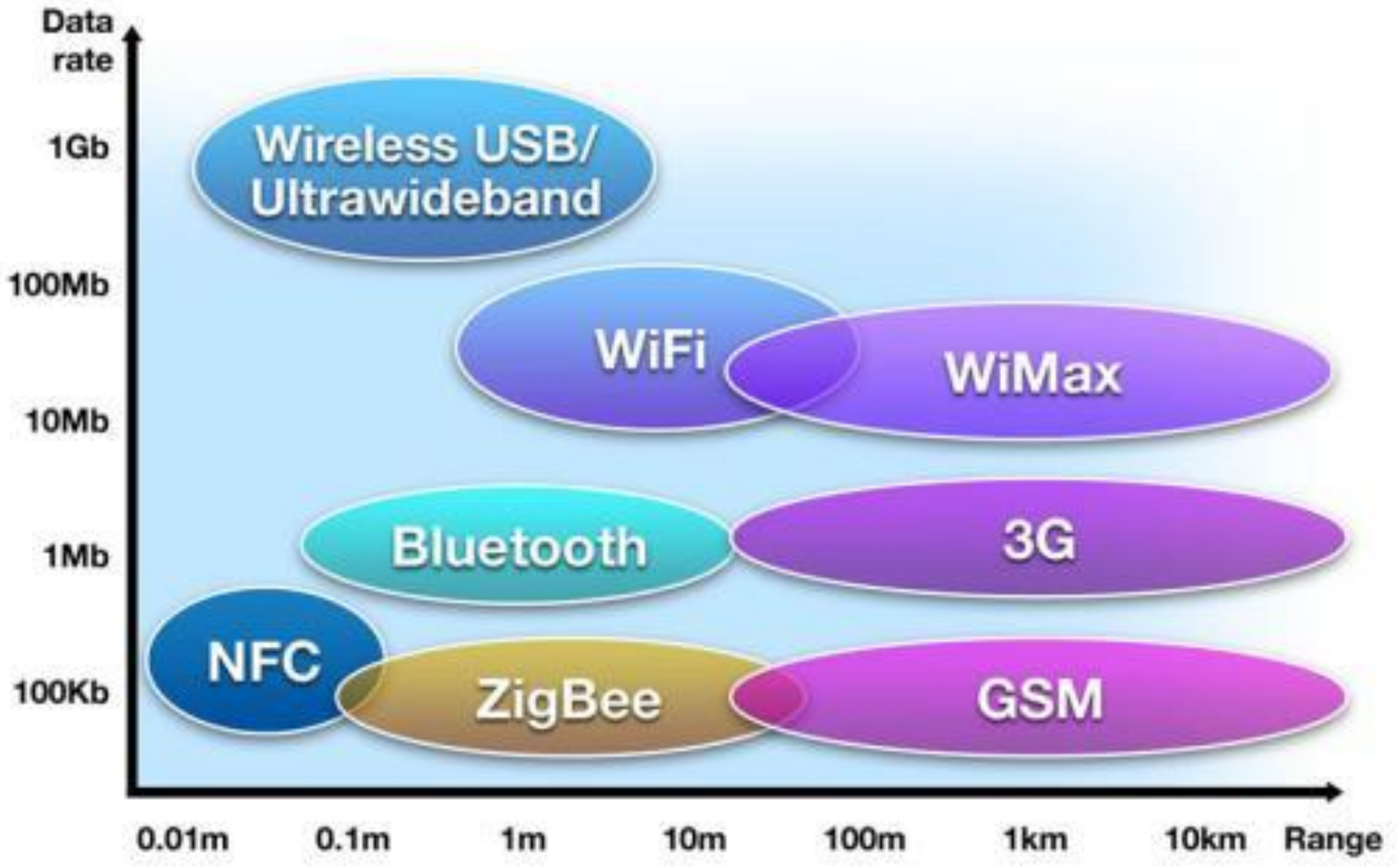
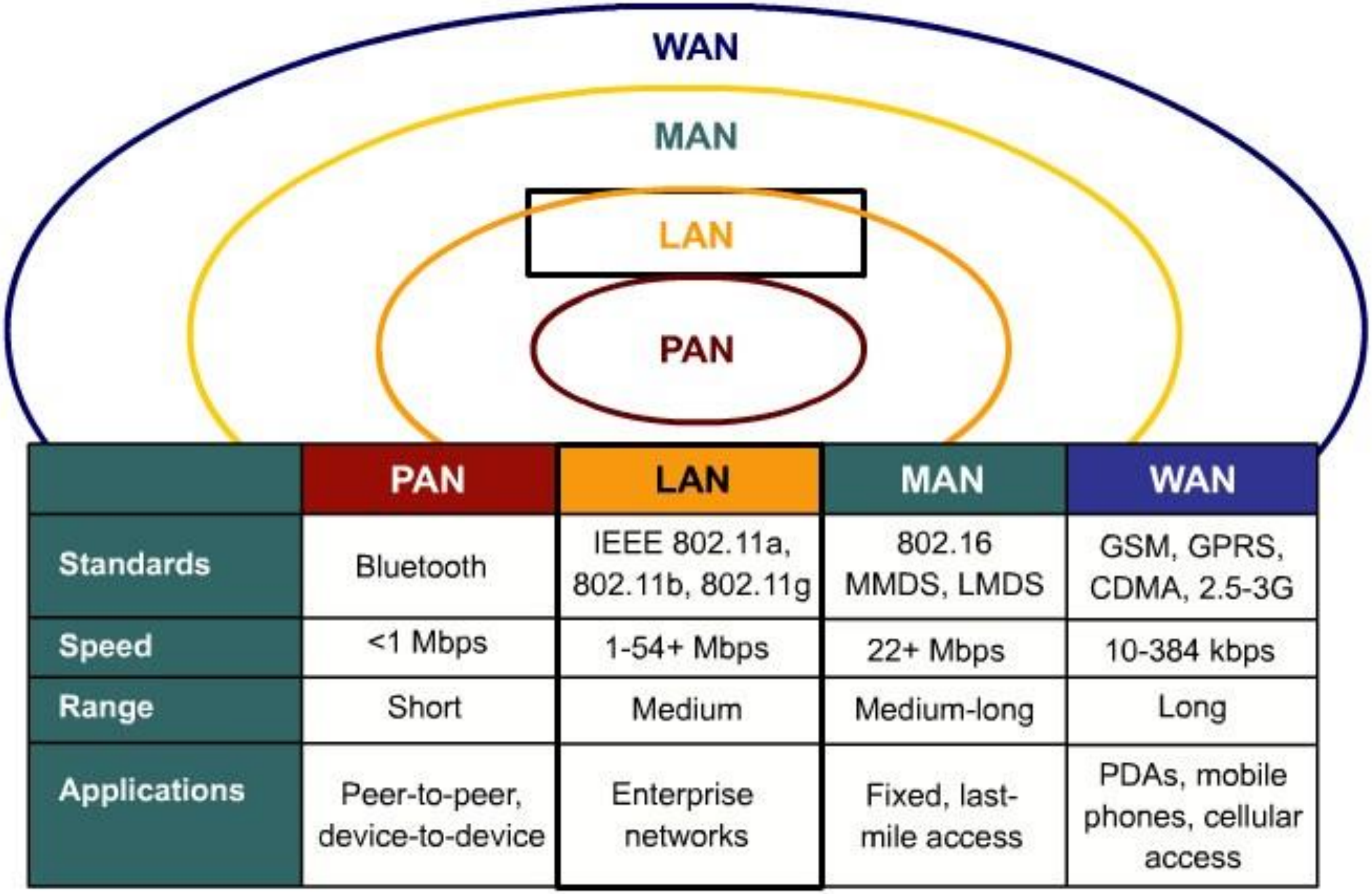
Introducing Wireless LANs

Wireless Data Technologies



Wireless Data Technologies (Cont.)



	PAN	LAN	MAN	WAN
Standards	Bluetooth	IEEE 802.11a, 802.11b, 802.11g	802.16 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Speed	<1 Mbps	1-54+ Mbps	22+ Mbps	10-384 kbps
Range	Short	Medium	Medium-long	Long
Applications	Peer-to-peer, device-to-device	Enterprise networks	Fixed, last-mile access	PDAs, mobile phones, cellular access

Wireless LAN (WLAN)

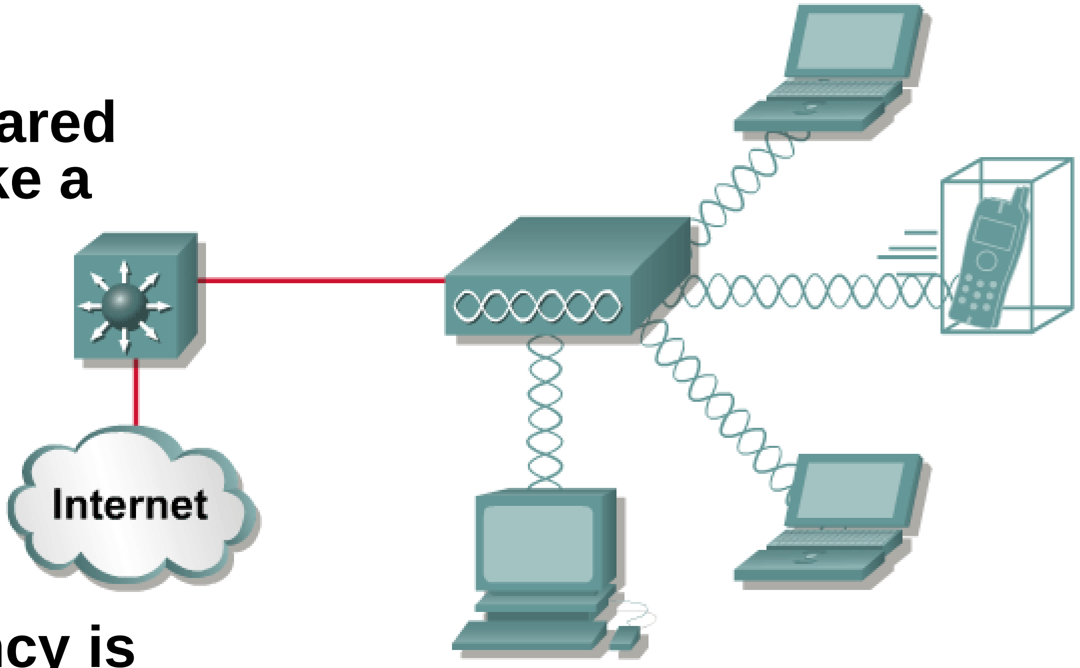
A WLAN is a shared network.

An access point is a shared device and functions like a shared Ethernet hub.

Data is transmitted over radio waves.

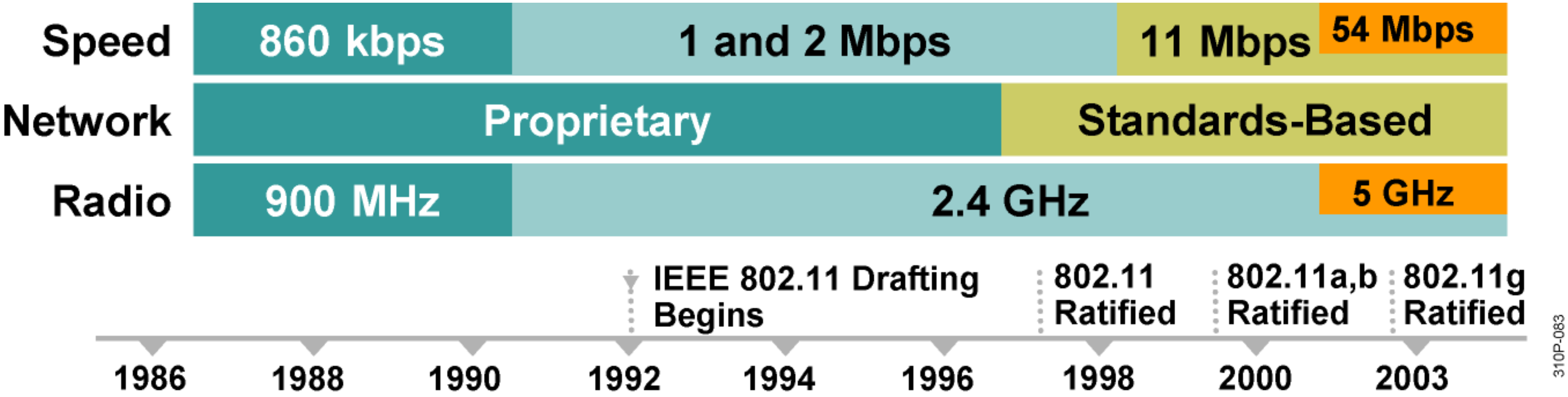
Two-way radio communications (half-duplex) are used.

The same radio frequency is used for sending and receiving (transceiver).



Wireless LAN Evolution

- Warehousing
- Retail
- Health care
- Education
- Businesses
- Home



Speed: 860 kbps | 1 and 2 Mbps | 11 Mbps | 54 Mbps

Network: Proprietary | Standards-Based

Radio: 900 MHz | 2.4 GHz | 5 GHz

IEEE 802.11 Drafting Begins

802.11 Ratified

802.11a,b Ratified

802.11g Ratified

1986 1988 1990 1992 1994 1996 1998 2000 2003

310P-083

What Are Wireless LANs?

They are:

- Local
- In building or campus for mobile users
- Radio or infrared
- Not required to have RF licenses in most countries
- Using equipment owned by customers

They are not:

- WAN or MAN networks
- Cellular phone networks
- Packet data transmission via celluar phone networks
  - Cellular digital packet data (CDPD)
  - General packet radio service (GPRS)
  - 2.5G to 3G services

Similarities Between WLAN and LAN

A wireless LAN is an 802 LAN.

- Transmits data over the air vs. data over the wire
- Looks like a wired network to the user
- Defines physical and data link layer
- Uses MAC addresses

The same protocols/applications run over both WLANs and LANs.

- IP (network layer)
- IPSec VPNs (IP-based)
- Web, FTP, SNMP (applications)

Differences Between WLAN and LAN

WLANs use radio waves as the physical layer.

- WLANs use CSMA/CA instead of CSMA/CD to access the network

Radio waves have problems that are not found on wires.

- Connectivity issues
  - Coverage problems
  - Multipath issues
  - Interference, noise
- Privacy issues

WLANs use mobile clients.

- No physical connection
- Battery-powered

WLANs must meet country-specific RF regulations.

More on CSMA/CA

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- The wireless 802.11 standard uses CSMA/CA or "collision avoidance." The method is used because the wireless stations have no way to detect collisions WHILE sending.
- Attempts to avoid collisions rather than detect them

How it works:

- Transmitting device listens to the network (senses the carrier) and waits for it to be free
- Device then waits a random period of time and transmits.
- If the receiver gets the frame intact, it sends back an ACK to the sender.
- If no ACK is received, the message is re-transmitted.
- If the channel is not clear, the node waits for a randomly chosen period of time (backoff factor), and then checks again to see if the channel is clear.

Wireless LAN Topologies

Wireless client access

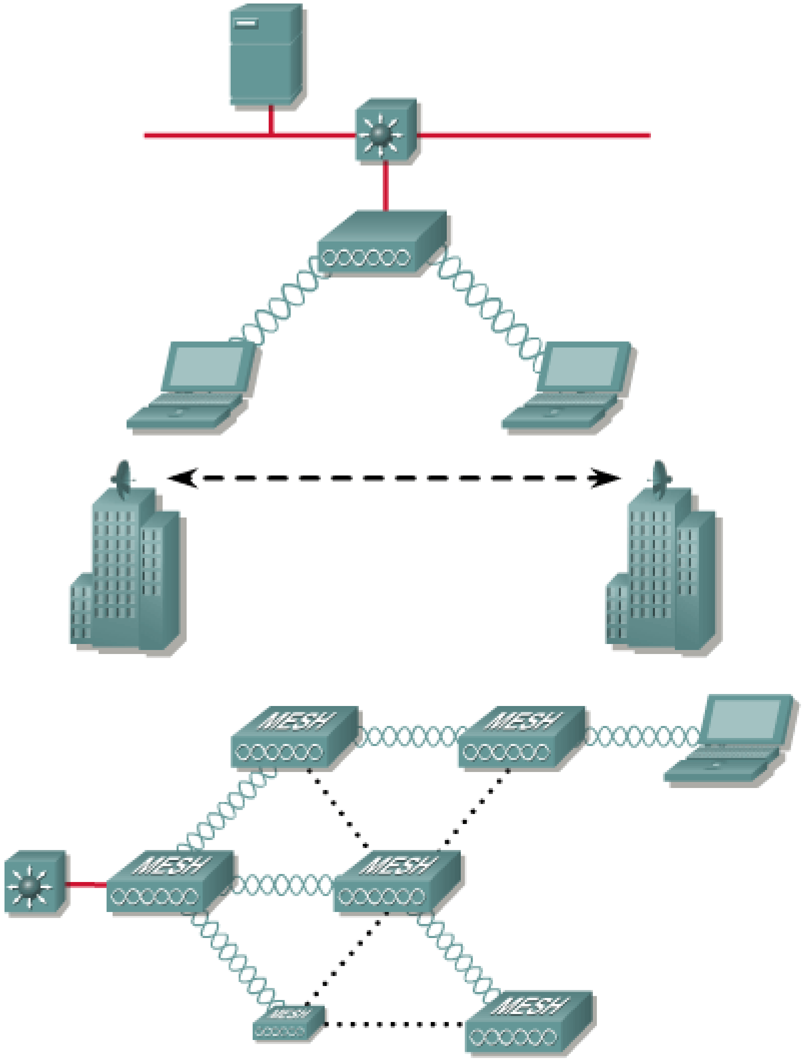
- Mobile user connectivity

Wireless bridging

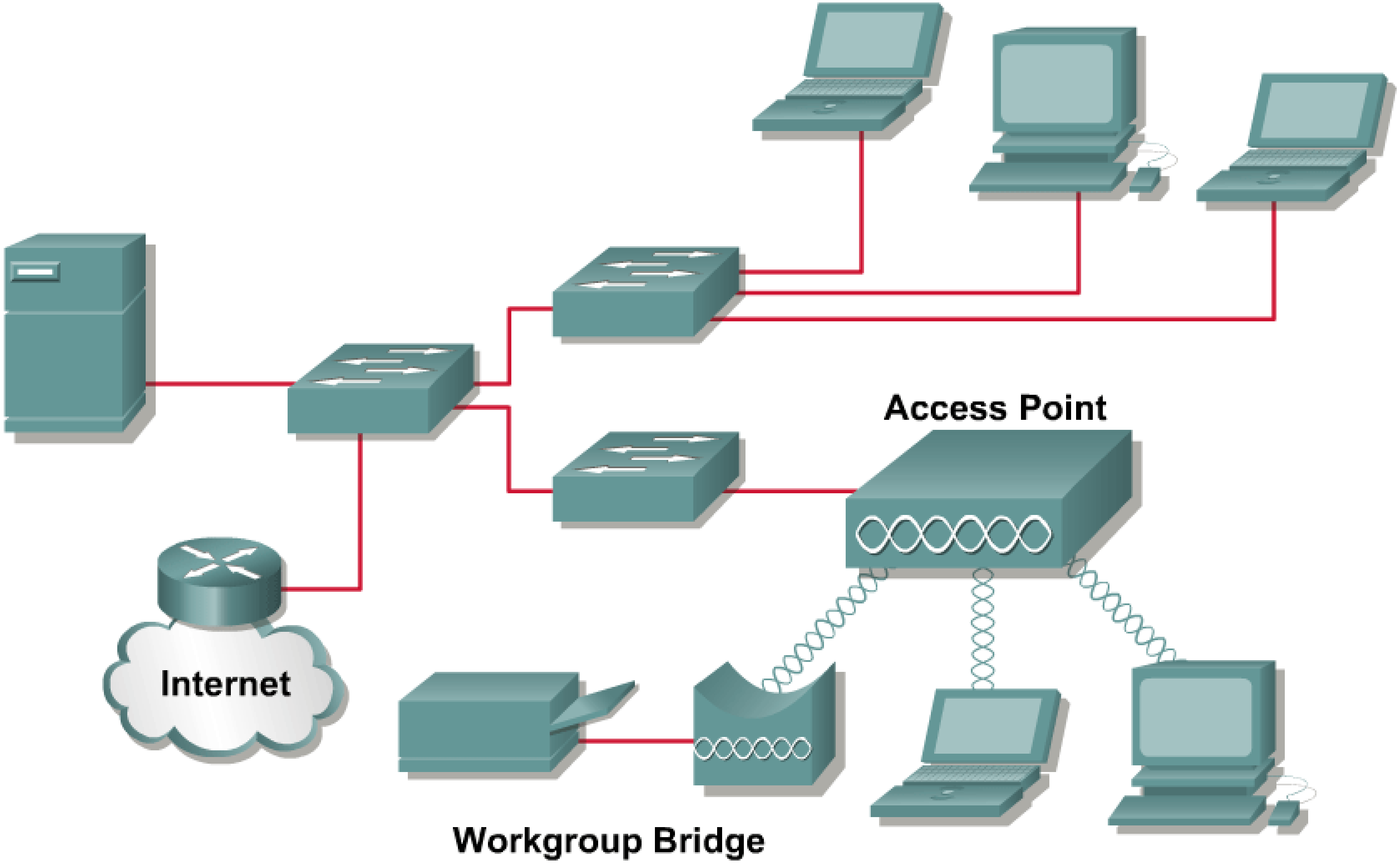
- LAN-to-LAN connectivity

Wireless mesh networking

- Combination of bridging and user connectivity



WLAN and LAN



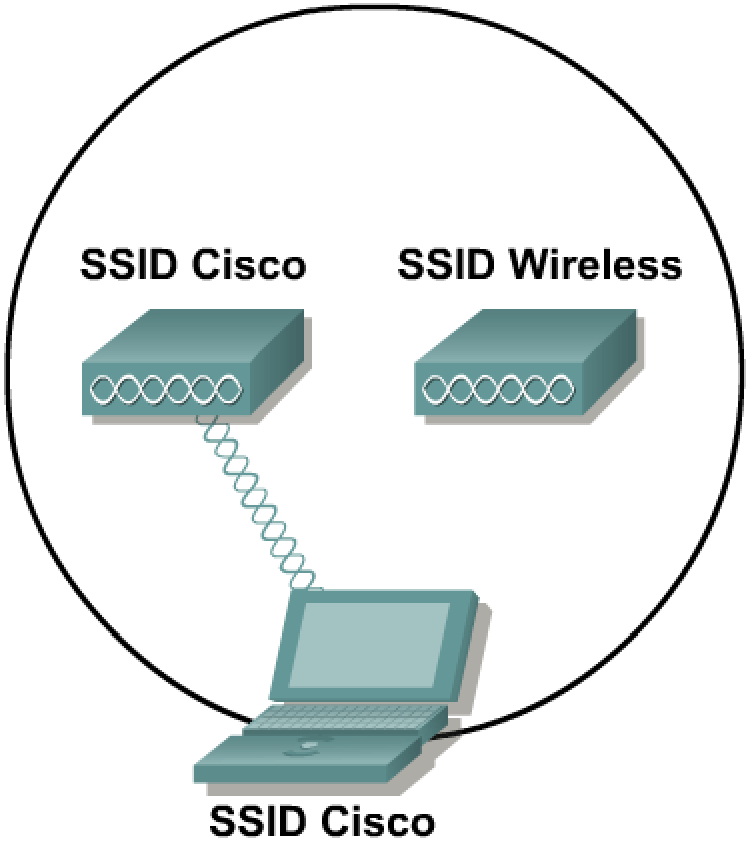
Service Set Identifier (SSID)

SSID is used to logically separate WLANs.

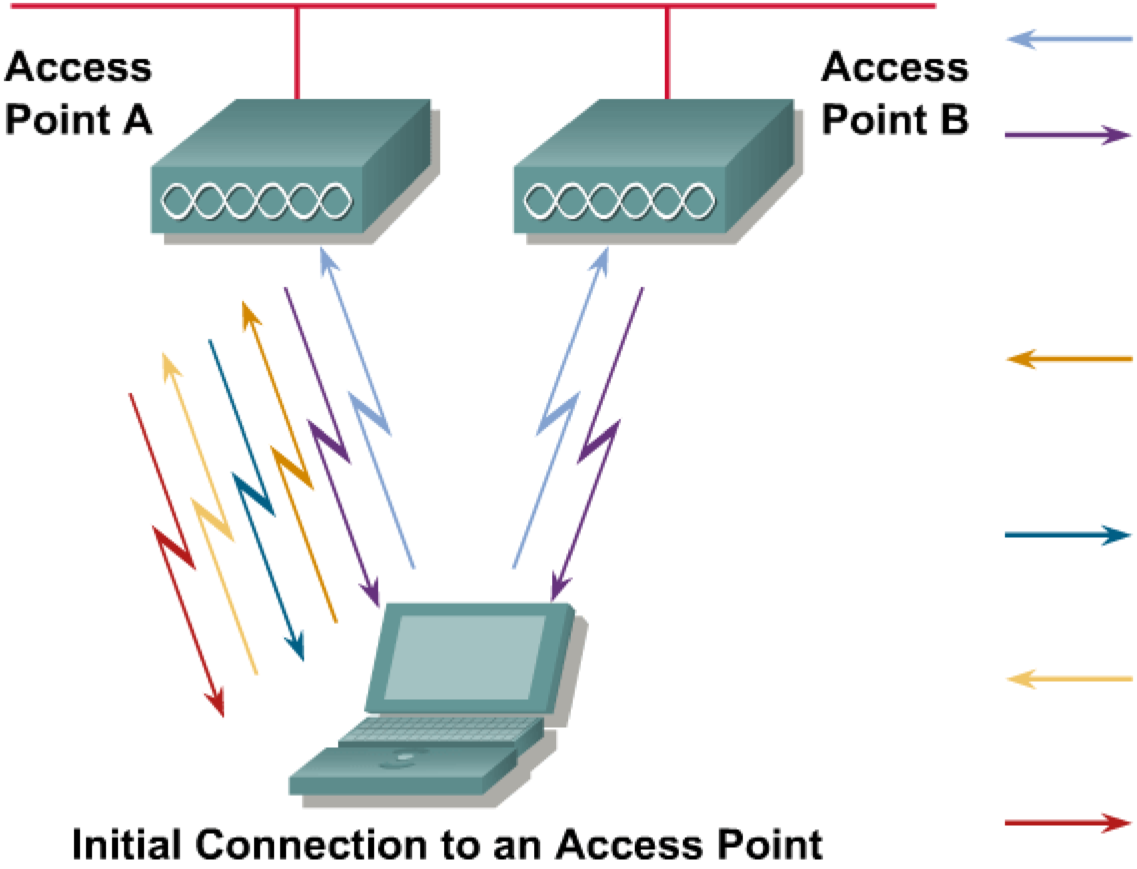
The SSID must match on client and access point.

Access point can broadcast SSID in beacon.

Client can be configured without SSID.



Association Process (Active Scanning)

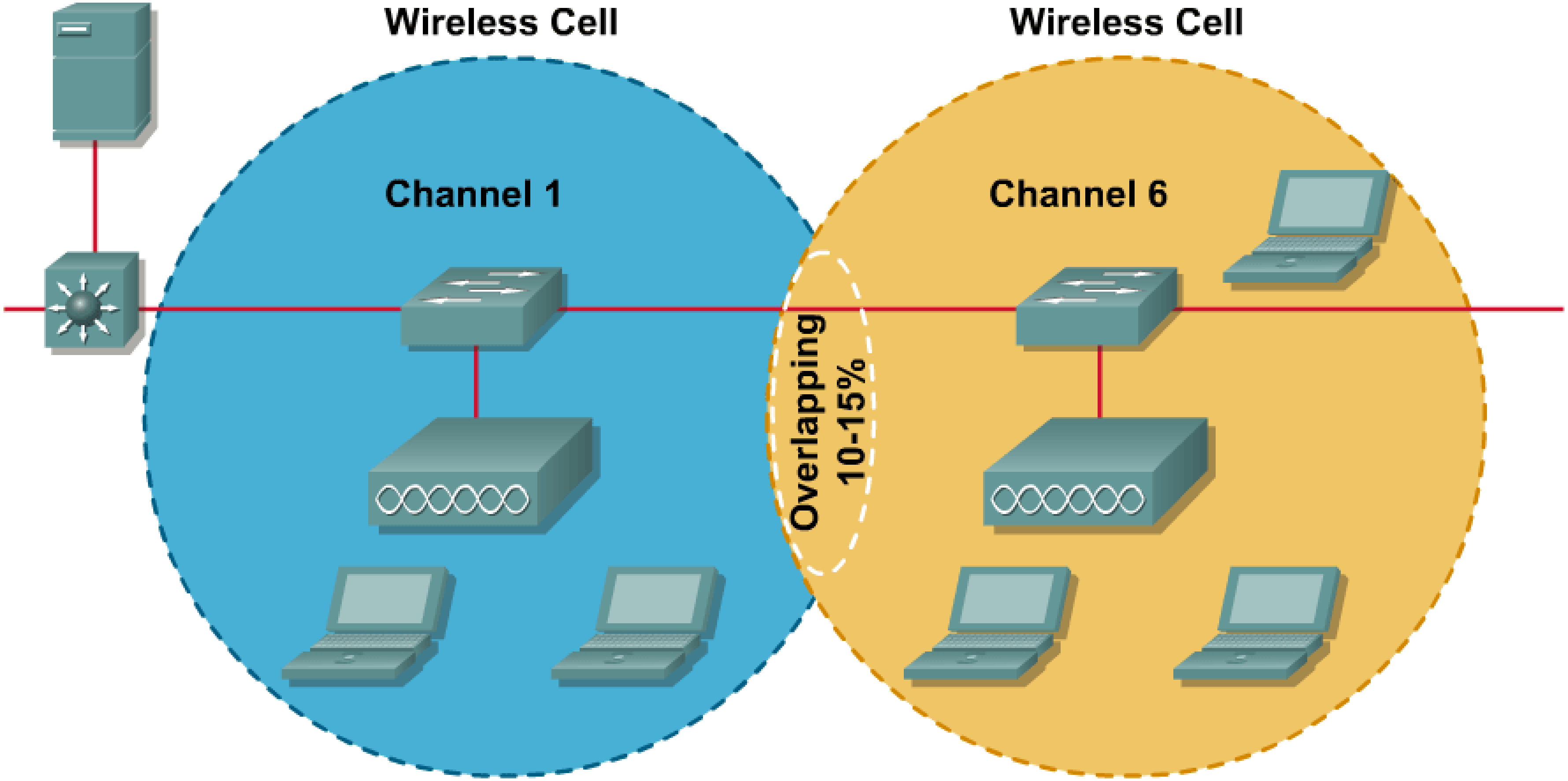


Initial Connection to an Access Point

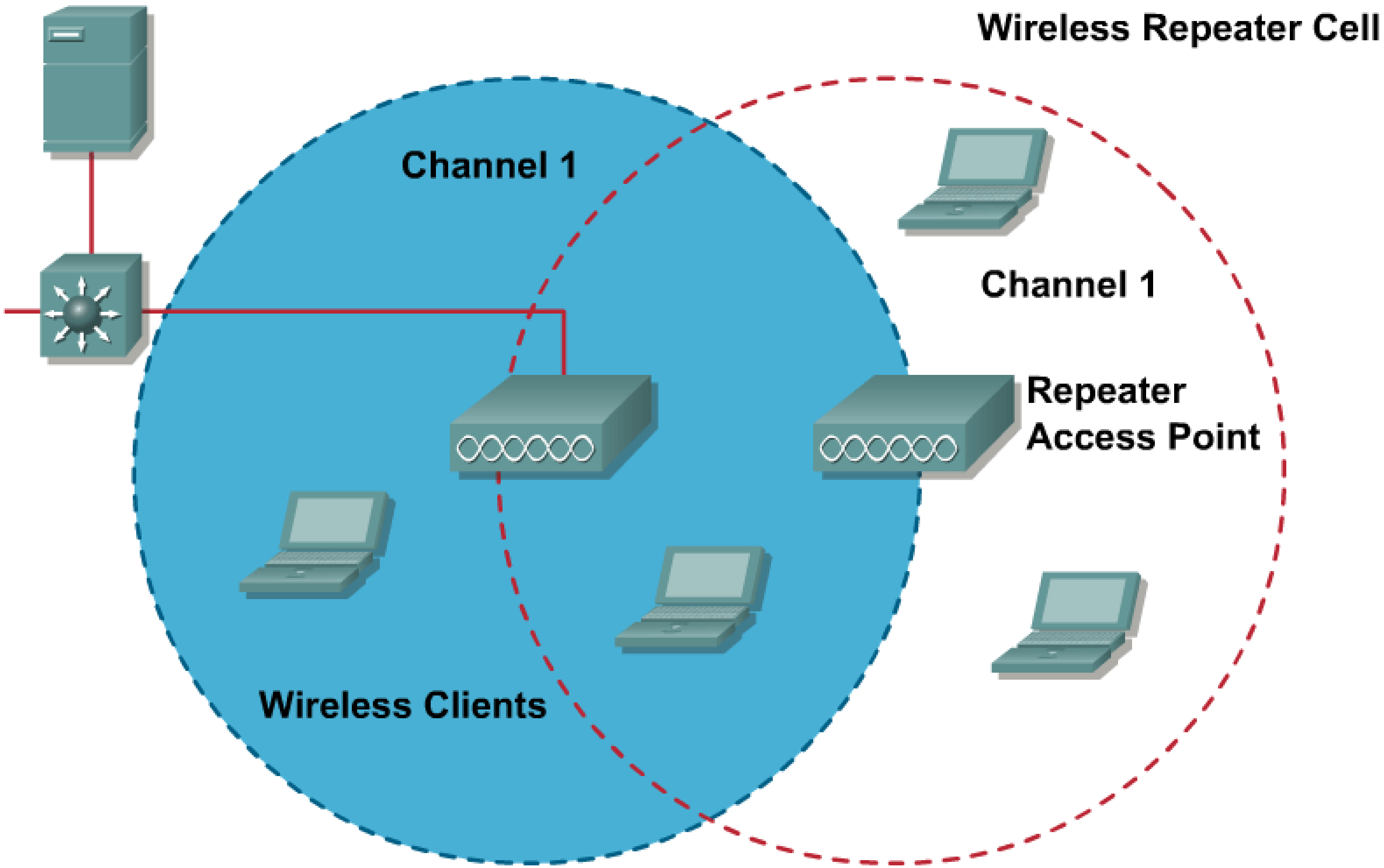
Steps to Association:

- Client Sends Probe
- AP Sends Probe Response
- Client Evaluates AP Response, Selects Best AP
- Client Sends Authentication Request to Selected AP (A)
- AP A Confirms Authentication and Registers Client
- Client Sends Association Request to Selected AP (A)
- AP A Confirms Association and Registers Client

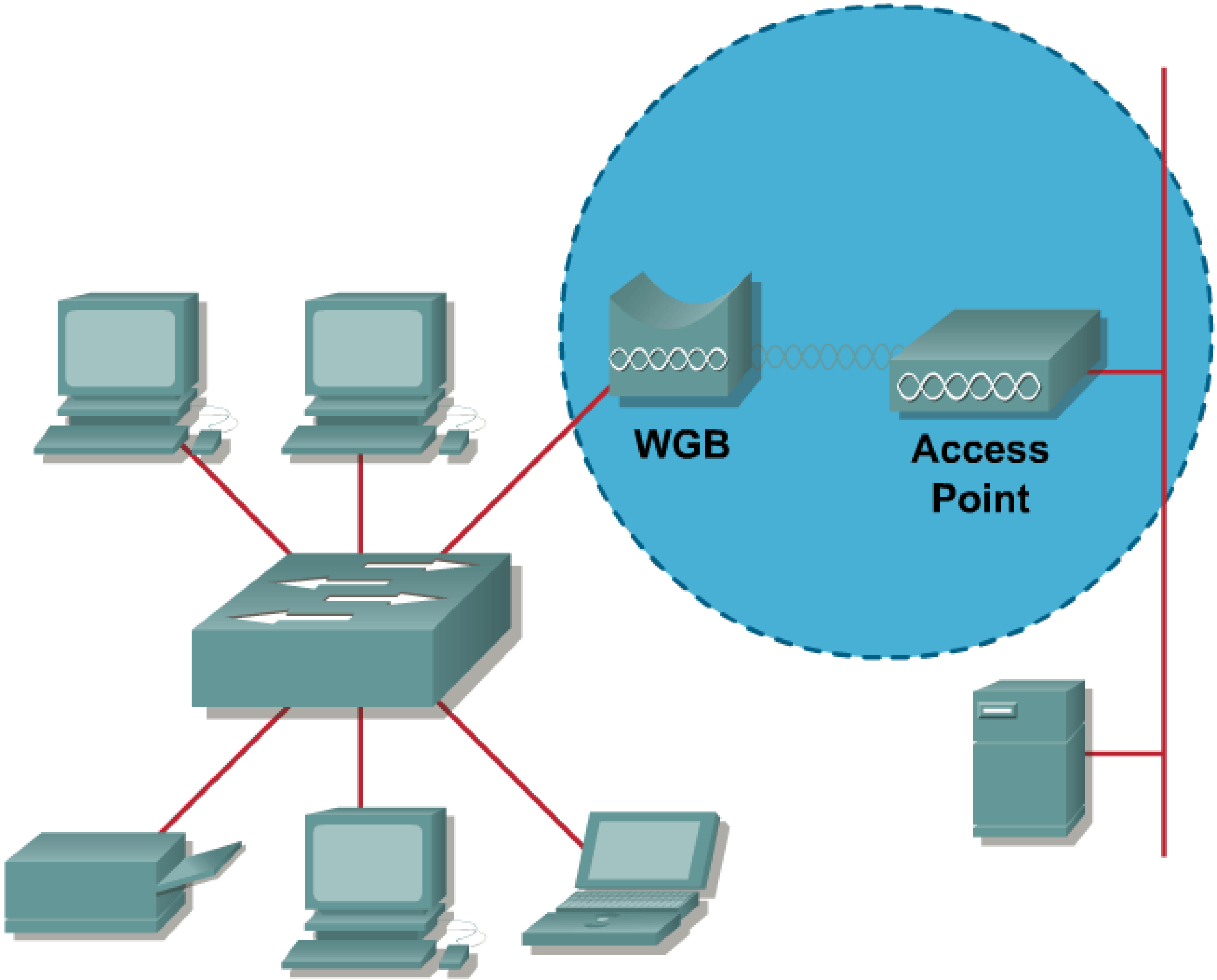
WLAN Access Topology



Wireless Repeater Topology

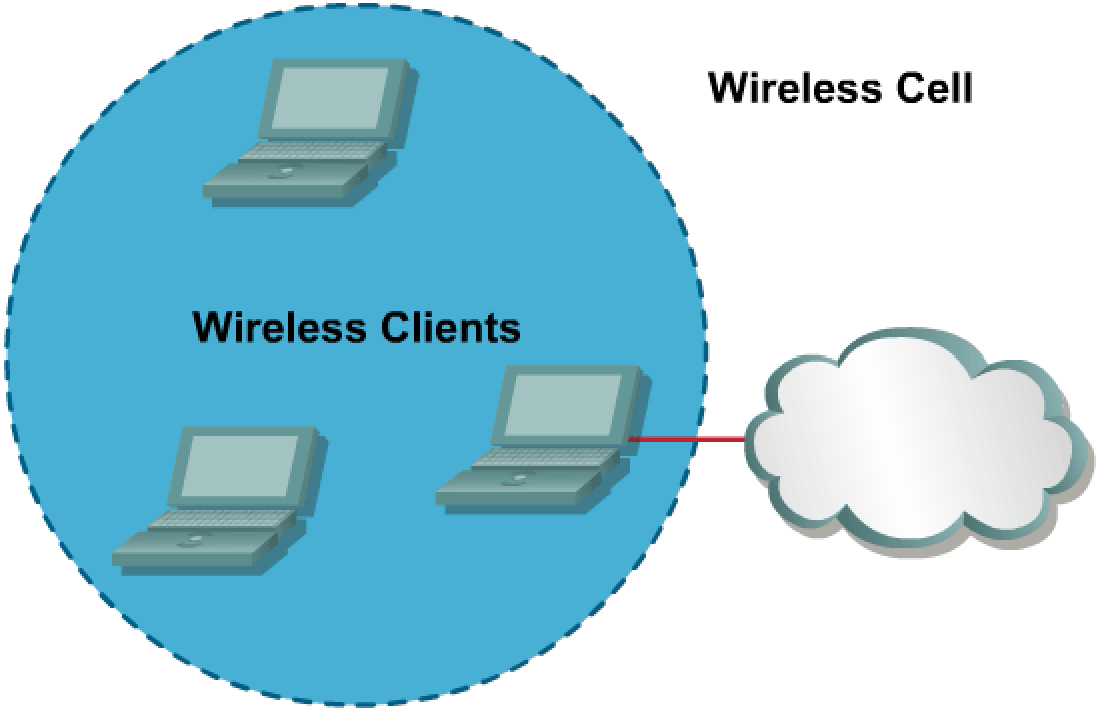


Workgroup Bridge Topology



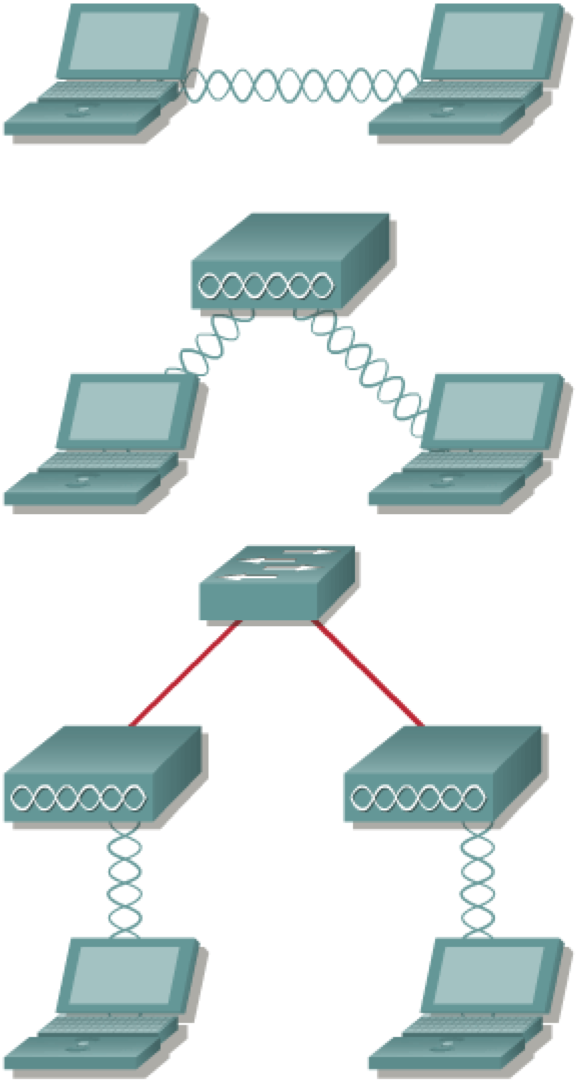
Alternative Peer-to-Peer Topology

Peer-to-Peer Configuration (Ad Hoc Mode)

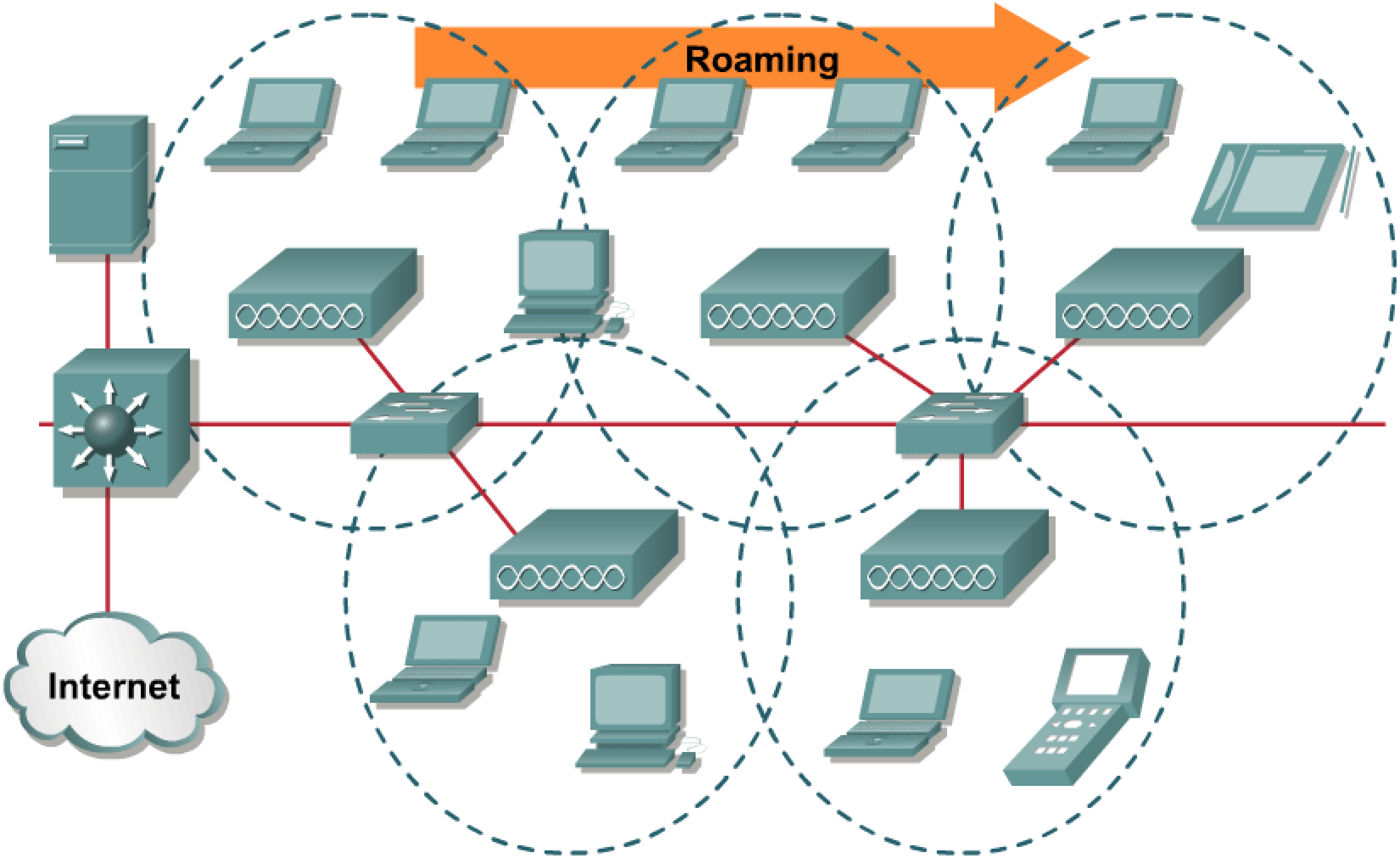


Service Sets & Modes

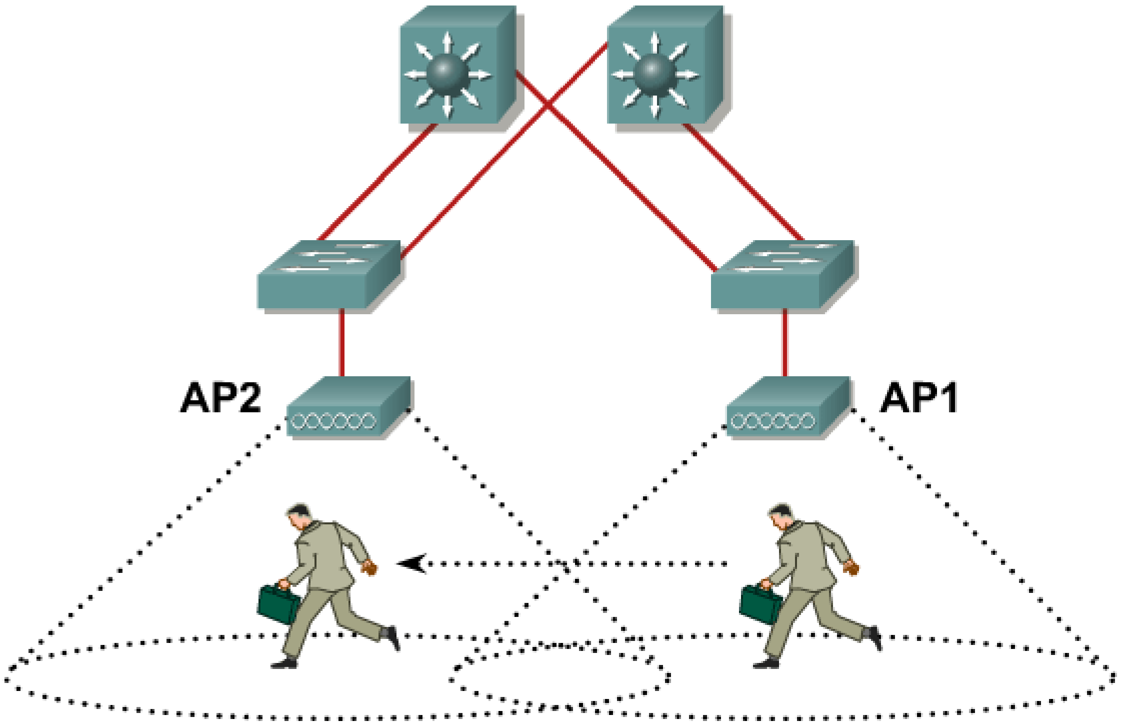
- Ad hoc mode
  - Independent Basic Service Set (IBSS)
    - Mobile clients connect directly without an intermediate AP.
- Infrastructure mode
  - Basic Service Set (BSS)
    - Mobile clients use a single AP for connecting to each other or to wired network resources.
  - Extended Services Set (ESS)
    - Two or more Basic Service Sets are connected by a common distribution system (DS).



Roaming Through Wireless Cells



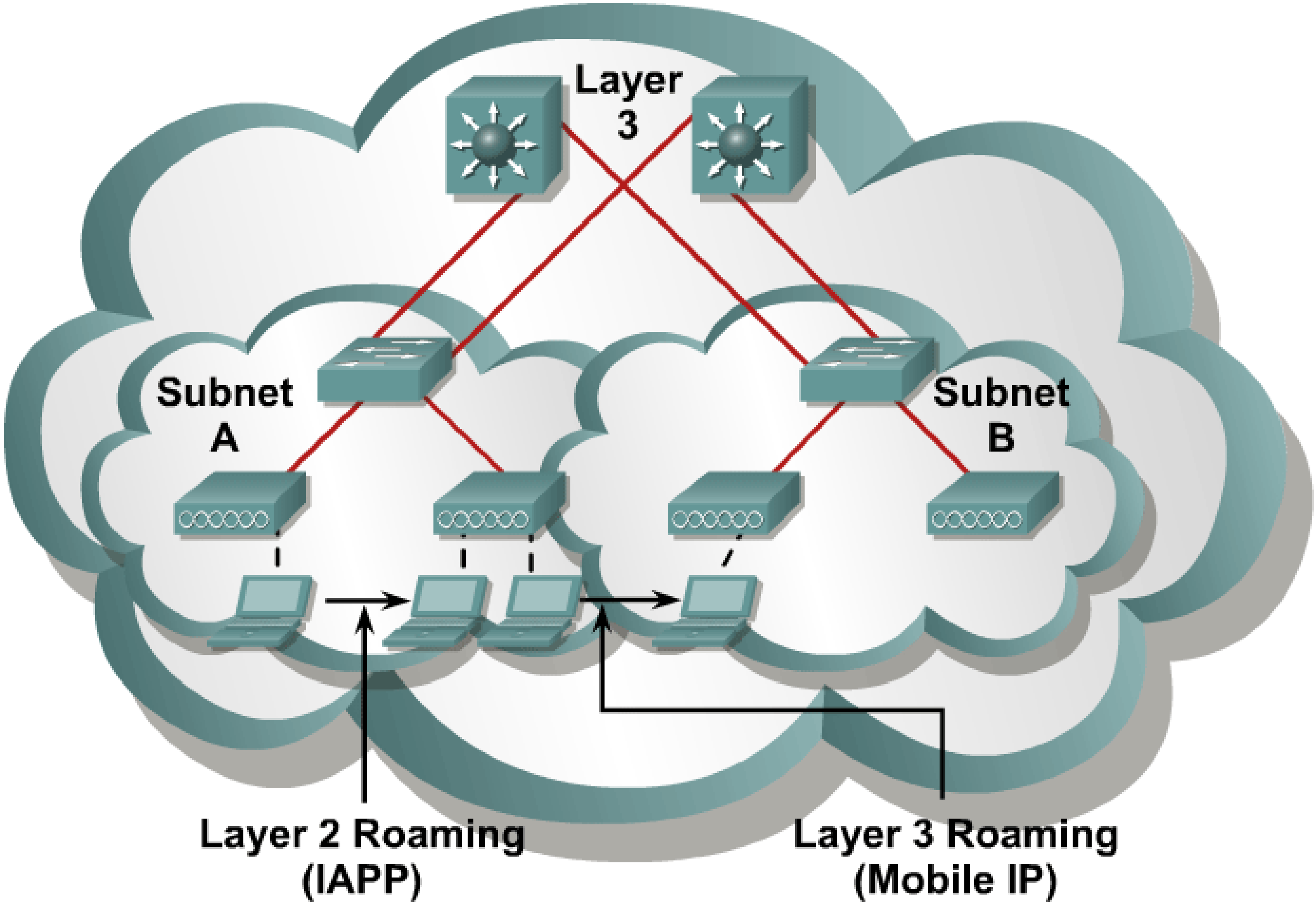
Client Roaming



- Maximum data retry count exceeded
- Too many beacons missed
- Data rate shifted
- Periodic intervals

- Roaming without interruption requires the same SSID on all access points.

Layer 2 vs. Layer 3 Roaming



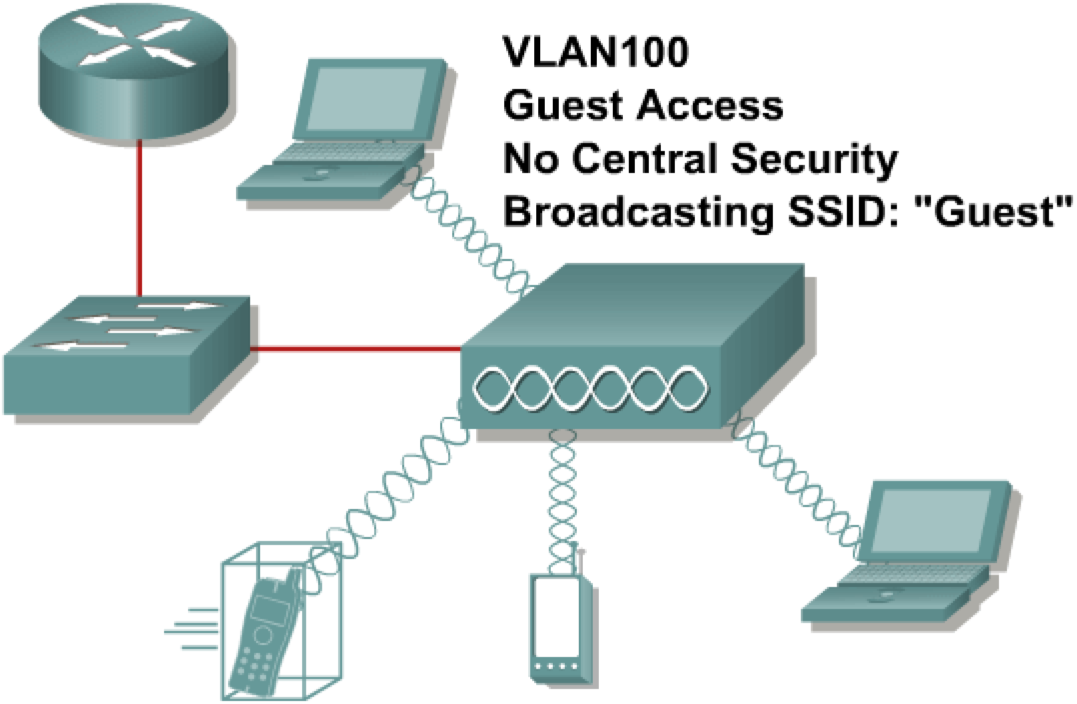
Wireless VLAN Support

Multiple SSIDs

Multiple security types

Support for multiple VLANs from switches

802.1Q trunking protocol



VLAN100
Guest Access
No Central Security
Broadcasting SSID: "Guest"

VLAN103
802.1x Security
SSID: "QOS"

VLAN101
Specialized User
Static WEP
Not Broadcasting
SSID: "static"

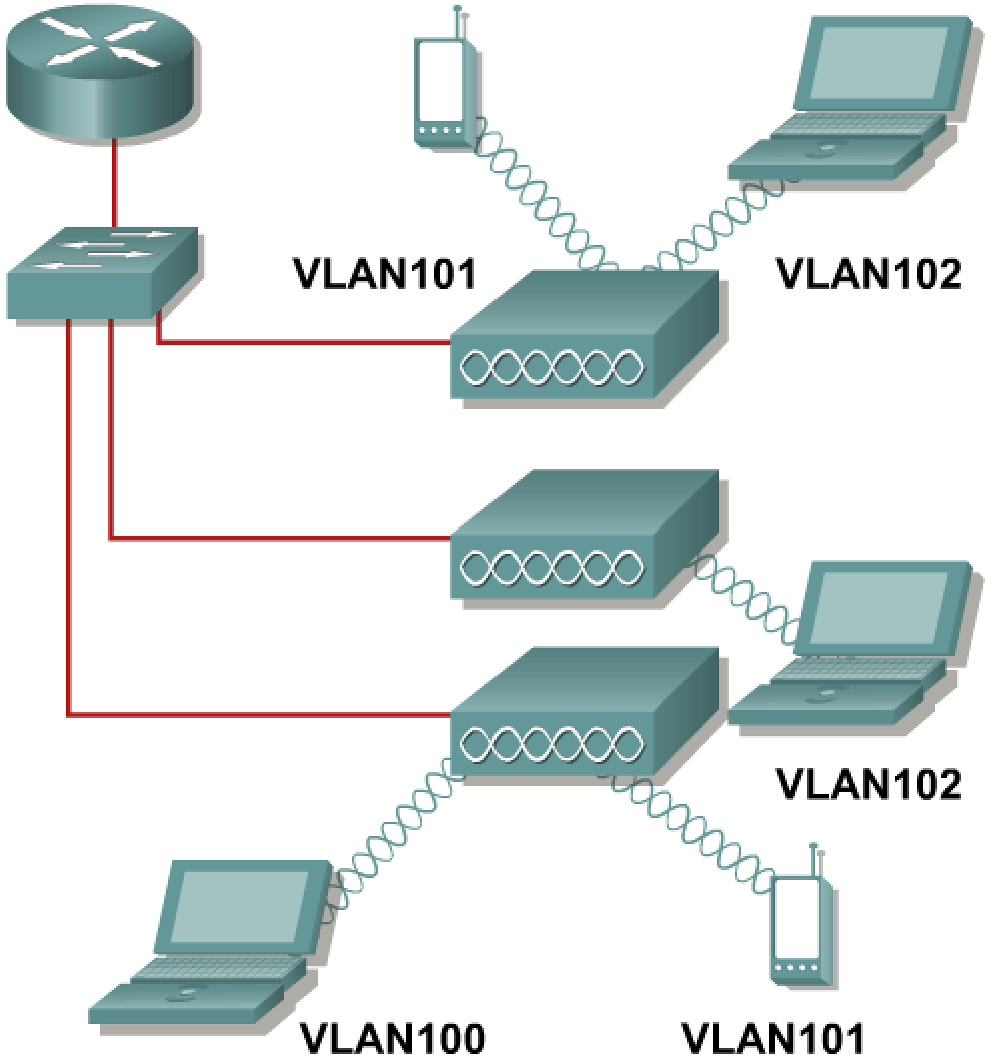
VLAN102
Corporate User
802.1x Security
SSID: "secure"

Wireless VLAN Support (Cont.)

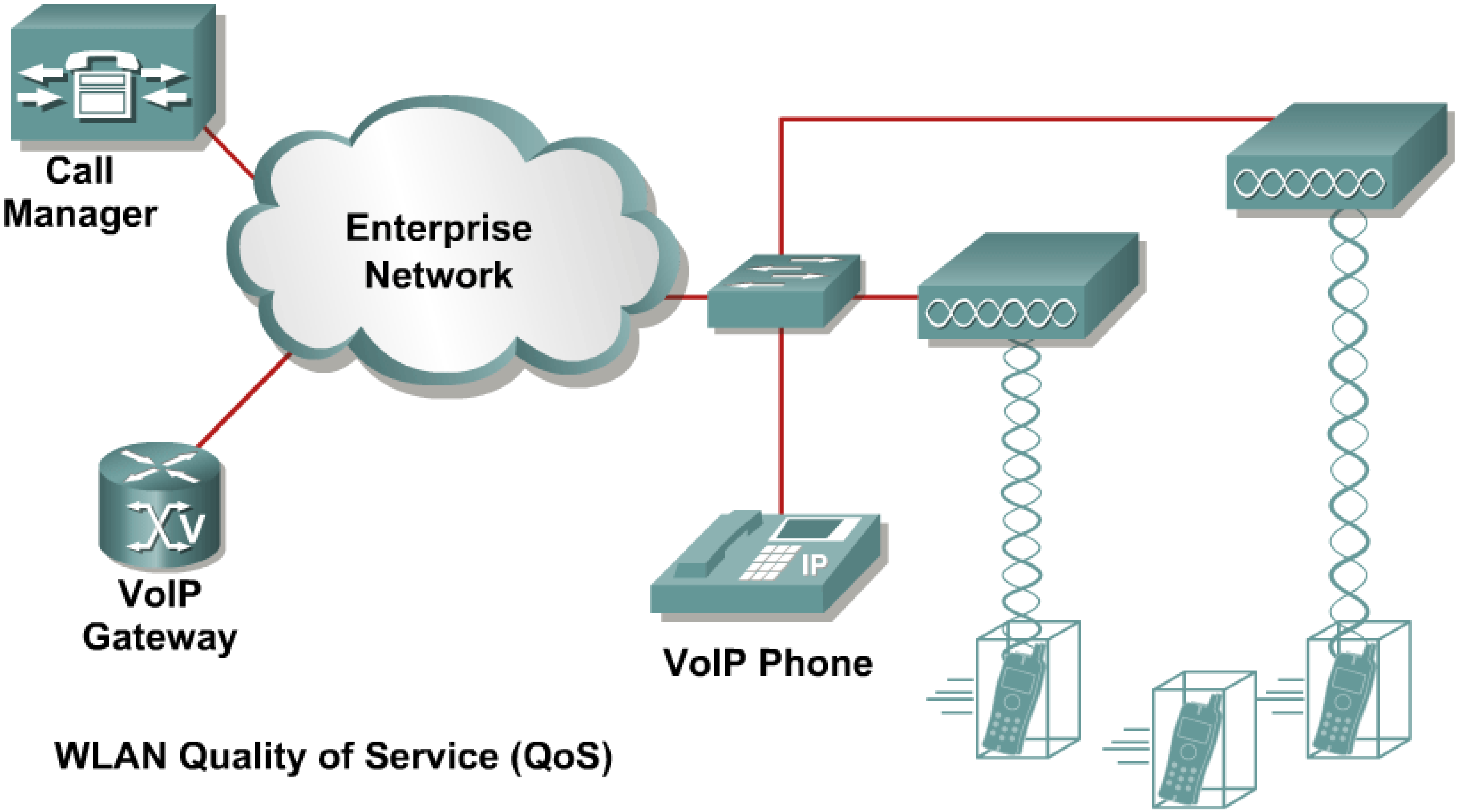
VLANs propagate across APs.

VLAN numbers are unique.

Autonomous access points handle up to 16 VLANs.



Enterprise Voice Architecture



WLAN Quality of Service (QoS)

Autonomous or Lightweight?

Most Cisco wireless access points/bridges are available as autonomous or lightweight devices.

Lightweight APs use Lightweight Access Point Protocol (LWAPP) and must have a LAN controller to function within the network.

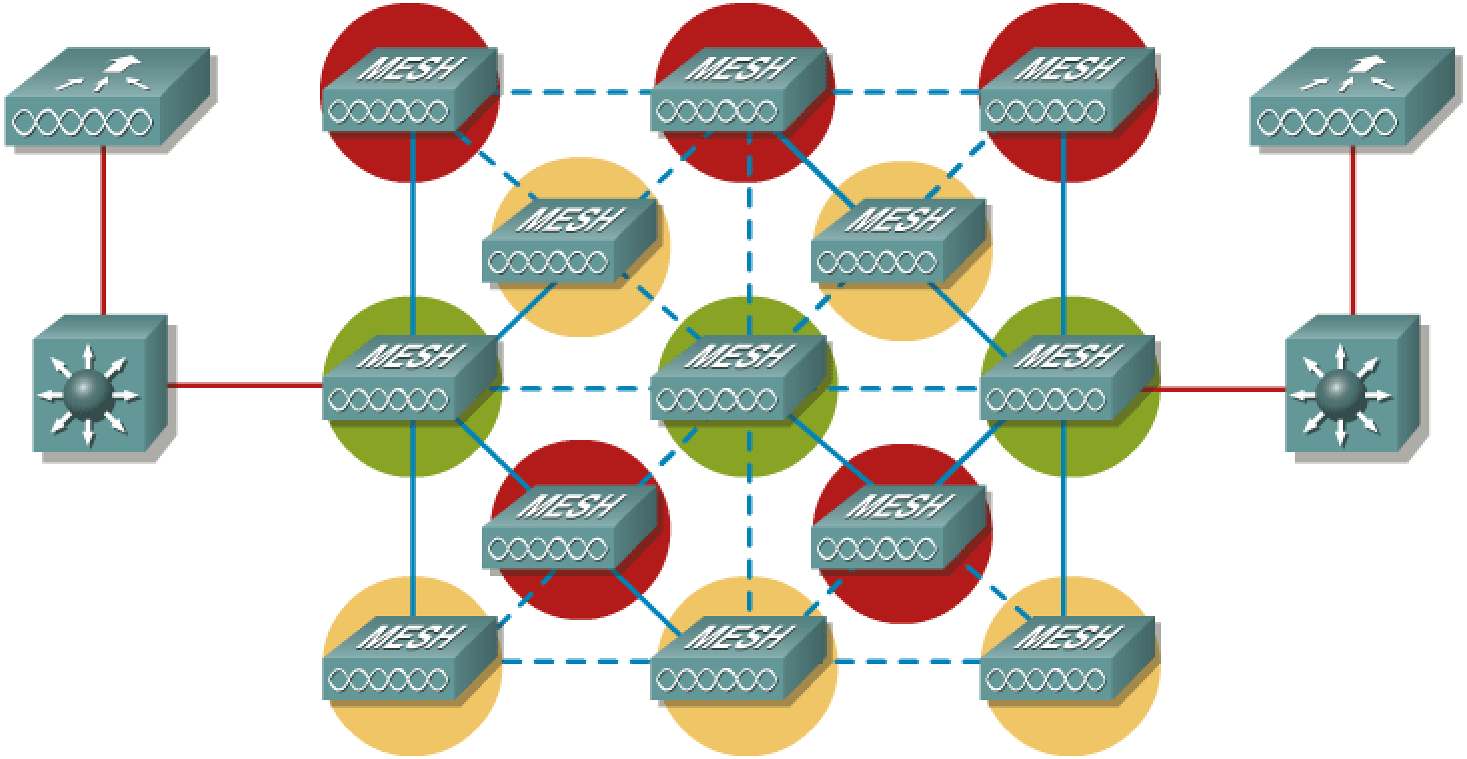
Autonomous APs can be configured via Cisco IOS.

Most Cisco autonomous APs can be software upgraded to function as lightweight APs.

The Cisco Networking Academy FWL course focused on autonomous APs.

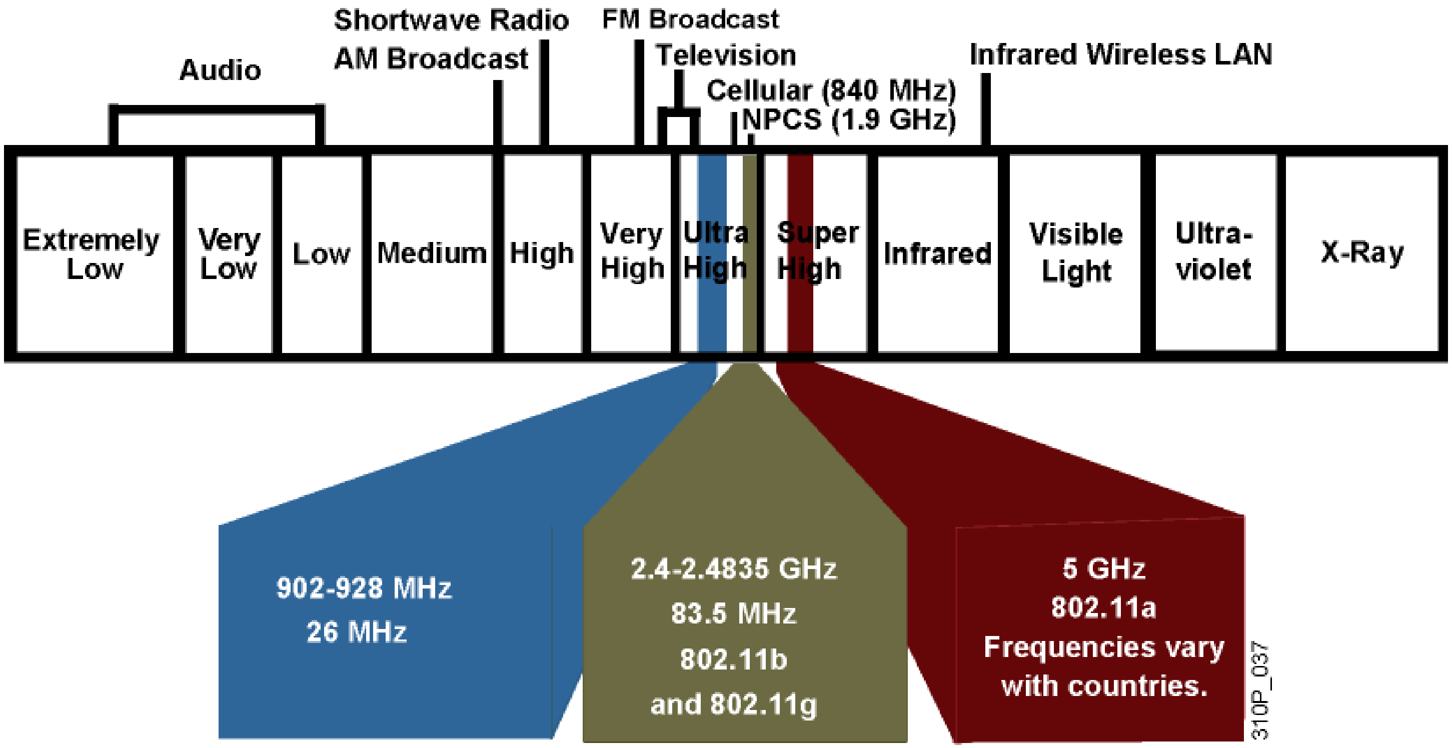
Wireless Mesh Networking

In a mesh network topology, devices are connected with redundant connections between nodes.



Explaining Wireless LAN Technology & Standards

Unlicensed Frequency Bands



- ISM: Industry, Scientific, and Medical frequency band
- No license required
- No exclusive use
- Best effort
- Interference possible

Radio Frequency Transmission

Radio frequencies are radiated into the air via an antenna, creating radio waves.

Radio waves are absorbed when they are propagated through objects (e.g. walls).

Radio waves are reflected by objects (e.g. metal surfaces).

This absorption and reflection can cause areas of low signal strength or low signal quality.

Radio Frequency Transmission

Higher data rates have a shorter transmission range.

- The receiver needs more signal strength and better SNR to retrieve information.

Higher transmit power results in greater distance.

Higher frequencies allow higher data rates.

Higher frequencies have a shorter transmission range.

WLAN Regulation and Standardization

Regulatory agencies

- FCC (United States)
- ETSI (Europe)

Standardization

- IEEE 802.11
- http://standards.ieee.org/getieee802/

Certfication of equipment

- Wi-Fi Alliance certifies interoperability between products.
- Certifications include 802.11a, 802.11b, 802.11g, dual-band products, and security testing.
- Certified products can be found at http://www.wi-fi.org.

Wi Fi®

CERTIFIED

Interoperable with:

2.4 GHz Band 11 Mbps ☑

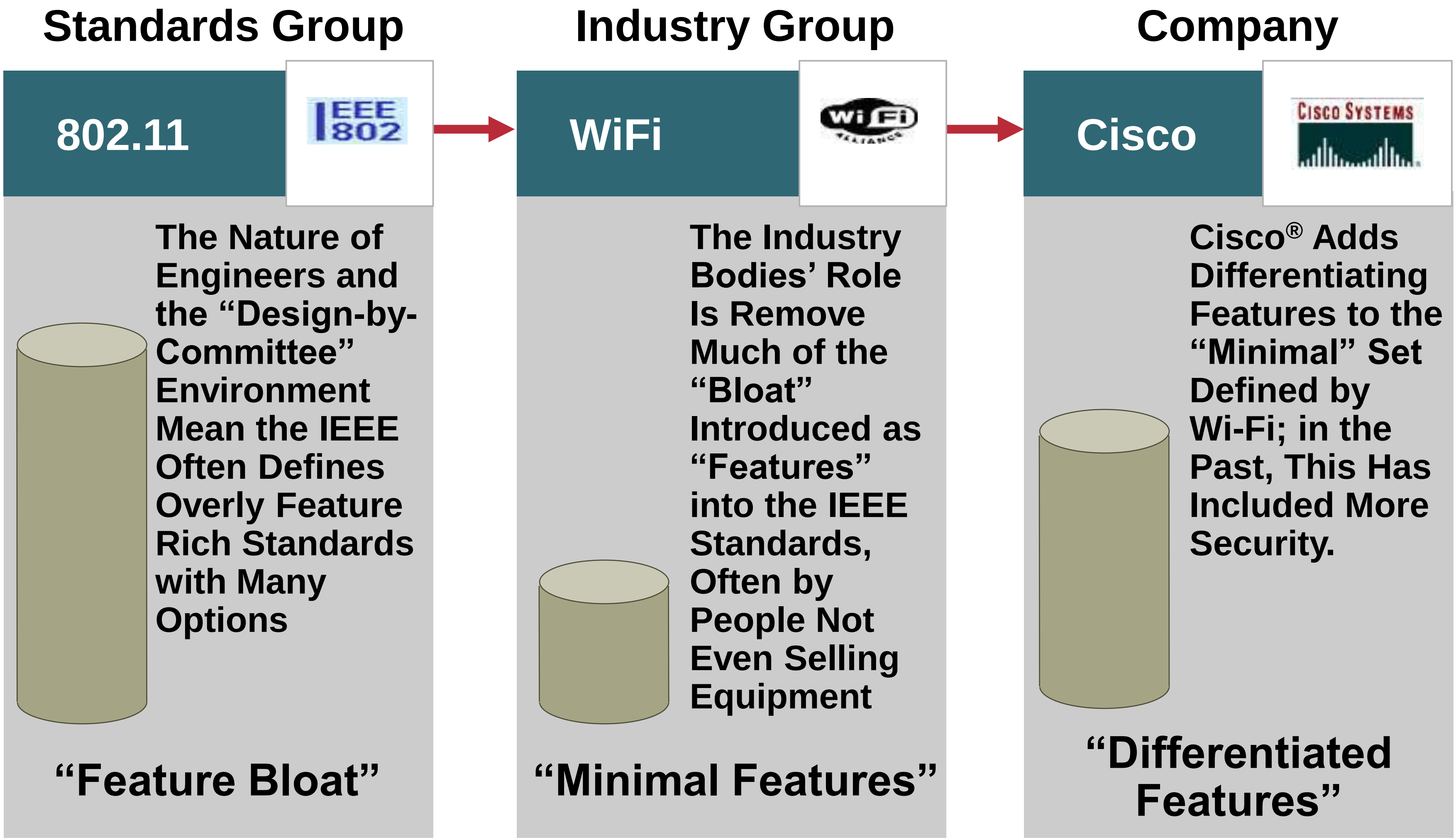
54 Mbps ☑

5 GHz Band 54 Mbps ☑

Wi-Fi Protected Access™ ☑

www.wi-fi.org

Standards and Implementation Process



Standards Group

802.11

The Nature of Engineers and the “Design-by-Committee” Environment Mean the IEEE Often Defines Overly Feature Rich Standards with Many Options

“Feature Bloat”

Industry Group

WiFi

The Industry Bodies’ Role Is Remove Much of the “Bloat” Introduced as “Features” into the IEEE Standards, Often by People Not Even Selling Equipment

“Minimal Features”

Company

Cisco

Cisco® Adds Differentiating Features to the “Minimal” Set Defined by Wi-Fi; in the Past, This Has Included More Security.

“Differentiated Features”

802.11b Standard

Standard was ratified in September 1999

Operates in the 2.4-GHz band

Specifies Direct Sequence Spread Spectrum (DSSS)

Specifies four data rates up to 11 Mbps

- 1, 2, 5.5, 11 Mbps

Provides specifications for vendor interoperability (over
the air)

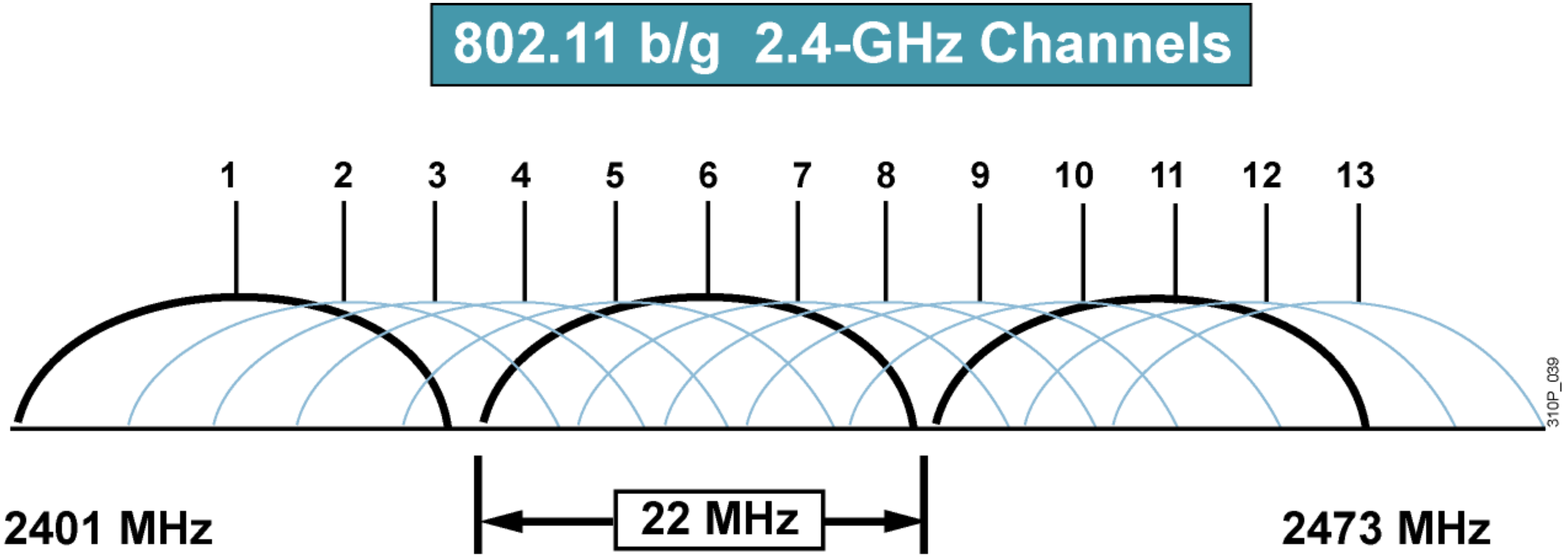
Defines basic security, encryption, and
authentication for the wireless link

Is the most commonly deployed wireless LAN
standard

2.4-GHz Channels

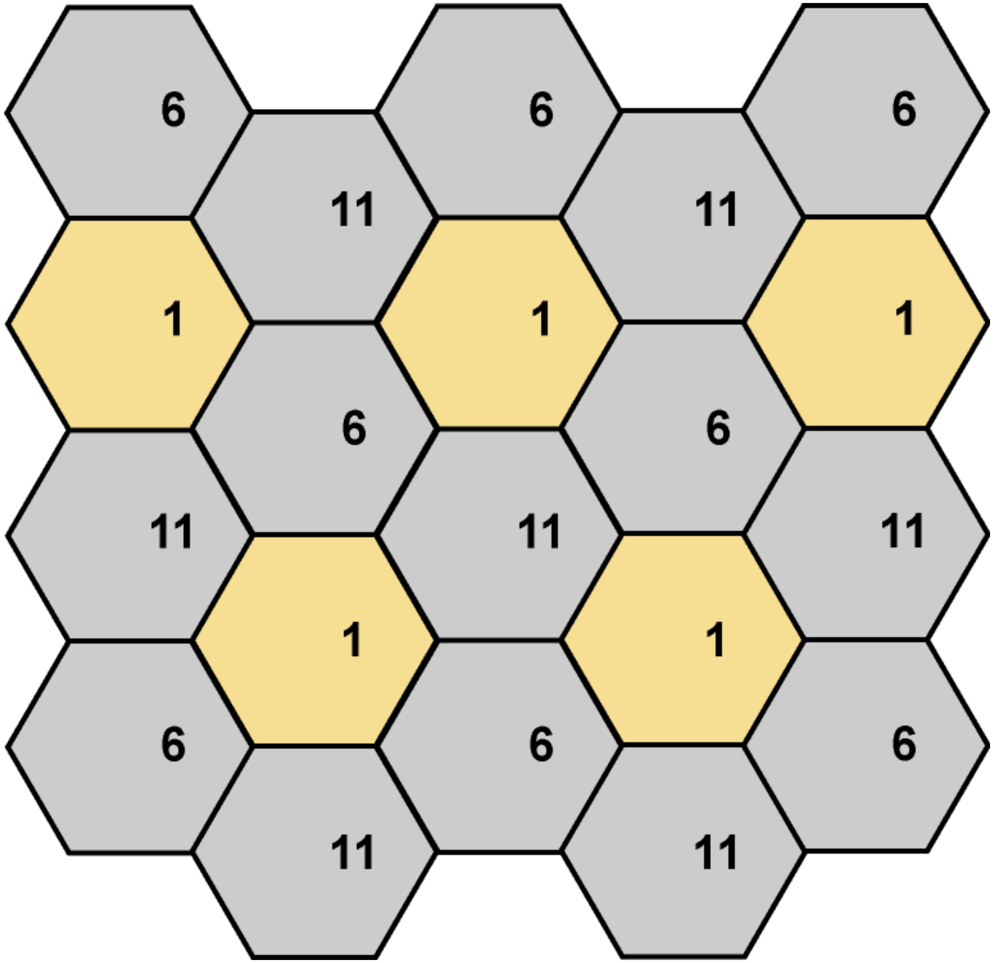
Channel Identifier	Channel Center Frequency	Channel Frequency Range [MHz]	Regulatory Domain		
			Americas	Europe, Middle East, and Asia	Japan
1	2412 MHz	2401 – 2423	X	X	X
2	2417 MHz	2406 – 2428	X	X	X
3	2422 MHz	2411 – 2433	X	X	X
4	2427 MHz	2416 – 2438	X	X	X
5	2432 MHz	2421 – 2443	X	X	X
6	2437 MHz	2426 – 2448	X	X	X
7	2442 MHz	2431 – 2453	X	X	X
8	2447 MHz	2436 – 2458	X	X	X
9	2452 MHz	2441 – 2463	X	X	X
10	2457 MHz	2446 – 2468	X	X	X
11	2462 MHz	2451 – 2473	X	X	X
12	2467 MHz	2466 – 2478		X	X
13	2472 MHz	2471 – 2483		X	X
14	2484 MHz	2473 – 2495			X

2.4-GHz Channel Use

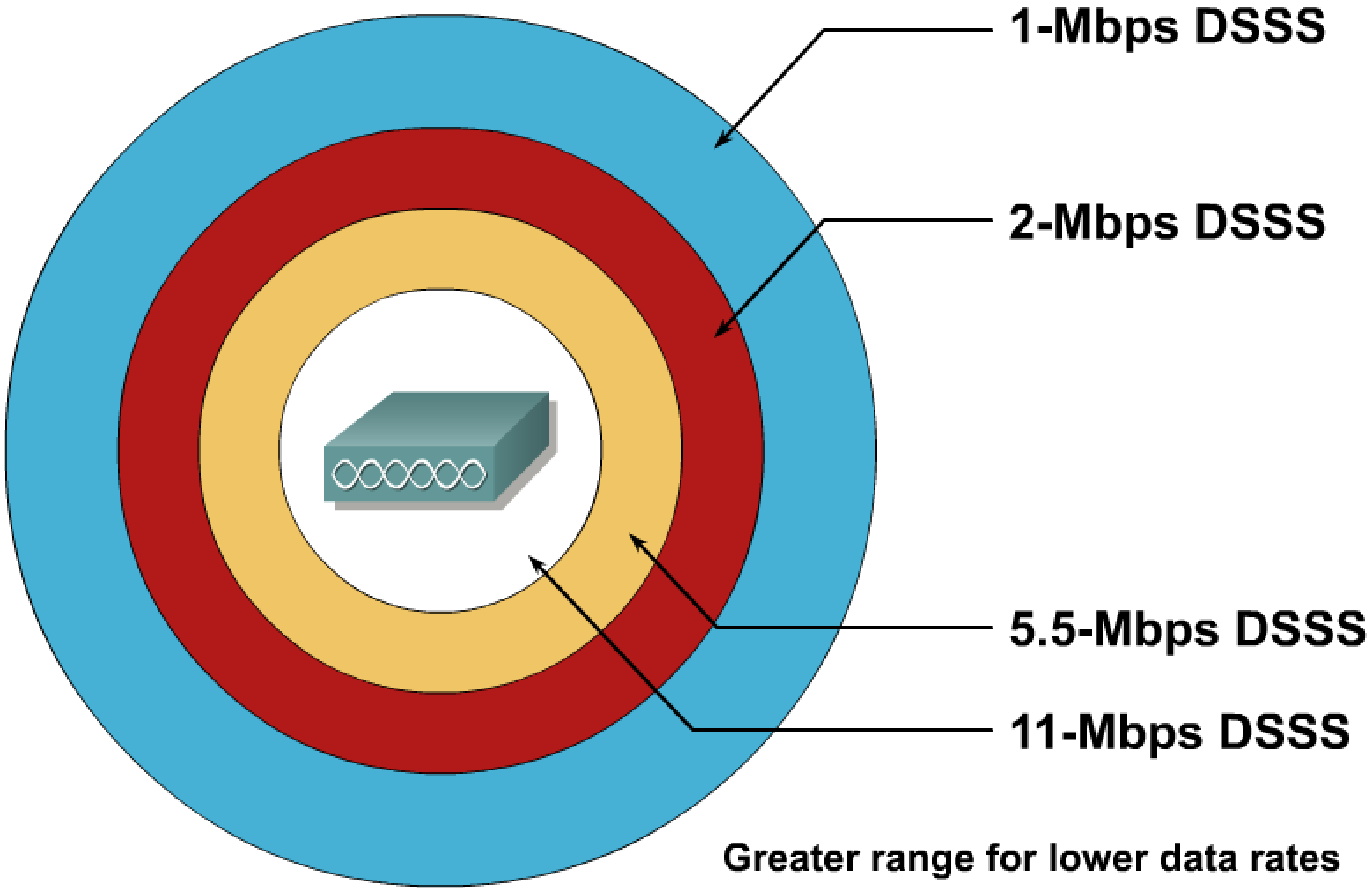


- Each channel is 22 MHz wide.
- North America: 11 channels
- Europe: 13 channels
- There are three nonoverlapping channels: 1, 6, 11.
- Using any other channels will cause interference.
- Three access points can occupy the same area.

802.11b/g (2.4 GHz) Channel Reuse



802.11b Access Point Coverage



1-Mbps DSSS

2-Mbps DSSS

5.5-Mbps DSSS

11-Mbps DSSS

Greater range for lower data rates

802.11a Standard

Standard was ratified September 1999

Operates in the 5-GHz band

Uses orthogonal frequency-division multiplexing (OFDM)

Uses eight data rates of up to 54 Mbps

- 6, 9, 12, 18, 24, 36, 48, 54 Mbps

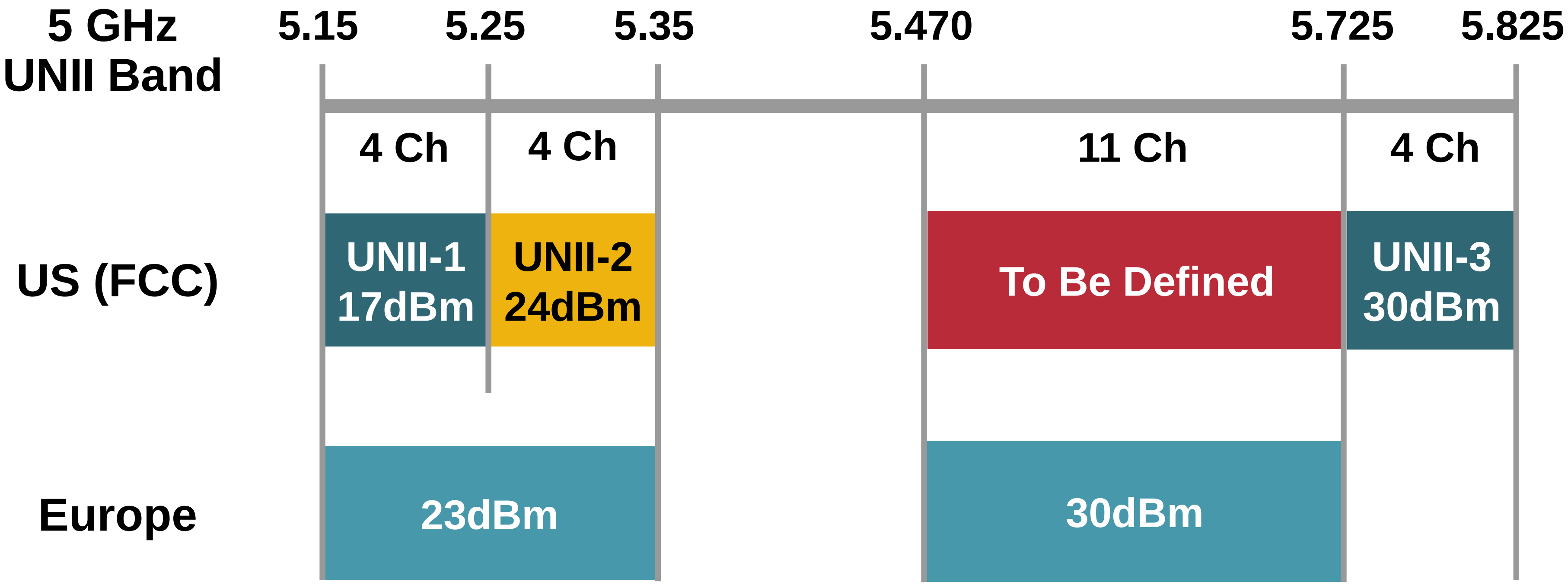
Has from 12 to 23 nonoverlapping channels (FCC)

Has up to 19 nonoverlapping channels (ETSI)

Regulations different across countries

- Transmit (Tx) power control and dynamic frequency selection required (802.11h)

Understanding the 5 GHz Spectrum



UNII-1: Indoor Use, Antenna Must Be Fixed to the Radio
UNII-2: Indoor/Outdoor Use, Fixed or Remote Antenna
(Must Implement 802.11h After Jul 19, 2007)
UNII-3: Indoor/Outdoor; Fixed, Pt-to-Pt Can Employ Higher Gain Antenna
Europe: Must Implement 802.11h

IEEE 802.11h
Spectrum Management

Primary use of 5 GHz bands outdoors is radar in many countries.

802.11h is an addition to the 802.11 family of standards.

802.11h rules are designed to minimize interference.

Uses Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).

Radios must comply to benefit from 11 new channels.

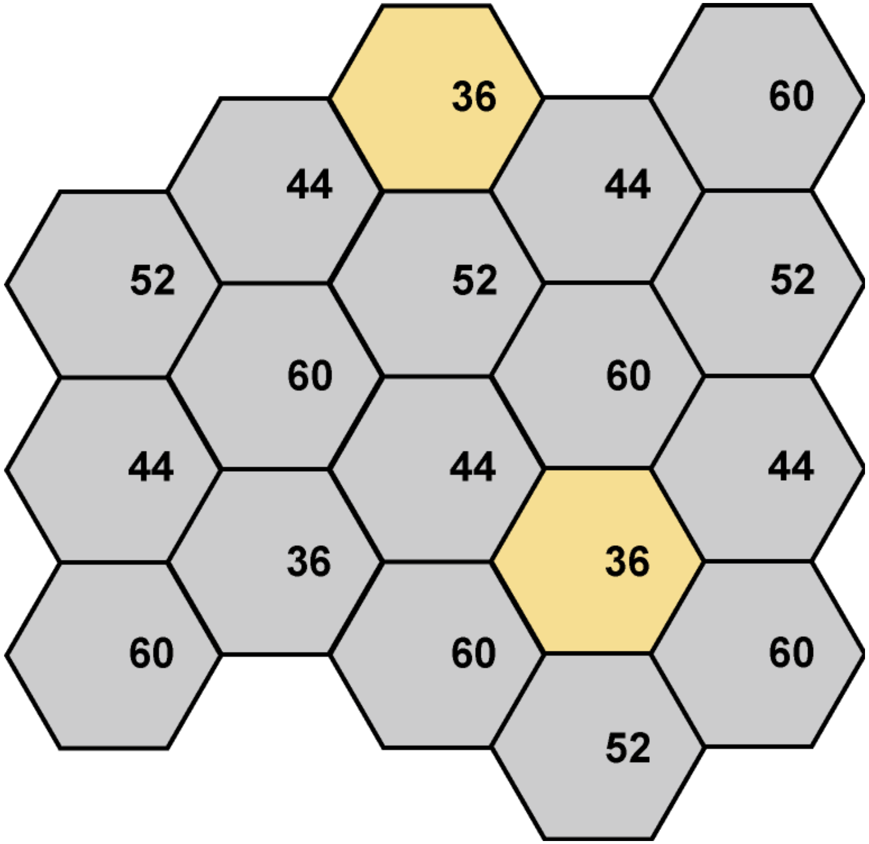
802.11a Channel Reuse

802.11h DFS not available

- Manual channel assignment required

802.11h DFS implemented

- Channel assignment done by Dynamic Frequency Selection (DFS)
- Only frequency bands can be selected



802.11g Standard

Standard was ratified June 2003

Operates in the 2.4-GHz band as 802.11b

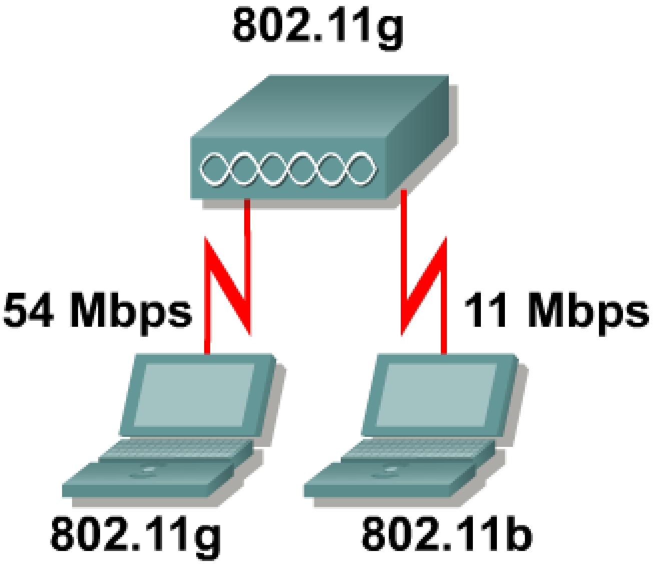
- Same three nonoverlapping channels: 1, 6, 11

DSSS (CCK) and OFDM transmission

12 data rates of up to 54 Mbps

- 1, 2, 5.5, 11 Mbps (DSSS / 802.11b)
- 6, 9, 12, 18, 24, 36, 48, 54 Mbps (OFDM)

Full backward compatiblity to 802.11b standard



802.11g Protection Mechanism

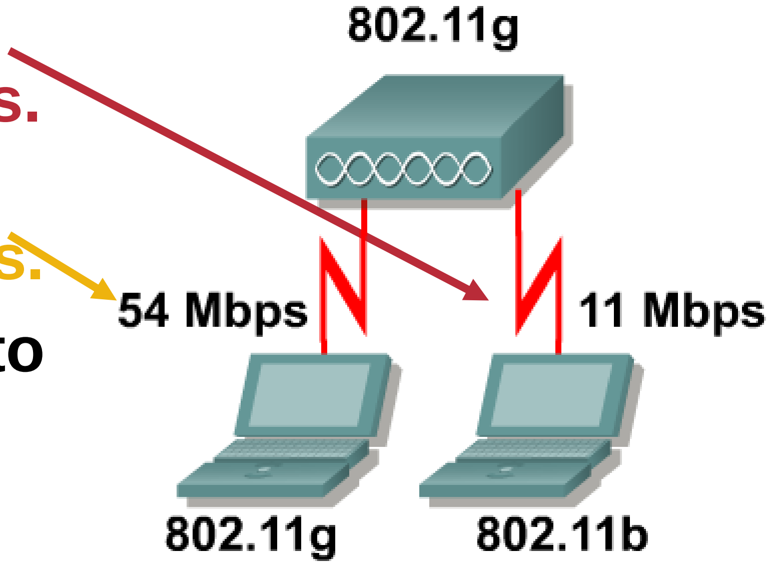
Problem: 802.11b stations cannot decode 802.11g radio signals.

802.11b/g AP communicates with 802.11b clients with max. 11 Mbps.

802.11b/g AP communicates with 802.11g clients with max. 54 Mbps.

802.11b/g AP activates RTS/CTS to avoid collisions when 802.11b clients are present.

Additonal overhead reduces throughput.



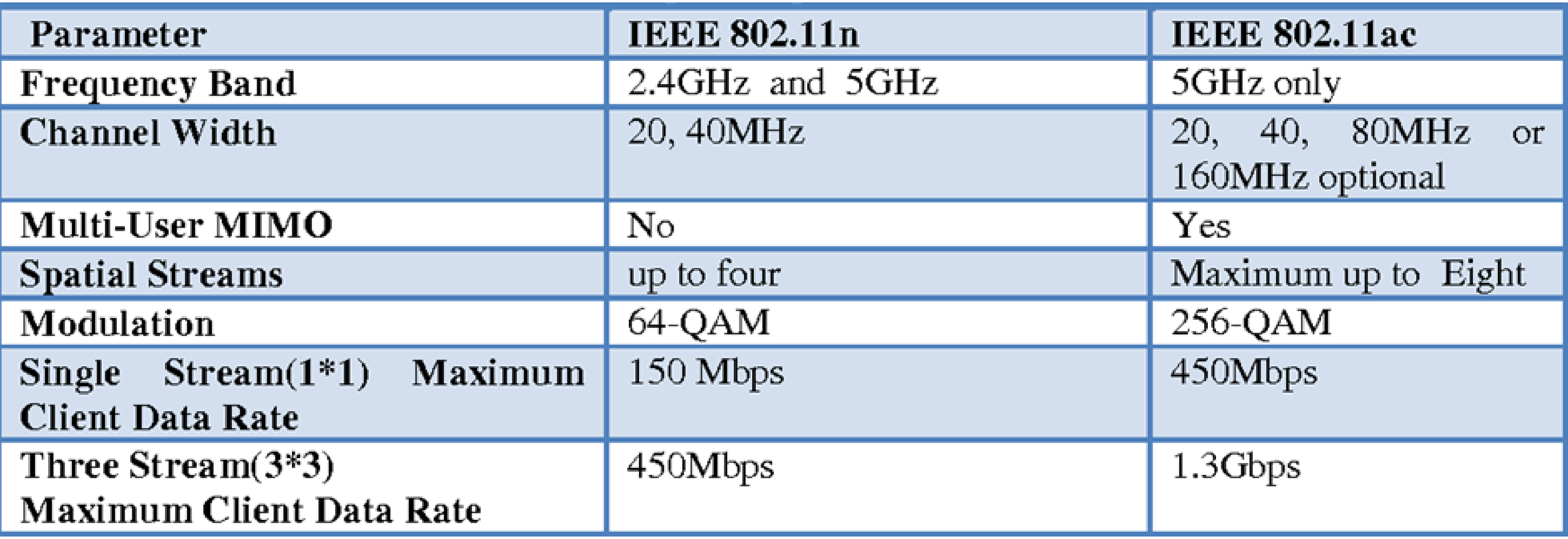
802.11 RF Comparison

	802.11b – 2.4 GHz	802.11g – 2.4 GHz	802.11a – 5 GHz
Pro	▪ Most commonly deployed WLAN standard	▪ Higher throughput ▪ OFDM technology reduces multipath issues	▪ Highest throughput ▪ OFDM technology reduces multipath issues ▪ Provides up to 23 nonoverlapping channels
Con	▪ Interference and noise from other services in the 2.4-GHz band ▪ Only 3 nonoverlapping channels ▪ Distance limited by multipath issues	▪ Interference and noise from other services in the 2.4GHz band ▪ Only 3 nonoverlapping channels ▪ Throughput degraded in the presence of 802.11b clients	▪ Lower market penetration

Comparison between 802.11b, 802.11g & 802.11a

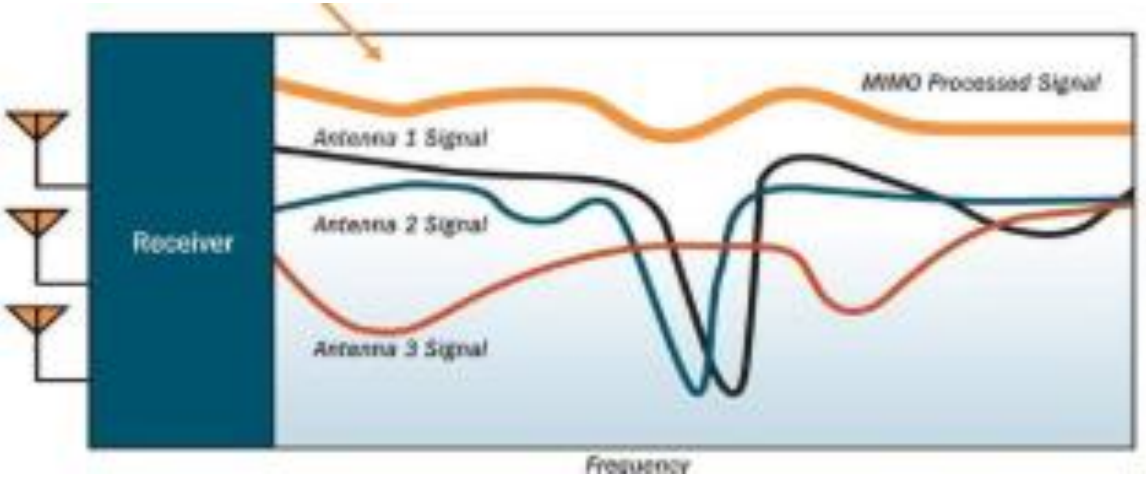
	802.11b	802.11g		802.11a
Ratified	1999	2003		1999
Frequency band	2.4 GHz	2.4 GHz		5 GHz
No of non-overlapping channels	3	3		Up to 23
Transmission	DSSS	DSSS	OFDM	OFDM
Data rates [Mbps]	1, 2, 5.5, 11	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
Throughput [Mbps]	Up to 6	Up to 22		Up to 28

Comparison between 802.11n & 802.11ac



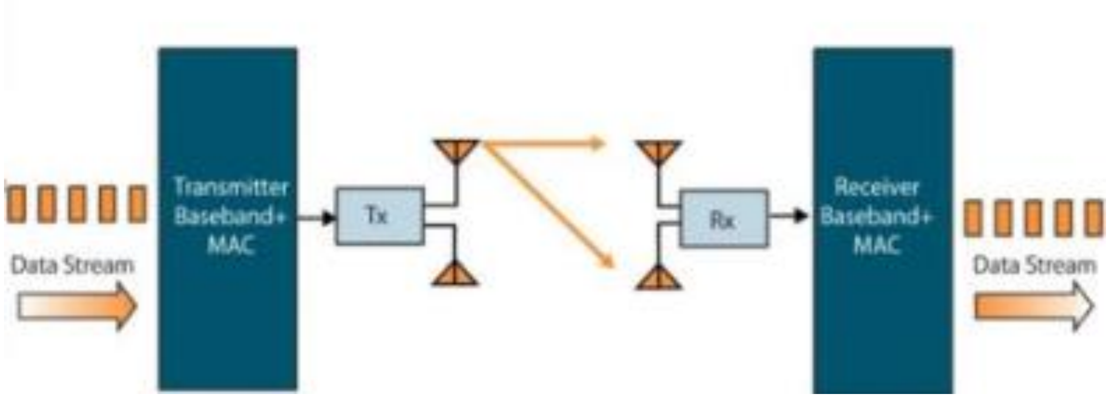
Parameter	IEEE 802.11n	IEEE 802.11ac
Frequency Band	2.4GHz and 5GHz	5GHz only
Channel Width	20, 40MHz	20, 40, 80MHz or 160MHz optional
Multi-User MIMO	No	Yes
Spatial Streams	up to four	Maximum up to Eight
Modulation	64-QAM	256-QAM
Single Stream(1*1) Maximum Client Data Rate	150 Mbps	450Mbps
Three Stream(3*3) Maximum Client Data Rate	450Mbps	1.3Gbps

802.11n MIMO

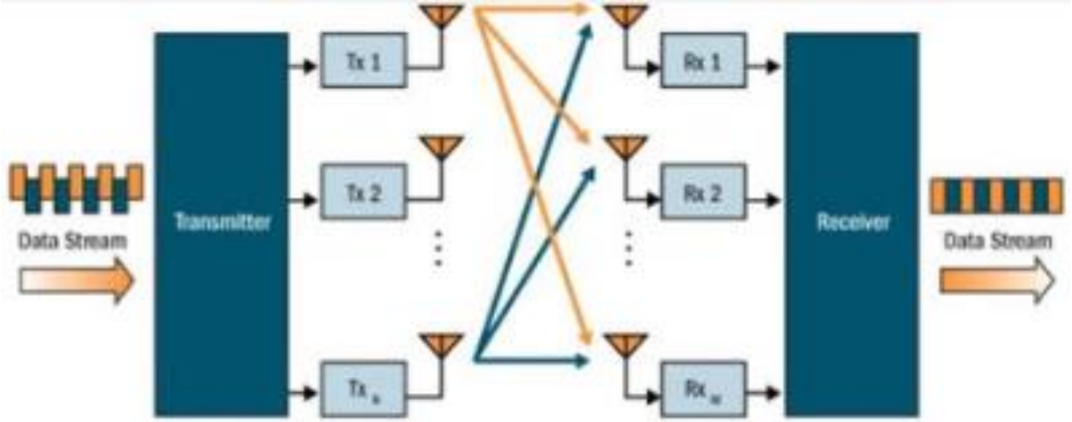


With MIMO all three signals are received and processed up the stack.
This significantly improves the receiver’s “ability to hear”

Spatial Multiplexing

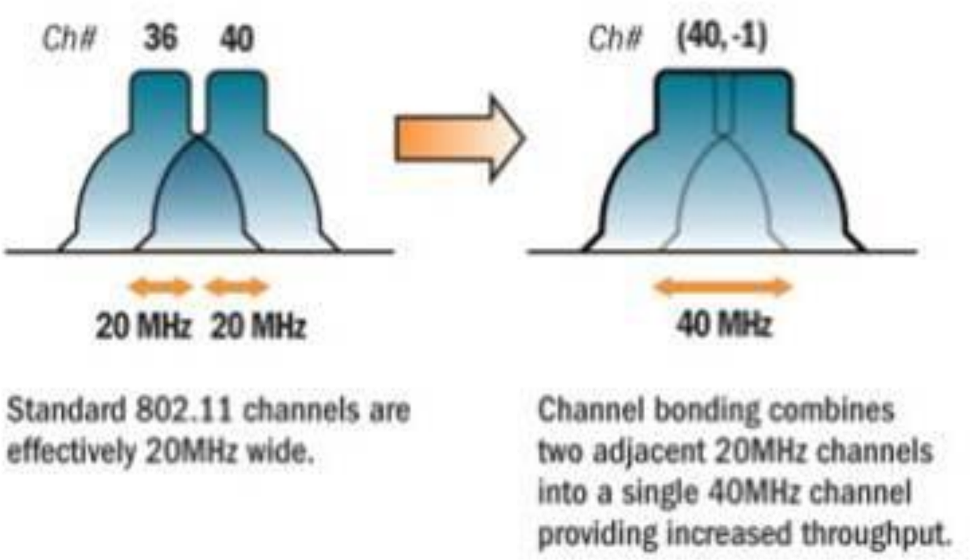


802.11 Classic Transmitter



Spatial Multiplexing - Two Streams

Channel Bonding

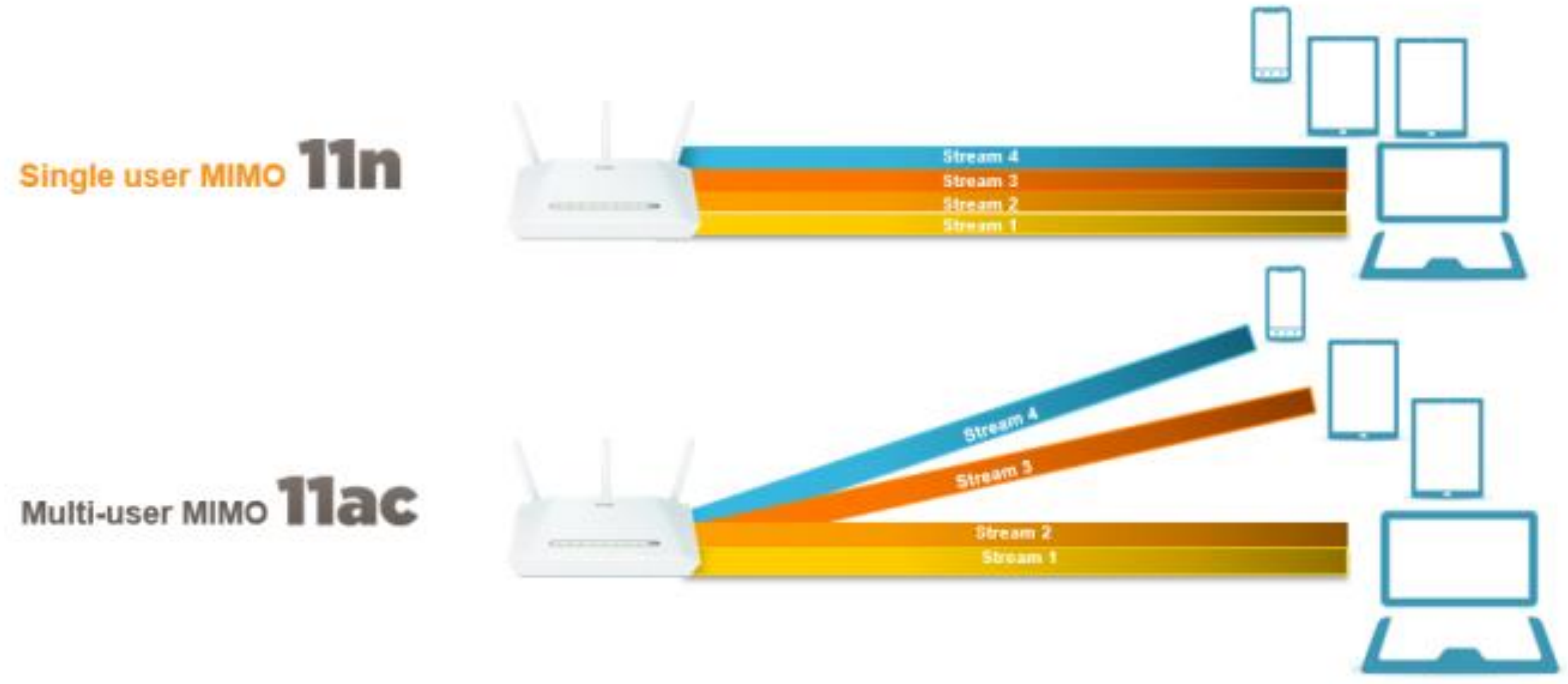


Standard 802.11 channels are effectively 20MHz wide.

Channel bonding combines two adjacent 20MHz channels into a single 40MHz channel providing increased throughput.

Channel bonding combines two adjacent channels, which effectively doubles the amount of available bandwidth.

SU-MIMO vs MU-MIMO



Ratified IEEE 802.11 Standards

802.11: WLAN 1 and 2 Mbps at 2.4 GHz

802.11a: WLAN 54-Mbps at 5 GHz

802.11b: WLAN 11-Mbps at 2.4 GHz

802.11d: Multiple regulatory domains

802.11e: Quality of Service

802.11f: Inter-Access Point Protocol (IAPP)

802.11g: WLAN 54-Mbps at 2.4 GHz

802.11h: Dynamic Frequency Selection (DFS)
Transmit Power Control (TPC) at 5 GHz

802.11i: Security

802.11j: 5-GHz channels for Japan

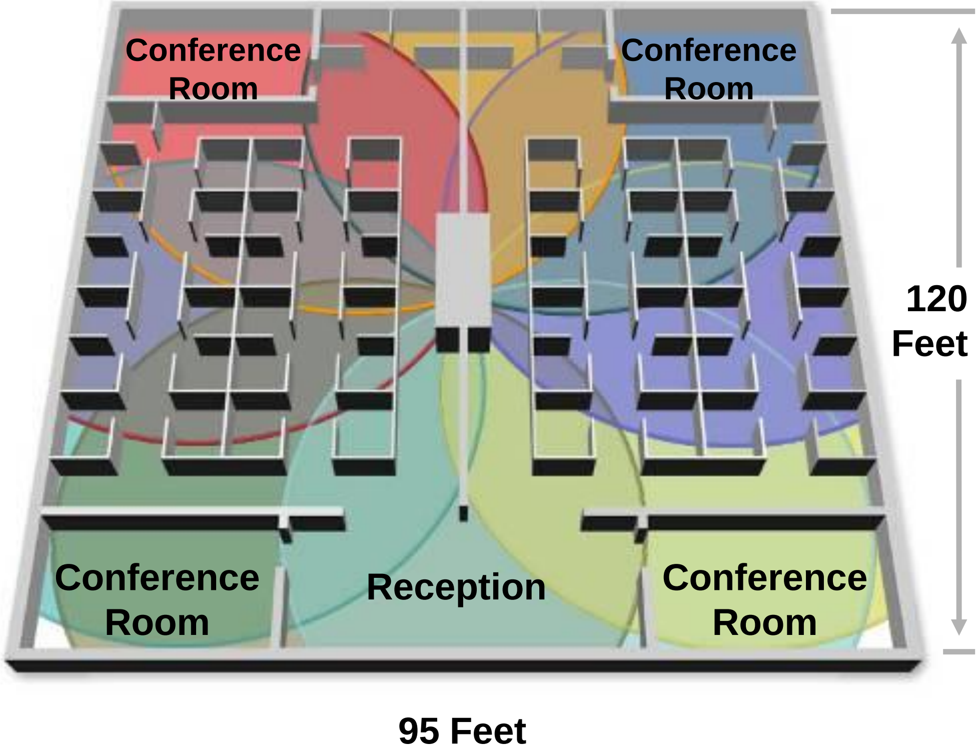
General Office Wireless LAN Design

Eight 802.11g access points deployed

7 users per access points with no conference rooms provides 3.8 Mbps throughput per user

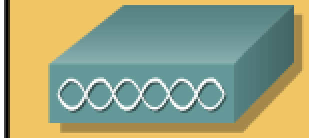
7 users + 1 conference room (10 users) = 17 total users, provides 1.5 Mbps throughput per user

54 Cubes—4 Conference Rooms



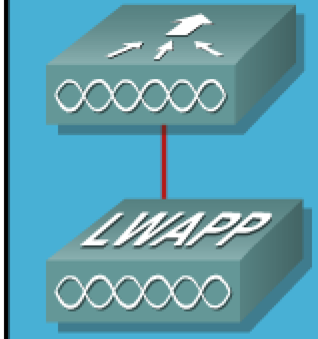
Cisco WLAN Implementation

Cisco offers 2 “flavors” of wireless solutions:



Distributed WLAN solution

- Autonomous AP



Centralized WLAN solution

- Lightweight AP
- Wireless LAN Controller (WLC)

Distributed WLAN Solution Components

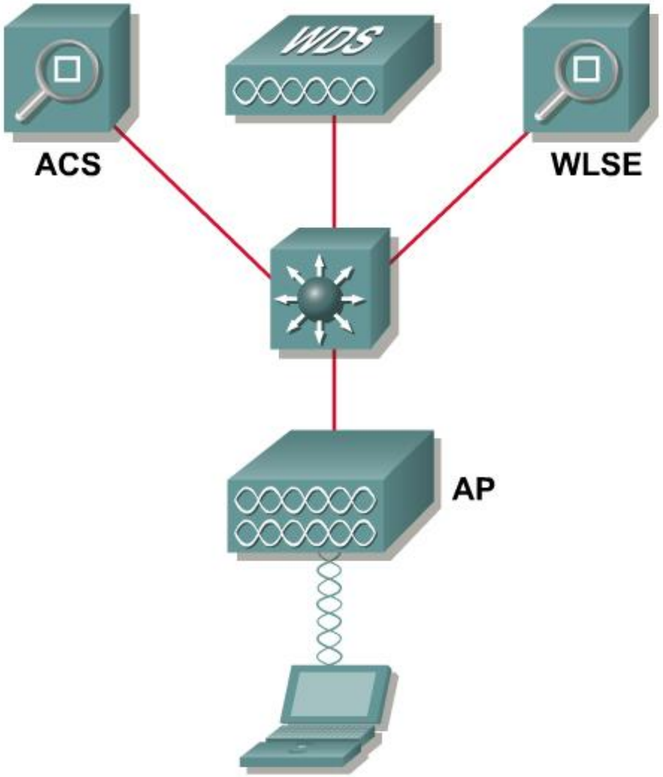
Autonomous access points

Network Infrastructure

Wireless Domain Services (WDS) – optional

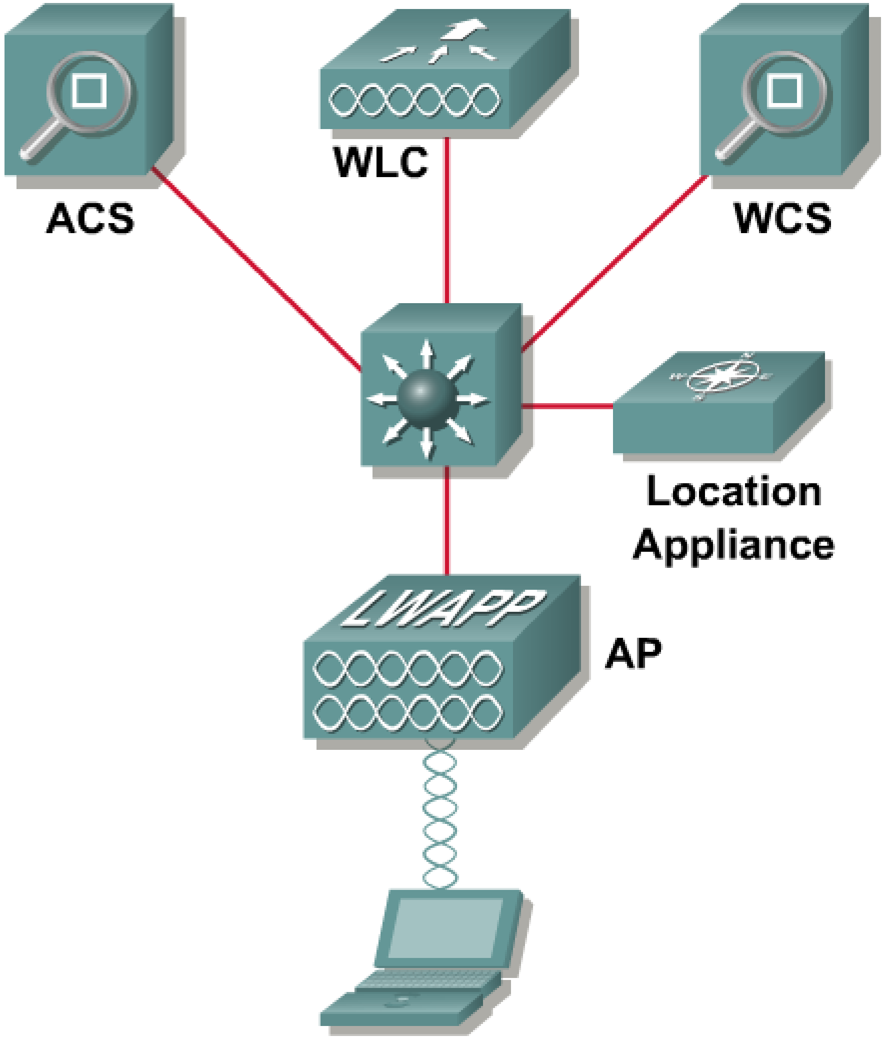
Wireless LAN Solution Engine (WLSE) – optional

Acess Control Server (ACS) – optional

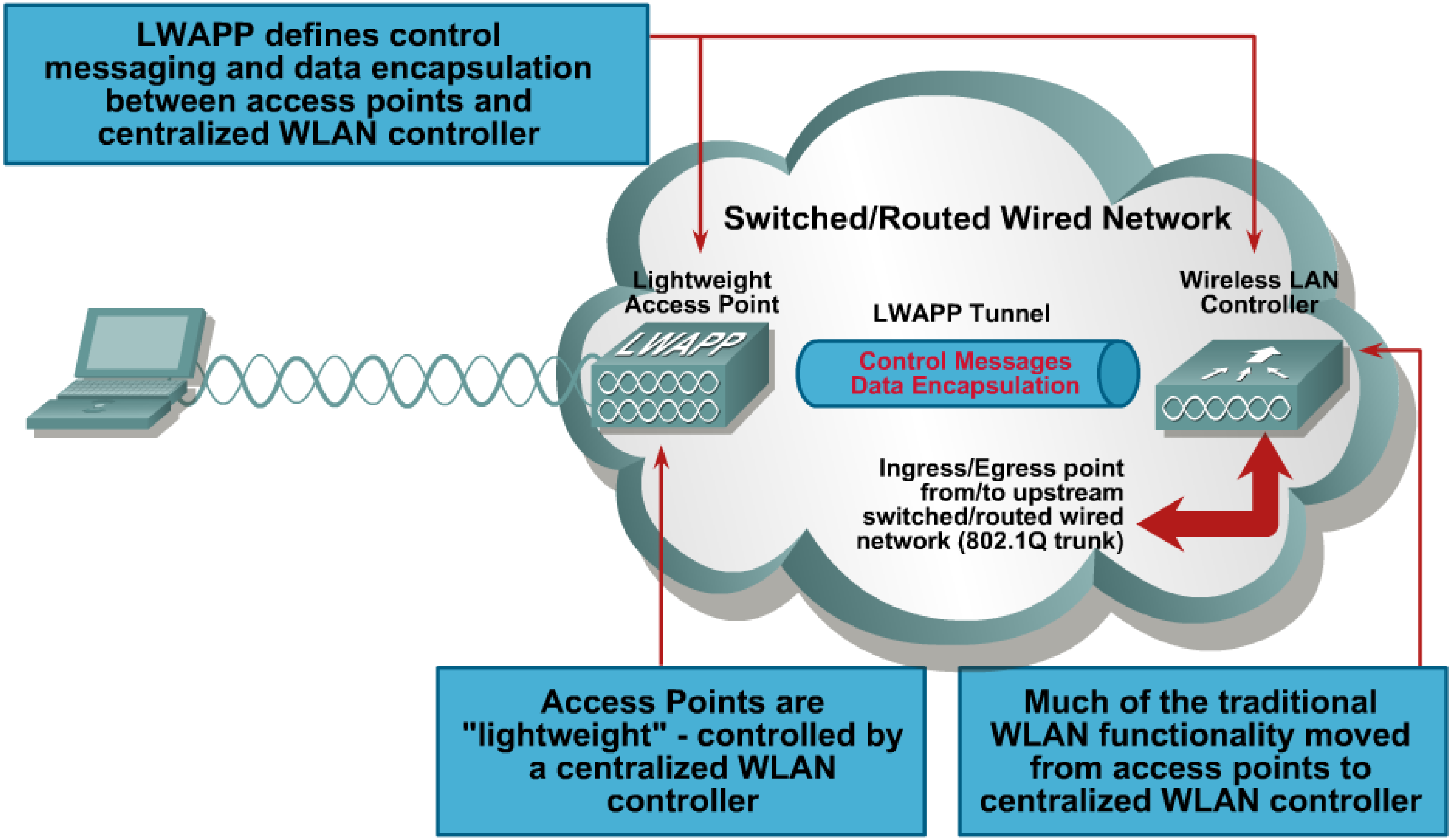


Centralized WLAN Solution Components

- Lightweight access points
- Network Infrastructure
- Wireless LAN controller (WLC) – required
- Wireless Control System (WCS) – optional
- Location appliance – optional
- Acess Control Server (ACS) – optional



Cisco Centralized WLAN Model


Switched/Routed Wired Network
Lightweight Access Point
LWAPP
LWAPP Tunnel
Control Messages
Data Encapsulation
Wireless LAN Controller
Ingress/Egress point from/to upstream switched/routed wired network (802.1Q trunk)

LWAPP defines control messaging and data encapsulation between access points and centralized WLAN controller

Access Points are "lightweight" - controlled by a centralized WLAN controller

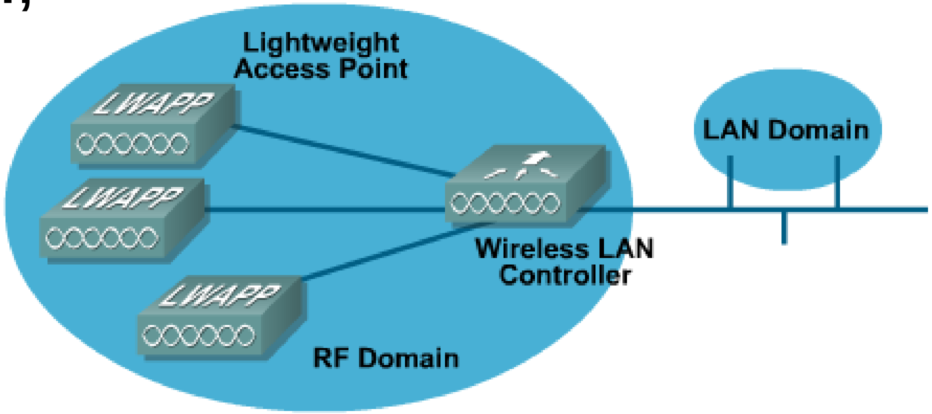
Much of the traditional WLAN functionality moved from access points to centralized WLAN controller

Why Lightweight APs?

A WLAN controller system is used to create and enforce policies across many different lightweight access points.

With centralized intelligence, functions essential to WLAN operations such as security, mobility, and quality of service (QoS), can be efficiently managed across an entire wireless enterprise.

- Splitting functions between the access point and the controller, simplifies management, improves performance, and increases security of large WLANs



Wireless LAN Solution Comparison

Distributed Solution	Wireless clients	Centralized Solution
Autonomous access points	Access points	Lightweight access points
Wireless Domain Services (WDS)	Control	WLAN controller
WLAN Solution Engine (WLSE)	WLAN management	WLAN Control System (WCS)
PoE switches, routers	Network infrastructure	PoE switches, routers
DHCP, DNS, AAA	Network services	DHCP, DNS, AAA

WLAN Security

Why WLAN Security?

Wide availability and low cost of IEEE 802.11 wireless equipment

802.11 standard ease of use and deployment

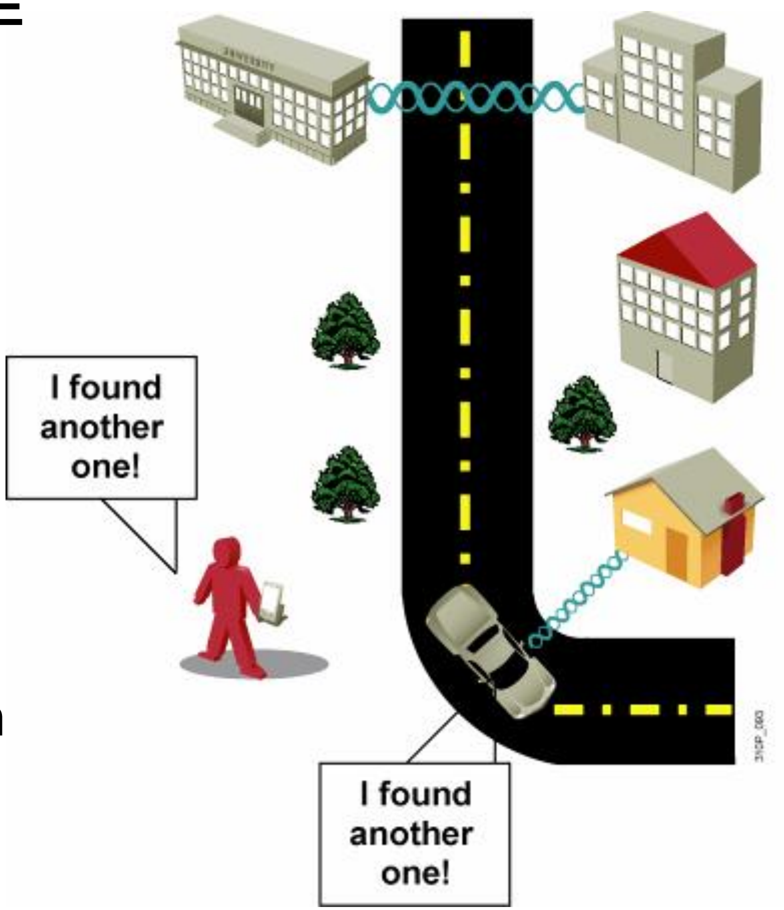
Availability of sniffers

Statistics on WLAN security

Media hype about
hot spots, WLAN hacking,
war driving

Nonoptimal implementation of encryption in standard Wired Equivalent Privacy (WEP) encryption

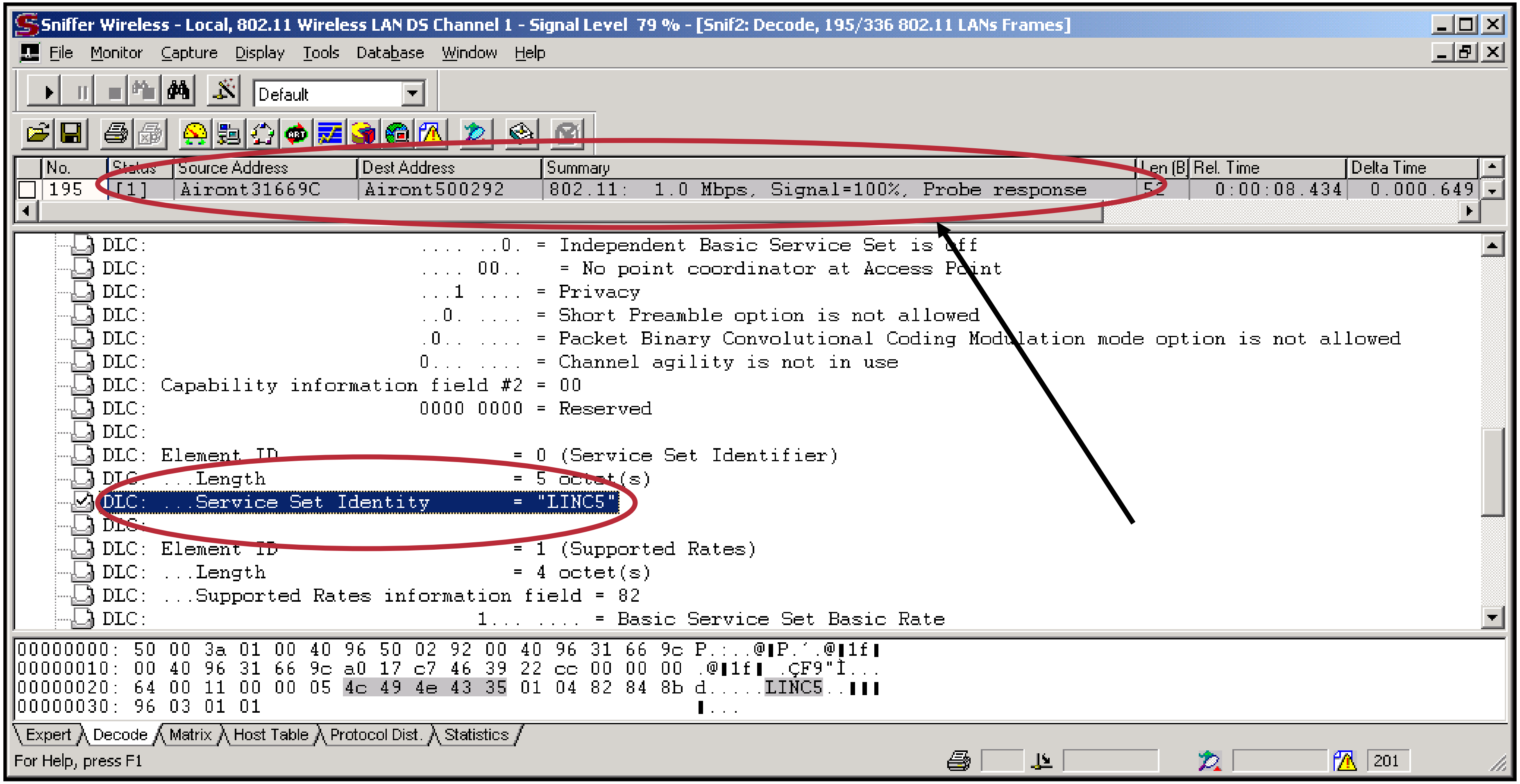
Authentication vulnerability



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.*	

WLAN Sniffing and SSID Broadcasting



Sniffer Wireless - Local, 802.11 Wireless LAN DS Channel 1 - Signal Level 79 % - [Snif2: Decode, 195/336 802.11 LANs Frames]

```
No.  Status Source Address  Dest Address     Summary                                               Len (B| Rel. Time     Delta Time
195  [1]    Airont31669C     Airont500292     802.11:   1.0 Mbps, Signal=100%, Probe response       52     0:00:08.434   0.000.649
```

```
DLC:                            .... ..0. = Independent Basic Service Set is off
DLC:                            .... 00..   = No point coordinator at Access Point
DLC:                            ...1 .... = Privacy
DLC:                            ..0. .... = Short Preamble option is not allowed
DLC:                            .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                            0... .... = Channel agility is not in use
DLC:  Capability information field #2 = 00
DLC:                            0000 0000 = Reserved
DLC:
DLC:  Element ID                      = 0 (Service Set Identifier)
DLC:  ...Length                       = 5 octet(s)
DLC:  ...Service Set Identity         = "LINC5"
DLC:
DLC:  Element ID                      = 1 (Supported Rates)
DLC:  ...Length                       = 4 octet(s)
DLC:  ...Supported Rates information field = 82
DLC:                                1... .... = Basic Service Set Basic Rate
```

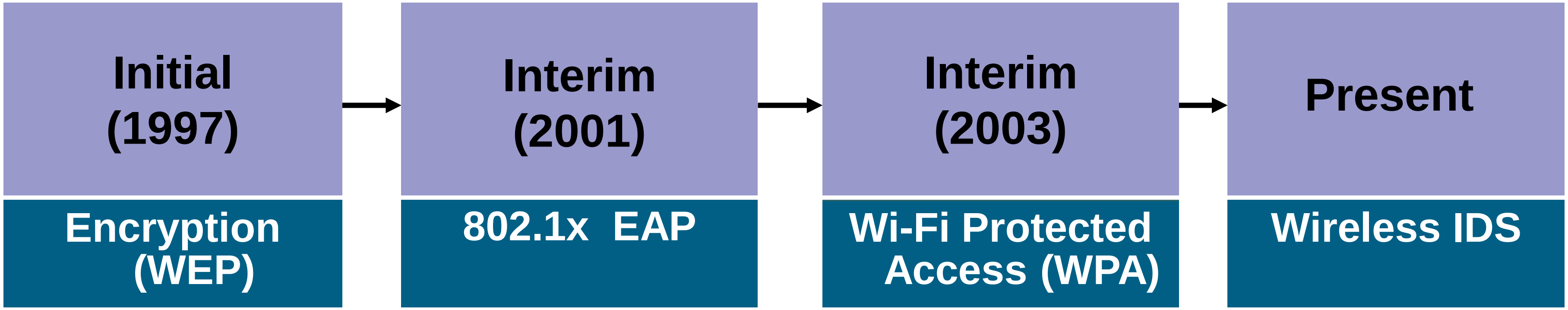
```
00000000: 50 00 3a 01 00 40 96 50 02 92 00 40 96 31 66 9c P.:..@▌P.´.@▌1f▌
00000010: 00 40 96 31 66 9c a0 17 c7 46 39 22 cc 00 00 00 .@▌1f▌ .ÇF9"Ì...
00000020: 64 00 11 00 00 05 4c 49 4e 43 35 01 04 82 84 8b d.....LINC5..▌▌▌
00000030: 96 03 01 01                                     ▌...
```

For Help, press F1

Mitigating the Threats

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

Evolution of Wireless LAN Security



Initial (1997)

Encryption (WEP)

- No strong authentication
- Static, breakable keys
- Not scalable

Interim (2001)

802.1x EAP

- Dynamic keys
- Improved encryption
- User authentication
- 802.1x EAP (LEAP, PEAP)
- RADIUS

Interim (2003)

Wi-Fi Protected Access (WPA)

- Standardized
- Improved encryption
- Strong, user authentication (e.g., LEAP, PEAP, EAP-FAST)

Present

Wireless IDS

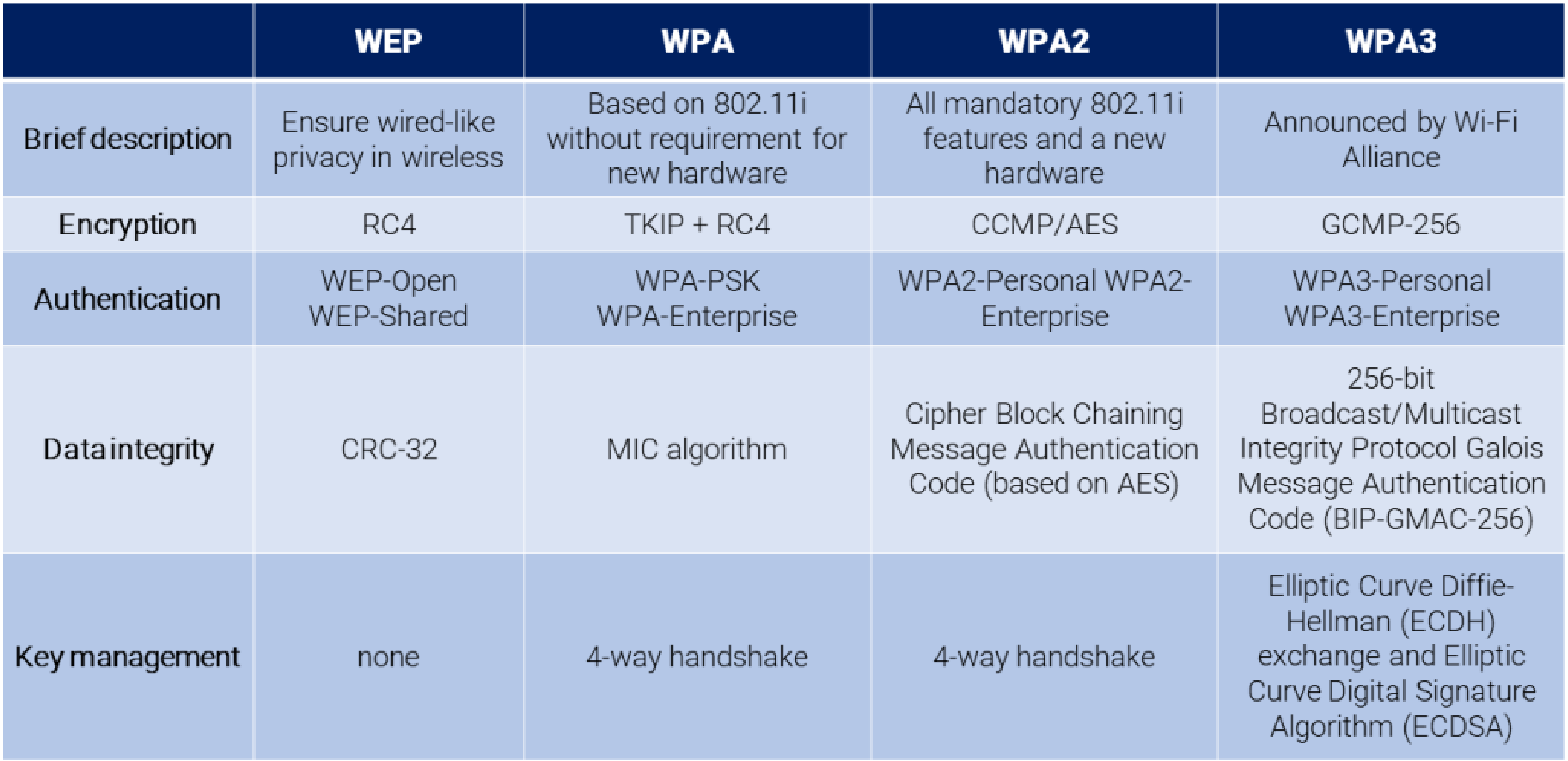
- Identification and protection against attacks, DoS

IEEE 802.11i

WPA2 (2004)

- AES strong encryption
- Authentication
- Dynamic key management

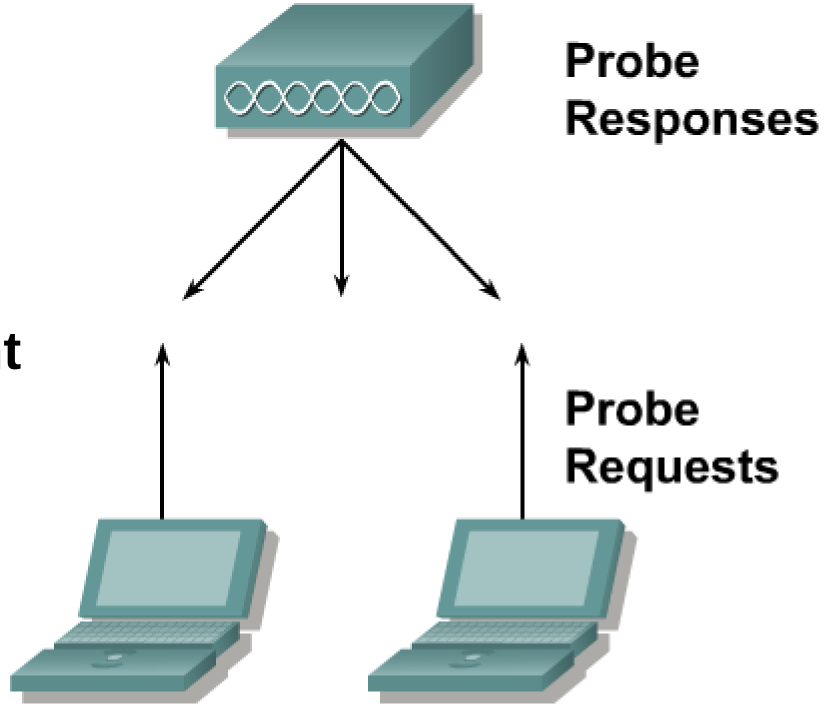
WLAN Security Summary



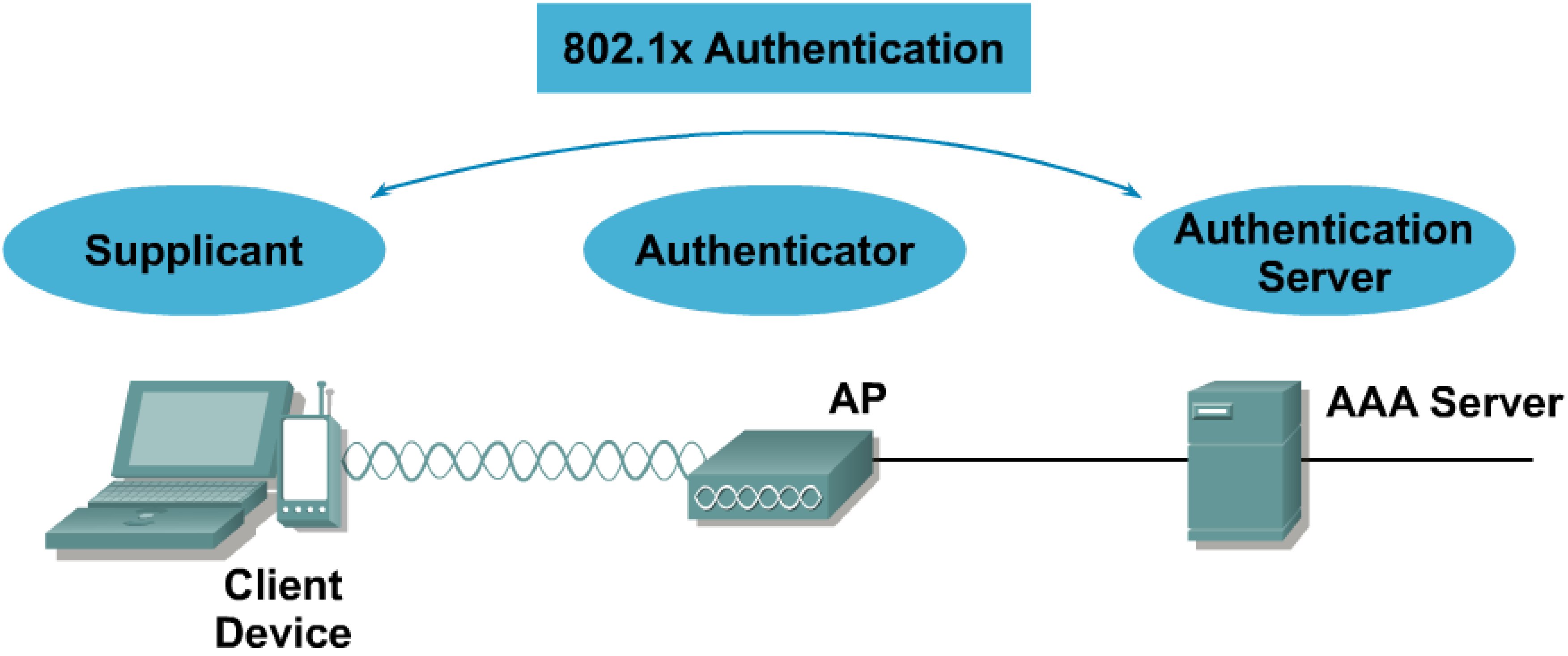
	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Wireless Client Association

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



WPA and WPA2 Authentication



802.1x Authentication

Supplicant

Authenticator

Authentication Server

AP

AAA Server

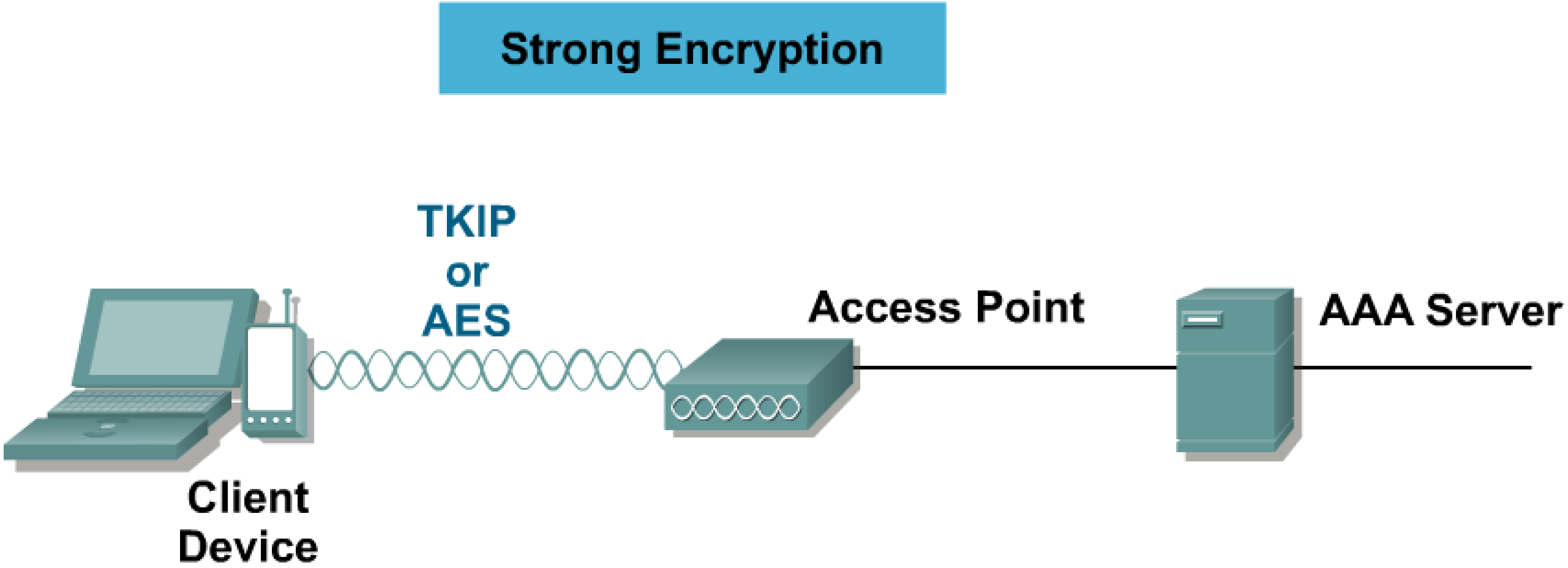
Client Device

Supplicant for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.

802.1x Support

Server Support for 802.1x Type: LEAP, PEAP, EAP-FAST, etc.

WPA and WPA2 Encryption



Wi-Fi Protected Access

What are WPA and WPA2?

- Authentication and encryption standards for Wi-Fi clients and APs
- 802.1x authentication
- WPA uses TKIP encryption
- WPA2 uses AES block cipher encryption

Which should I use?

- Gold, for supporting NIC/OSs
- Silver, if you have legacy clients
- Lead, if you absolutely have no other choice.

Gold

WPA2/802.11i

- EAP-Fast
- AES

Silver

WPA

- EAP-Fast
- TKIP

Lead

Dynamic WEP

- EAP-Fast/LEAP
- VLANs + ACLs

WLAN Security Summary

Open Access

No Encryption, Basic Authentication

Public “Hotspots”

Basic Security

40-bit or 128-bit Static WEP Encryption, WPA

Home Use

Enhanced Security

802.1x, TKIP Encryption, Mutual Authentication, Scalable Key Mgmt., Etc.

Enterprise

Remote Access

Virtual Private Network (VPN)

Business Traveler, Telecommuter

CISCO