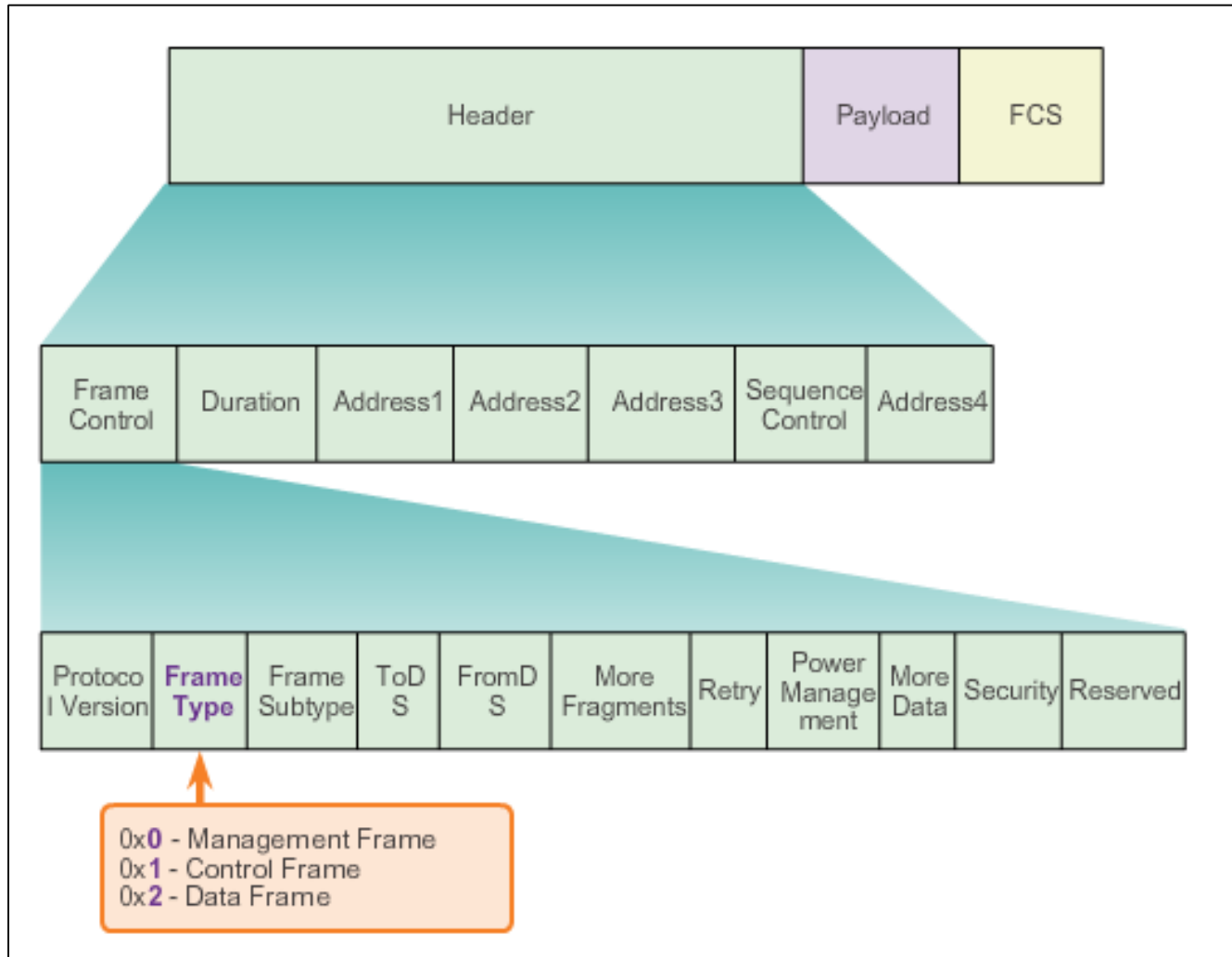
Frame Control Subfields





## 802.11 Frame Structure

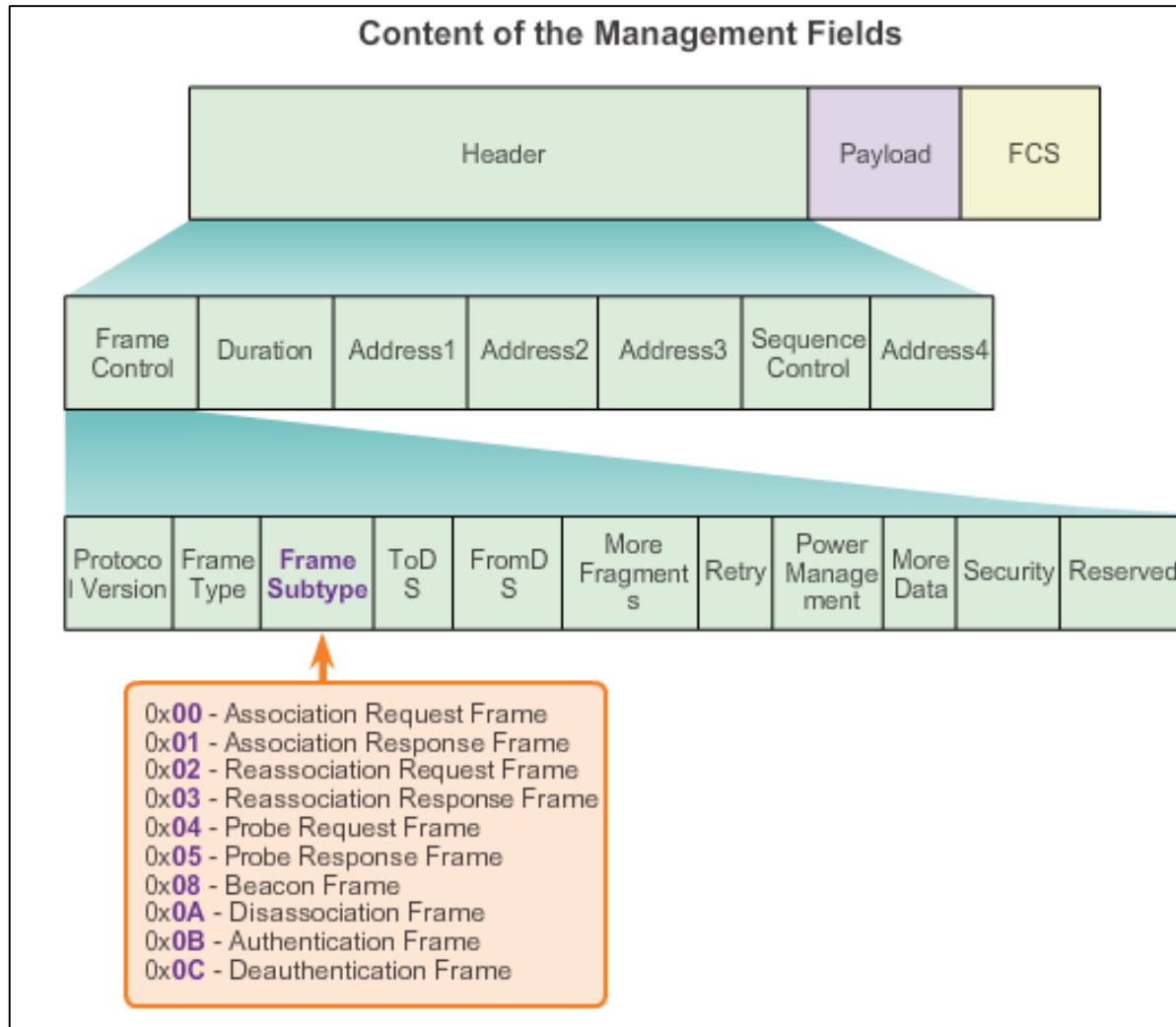
# Wireless Frame Type





# 802.11 Frame Structure

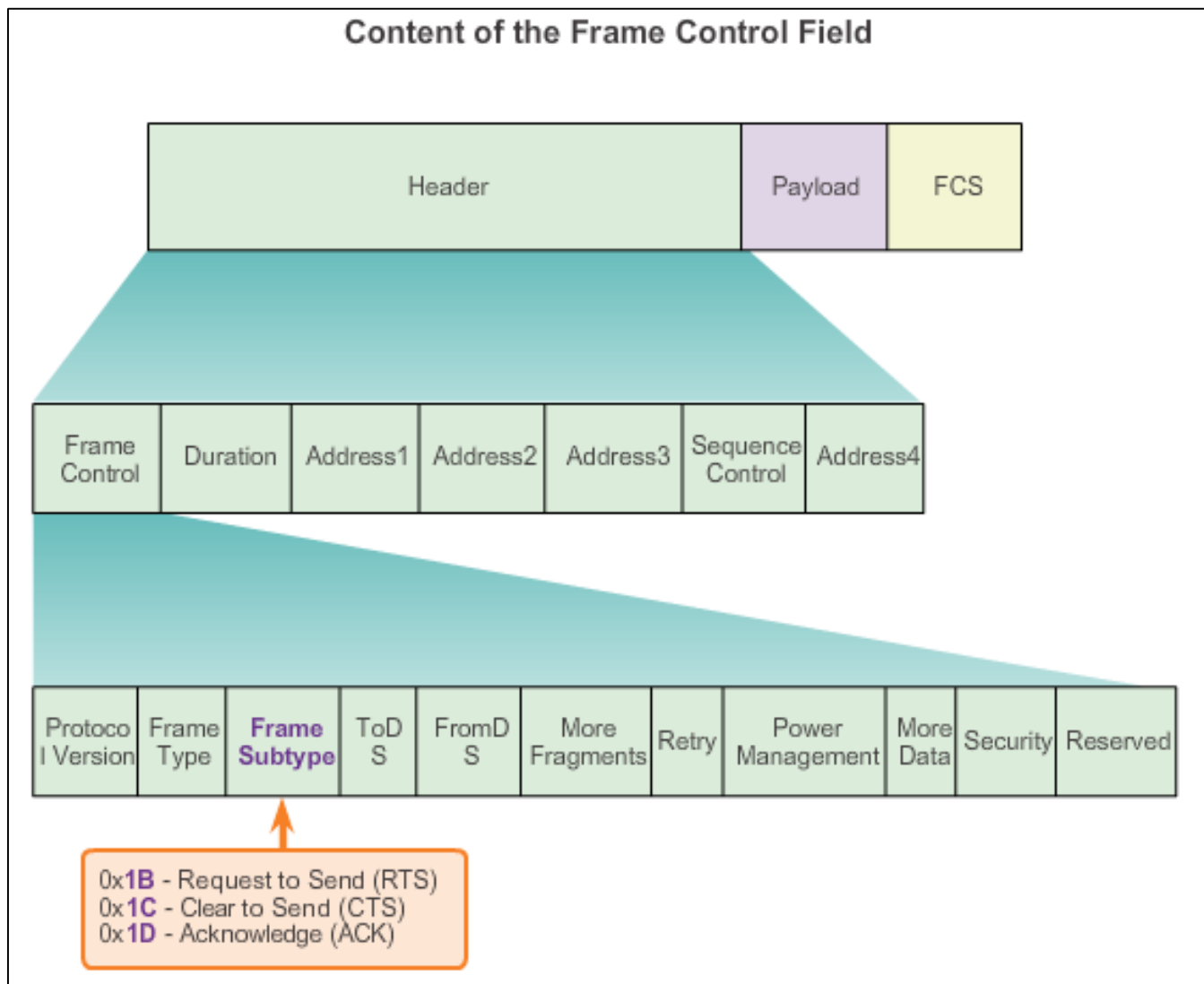
## Management Frames





# 802.11 Frame Structure

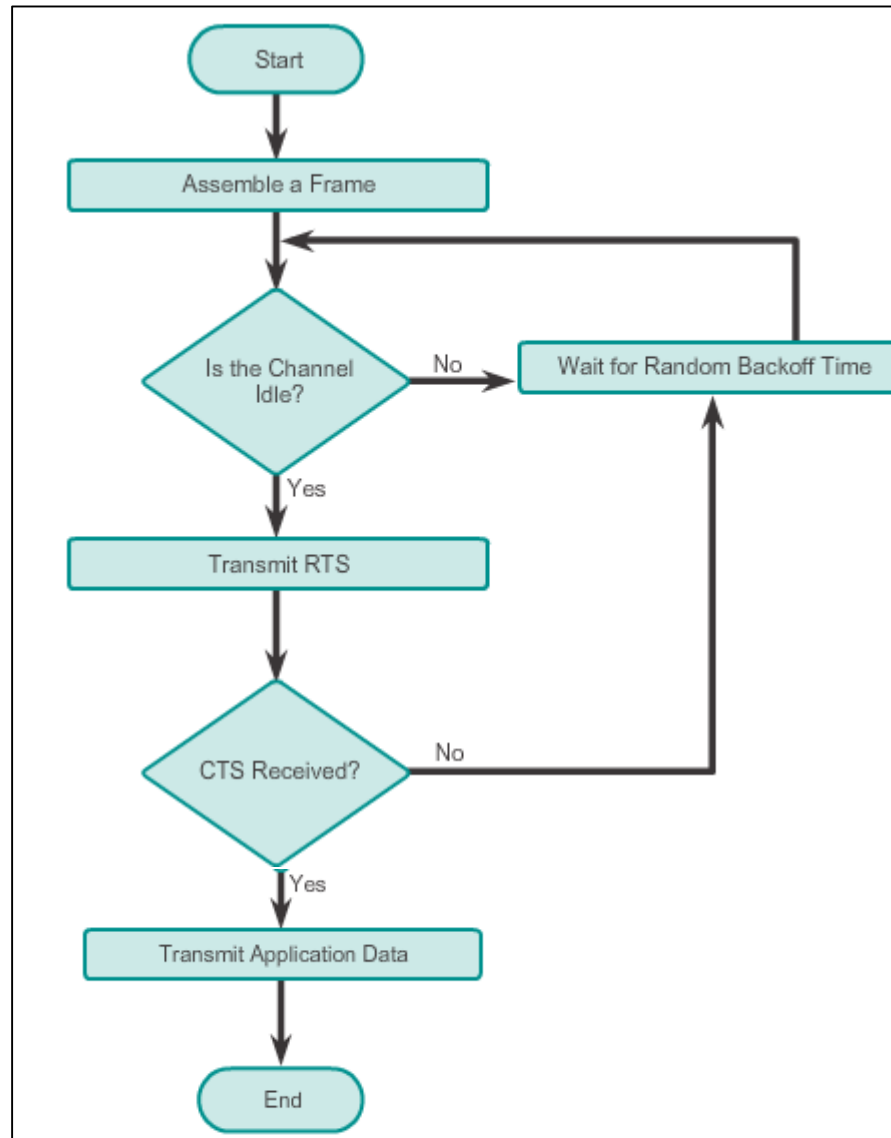
## Control Frames





# Wireless Operation CSMA/CA

## CSMA/CA Flowchart

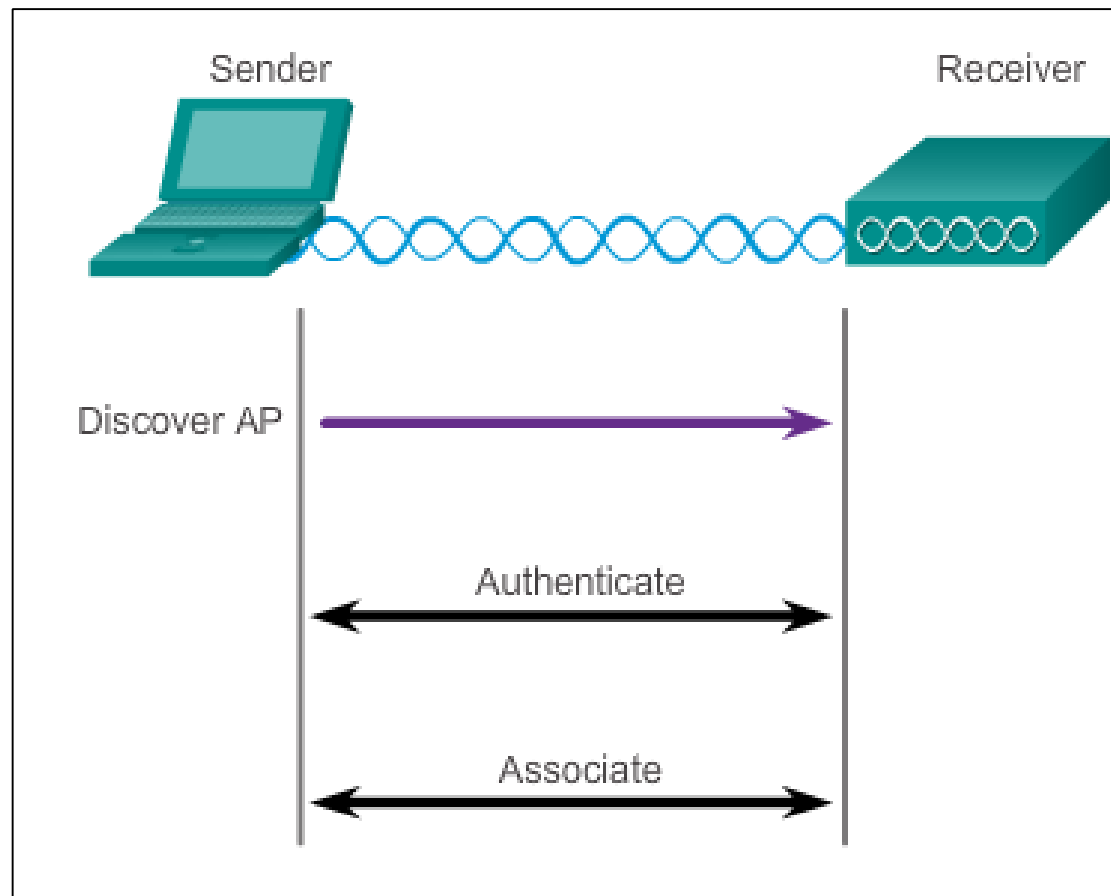




## Wireless Operation

# Wireless Clients and Access Point Association

### Three-Stage Process





## 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.



## Wireless Operation

# Discovering APs

### Passive mode

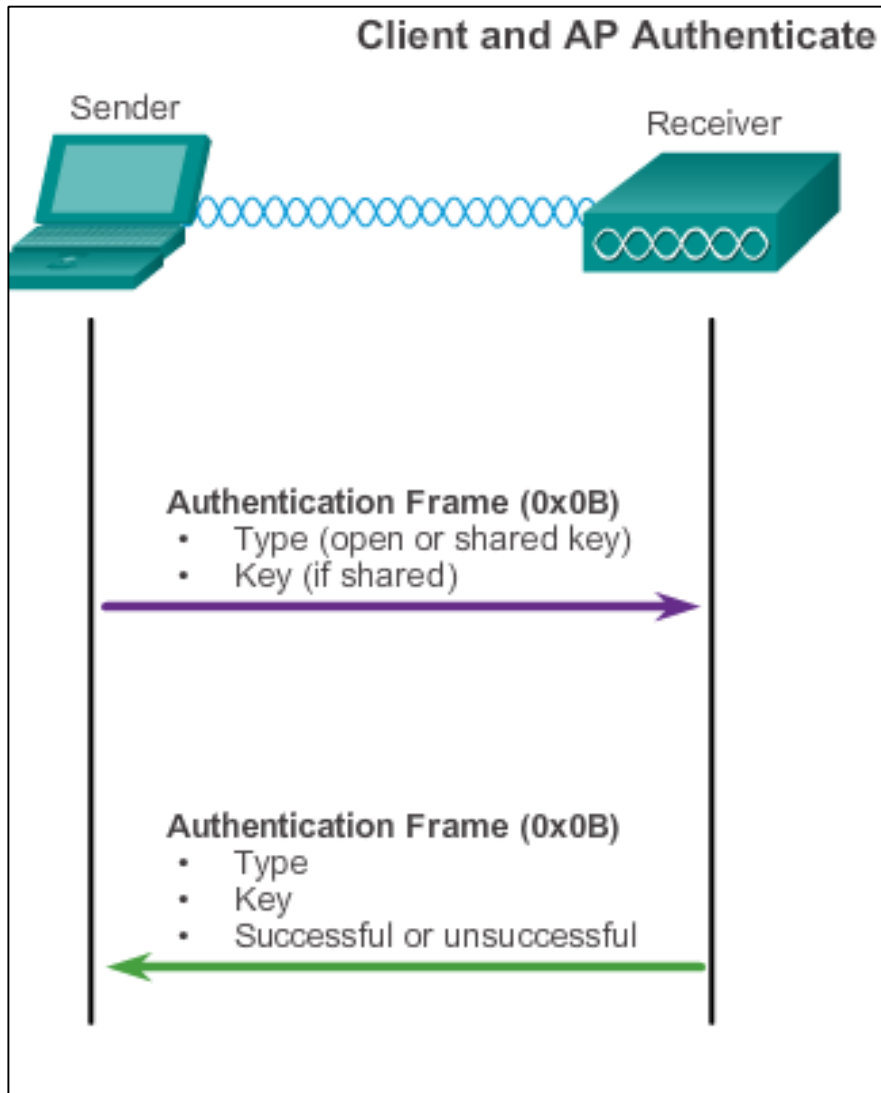
- AP advertises its service by sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- The beacon's primary purpose is to allow wireless clients to learn which networks and APs are available in a given area.

### 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.



## Wireless Operation Authentication



- **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.





## Channel Management

# 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.



## Channel Management

# Frequency Channel Saturation (cont.)

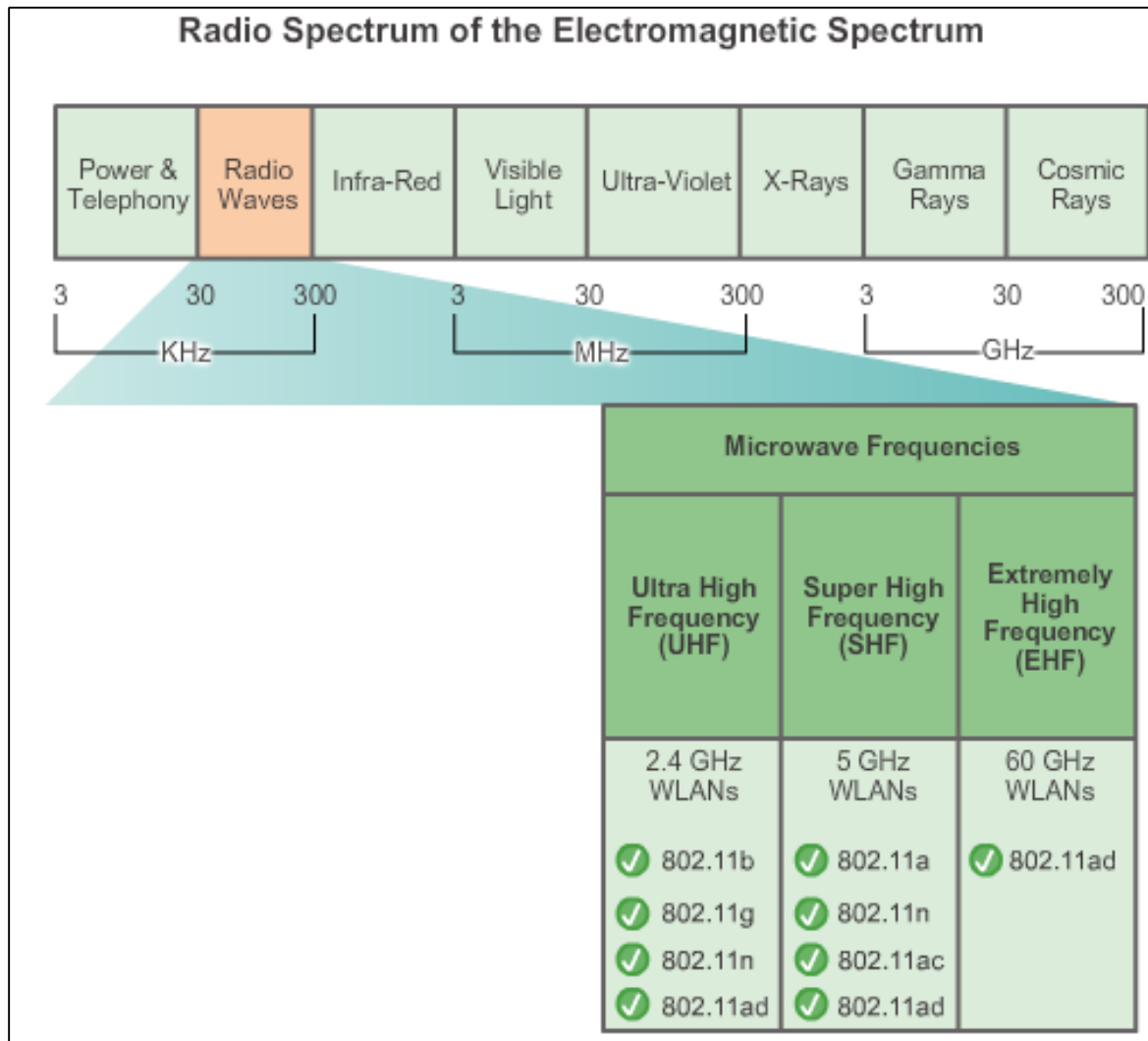
### Orthogonal Frequency-Division Multiplexing (OFDM)

- 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.



# Channel Management

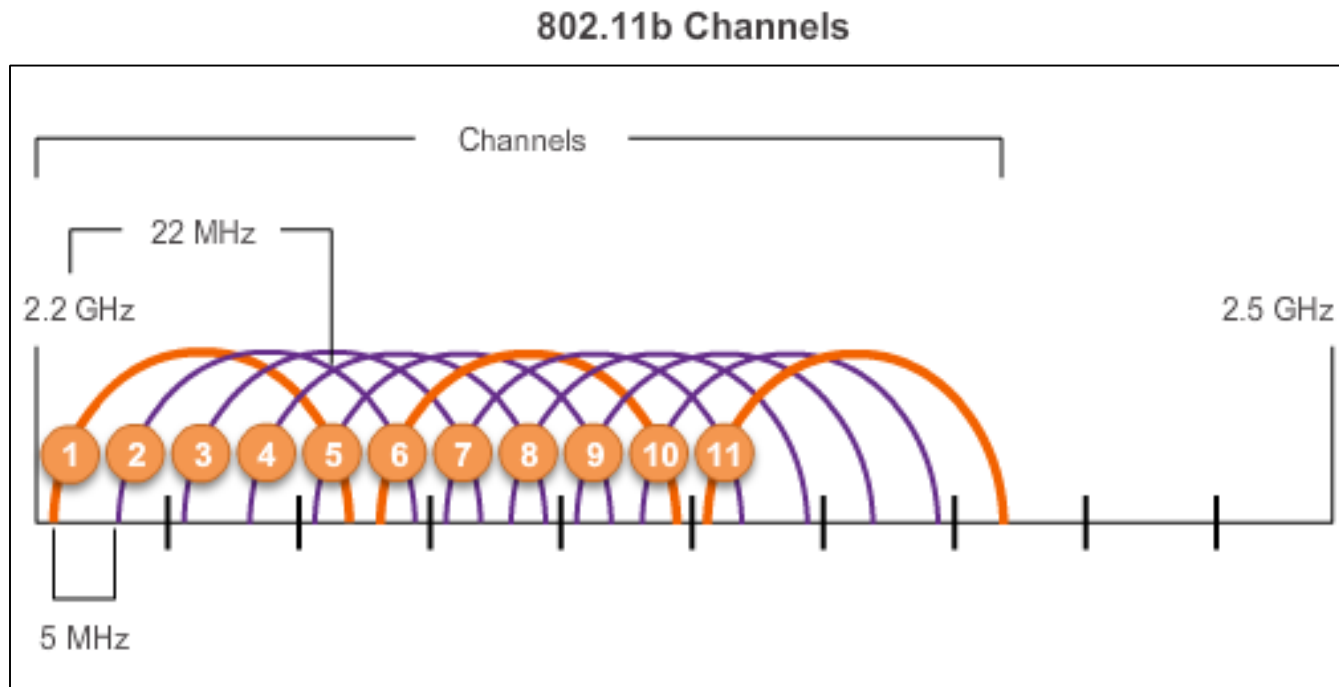
## Selecting Channels





## Channel Management

# Selecting Channels (cont.)

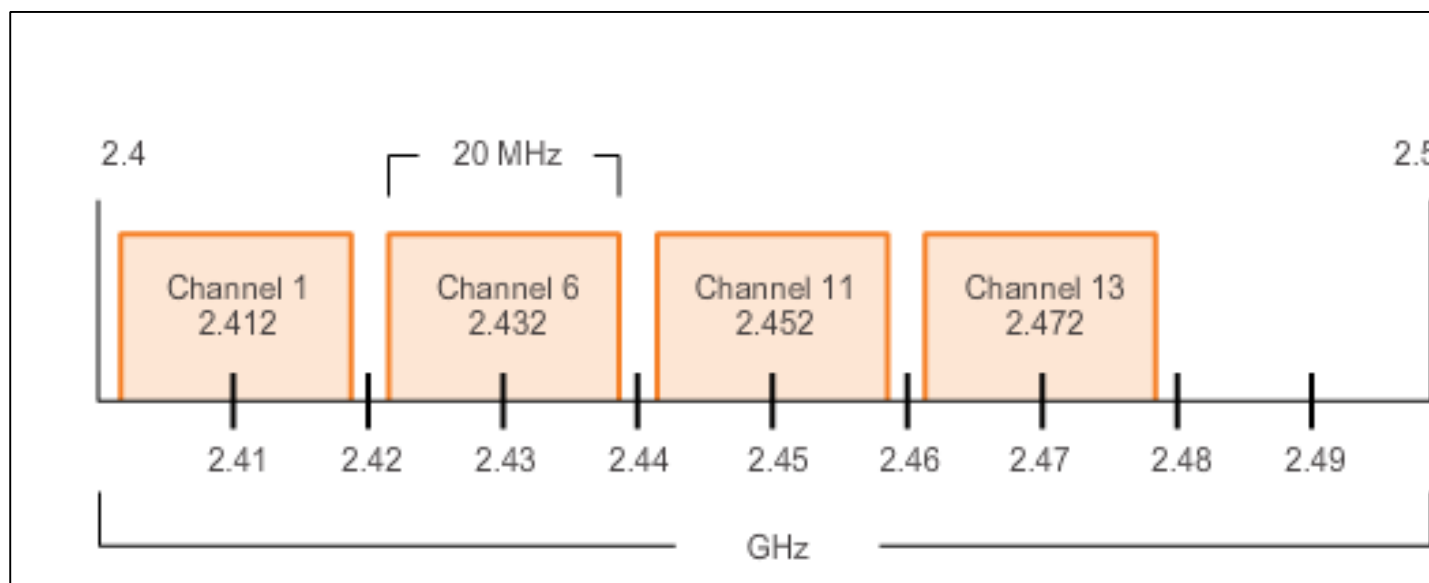


The solution to 802.11b interference is to use nonoverlapping channels 1, 6, and 11.

## Channel Management

# Selecting Channels (cont.)

802.11g/n (OFDM) Channel Width 20 MHz



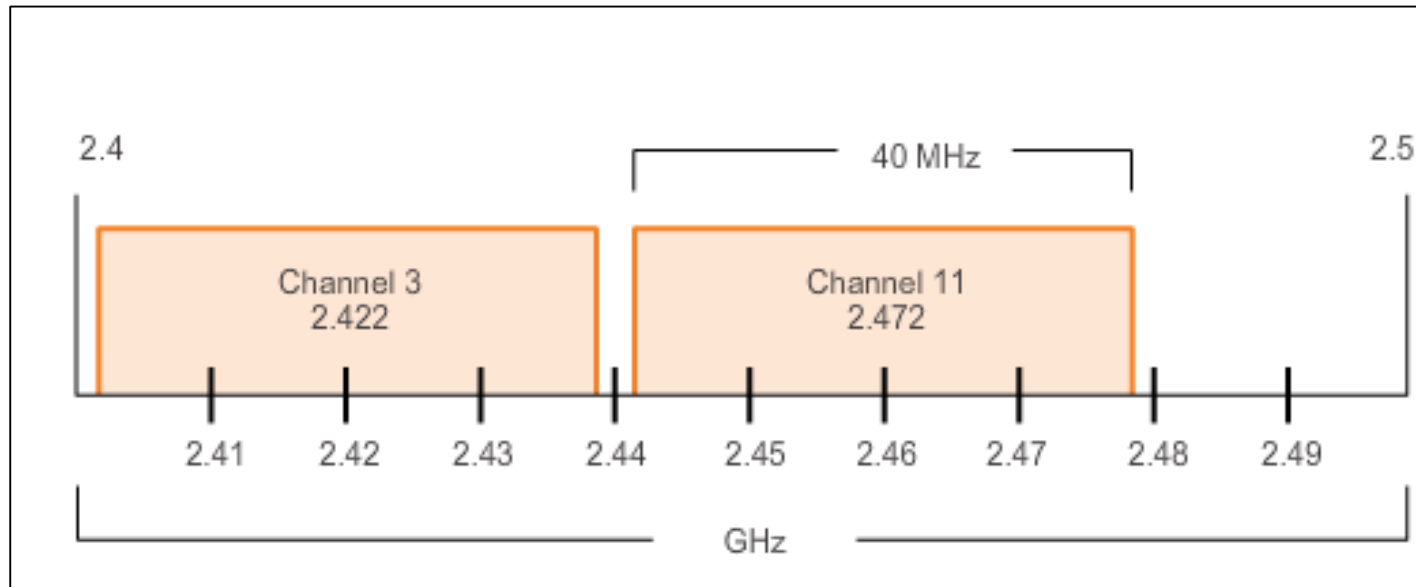
Use channels in the larger, less-crowded 5 GHz band, reducing “accidental denial of service (DoS),” this band can support four non-overlapping channels.



## Channel Management

# Selecting Channels (cont.)

802.11n (OFDM) Channel Width 40 MHz

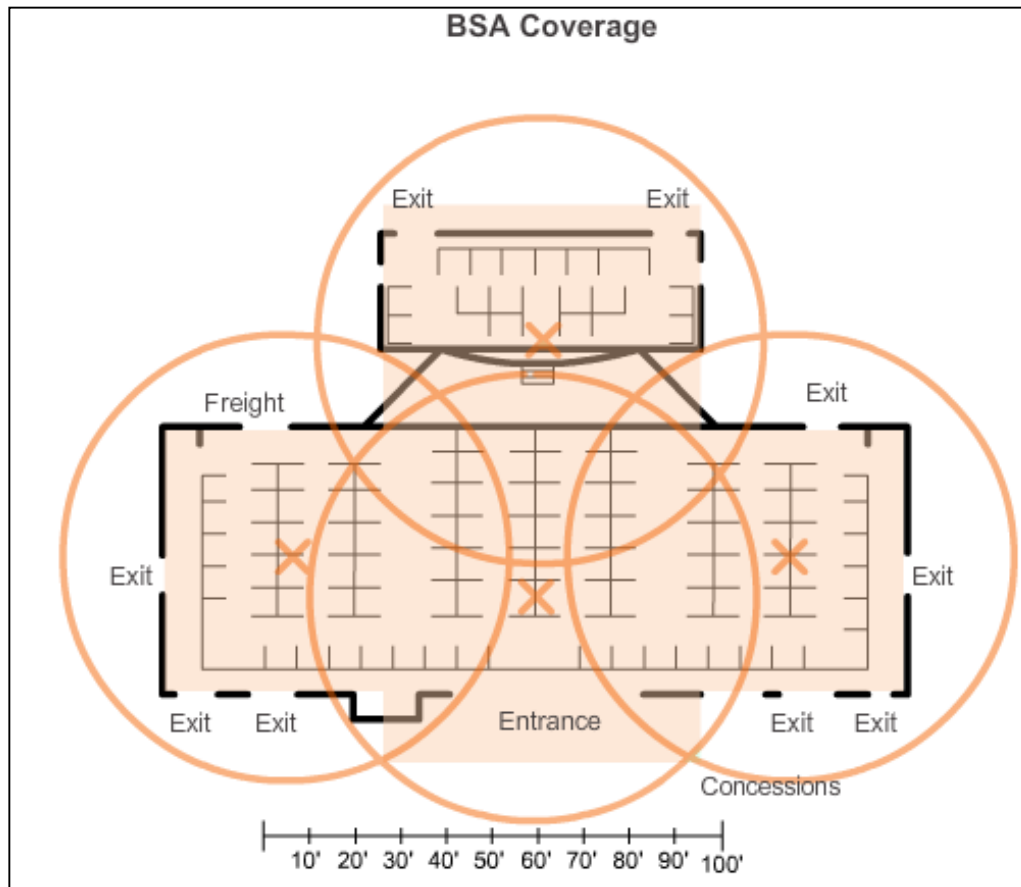


Channel bonding combines two 20-MHz channels into one 40-MHz channel.



## Channel Management

# Planning a WLAN Deployment



- 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



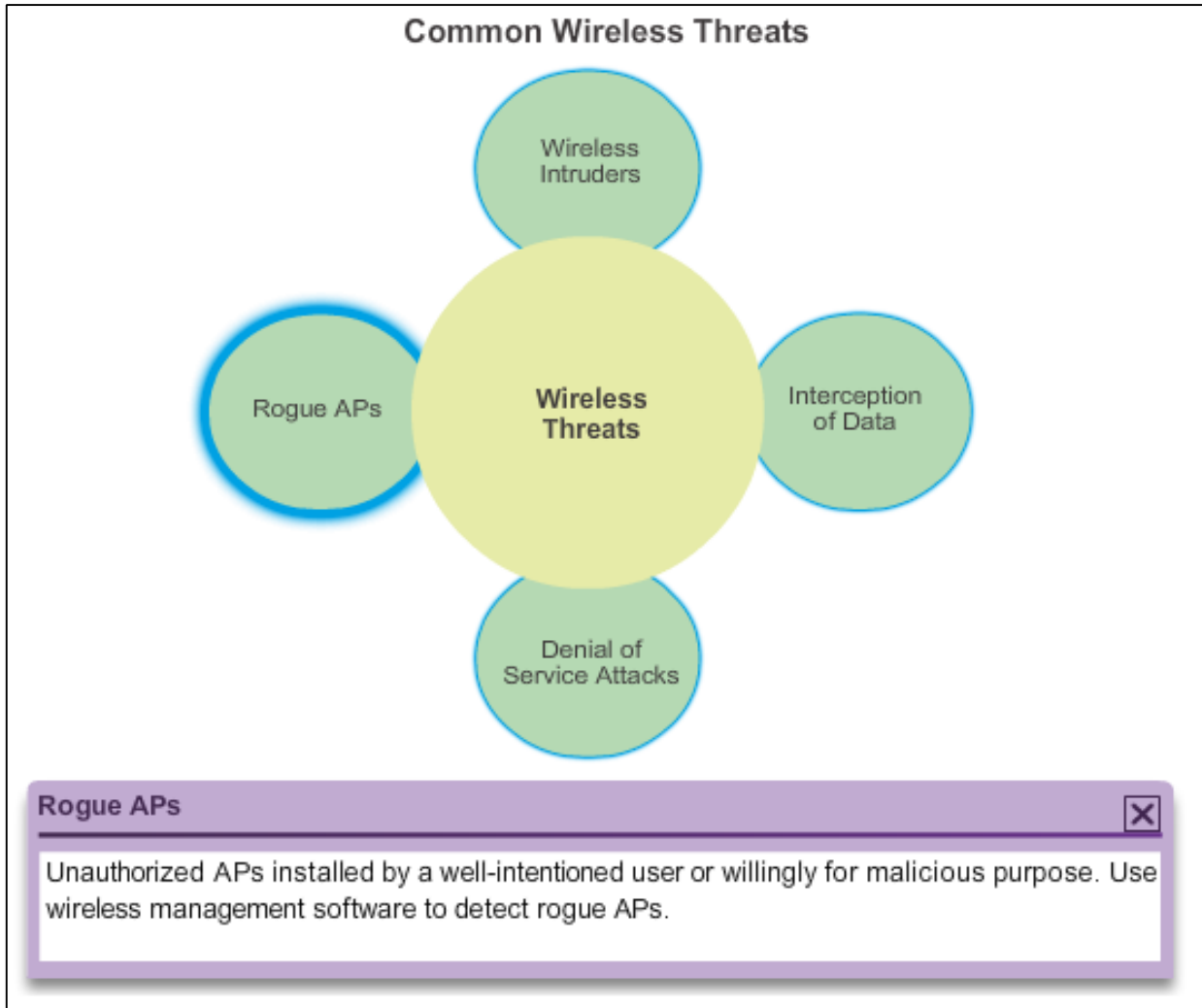
Cisco | Networking Academy®  
Mind Wide Open™





# WLAN Threats

## Securing Wireless





## WLAN Threats

# 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.



## WLAN Threats

# 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.



## WLAN Threats

# 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.



## WLAN Threats

# Man-in-the-Middle Attack

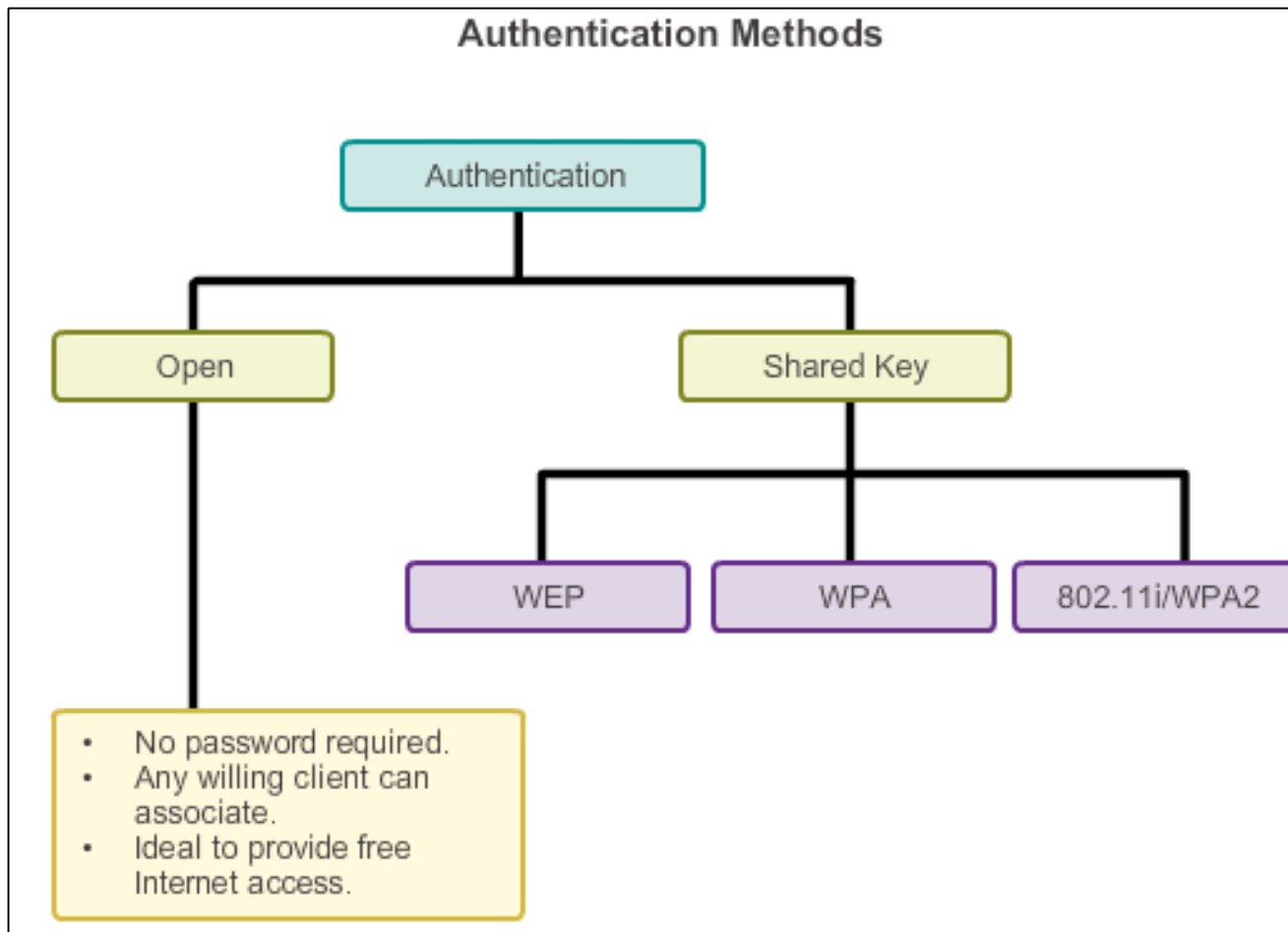
“Evil twin AP” attack:

- 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.

## Securing WLANs

# Wireless Security Overview

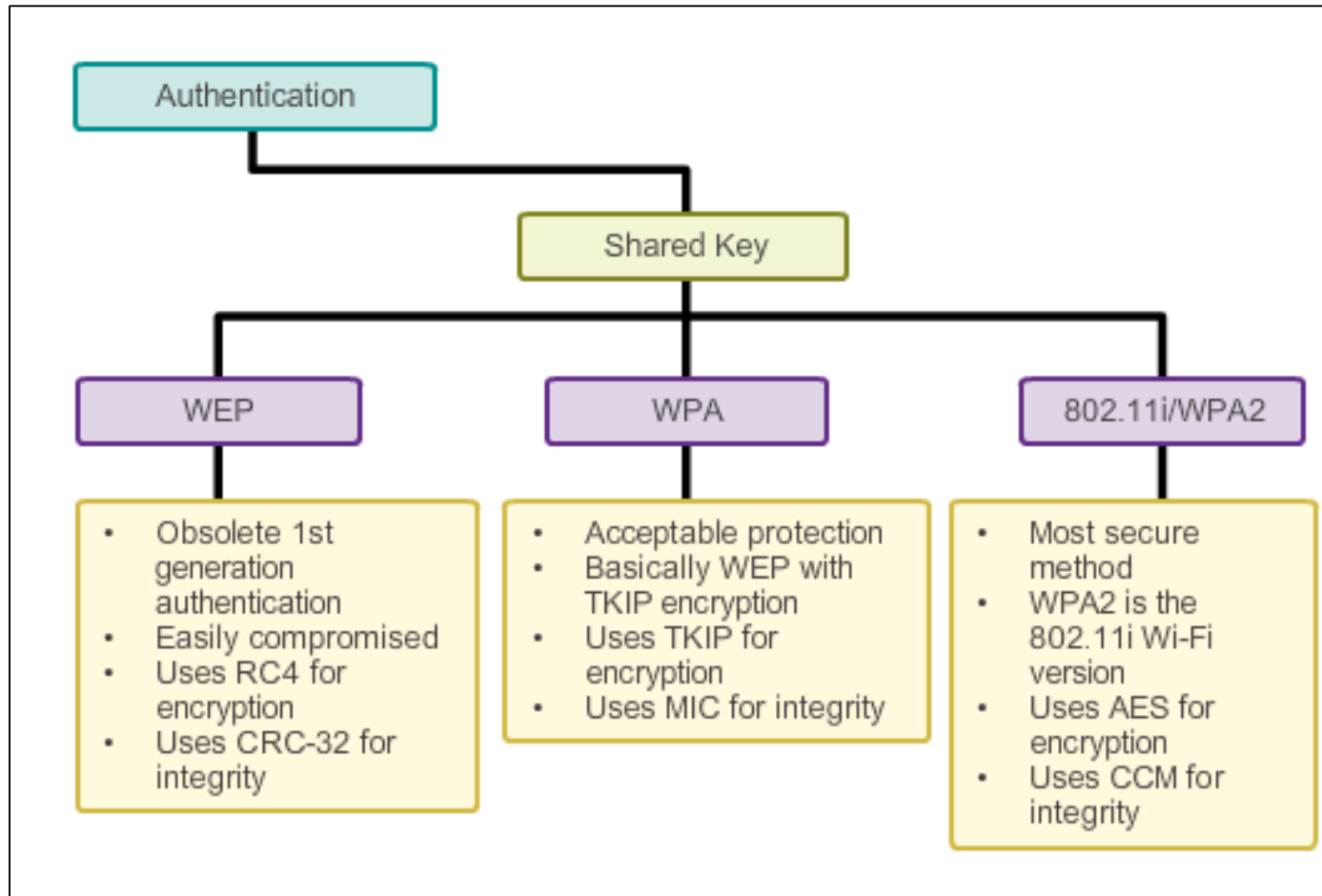
Use authentication and encryption to secure a wireless network.





## Securing WLANs

# Shared Key Authentication Methods





## Securing WLANs

# 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.





## Securing WLANs

# 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.



## Securing WLANs

# Authentication in the Enterprise

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

### Entering the RADIUS Server Specifics

The screenshot shows the 'Wireless' configuration page in a web browser. The page has tabs for 'Wireless', 'MAC Filtering', 'WPA Protected Setup', and 'Simple Tap'. The 'Wireless' tab is active, showing settings for two networks: '2.4 GHz network' and '5 GHz network'.

**2.4 GHz network:**

- Network: ☒ Enabled
- Network name (SSID):
- RADIUS server:
- RADIUS port:
- Shared key:
- Network mode:
- Security mode:
- Channel width:
- Channel:

**5 GHz network:**

- Network: ☒ Enabled
- Network name (SSID):
- Password:
- Network mode:
- Security mode:
- Channel width:
- Channel:

At the bottom of the configuration area are buttons for 'OK', 'Cancel', and 'Apply'.



## 8.4 Wireless LAN Configuration



Cisco | Networking Academy®  
Mind Wide Open™



## Configure a Wireless Router

# 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



## Configure a Wireless Router

# 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 EA6500

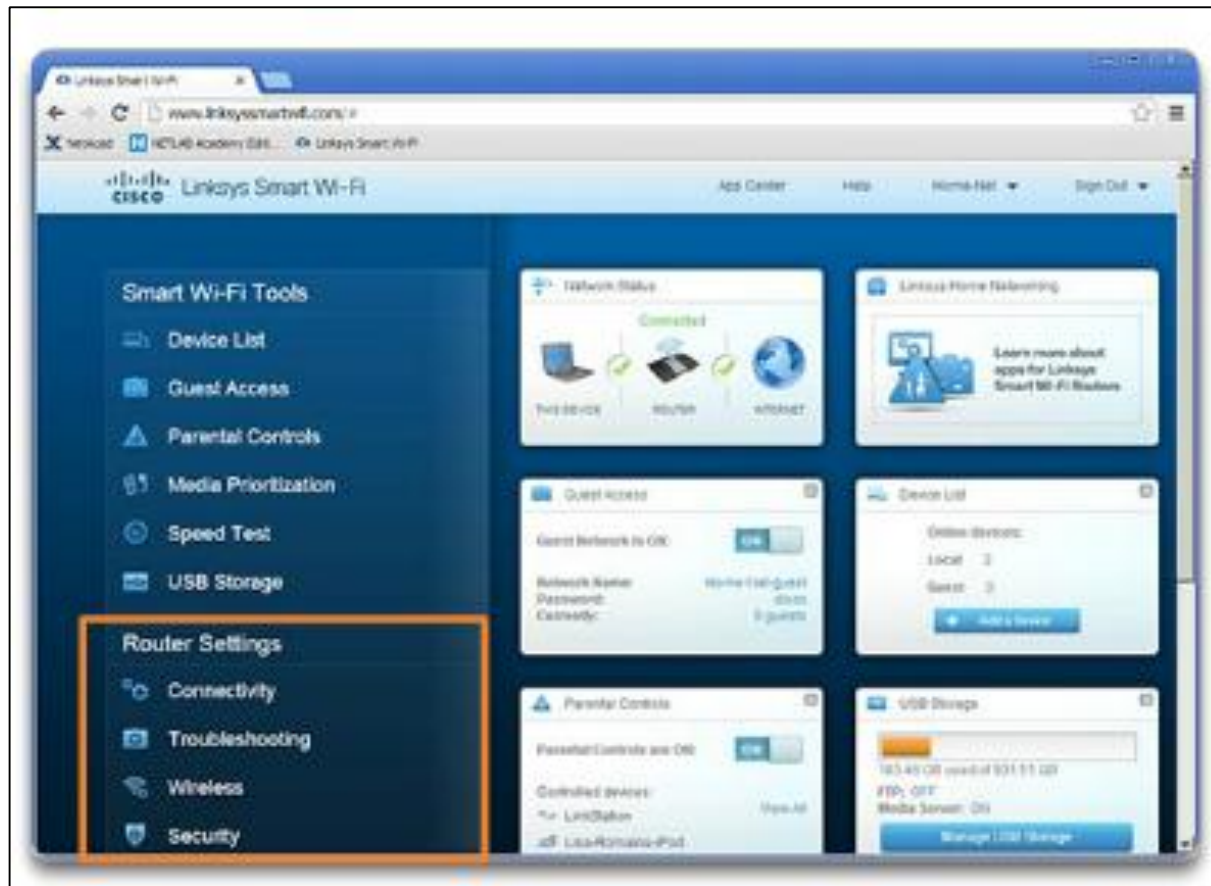




# Configure a Wireless Router

## 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.





## Configure a Wireless Router

# 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.



## Configuring Wireless Clients

# 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.



## Troubleshoot WLAN Issues

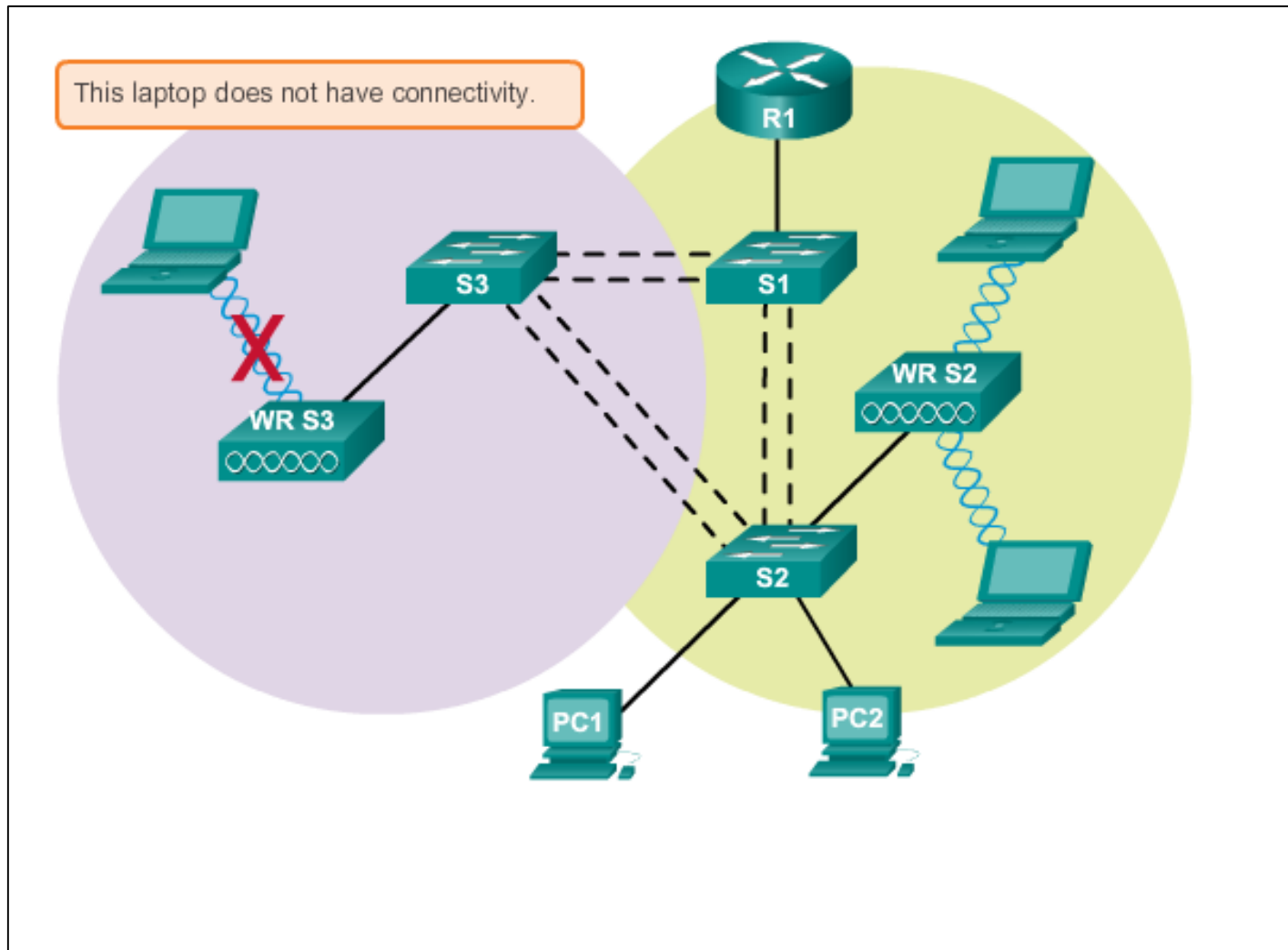
# Troubleshooting Approaches

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.

## Troubleshoot WLAN Issues

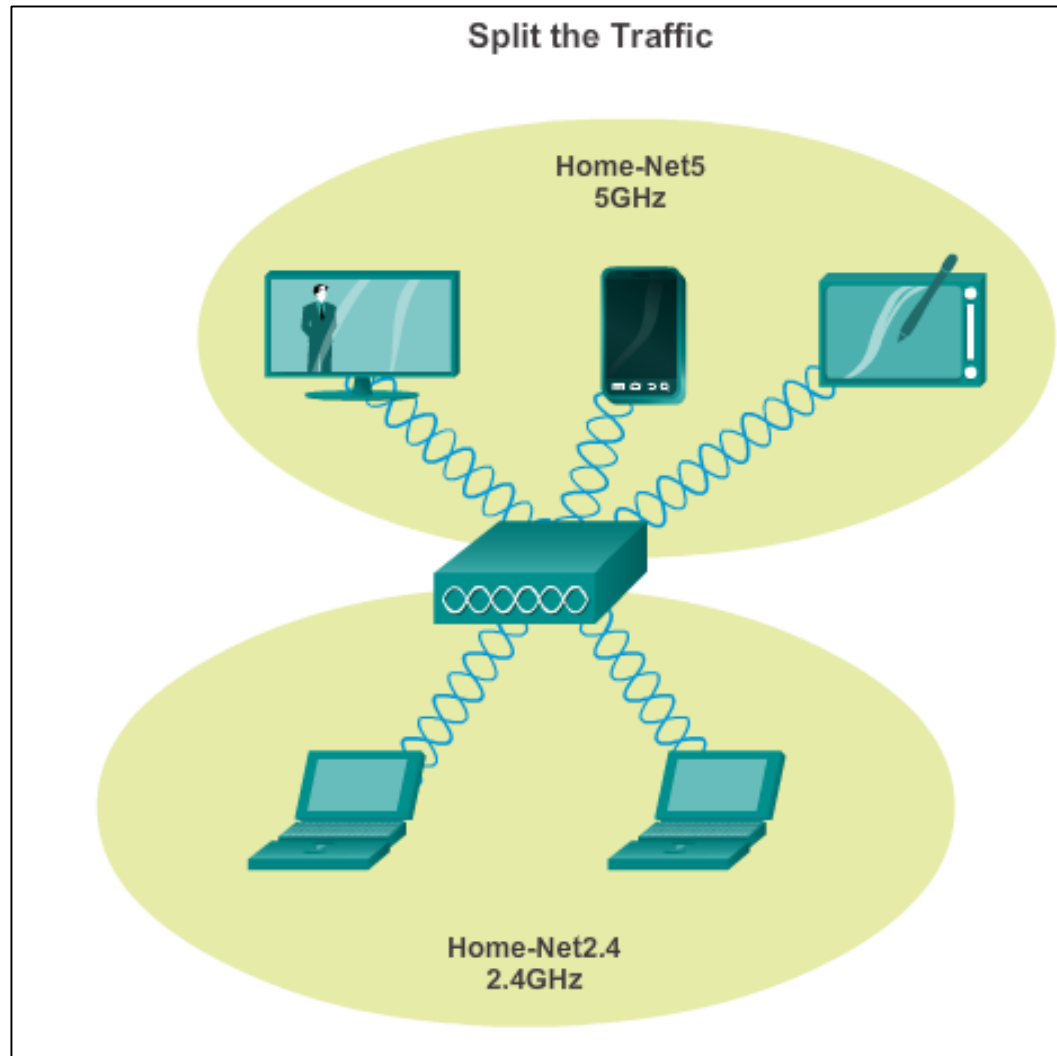
# Wireless Client Not Connecting





## Troubleshoot WLAN Issues

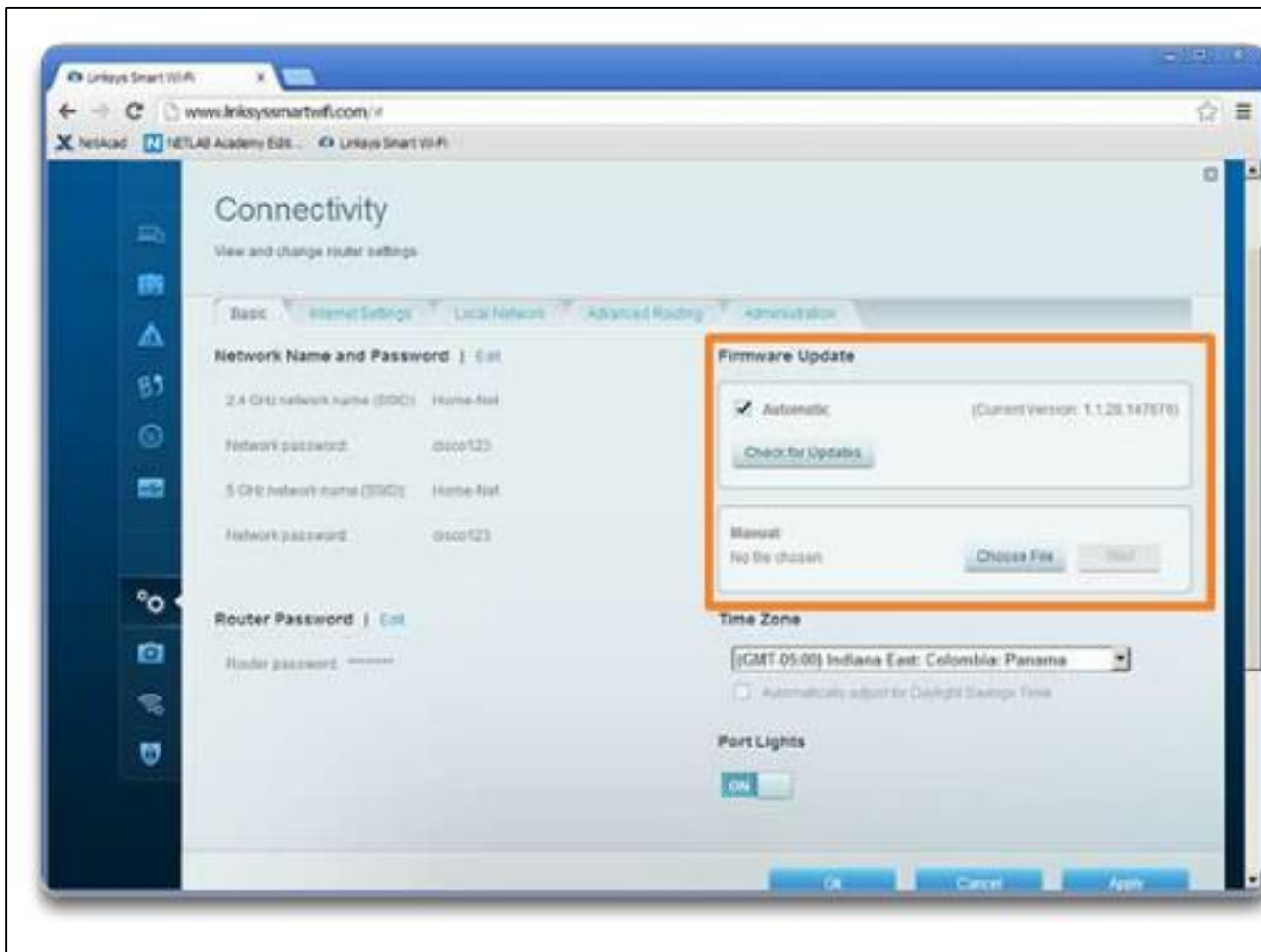
# Troubleshooting When the Network Is Slow





# Troubleshoot WLAN Issues

## 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 omnidirectional 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.

