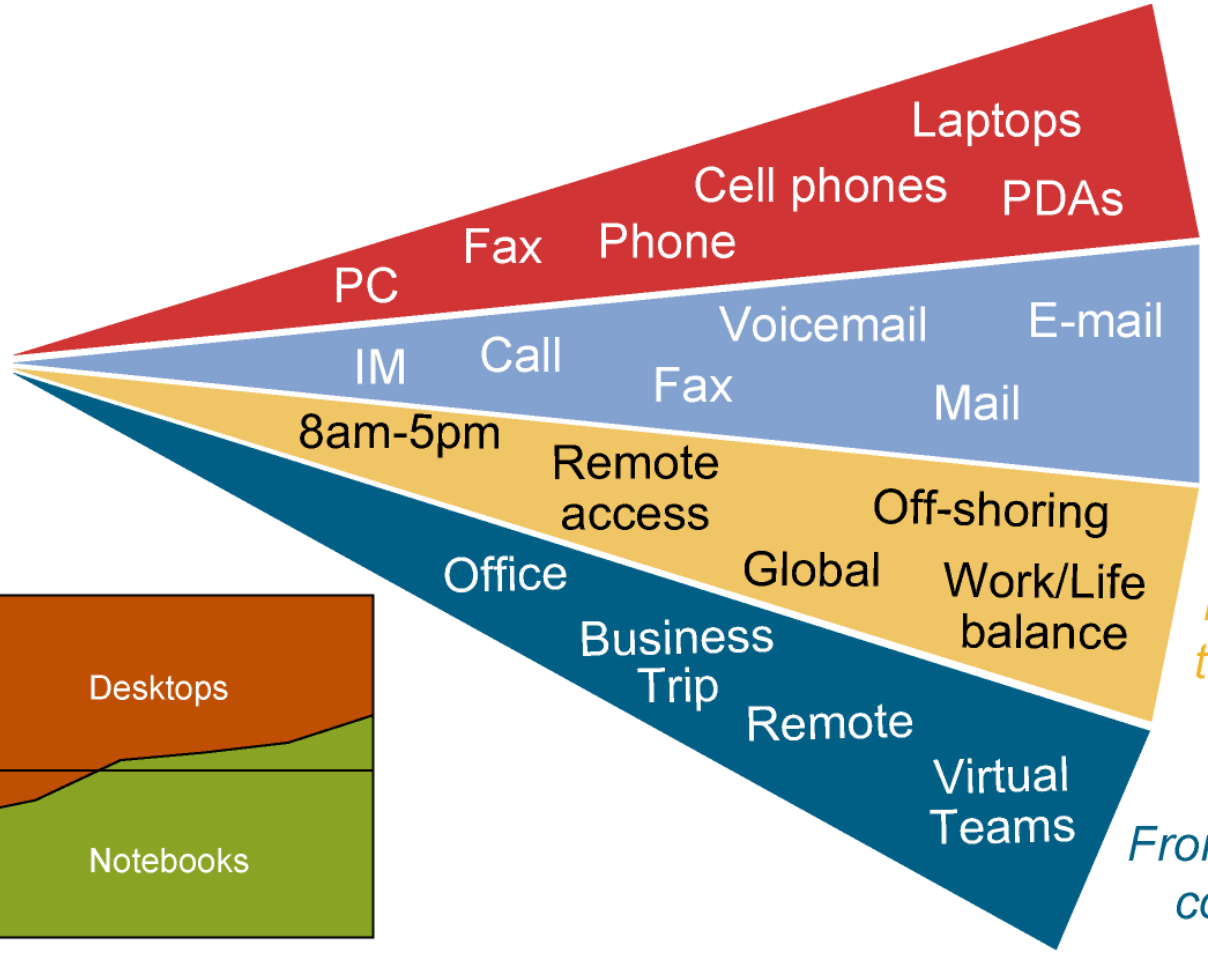
Exploring Wireless Networking

Wireless LANs

Market Trends



More notebooks sold than desktops

301P_403

Differences Between WLAN and LAN

- WLANs use radio waves as the physical layer.
  - WLANs use CSMA/CA instead of CSMA/CD for media access.
  - Two-way radio (half-duplex) communication.
- Radio waves have problems that are not found on wires.
  - Connectivity issues:
    - Coverage problems
    - Interference, noise
  - Privacy issues
- Access points are shared devices similar to an Ethernet hub for shared bandwidth.
- WLANs must meet country-specific RF regulations.

Radio Frequency Transmission

- Radio frequencies are radiated into the air via an antenna, creating radio waves.
- Objects can affect radio wave propagation resulting in:
  - Reflection
  - Scattering
  - Absorption
- Higher frequencies allow higher data rates; however, they have a shorter range.

Organizations That Define WLAN

ITU-R:

- International Telecommunication Union-Radiocommunication Sector
- Regulates the RF used in wireless

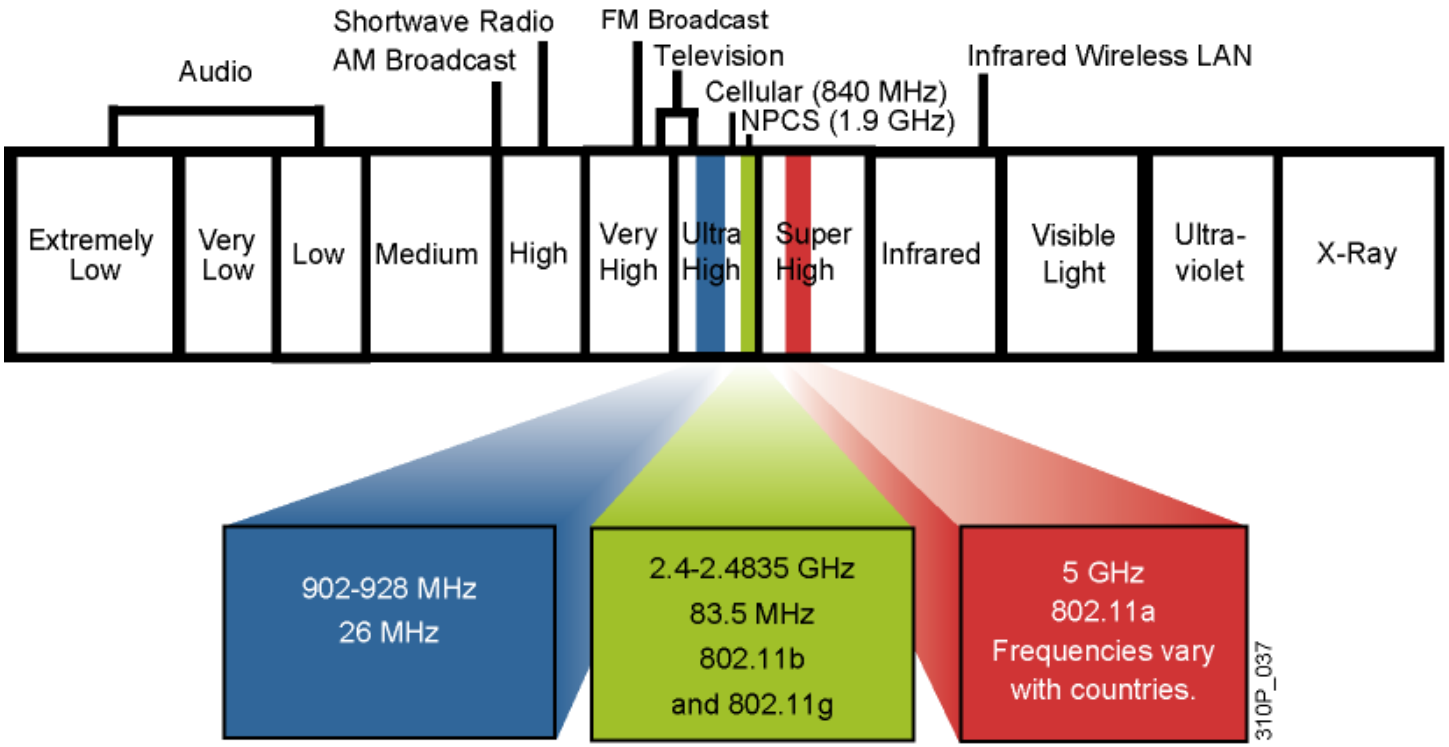
IEEE:

- Institute of Electrical and Electronic Engineers
- 802.11 documents wireless technical standards

Wi-Fi Alliance:

- Global nonprofit industry trade association
- Promote wireless growth through interoperability certification

ITU-R with FCC Wireless



- ISM: industry, scientific, and medical frequency band
- No license required
- No exclusive use
- Best-effort
- Interference possible

IEEE 802.11 Standards Comparison

	802.11b	802.11a	802.11g	
Frequency band	2.4 GHz	5 GHz	2.4 GHz	
No. of channels	3	Up to 23	3	
Transmission	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)
Data rates [Mb/s]	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54

Wi-Fi Certification

Wi-Fi Alliance **certifies** interoperability between products.

- Products include 802.11a, 802.11b, 802.11g, dual-band products, and security testing.
- Provides assurance to customers of migration and integration options.

Cisco is a founding member of the Wi-Fi Alliance.

Certified products can be found at http://www.wi-fi.com.

Summary

- People now expect to be connected at any time and place. However, the most tangible benefit of wireless is the cost reduction.
- Both WLANs and LAN use CSMA. However WLANs use collision avoidance while LANs use collistion detection.
- Radio frequencies are radiated into the air by antennas, where they are affected by reflection, scattering, and absorption.
- The IEEE defines the 802.11 standards.

Summary (Cont.)

- The ITU-R local FCC wireless bands are unlicensed.
- The 802.11 standards are a set of standards that define the frequencies and radio bands for WLANs.
- One of the primary benefits of the Wi-Fi Alliance is to ensure interoperability among 802.11 products.

Understanding WLAN Security

Wireless LANs

Wireless LAN Security Threats

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network *The weakness is another reminder of the difficulty in implementing effective network security.*	

Mitigating the Threats

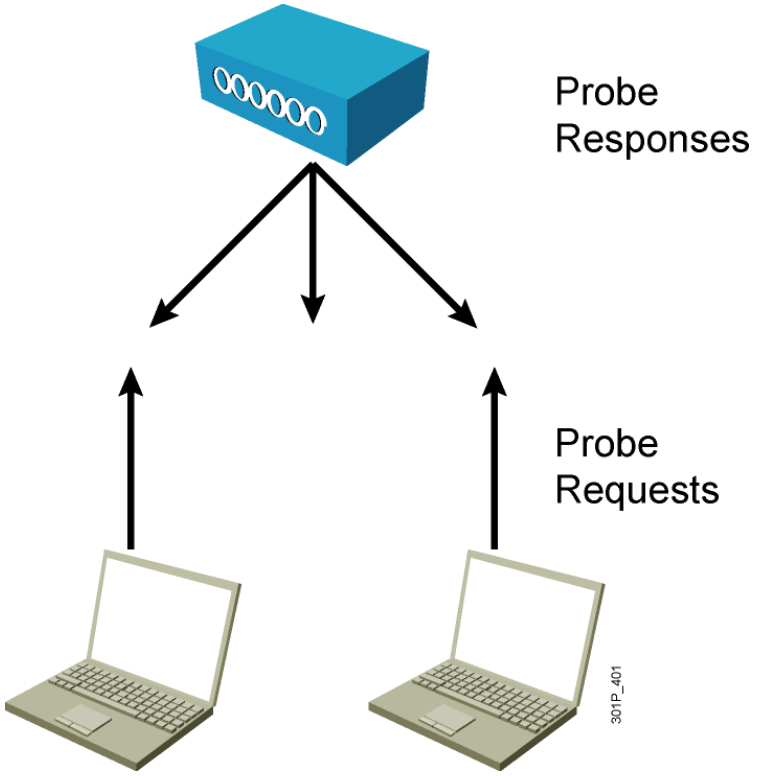
Control and Integrity	Privacy and Confidentiality	Protection and Availability
Authentication	Encryption	Intrusion Prevention System (IPS)
Ensure that legitimate clients associate with trusted access points.	Protect data as it is transmitted and received.	Track and mitigate unauthorized access and network attacks.

Evolution of Wireless LAN Security

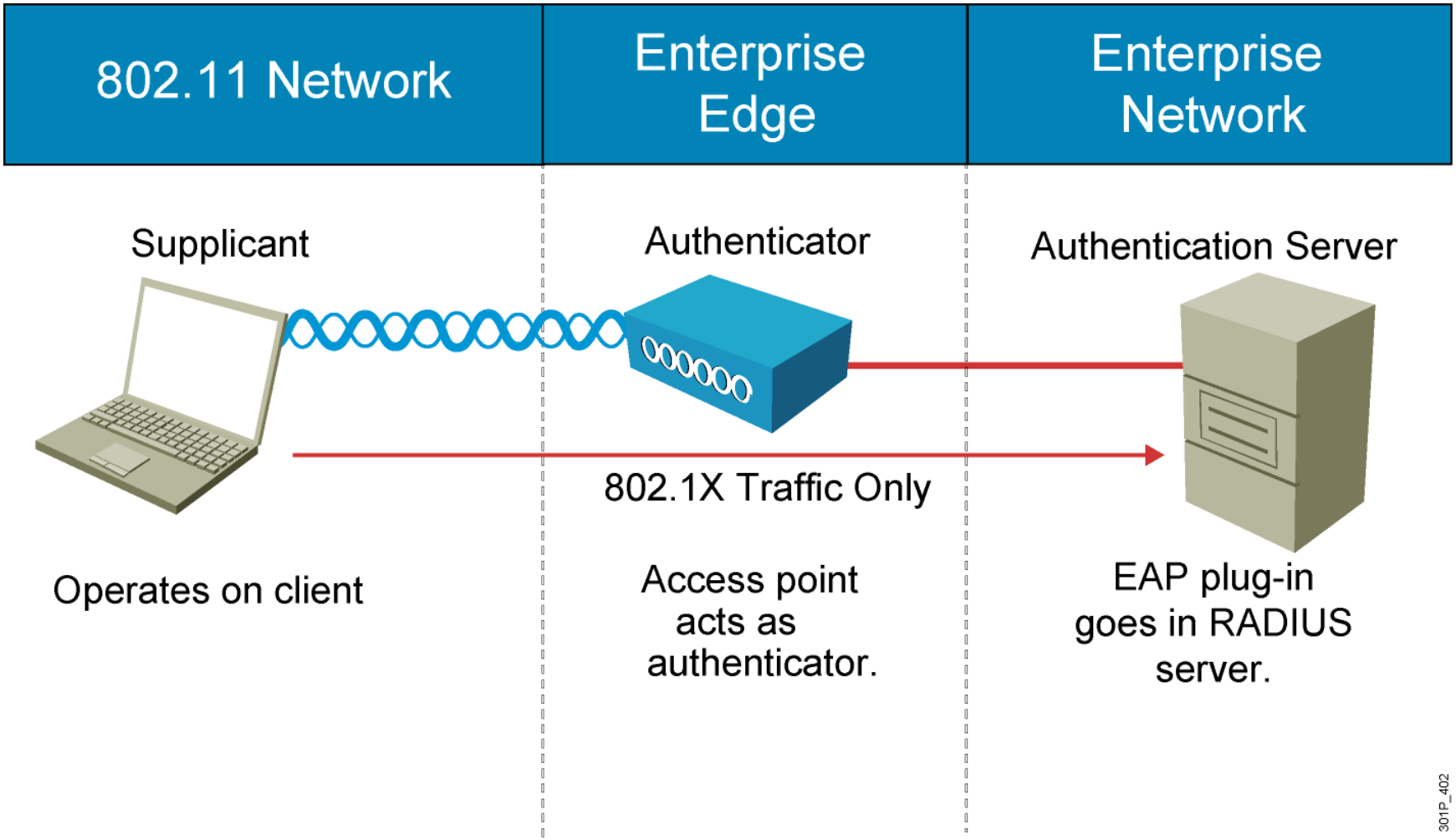
WEP	802.1x EAP	WPA	802.11i / WPA2
▪ Basic encryption ▪ No strong authentication ▪ Static, breakable keys ▪ Not scalable ▪ MAC filters and SSID-cloaking also used to complement WEP	▪ Dynamic keys ▪ Improved encryption ▪ User authentication ▪ 802.1X EAP (LEAP, PEAP) ▪ RADIUS	▪ Standardized ▪ Improved encryption ▪ Strong, user authentication (such as, LEAP, PEAP, EAP-FAST)	▪ AES strong encryption ▪ Authentication ▪ Dynamic key management

Wireless Client Association

- Access points send out beacons announcing SSID, data rates, and other information.
- Client scans all channels.
- Client listens for beacons and responses from access points.
- Client associates to access point with strongest signal.
- Client will repeat scan if signal becomes low to reassociate to another access point (roaming).
- During association, SSID, MAC address, and security settings are sent from the client to the access point and checked by the access point.



How 802.1X Works on the WLAN



WPA and WPA2 Modes

	WPA	WPA2
Enterprise mode (Business, education, Government)	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal mode (SOHO, home and personal)	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Summary

- It is inevitable that hackers will attack unsecured WLANs.
- The fundamental solution for wireless security is authentication and encryption to protect wireless data transmission.
- WLAN standards evolved to provide more security.
  - WEP
  - 802.1x EAP
  - WPA
  - 802.11i/WPA2
- Access points send out beacons announcing SSIDs, data rates, and other information.

Summary (Cont.)

- With 802.1X, the access point, acting as the authenticator at the enterprise edge, allows the client to associate using open authentication.
- WPA provides authentication support via IEEE 802.1X and PSK.
  - Enterprise mode is a term given to products that are tested to be interoperable in both PSK and IEEE 802.1x/EAP modes of operation for authentication.
  - Personal mode is a term given to products tested to be interoperable in the PSK-only mode of operation for authentication.

Implementing a WLAN

Wireless LANs

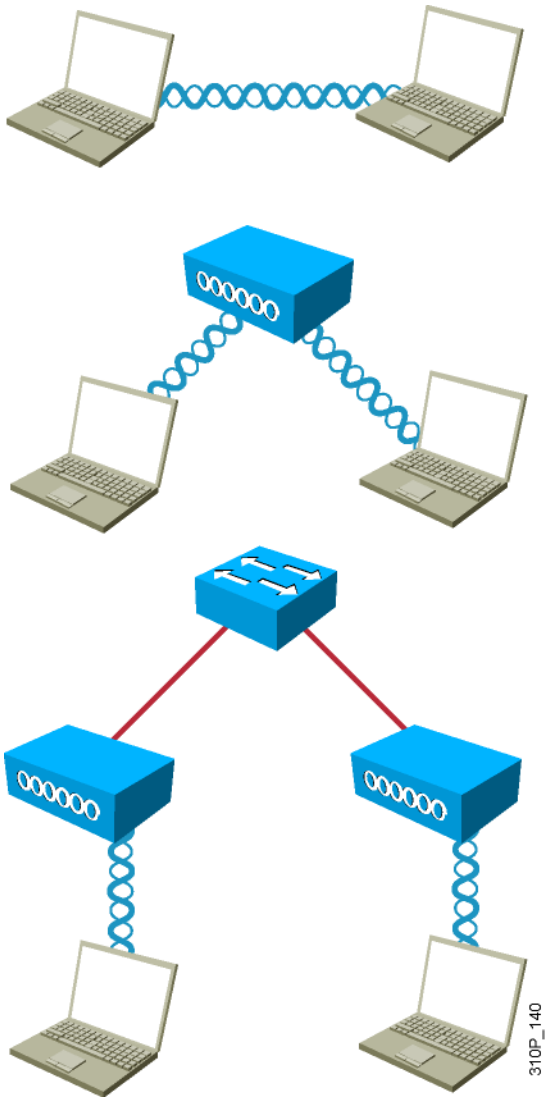
802.11 Topology Building Blocks

Ad hoc mode:

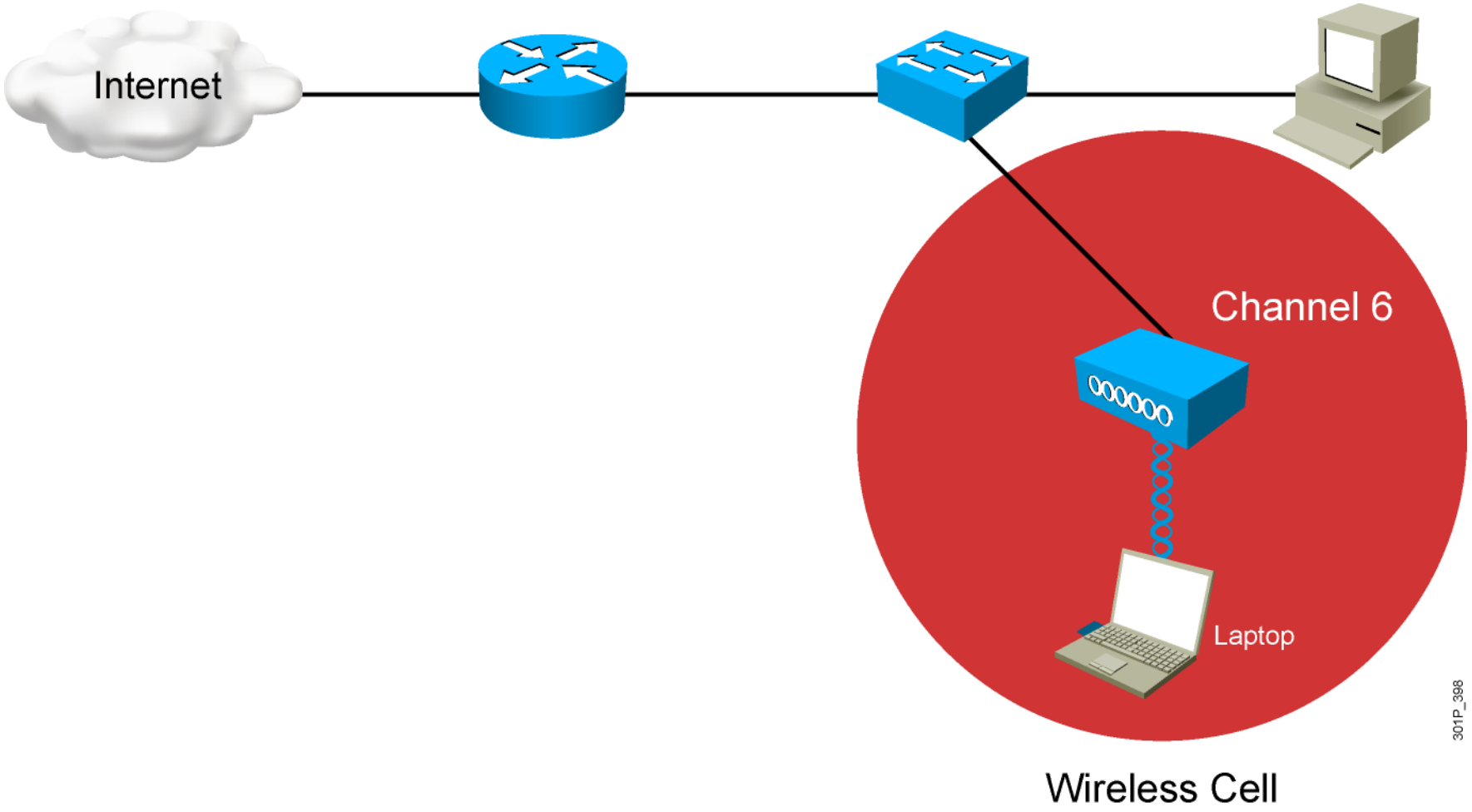
- Independent Basic Service Set (IBSS)
  - Mobile clients connect directly without an intermediate access point.

Infrastructure mode:

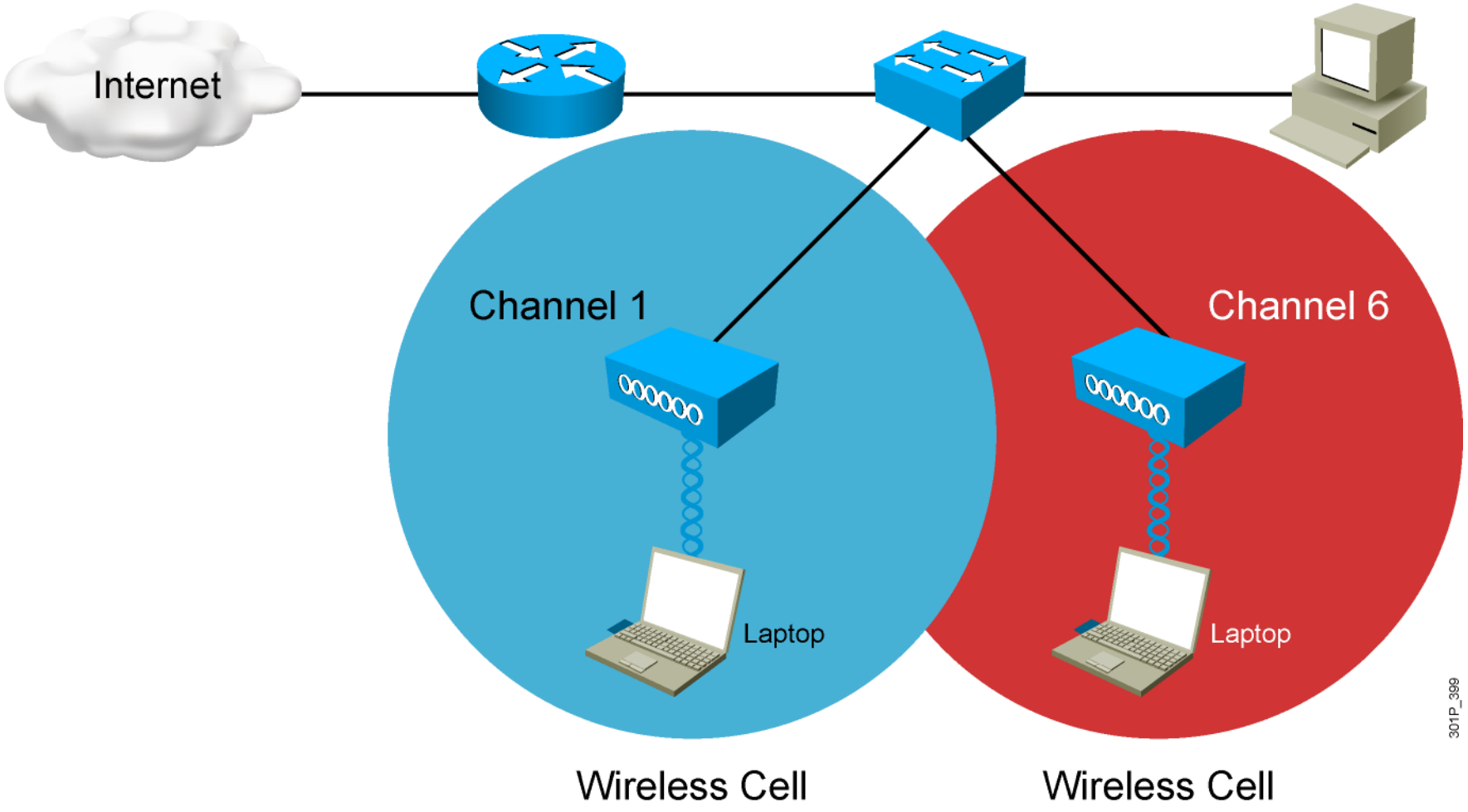
- Basic Service Set (BSS)
  - Mobile clients use a single access point for connecting to each other or to wired network resources.
- Extended Service Set (ESS):
  - Two or more BSSs are connected by a common distribution system .



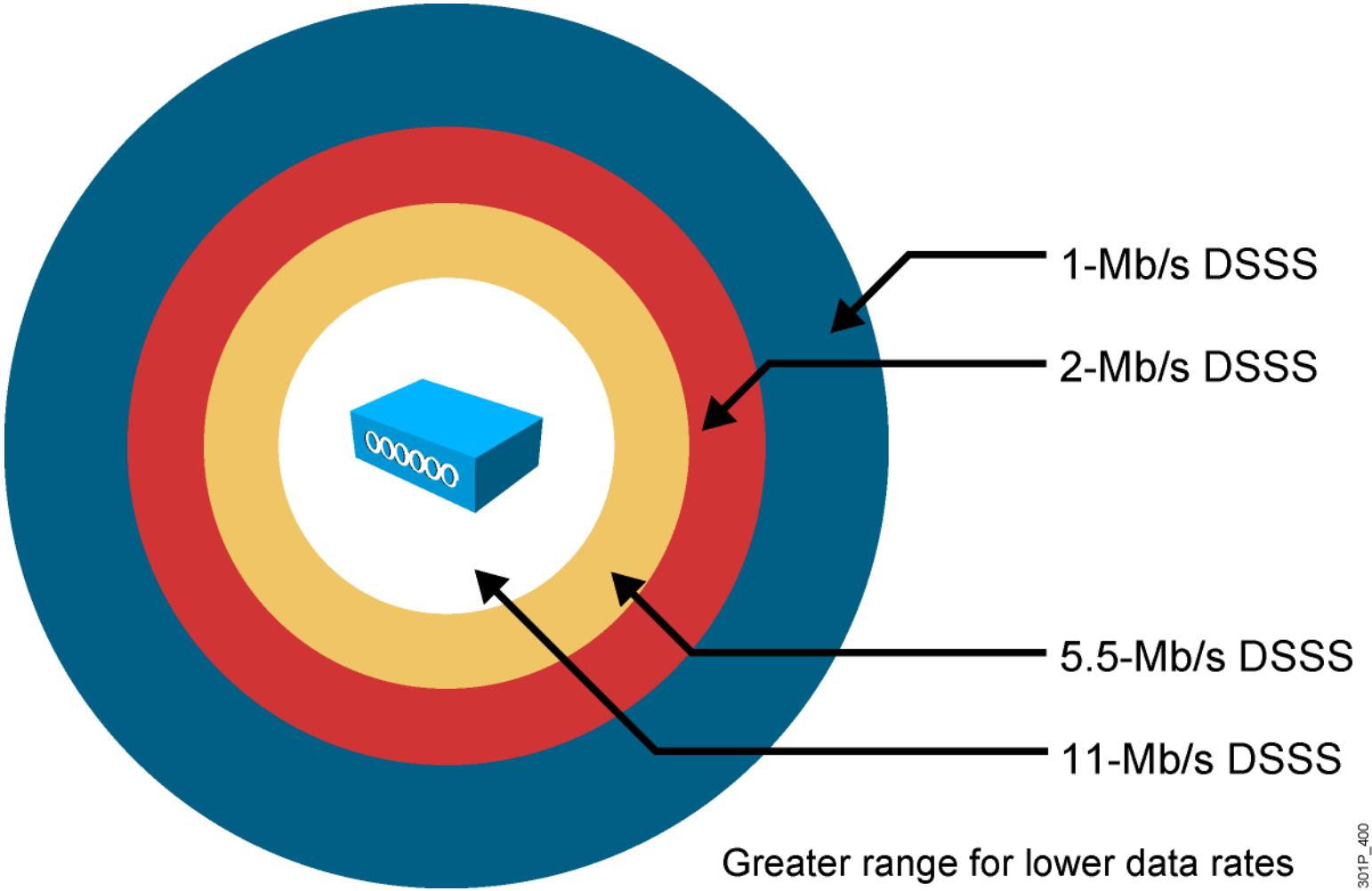
BSA Wireless Topology—Basic Coverage



ESA Wireless Topology—Extended Cover



Wireless Topology Data Rates—802.11b



Access Point Configuration

Basic parameters:

- IP address (static or using DHCP), subnet mask, and default gateway
- Wireless protocol (802.11g only, 802.11a/b/g, 802.11a)
- Channel adjustment if needed—channel 1,6, or 11 pending interference
- Power adjustment if needed—or could change antenna

Security parameters:

- Service Set Identifier (SSID)—identifies your network
- Authentication method—usually WPA or WPA2 PSK
- Encryption method—usually TKIP, or AES if hardware-supported

Steps to Implement a Wireless Network

Step 1: Verify local *wired* operation—DHCP and ISP.

Step 2: Install the access point.

Step 3: Configure the access point—SSID, no security.

Step 4: Install one wireless client—no security.

Step 5: Verify wireless network operation.

Step 6: Configure wireless security—WPA with PSK.

Step 7: Verify the wireless network operation.

Wireless Clients

Wireless Zero Configuration (WZC):

- Default on Windows XP or later operating system
- Limited features for basic PSK
- Verify that users have the correct encryption type and password

Cisco Compatible Extensions Program

- Accelerated feature deployment of third-party clients
- Wide deployment of various vendors

Cisco Secure Services Client

- Enterprise full-featured wireless client supplicant
- Wired and wireless

Common Wireless Network Issues

Most problems are due to incorrect configuration:

- Verify that the access point is running the latest revision of firmware.
- Verify the channel configuration. Try channels 1, 6, or 11.
- Verify that users have the correct encryption type and password.

Other common problems:

- RF interference
- Not connected
- Radio not enabled
- Poor antenna location

Wireless Troubleshooting

- Locate the access point near the center of your home or office.
- Avoid mounting the access point next to metal objects.
- Keep the access point out of the line of sight of devices that contain metal.
- Verify connectivity without the security of PSK.
- Avoid RF interference from other equipment (gaming, monitors, phones).
- If the home or office is large, you may need two or more access points.
- Make sure the access point works over a unique channel not in use by other adjacent access point deployments.

Summary

- 802.11 topologies operate in various modes:
  - In ad hoc mode, clients connect directly without an intermediate access point.
  - In infrastructure mode, clients connect through an access point. There are two submodes, Basic Service Set (BSS) and Extended Service Set (ESS).
- BSS wireless topology consists of the basic service area (BSA) and the extended service area (ESA).

Summary (Cont.)

- Wireless access points can be configured through a CLI or, more commonly, a browser GUI.
- The basic approach to wireless implementation is to gradually configure and test incrementally.
- Currently there are many form factors available to add wireless to laptops:
  - Wireless Zero Configuration
  - Cisco Compatible Extensions
  - Cisco Secure Services Client
- You can troubleshoot wireless by breaking the environment into the wired network and the wireless network.
- WLAN data rates are affected by standards, access point placement, and distances.