802.11 LAN inalámbricas: una visión general de tecnología

RAUL BAREÑO GUTIERREZ

Cisco | Networking Academy®
Mind Wide Open™

OBJECTIVES

Describe IEEE 802.11 wireless LAN (WLAN) and related network standards and specifications

Describe the components and network architectures used in WLANs

Identify the characteristics of RF technology

Describe radio signaling and the operation of equipment used in a WLAN

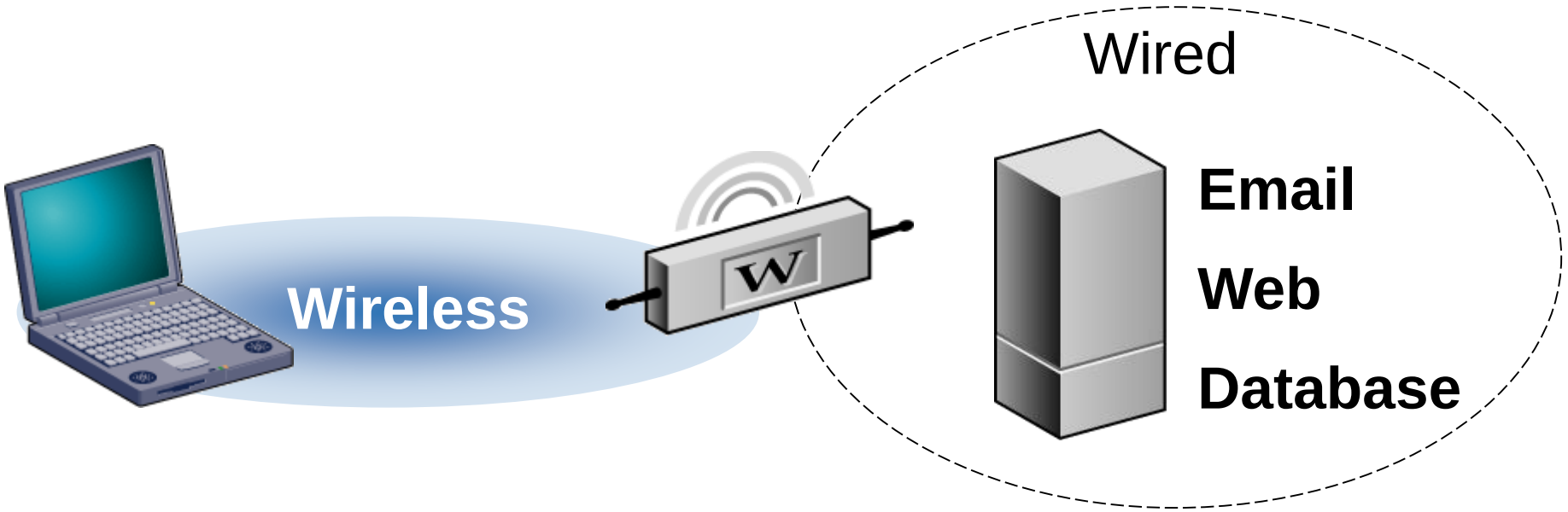
Identify common security threats and countermeasures for WLANs including authentication and encryption methods and protocols

Explain the use of Virtual Local Area Networks (VLANs) to enhance security within an enterprise WLAN implementation

Design a basic WLAN

Identify the key steps of a site survey to prove the viability of a WLAN design

WLAN INTRODUCTION



- Network access without wires
- Move around freely within wireless coverage areas

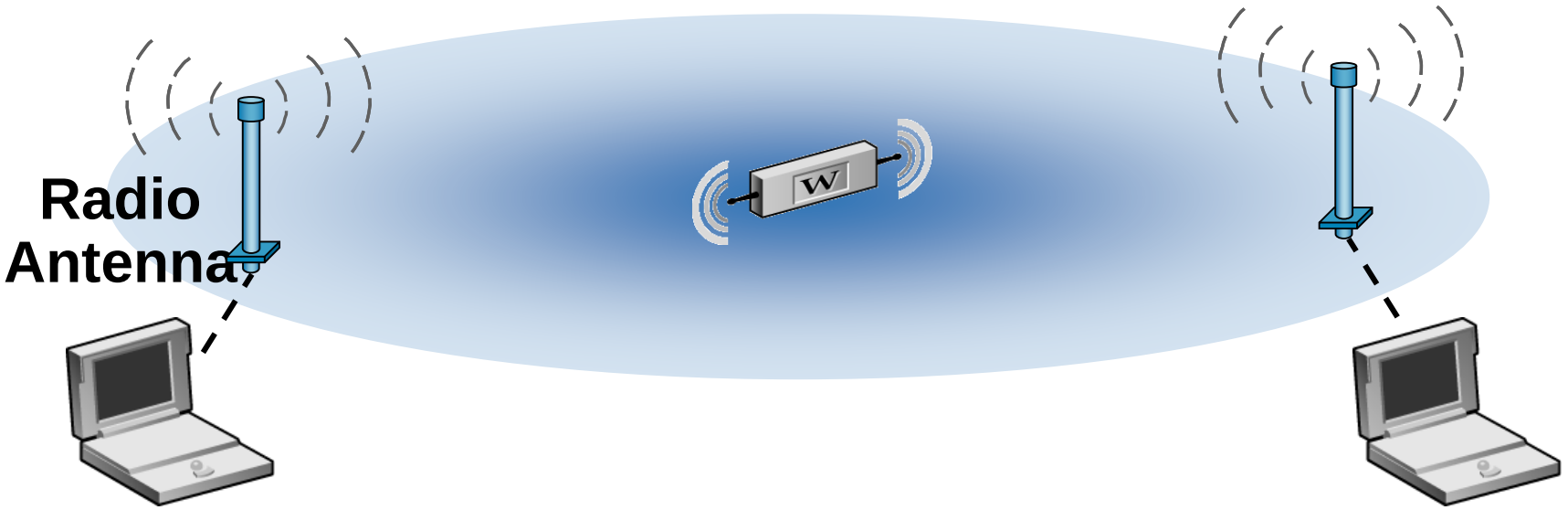
WLAN BENEFITS

- Increased user mobility
- Increased user productivity
- Network flexibility and portability
- Ease and speed of deployment
- Cost and/or time savings
- Improved aesthetics
- Shared resources
- Increased connectivity options
- Improved efficiency and reduced costs

WLAN OVERVIEW

- Defined by the IEEE 802.11 specifications
- Also known as Wi-Fi and/or “Hot Spots”

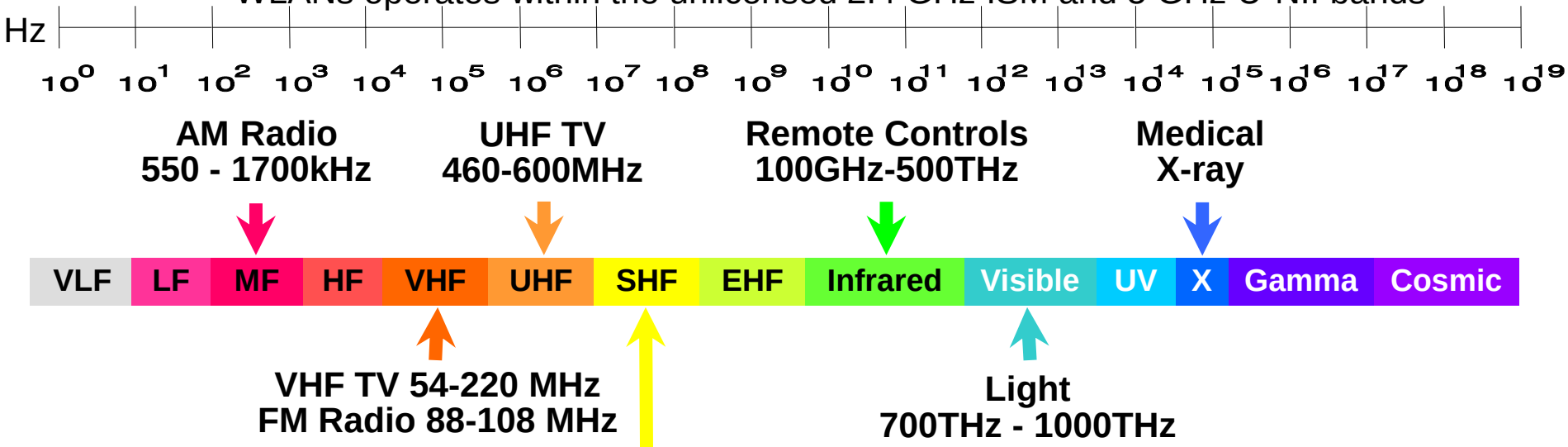
WLAN CONCEPTS



- Uses RF technology to transmit and receive data
- RF signals pass through most objects
- Not immune to signaling issues: Absorption, Reflection, Refraction, Diffraction, and Scattering

OVERALL SPECTRUM

- Regulated by individual countries
- WLANs operates within the unlicensed 2.4 GHz ISM and 5 GHz U-NII bands



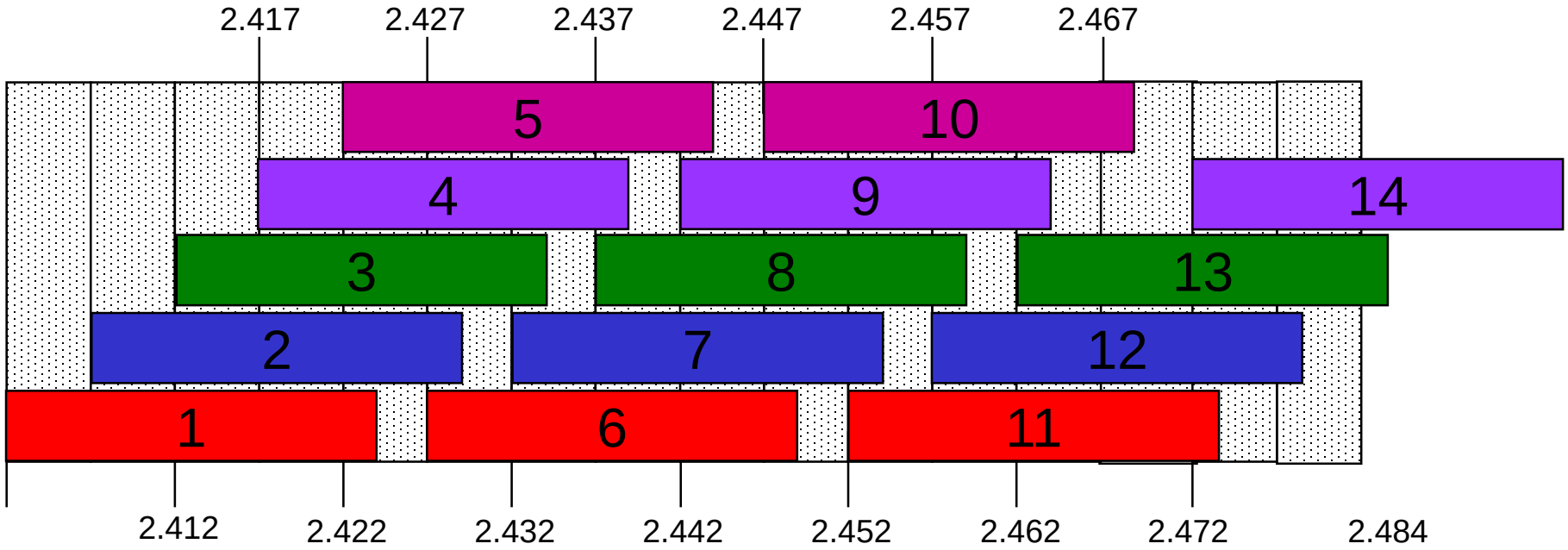
Super High Frequency:

800-900 MHz Cellular
900 MHz Indoor Wireless
1.8-2 GHz PCS
Unlicensed Bands { 2.4 GHz ISM, 5 GHz U-NII
1-18 GHz Terrestrial Microwave

CHANNELS IN THE 2.4 GHz BAND

Channel ID	Frequency (GHz)	US / Canada X'10' / X'20' (FCC / IC)	Europe X'30' (ETSI)	Spain X'31'	France X'32'	Japan X'40'	Japan X'41'
1	2.412	X	X				X
2	2.417	X	X				X
3	2.422	X	X				X
4	2.427	X	X				X
5	2.432	X	X				X
6	2.437	X	X				X
7	2.442	X	X				X
8	2.447	X	X				X
9	2.452	X	X				X
10	2.457	X	X	X	X		X
11	2.462	X	X	X	X		X
12	2.467		X		X		X
13	2.472		X		X		X
14	2.484					X	

2.4 GHz CHANNEL RANGES



SPREAD SPECTRUM

- FHSS systems use a radio carrier that “hops” from frequency to frequency in a pattern known to both transmitter and receiver
  - Easy to implement
  - Resistant to noise
  - Limited throughput (1-3 Mbps @ 2.4 GHz)
- DSSS & HR/DSSS systems convert data bits to a wide bit pattern called a “chip”
  - Updated definition, HR/DSSS provides higher throughput than FH (up to 11 Mbps @ 2.4 GHz)
  - Better range or coverage
  - Less resistant to noise (made up for by redundancy)

5 GHz BAND

> Regulatory classes for 5 GHz bands in the USA

Regulatory Class	Channel Starting Frequency (GHz)	Channel Spacing (MHz)	Channel Set	Transmit Power Limit (mW)	Emission Limits Set	Behavior Limits Set
1	5	20	36,40,44,48	40	1	1, 2
2	5	20	52,56,60,64	200	1	1
3	5	20	149,153,157,161	800	1	1
4-255	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

5 GHz BAND (continued)

> Regulatory classes for 5 GHz bands in Europe

Regulatory Class	Channel Starting Frequency (GHz)	Channel Spacing (MHz)	Channel Set	Transmit Power Limit (EIRP)	Emission Limits Set	Behavior Limits Set
1	5	20	36,40,44,48	200	1	2,3
2	5	20	52,56,60,64	200	1	1,3,4
3	5	20	100,104,108, 112,116,120, 124,128,132, 136,140	1 W	1	1,3,4
4-255	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

5 GHz BAND (continued)

> Regulatory classes for 4.9 and 5 GHz bands in Japan

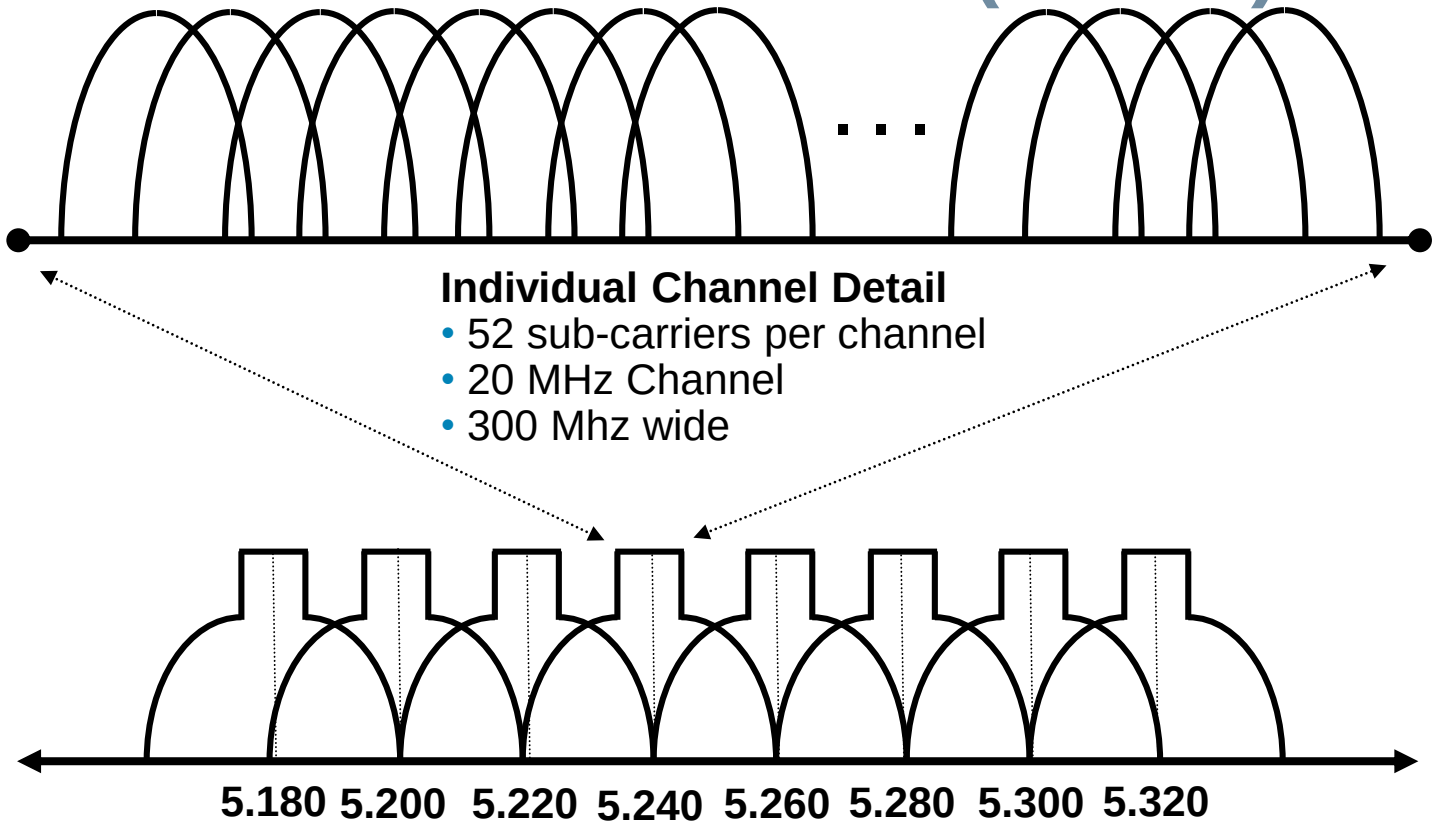
Regulatory Class	Channel Starting Frequency (GHz)	Channel Spacing (MHz)	Channel Set	Transmit Power Limit (dBm)	Emission Limits Set	Behavior Limits Set
1	5	20	34,38,42,46	22	1	1,2,6
2	5	20	8,12,16	24	2	5,6,7
3	5	20	8,12,16	24	2	5,6,8
4	5	20	8,12,16	24	3	5,6,7
5	5	20	8,12,16	24	3	5,6,8
6	5	20	8,12,16	22	1	5,6,8
7	4	20	184,188,192,196	24	2	5,6,7
8	4	20	184,188,192,196	24	2	5,6,8
9	4	20	184,188,192,196	24	3	5,6,7
10	4	20	184,188,192,196	24	3	5,6,8
11	5	20	34,38,42,46	22	1	5,6,8
12	5	10	7,8,9,11	24	2	5,6,7

5 GHz BAND (continued)

> Regulatory classes for 4.9 and 5 GHz bands in Japan

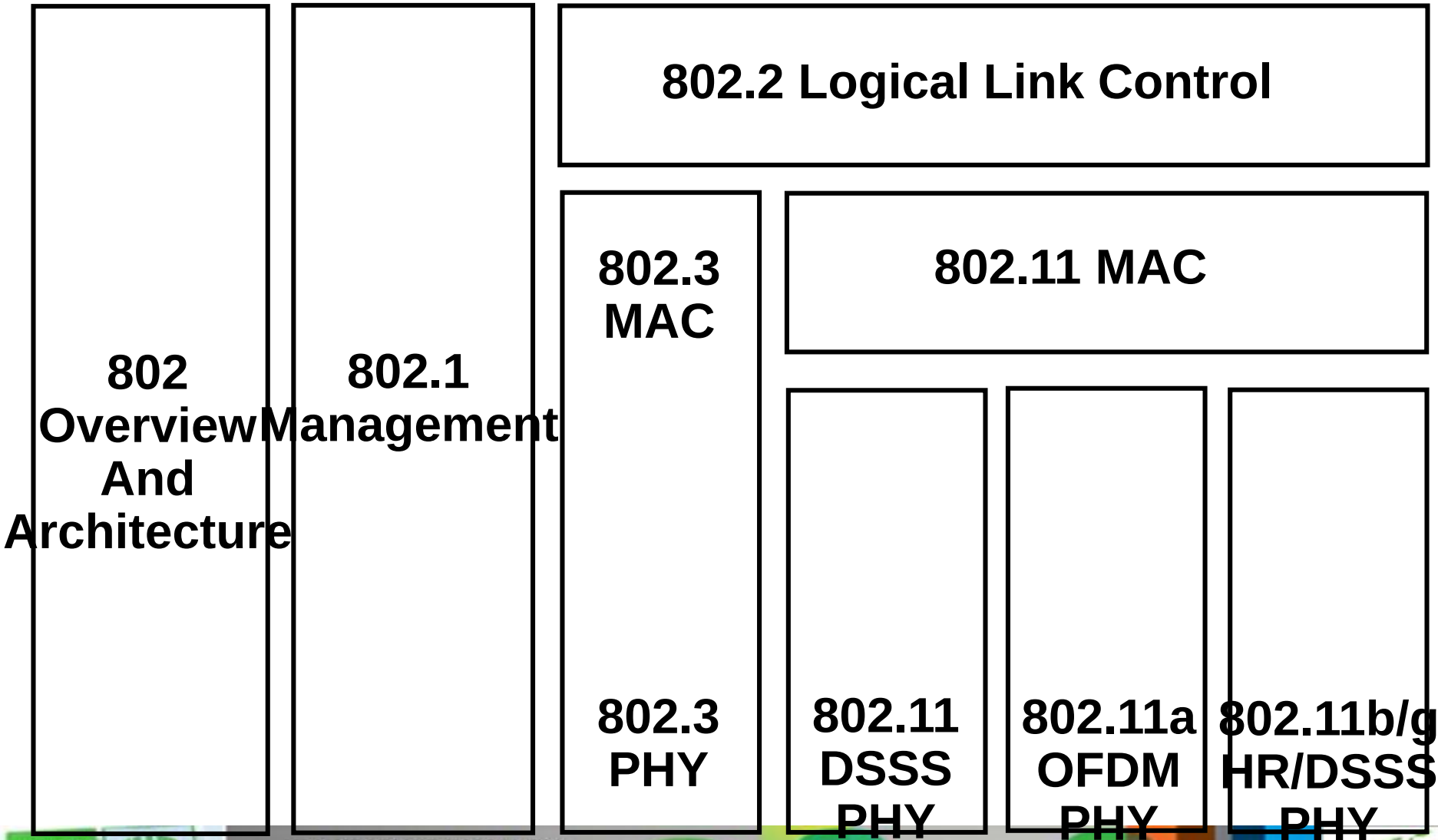
Regulatory Class	Channel Starting Frequency (GHz)	Channel Spacing (MHz)	Channel Set	Transmit Power Limit (dBm)	Emission Limits Set	Behavior Limits Set
13	5	10	7,8,9,11	24	2	5,6,8
14	5	10	7,8,9,11	24	3	5,6,7
15	5	10	7,8,9,11	24	3	5,6,8
16	5	10	8,12,16	22	2	5,6,7
17	4	10	183,184,185, 187,188,189	24	2	5,6,8
18	4	10	183,184,185, 187,188,189	24	3	5,6,7
19	4	10	183,184,185, 187,188,189	24	3	5,6,8
20	4	10	183,184,185, 187,188,189	17	1	5,6,8
21-255	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved

ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING (OFDM)



5 GHz U-NII Band

IEEE 802.11 BASICS



802.11a SUMMARY

- Operates in the 5 GHz U-NII bands, “Wi-Fi5”
  - 8 channels total in the lower and middle bands
- Supports OFDM at data rates up to 54 Mbps including:
  - 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps
- Coverage up to 50 meters (164 feet)
- Uncrowded frequency band
  - 8 non-overlapping channels
  - Less populated frequency
- Will not interoperate with 802.11b/g systems
- Global deployment issues may exist

802.11b/g SUMMARY

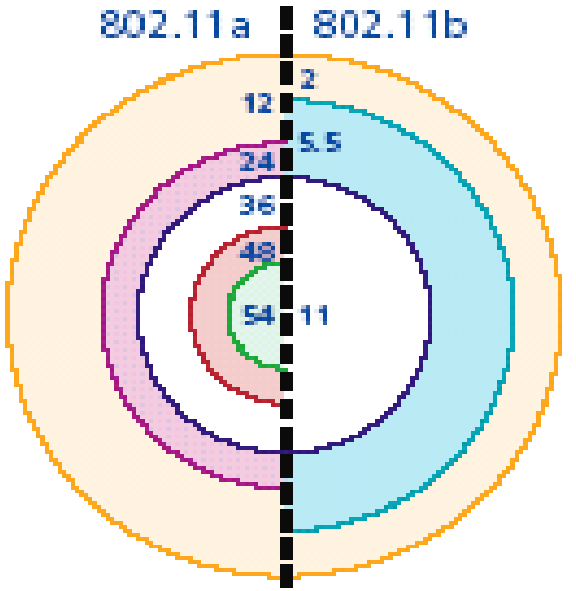
- Operates in the 2.4 GHz ISM band
  - 14 total channels
  - Only 1-3 channels usable at any time
- 802.11b supports data rates up to 11 Mbps
  - Uses DSSS
- 802.11g supports data rates up to 54 Mbps
  - Similar data rates as 802.11a
  - Backward compatible with 802.11b
- Coverage up to 100 meters (328 feet)
- Most commonly implemented standard, “Wi-Fi”
- Crowded frequency band

802.11 COMPARISONS

	802.11a	802.11b	802.11g
Data rates	Up to 54 Mbps (54, 48, 36, 24, 18, 12 and 6 Mbps)	Up to 11 Mbps (11, 5.5, 2, & 1 Mbps)	Up to 54 Mbps (54, 33, 22, 11, 5.5, 2, and 1 Mbps)
Range	50 Meters	100 Meters	100 Meters
Bandwidth	5 GHz U-NII	2.4 GHz ISM	2.4 GHz ISM
Modulation	OFDM	DSSS	DSSS, OFDM, and modified versions

DATA AND THROUGHPUT RATES

- Data rates will drop as distance to AP increases as a result of reduced signal quality
- Actual throughput is about one-half of actual data or link rate
- Throughput rates affected by:
  - Multicast rate (defaults at a rate of 1 Mbps)
  - Framing overhead
  - Collision avoidance mechanisms



Example of range / data rate differences between 802.11a and 802.11b

ATHEROS HIGH SPEED TECHNOLOGIES

- Super G and Super AG
  - Proprietary features built into Atheros chipsets
  - Allows 108 Mbps maximum data rate or link speed and increased throughput up to 60 Mbps
  - Bonds two channels in the 2.4 GHz or 5 GHz spectrum
  - Three possible modes: Base Mode – 22 Mbps throughput
    - Super or Static Turbo Mode – 40 Mbps throughput
    - Dynamic Turbo Mode – 60 Mbps throughput

RELATED PUBLISHED AND PROPOSED WLAN STANDARDS

- 802.11c – Bridge Operation Procedures
- 802.11d – Country Compatibility (Roaming)[1]
- 802.11e – QoS Enhancements
- 802.11f – Inter-Access Point Protocol (IAPP)[2]

Published Date

- 1 - 2001
- 2 - 2003

RELATED PUBLISHED AND PROPOSED WLAN STANDARDS (continued)

- 802.11h – Spectrum and Power Control Management[3]
- 802.11i – Enhanced Security[4]
- 802.11j – Channel Selection for Japan[5]
- 802.11k – Radio Resource Measurement Enhancements
- 802.11l – (letter skipped)
- 802.11m – Maintenance of the IEEE Standard
- 802.11n – Enhancement for Higher Throughput

RELATED PUBLISHED AND PROPOSED WLAN STANDARDS (continued)

- 802.11p - Wireless Access for the Vehicular Environment (WAVE)
- 802.11r - Fast roaming
- 802.11s - Wireless mesh networking
- 802.11T - Wireless Performance Prediction (WPP)
- 802.11u - Interworking with non-802 networks
- 802.11v - Wireless network management

OTHER RELATED STANDARDS

- 802.3af – Power Over Ethernet[6]
- 802.1X – Authentication[7]
- LWAPP – Lightweight Access Point Protocol
- CAPWAP – Control and Provisioning of Wireless Access Points

STANDARDS & CERTIFICATIONS ORGANIZATIONS

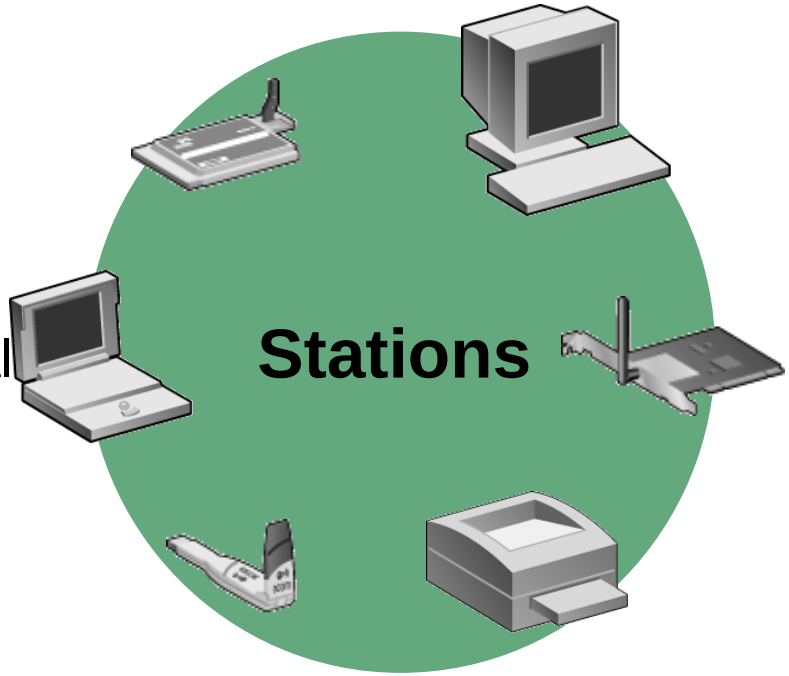
http://www.ieee.org/

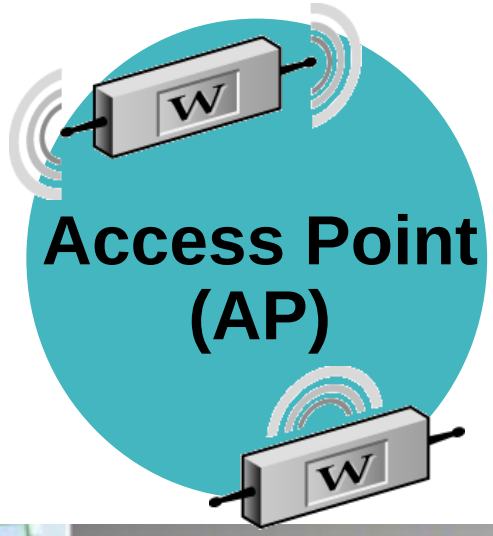
http://www.fcc.gov/

http://www.wi-fi.org/

WIRELESS COMPONENTS

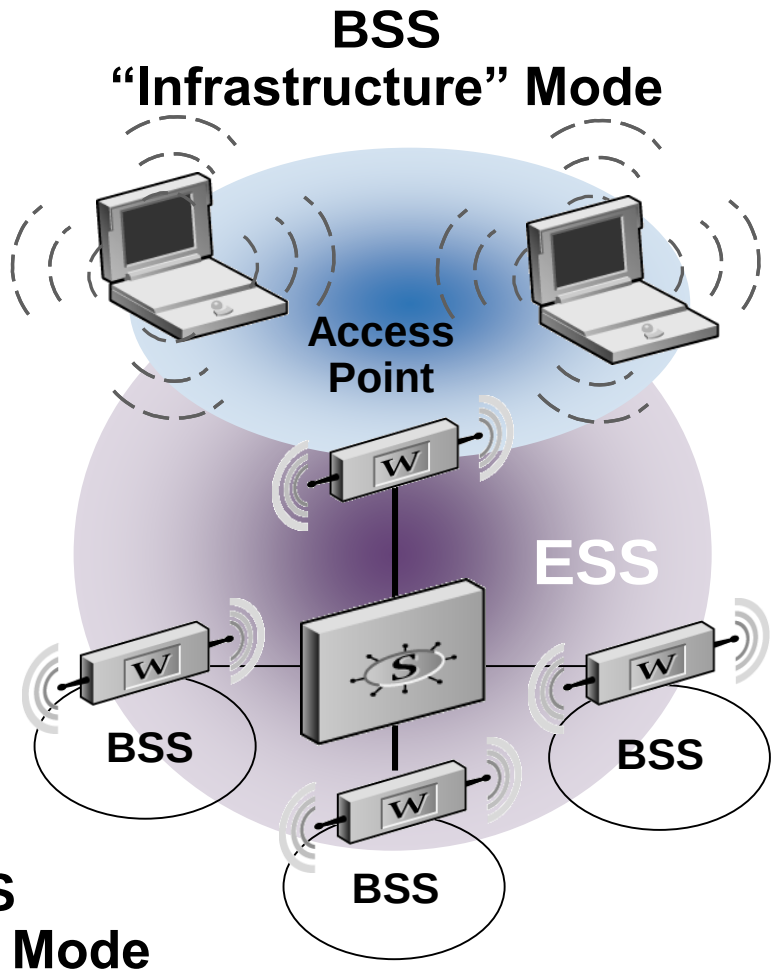
- Wireless Medium
- Stations and access points
  - –Transceivers to move data
  - –Antennas used for radio signal
- Distribution system

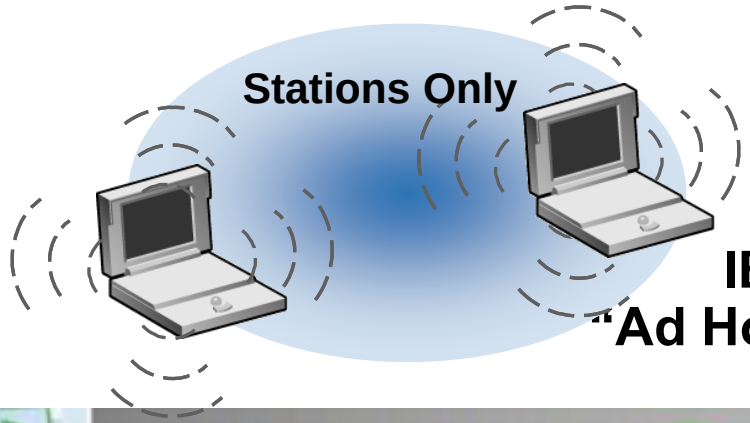




BASIC SERVICE SETS

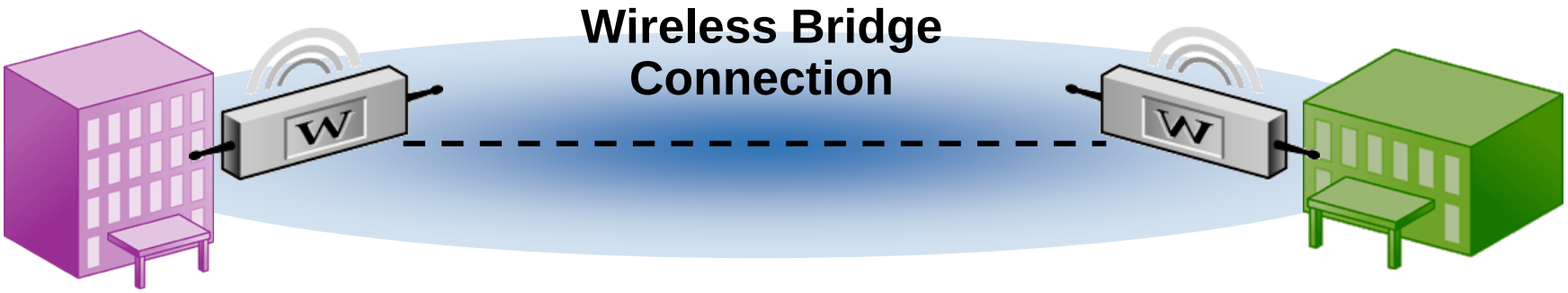
- Infrastructure Basic Service Set (Infrastructure BSS)
  - Both AP and stations are used
- Independent Service Set (IBSS)
  - a.k.a. “Ad Hoc” mode or “Peer-to-Peer” Mode
  - No access point is used
- Extended Service Set (ESS)





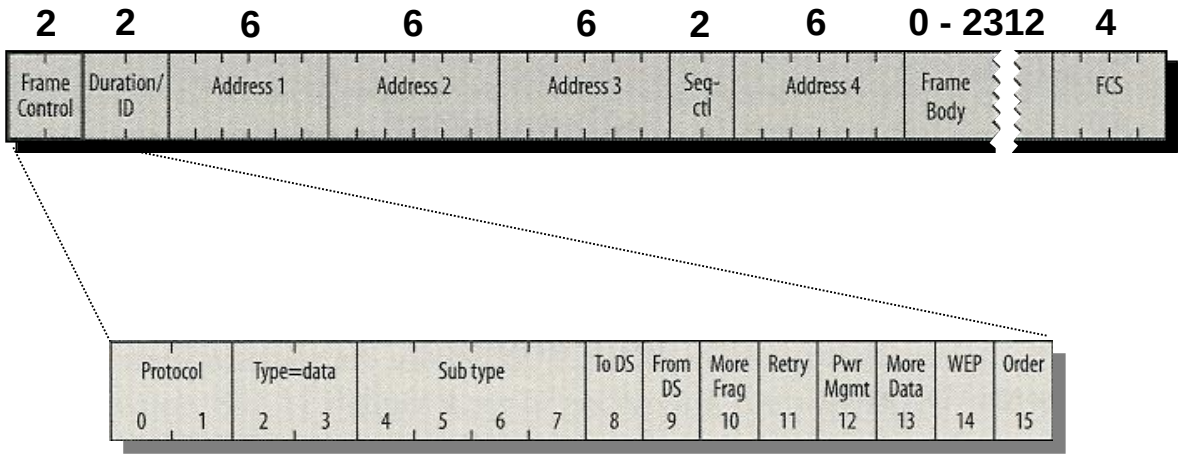
WIRELESS BRIDGE

- Connects two remote sites wirelessly
- A.K.A. Wireless Distribution System (WDS)
- Implemented by enabling a configuration option on an AP

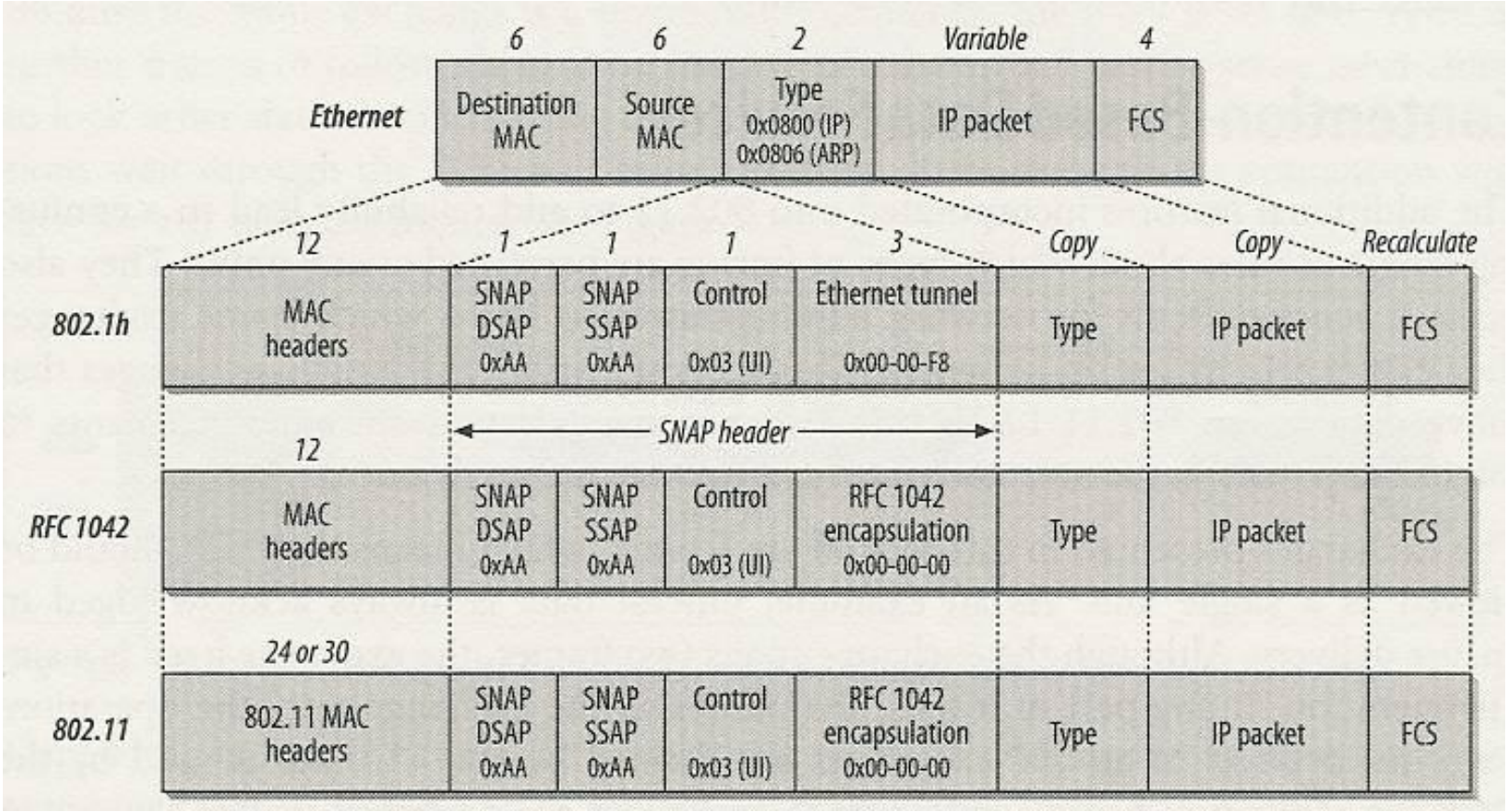


GENERIC 802.11 MAC FRAME

- Three types of frames with several subtypes:
- Management
  - Probe
  - Beacon
  - Authentication
  - Association
  - Reassociation
  - Disassociation
  - Deauthentication
- Control
  - Request-to-Send
  - Clear-to-Send
  - Acknowledgement
- Data

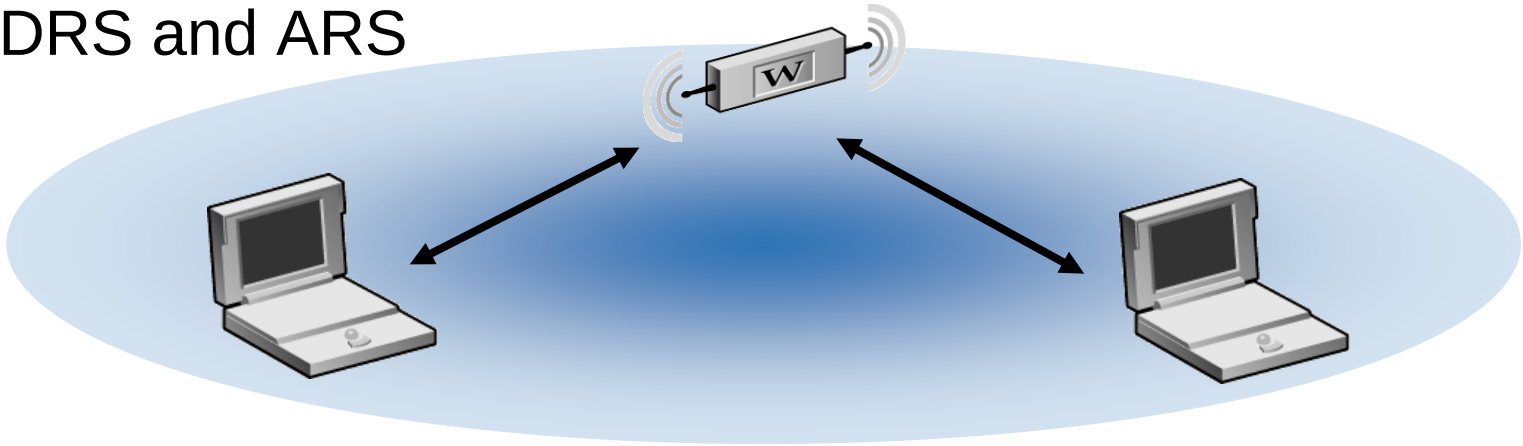


802.2 ENCAPSULATION



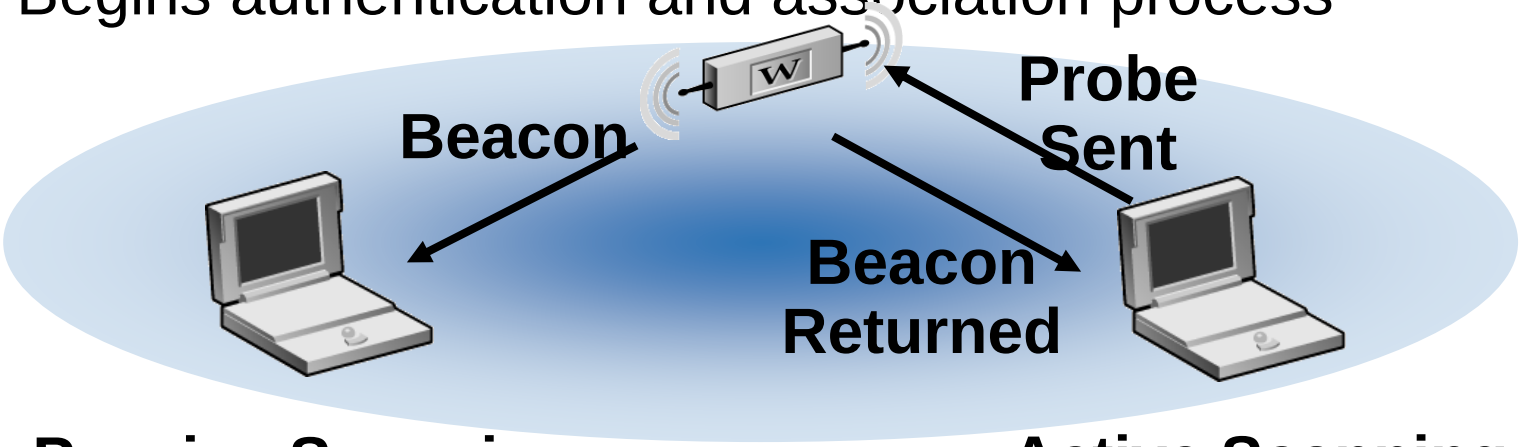
WIRELESS MANAGEMENT PROCESSES

- Scanning
- Station (user) Authentication and Association
- Beacon Management
- Power Management Mode
- DRS and ARS



SCANNING

- Station identifies if wireless network present
- Passively listens for or actively probes for beacon frames
- Builds a table of APs from the beacons
- Begins authentication and association process



AUTHENTICATION & ASSOCIATION

Open System Authentication

Authentication request including identity, algorithm – open system, sequence number 1

Authentication response including algorithm – open system, sequence number 2, status code (association Success/denied/rejected/other)

Shared Key Authentication

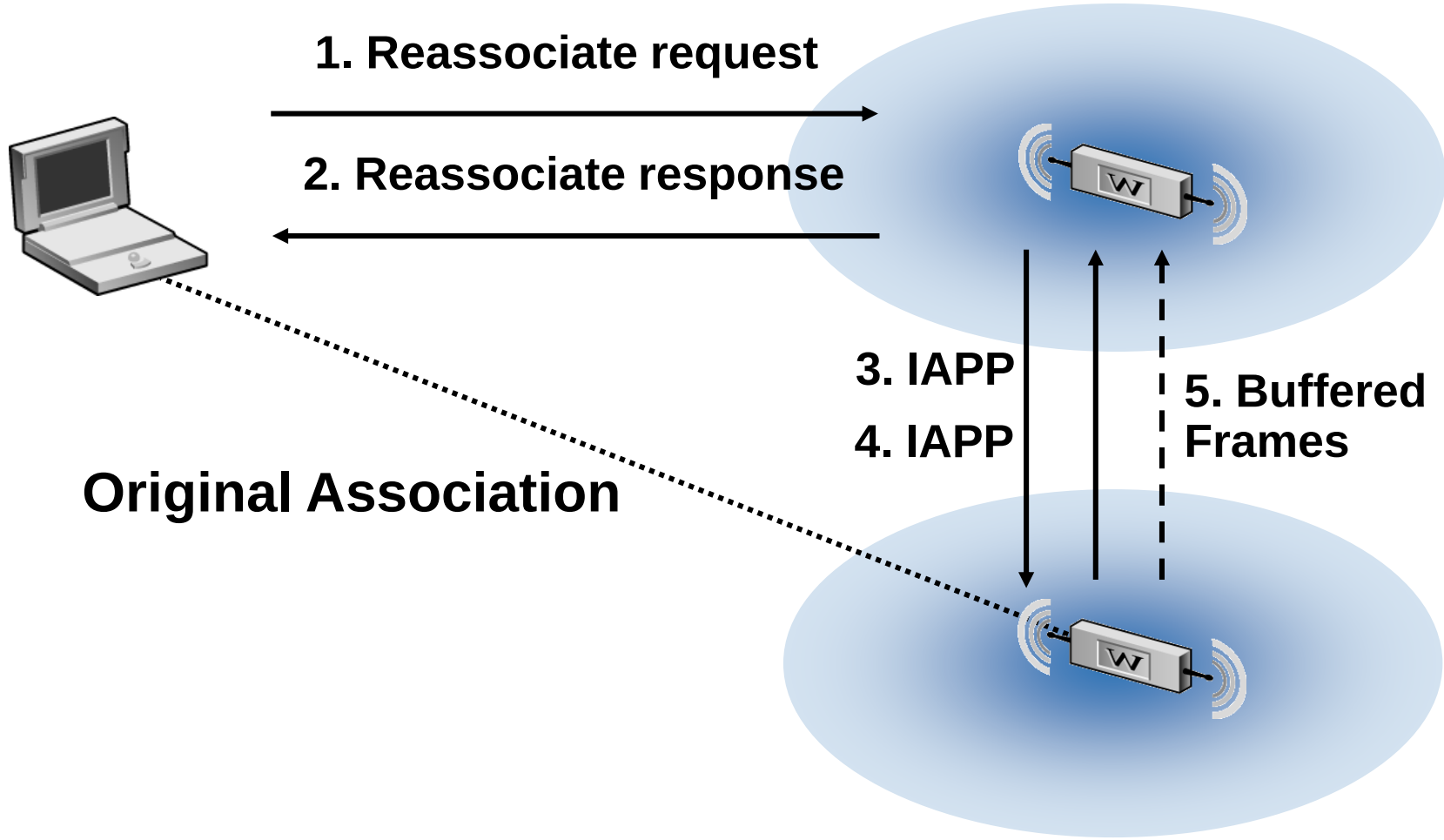
Authentication request

Challenge Response

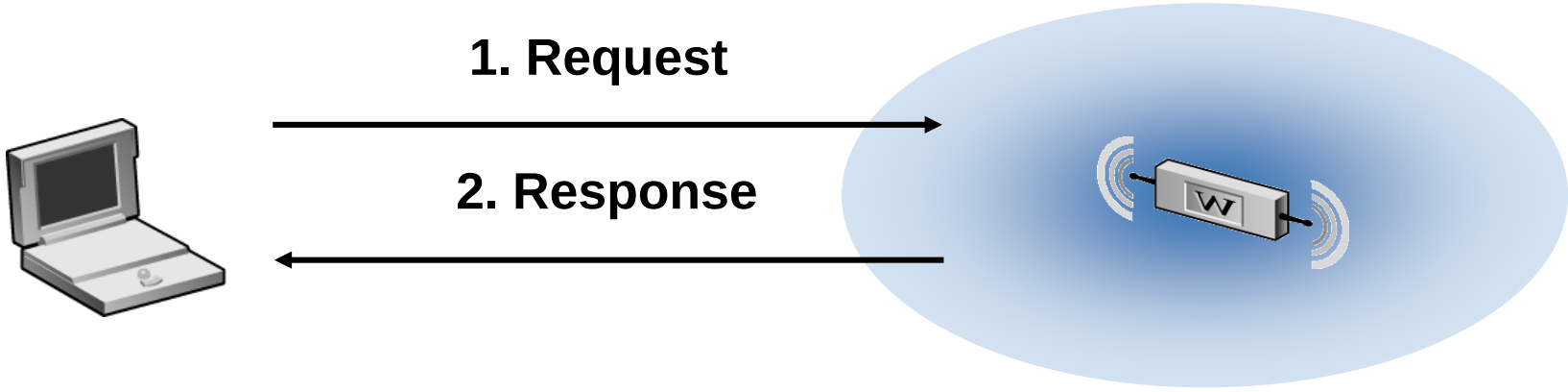
Challenge Text

Status (success, deny, reject)

ROAMING & REASSOCIATION



DISASSOCIATION & DEAUTHENTICATION



- Disassociation ends the association relationship and removes the station from the WLAN
- Deauthentication breaks the authentication between a station and AP
- Used when the station has not properly joined a network, performed an incorrect operation, or has left the cell service area

BEACON MANAGEMENT

- Used during scanning to identify presence of a WLAN
- Used in both FHSS and DSSS WLANs
- Transmitted at regular intervals
  - About 10 times per second
- Provide network parameters for joining
- Stations must be close enough to hear beacons from an AP
- Provides time synchronization between station and AP
- Provides channel usage information
- Beacons are transmitted from the AP at the lowest supported (configured) data rate

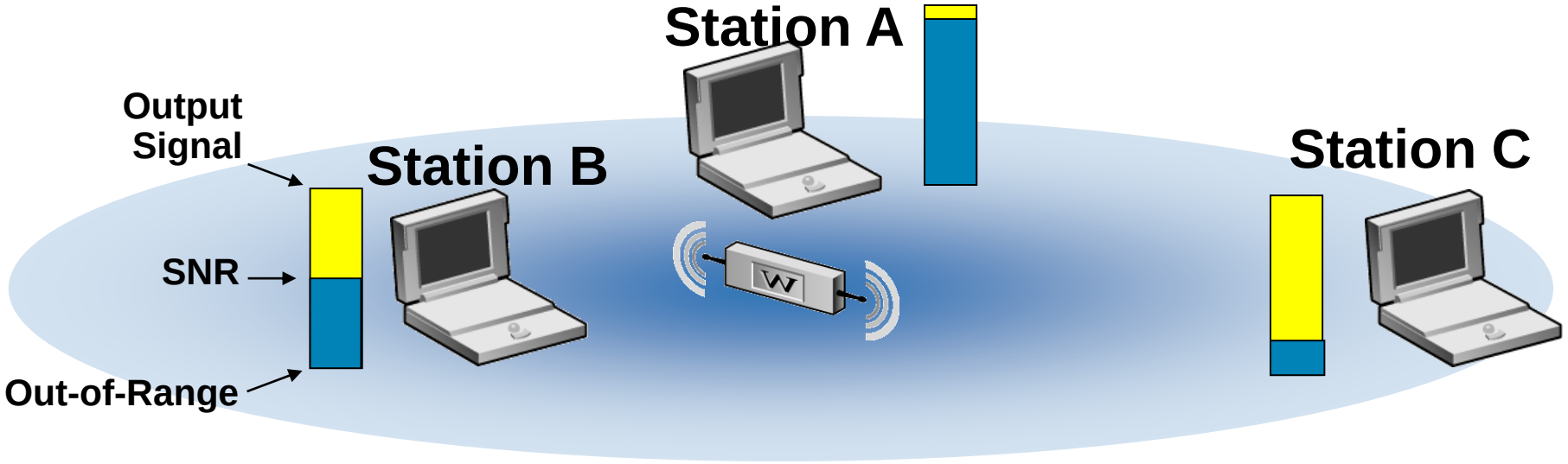
POWER MANAGEMENT MODE

- Allows stations to go into “sleep” mode to conserve battery power
- Defines how long a station will be down (in milliseconds)
- Frames to be buffered at the AP until station wakes up
- Relies on the time synchronization performed through beacon management
- Station wakes up after predetermined interval and receives any buffered frames from the AP

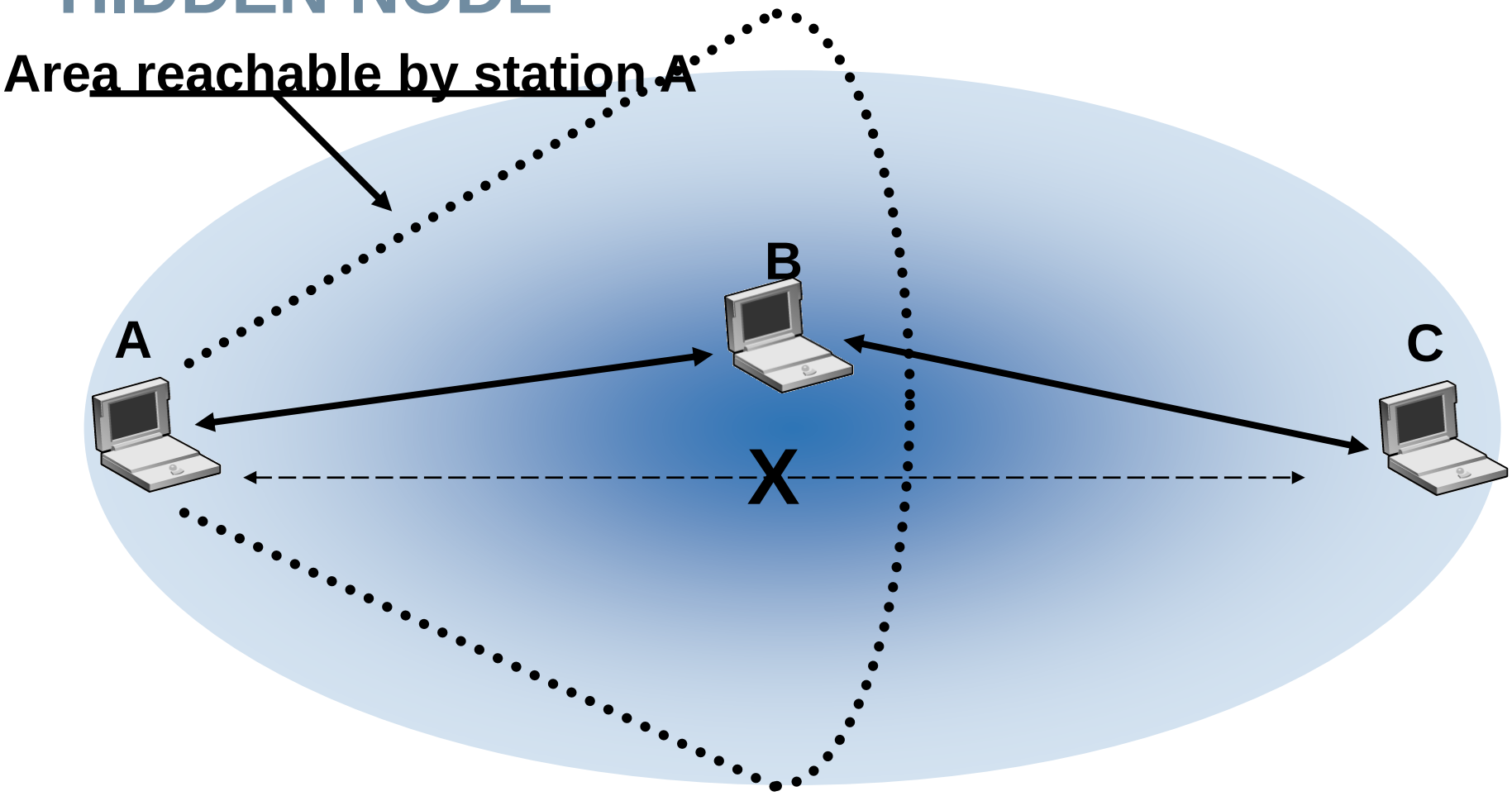
- Two modes:
  - Power Save Polling Mode (PSP) – station using power saving when available
  - Continuous Aware Mode (CAM) – power saving is not in use and the station is always on and ready to transmit and receive

DYNAMIC RATE SHIFTING

- Automatically adjust data rates based on signal quality
- Automatically adjusted by the AP
- For example:
  - Station A has a high quality signal and operates at 11 Mbps
  - Station B has a medium quality signal and operates at 5.5 Mbps
  - Station C has minimal signal and is operating at 1 Mbps

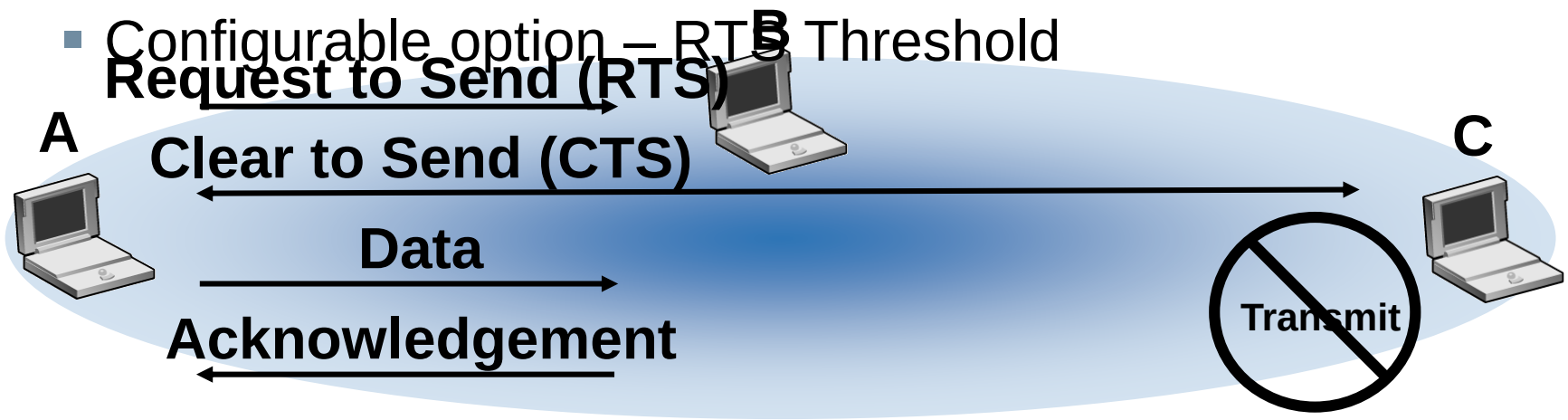


HIDDEN NODE

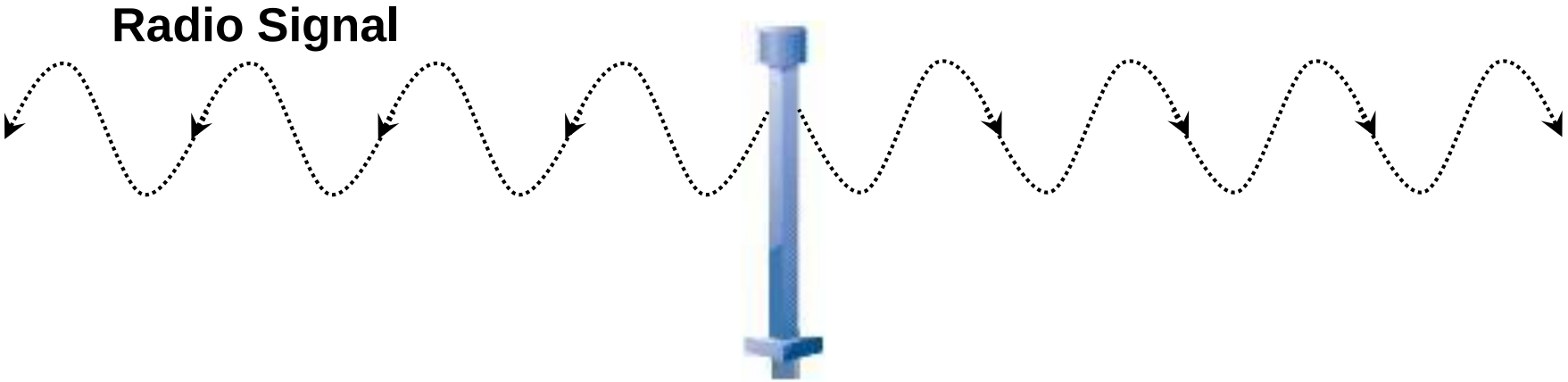


RTS/CTS HANDSHAKING

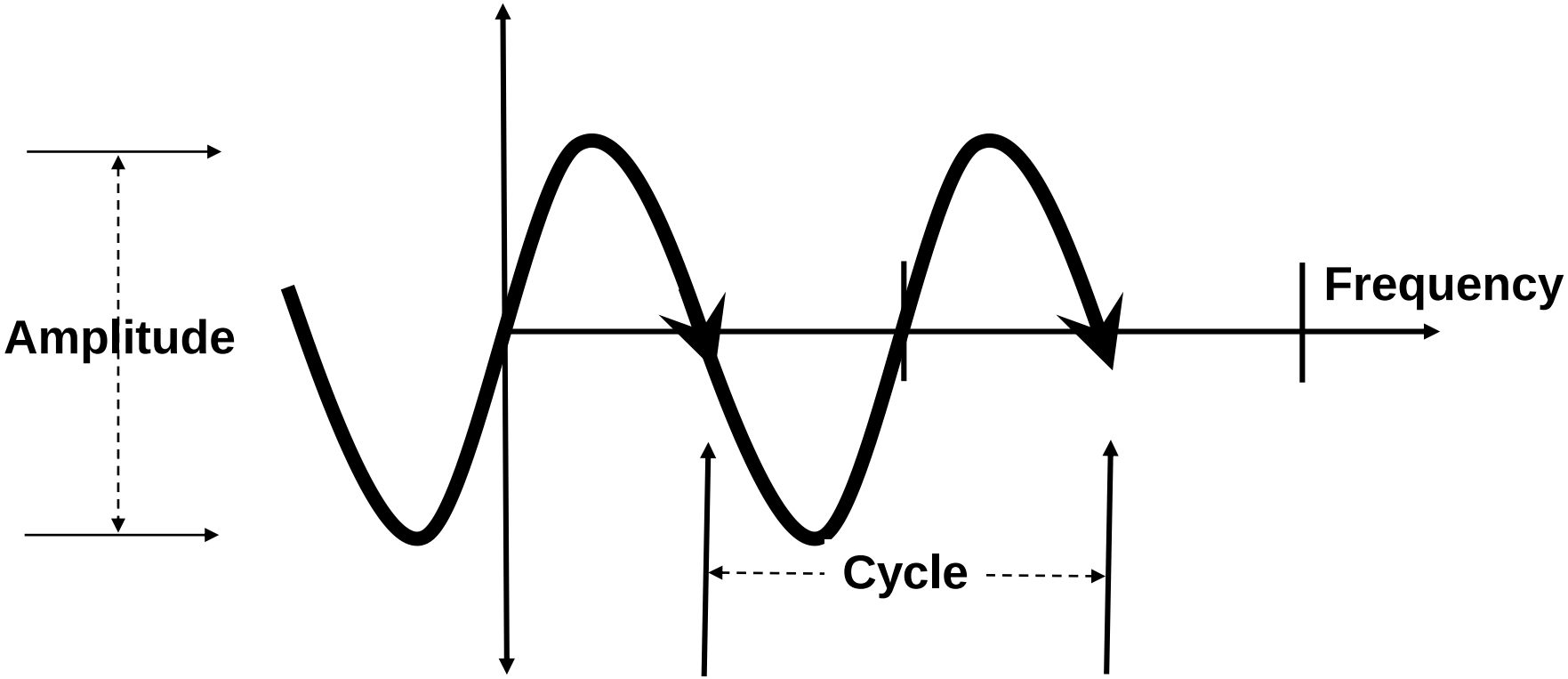
- Used to provide CSMA/CA control
- Avoids bandwidth loss due to collisions
- Short control messages (frames) sent to start or stop transmission
- Configurable option – RTS Threshold



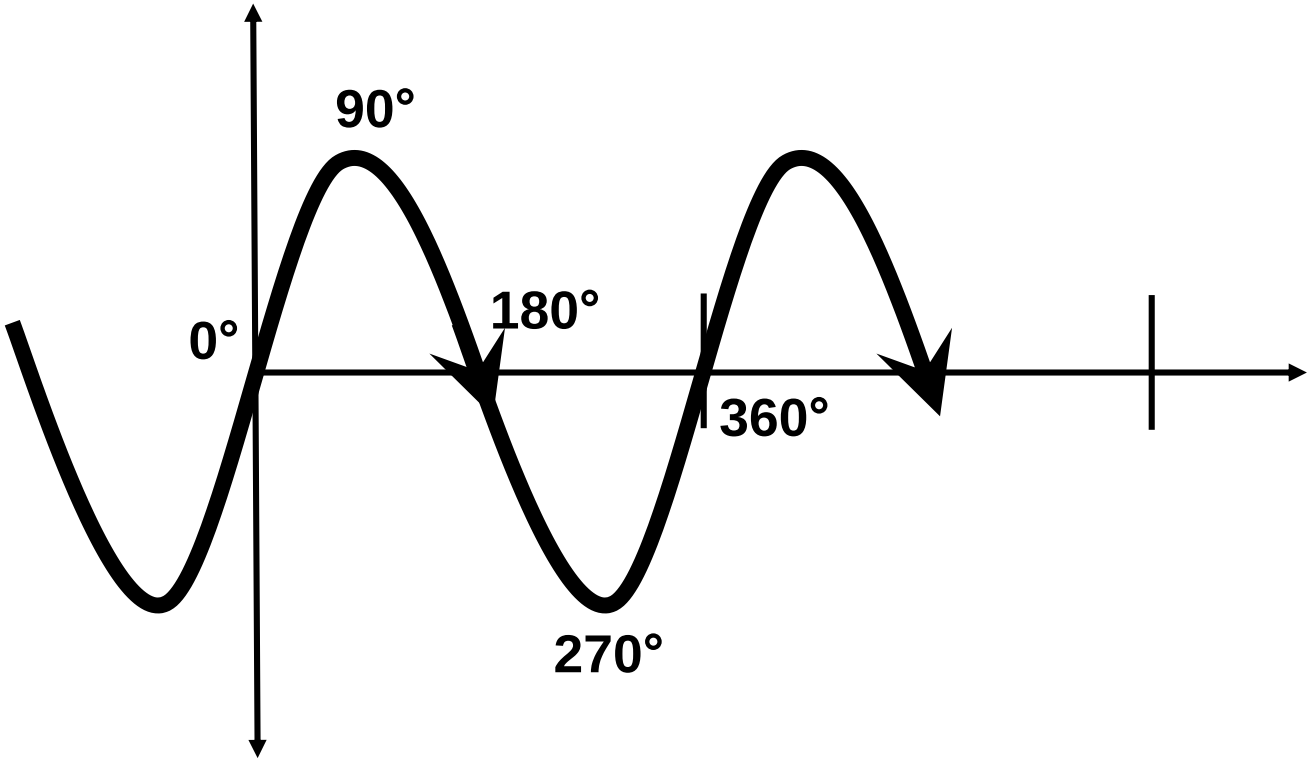
CELL SIGNALING CHARACTERISTICS



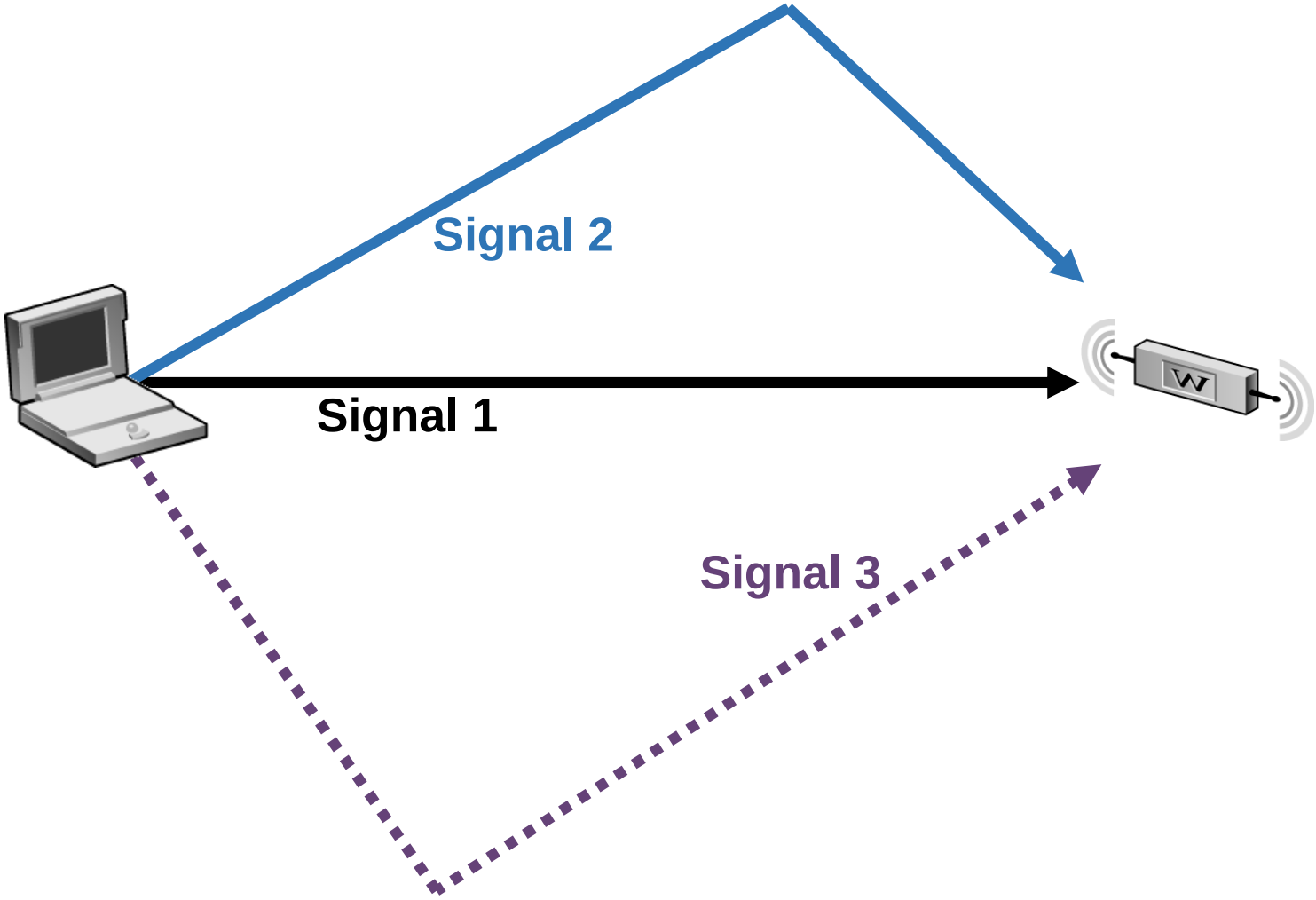
SIGNAL CHARACTERISTICS



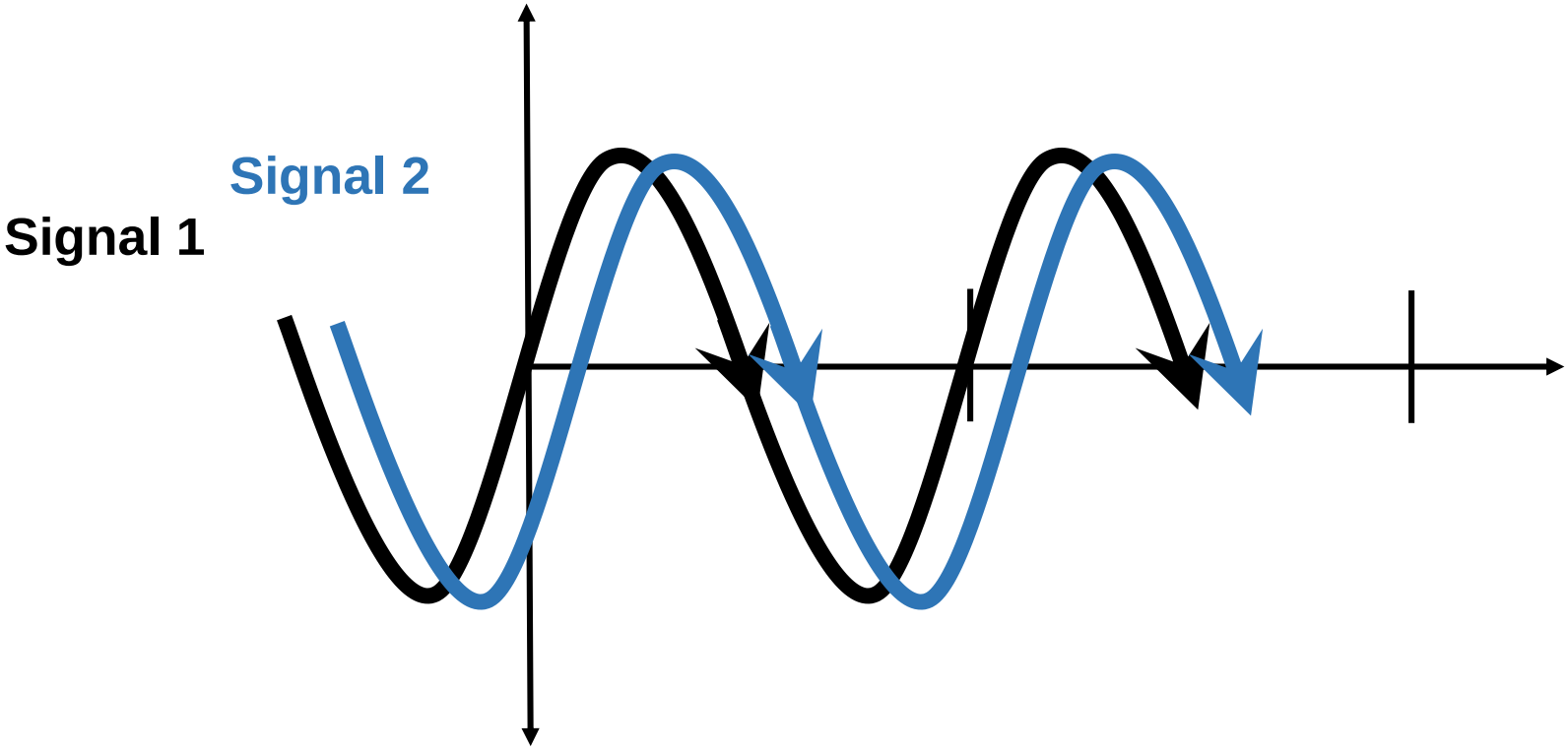
SIGNAL PHASE

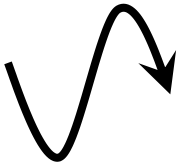


SIGNAL PROPAGATION



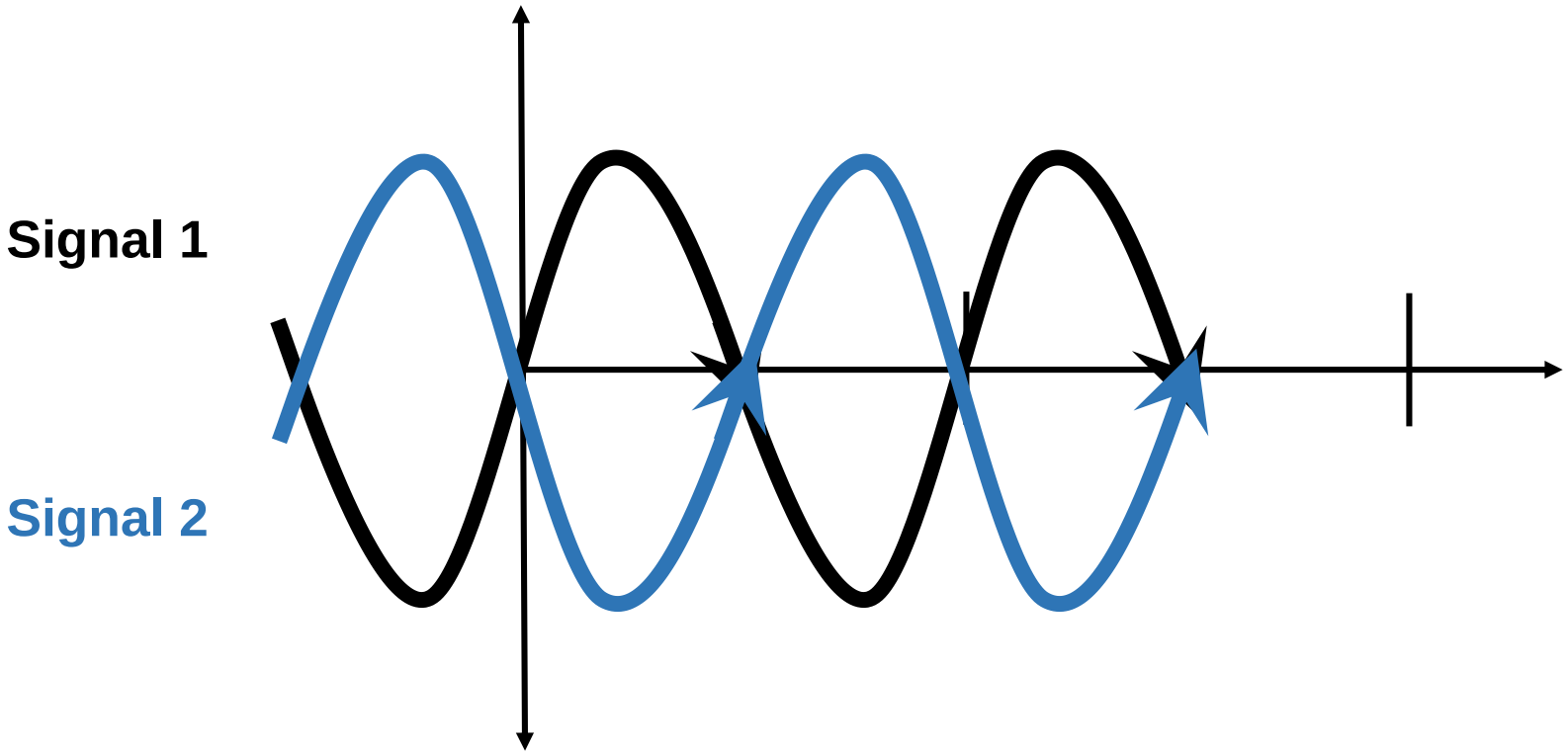
PHASE SHIFT

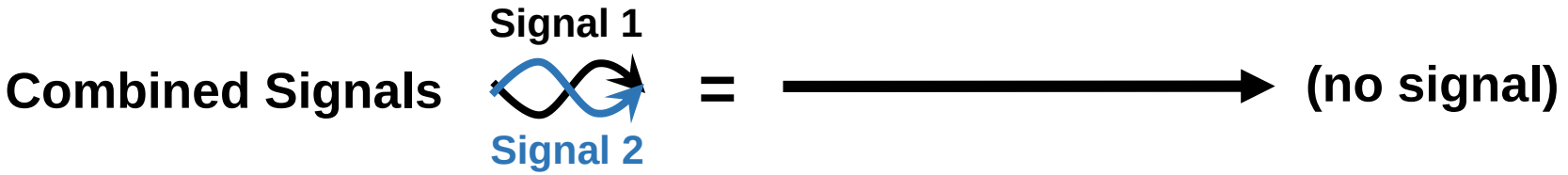


Combined Signals  +  =  Increased Gain

Signal 1 Signal 2

OUT-OF-PHASE

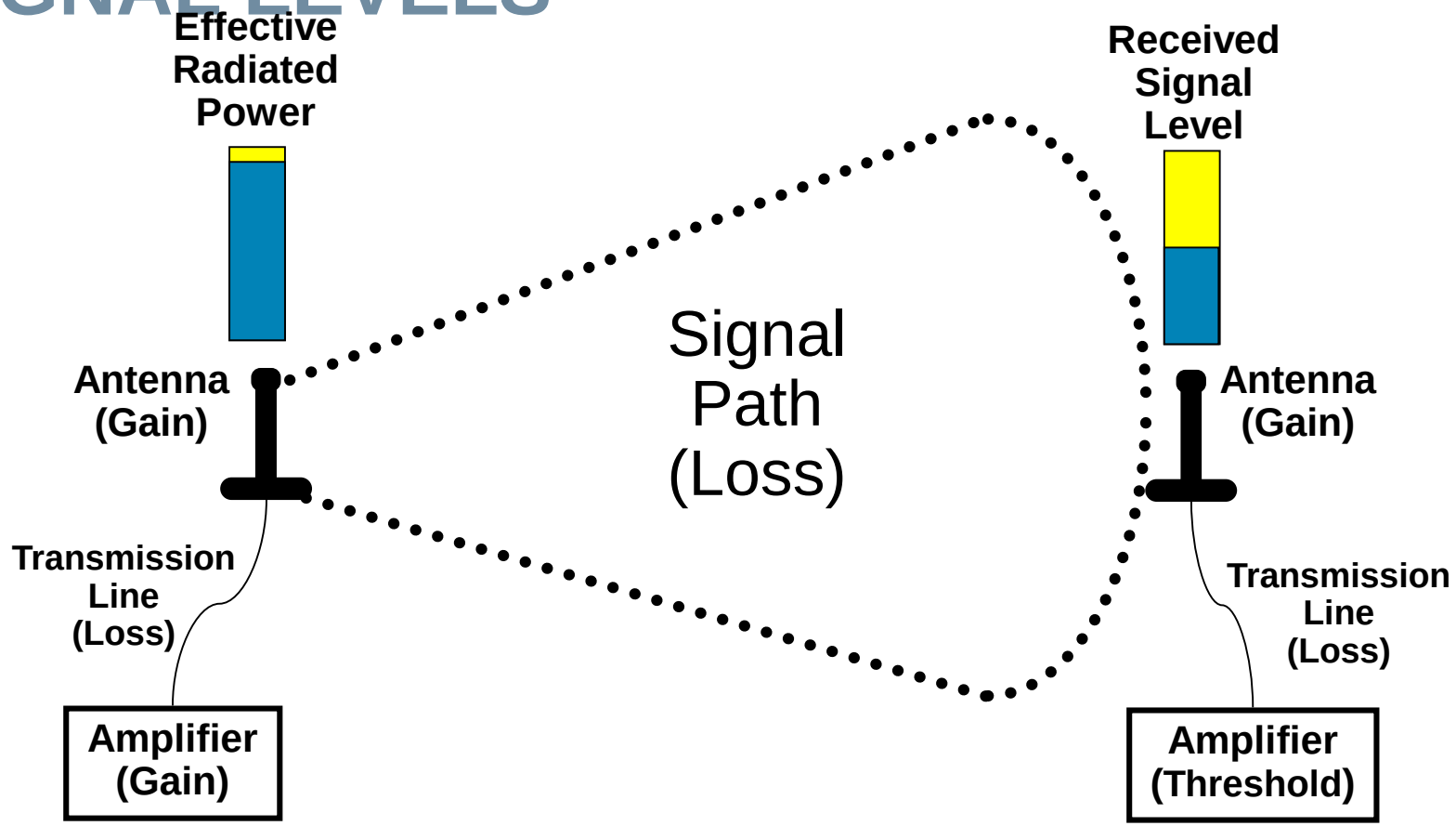

Signal 1
Signal 2


Combined Signals
Signal 1
Signal 2
=
(no signal)

WATTS VERSUS DECIBELS

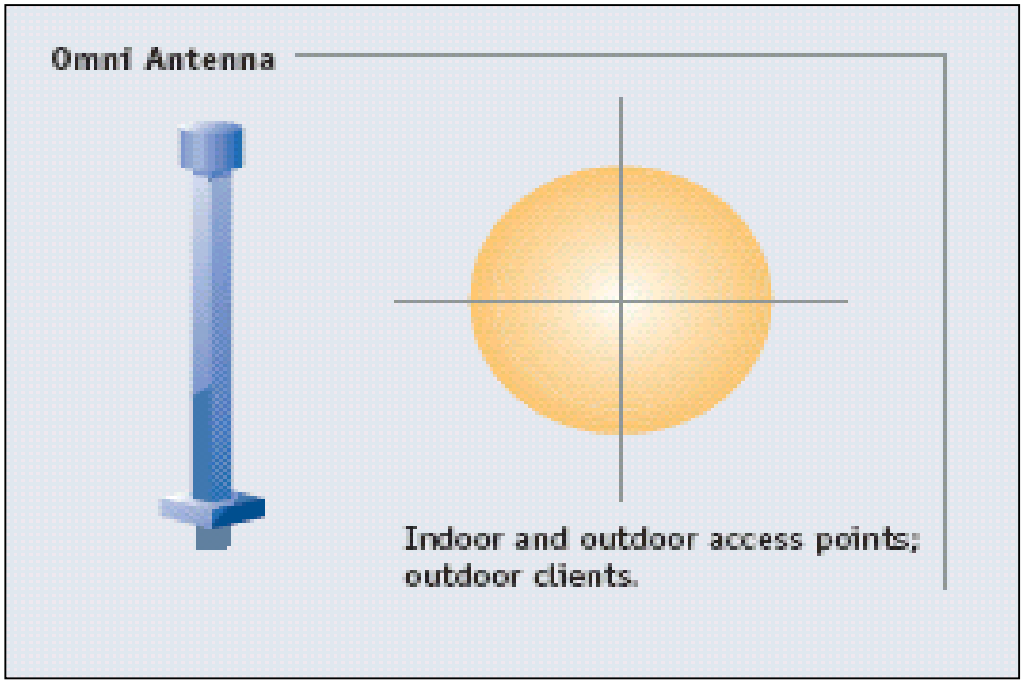
dBm	Watts	dBm	Watts	dBm	Watts
0	1.0 mW	16	40 mW	32	1.6 W
1	1.3 mW	17	50 mW	33	2.0 W
2	1.6 mW	18	63 mW	34	2.5 W
3	2.0 mW	19	79 mW	35	3 W
4	2.5 mW	20	100 mW	36	4 W
5	3.2 mW	21	126 mW	37	5 W
6	4 mW	22	158 mW	38	6 W
7	5 mW	23	200 mW	39	8 W
8	6 mW	24	250 mW	40	10 W
9	8 mW	25	316 mW	41	13 W
10	10 mW	26	398 mW	42	16 W
11	13 mW	27	500 mW	43	20 W
12	16 mW	28	630 mW	44	25 W
13	20 mW	29	800 mW	45	32 W
14	25 mW	30	1.0 W	46	40 W
15	32 mW	31	1.3 W	47	50 W

SIGNAL LEVELS



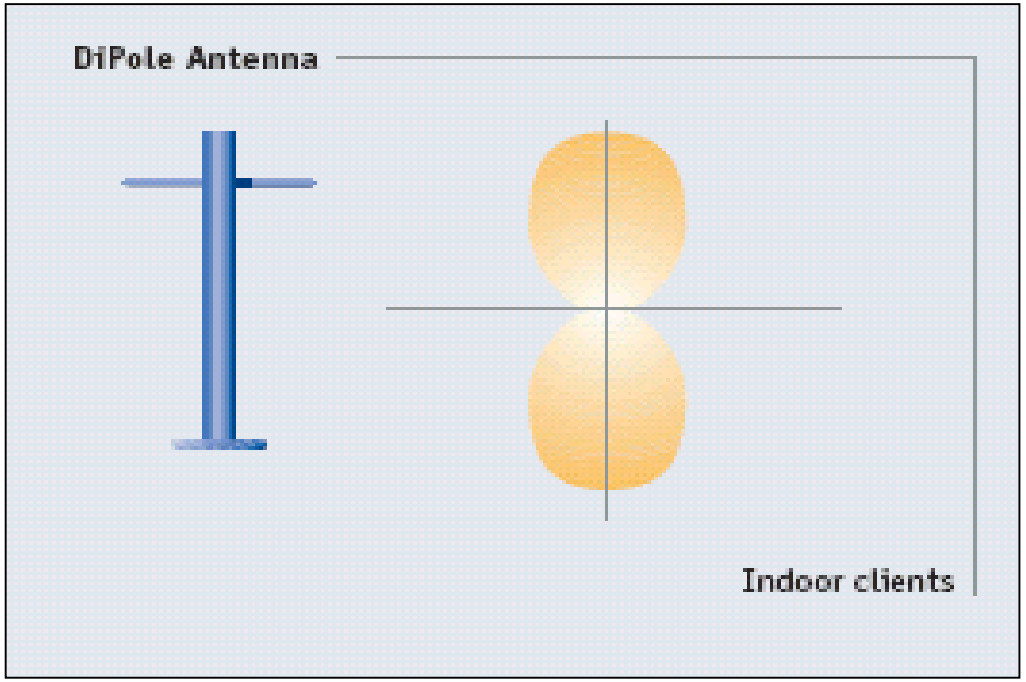
OMNIPOLE ANTENNA

- Transmits signals equally on a horizontal plane
- Coverage cell is best horizontally but not vertically
  - Round (horizontal plane)
  - Donut shaped (on all three dimensions)
- Typically used indoors
- Low gain between 3-10 dBi of gain (low gain)



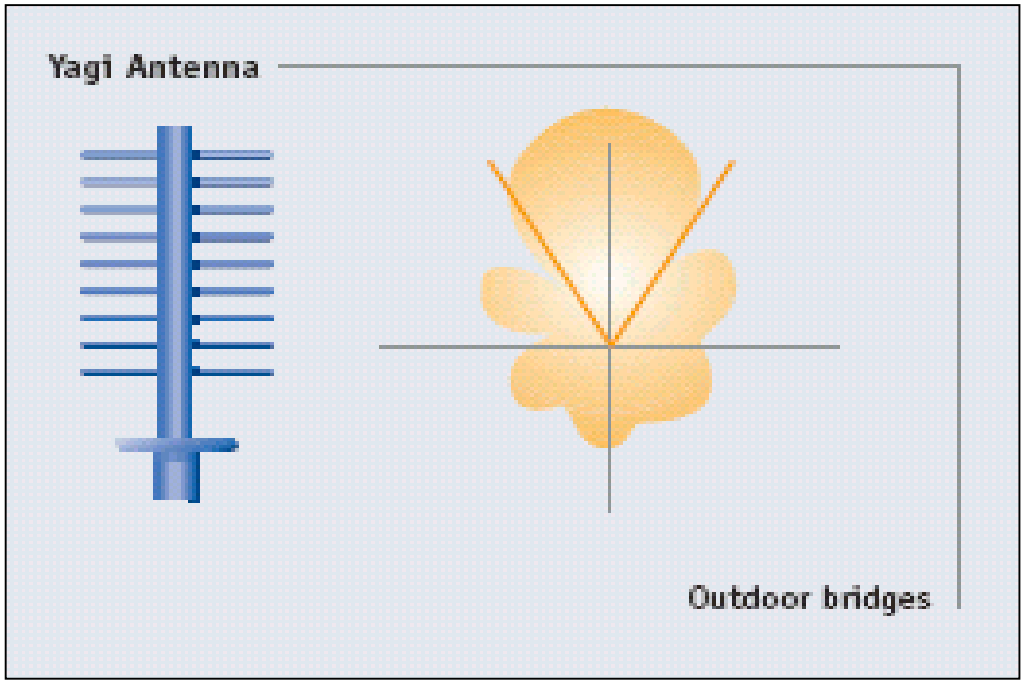
DIPOLE ANTENNA

- Figure 8 transmission pattern
- Low gain though it achieves greater distance
- Typically used indoors for hallways or corridors
- Not as good for ceiling mounting



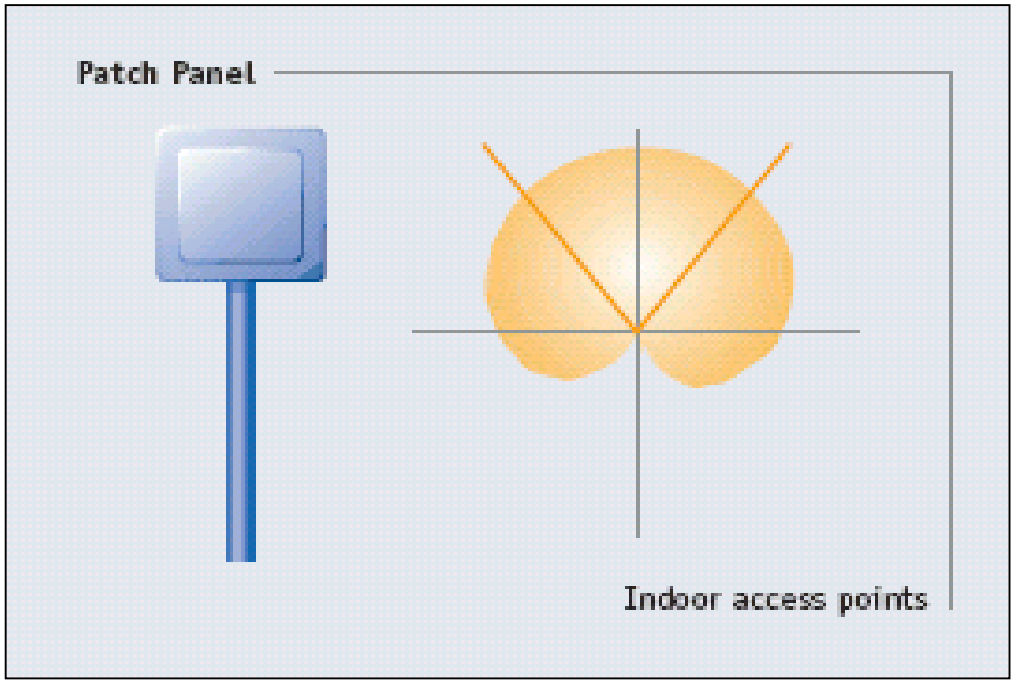
YAGI OR SEMI-DIRECTIONAL ANTENNA

- Semi-directional, more focused transmission pattern
- Provides moderately high gain, 12-18 dBi
- Flat in design so it can be used against a wall or in a corner
- Has an extended forward reach which is good for indoor and/or outdoor use
  - Short to medium range bridging
  - Along narrow hallways and corridors



PATCH PANEL OR PARABOLIC ANTENNA

- Semi- or highly-directional, more focused, narrower transmission pattern
- Can provide up to 24 dBi in gain (regulatory concerns)
- Good for indoor or outdoor use
  - Along narrow hallways and corridors
  - Highly-directional designs cover distances of up to 20 miles



CHOOSING THE RIGHT ANTENNA

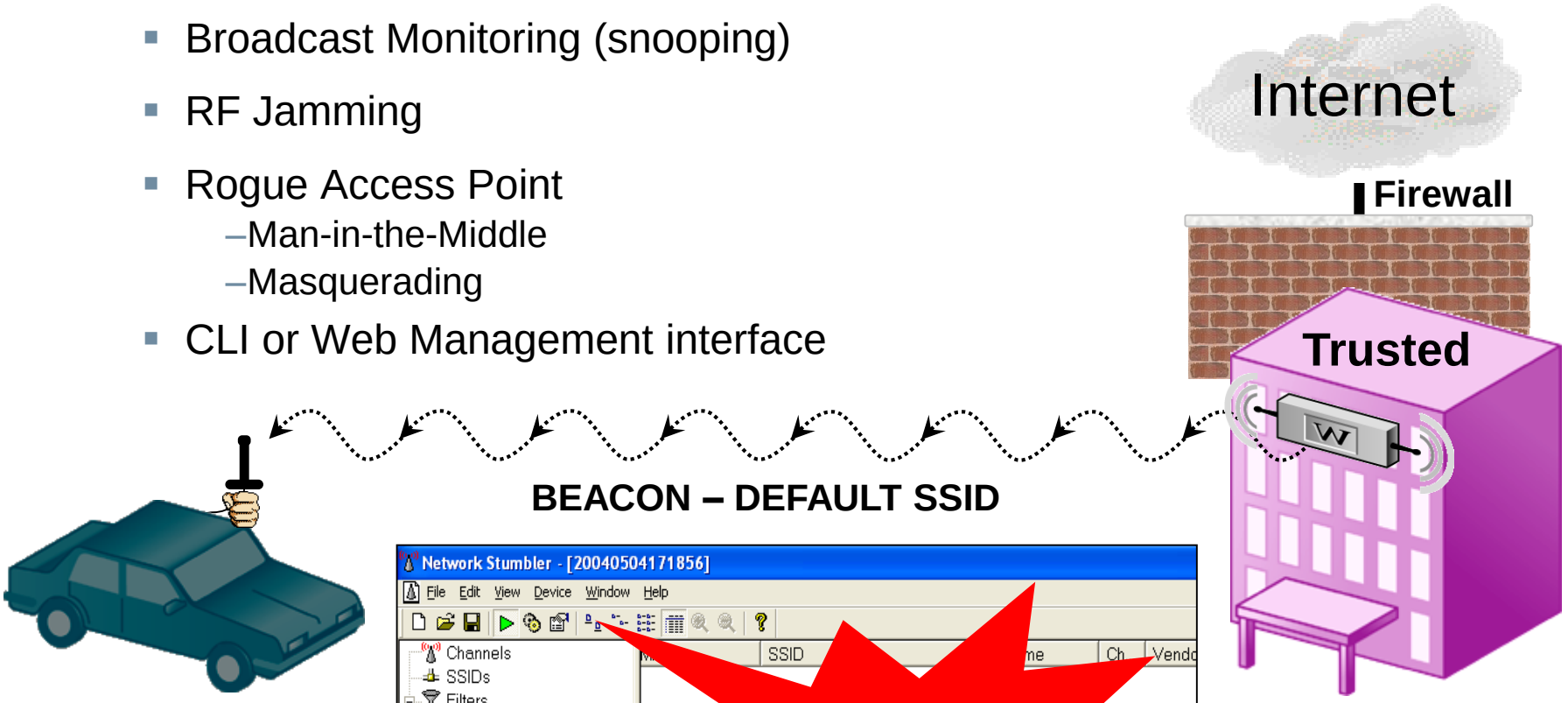
- When choosing the best antenna to use take in consideration:
  - Coverage area
  - Number of users
  - Installation location
  - Obstructions
- Be aware of regulatory limits
  - EIRP is limited to 36 dBi

WLAN SECURITY INTRODUCTION

- Design characteristics
  - Easy Accessibility for Users
  - Optimal Coverage
  - Data Privacy
  - Network Security
- Are not naturally secure
  - Open System, simple association
  - No encryption for transmitted data
  - Create holes in firewalls and trusted zones
- Prone to hackers and “war driving”

TYPES OF WIRELESS ATTACKS

- Broadcast Monitoring (snooping)
- RF Jamming
- Rogue Access Point
  - Man-in-the-Middle
  - Masquerading
- CLI or Web Management interface



WLAN SECURITY FRAMEWORK

- WLAN security components
  - User authentication
  - Key management – computation and distribution
  - Data Encryption – privacy and integrity
- Implementation hierarchy
  - Open Access – Open system authentication, no encryption
  - Baseline security – Open system authentication, WEP
  - Enhanced security – 802.1x authentication, AES or TKIP encryption

SECURITY PROTOCOLS

- Local MAC Filtering
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
  - Temporal Key Integrity Protocol (TKIP)
- WPA2 – 2nd generation WPA
  - Advanced Encryption Standard (AES)
- 802.1X Authentication
  - Several types of EAP (Extensible Authentication Protocol)
  - Several types of PEAP (Protected EAP)
  - 3Com Dynamic Security Link
  - Lightweight Extensible Authentication Protocol (LEAP)

LOCAL MAC AUTHENTICATION

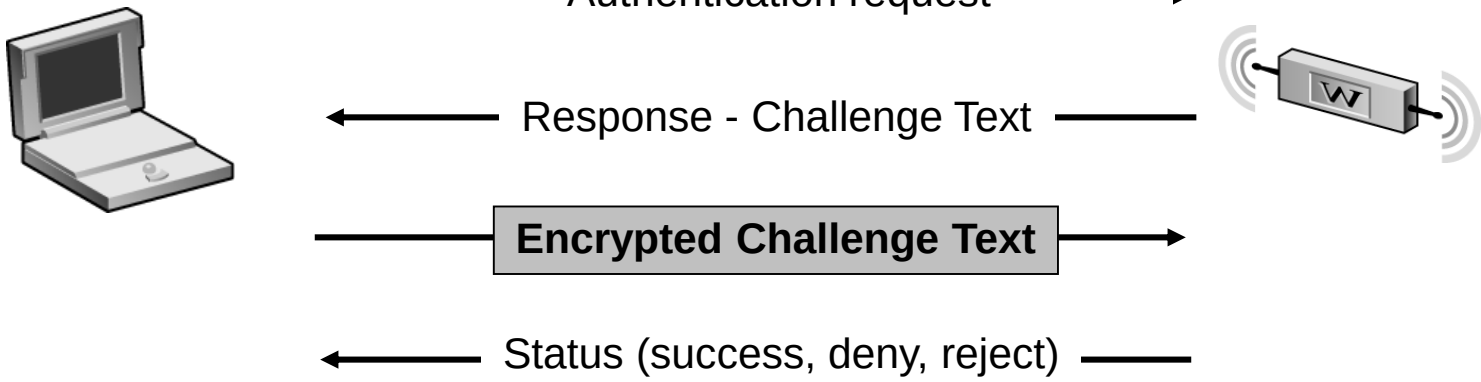
- Allow or deny authentication to a station
  - MAC address-based
  - Not user authentication
- Good for small WLAN implementations
  - Approximately 50 users or less
- Issues
  - Forged MAC address
  - Not totally secure
  - Administratively difficult to maintain in large networks

WIRED EQUIVALENT PRIVACY (WEP)

- A shared key encryption and authentication mechanism for 802.11 WLANs
  - Original 802.11 security implementation
  - Improves privacy and integrity
- Used between the station and AP only
- Only payload data, not header, is encrypted
    - Management and control frames not encrypted
  - Uses 64 or 128 bit encryption method
    - a.k.a. 40 and 104 bit RC4 encryption
    - Static keys
  - Up to four user configurable, shared keys
    - a.k.a. “Shared Key Authentication”
    - Keys must be same end-to-end among all systems
  - Verifies transmitted data is same as received data
- Not very secure

WEP SHARED KEY AUTHENTICATION

Shared Key Authentication



WI-FI PROTECTED ACCESS (WPA)

- Improves security as compared to WEP
- Introduced in 2002
- Enhanced data encryption
  - WPA - using Temporal Key Integrity Protocol (TKIP)
  - WPA2 - using Advanced Encryption Standard (AES)
- User authentication implemented using either:
  - 802.1x Authentication (enterprise applications)
  - Pre-Shared Key (SOHO applications)
    - Manually-entered keys or passwords
    - Designed to be easy to set up for the home user.
- Forward compatible with 802.11i Enhanced Security
- Susceptible to DoS attacks

TEMPORAL KEY INTEGRITY PROTOCOL (TKIP)

- Allows WEP security to be upgraded, adds
  - Message integrity check (for weak key attacks)
  - Per-packet key mixing
  - Key management and distribution
- Each key is used to encrypt one and only one data packet

IEEE 802.11i ENHANCED SECURITY

- Enhances the current 802.11 MAC to provide improvements in security and authentication mechanisms
- Based on federal encryption standard AES (Advanced Encryption Standard)
  - Replaces Triple DES (Data Encryption Standard)
  - Requires hardware acceleration
  - Rijndael algorithm
  - Symmetric block cipher
  - Keys 128, 192, 256 bits

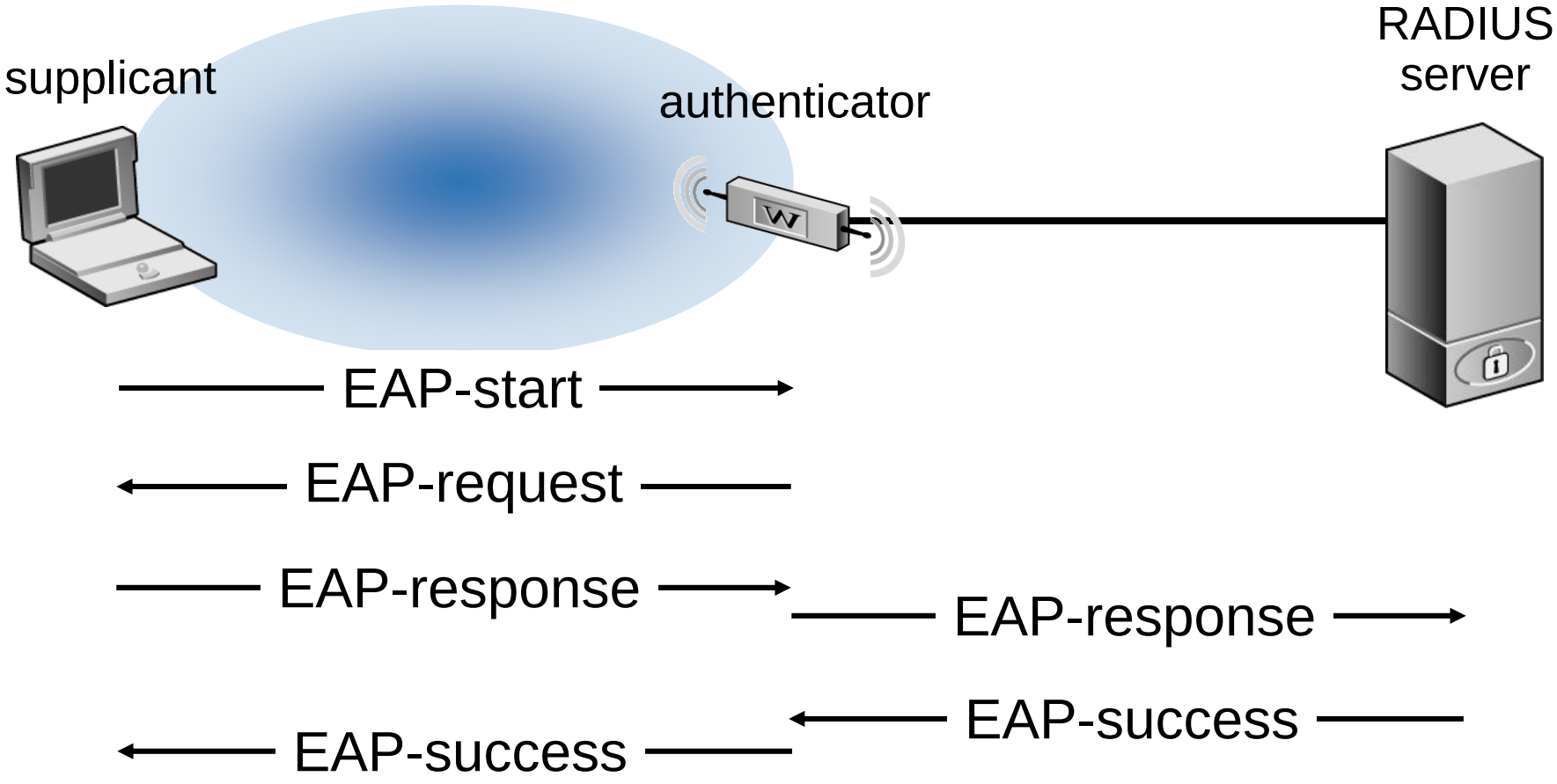
802.1x AUTHENTICATION

- Framework for authenticating and controlling user traffic to protect wired and wireless LANs
  - Centralized authentication rather than distributed at each AP
    - Messages forwarded to RADIUS authentication server
  - Access control still maintained at the AP
  - Must choose authentication method
- Uses dynamically varying encryption keys
- Supported in Microsoft's Windows XP, Funk, and Meeting House operating systems (supplicant and authenticator)
- Scales well for large enterprise networks

802.1x AUTHENTICATION METHODS

- EAP-MD5 (Extensible Authentication Protocol-Message Digest 5)
- EAP-TLS (EAP-Transport Layer Security)
- EAP-TTLS (EAP-Tunneled TLS) / MSCHAPv2 (Microsoft Challenge Handshake Protocol)
- EAP-SIM (Subscriber Identity Module)
- PEAPv0 (Protected EAP) / EAP-MSCHAPv2
- PEAPv1/EAP-GTC (Generic Token Card)
- 3Com Dynamic Security Link
- Lightweight Extensible Authentication Protocol (LEAP)

802.1x COMMUNICATIONS



RADIUS AUTHENTICATION SUPPORT

- RADIUS Centralized User Authentication is performed between the wireless client and the RADIUS server, in conjunction with the IEEE 802.1x standard-based network log-in
- Any RADIUS server supporting EAP-MD5, EAP-TLS, EAP-TTLS
  - 802.1x implementation to provide a secure authentication solution for wireless stations
  - 3Com's Universal Client Certificate supporting EAP-TLS enables RADIUS servers that support EAP-TLS to achieve Dynamic Key Distribution (Per-User / Per-Session key management)
- RADIUS Accounting
  - Username, start time, stop time, packet input/output

EAP-MD5

- Converts a message of arbitrary length to a 128 bit value
- Never sends password in clear text
- Supported on most RADIUS servers
  - Cisco
  - Funk
  - Microsoft

EAP-TLS

- Authenticates station and user
  - Station by use of a digital certificate
  - User by username and password
- Requires support for Digital Certificates (server-side and client-side)
- 3Com also adds 128 Dynamic Key encryption
  - Key changes every 15 minutes
- Supported in high end RADIUS Servers
  - Microsoft
  - Funk Steel-Belted Radius
  - Cisco

EAP-TTLS

- Tunneled EAP-TLS
  - Eliminates the need for client-side digital certificates, but still requires server-side digital certificates
  - But can use MS-CHAP for password checking
- Currently only supported in Funk Software Odyssey Server

EAP-SIM

- Created for the GSM mobile telecom industry
- Uses a smartcard which securely stores the key identifying a mobile subscriber for authentication
- No native OS support

PEAPv0/EAP-MSCHAPv2

- Commonly known as PEAP
- Competes with EAP-TTLS
- Uses TLS and digital certificates
- Two-phase TLS authentication
- Uses TLS encryption
- Allows for support of token cards

PEAPv1/EAP-GTC

- Created by Cisco as an alternative to PEAP
- Allows the use of an inner authentication protocol other than Microsoft's MSCHAPv2
- No native OS support

3COM DYNAMIC SECURITY LINK

- Per user, per session dynamic key with 128-bit encryption
  - Unique key automatically generated between the AP & wireless client each session
  - Keys are done in the background, automatically, not entered manually
- Internal database supports 1000 usernames/passwords
- Provides a superior security solution when AP is deployed in networks without a centralized authentication server

LEAP

- Cisco-only Protocol - used to fix WEP
  - Requires Cisco or Funk RADIUS Server
  - Requires Cisco APs
  - Requires Cisco or 3Com X-Jack® client cards
  - Is only Dynamic Session Keys (Like DSL)
  - Very expensive solution for not being Dynamic Encryption Keys

SECURITY CHECKLIST

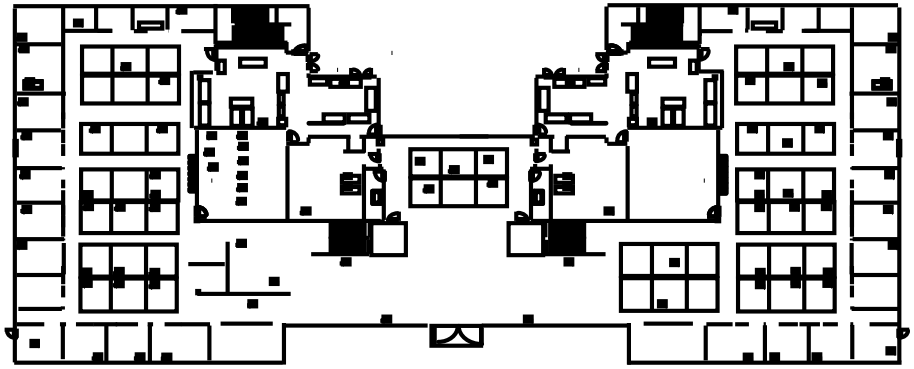
1. Change default settings on the access point
2. Disable SSID broadcast
3. Change the default radio channel
4. Isolate APs into an untrusted zone
5. Enable some form of encryption
6. Limit RF coverage
7. Restrict traffic to specific applications

SECURITY CHECKLIST (continued)

8. Local MAC access
9. Disable DHCP if only a few, no roaming users
10. Maximize IP address assignments if using DHCP
11. Centralize authentication services
12. Perform regular scans and audits
13. Restrict use to authorize personnel
14. Integrate user policies
15. Implement VPNs to secure trusted WLANs

SITE SURVEY

- Preliminary investigation
  - Floor plans or blueprints
- Site analysis to determine best installation practices
  - Document the site characteristics
  - Discover RF interferences
  - Define equipment quantity and placement
  - Define infrastructure needs
- Interview network administrator
  - Identify the purpose of the WLAN
  - Determine business requirements
- Test and revise draft network design



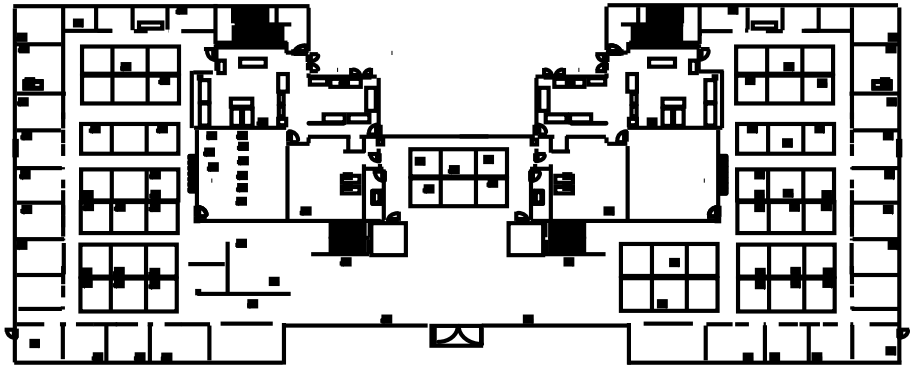
Floor Plan

IDENTIFY BUSINESS REQUIREMENTS

- What is the coverage
  - indoor and/or outdoor requirements
- What are throughput and capacity expectations and/or requirements
- Identify number of current wireless users
  - Anticipated growth
- What is user mobility, roaming characteristics
  - Continuous connectivity or automatic reconfiguration
- What are the security needs
- What are the IP network requirements
  - Is address translation an option
  - VPN requirements
- Identify application requirements
  - Bandwidth or delay sensitive applications
  - Real-time applications

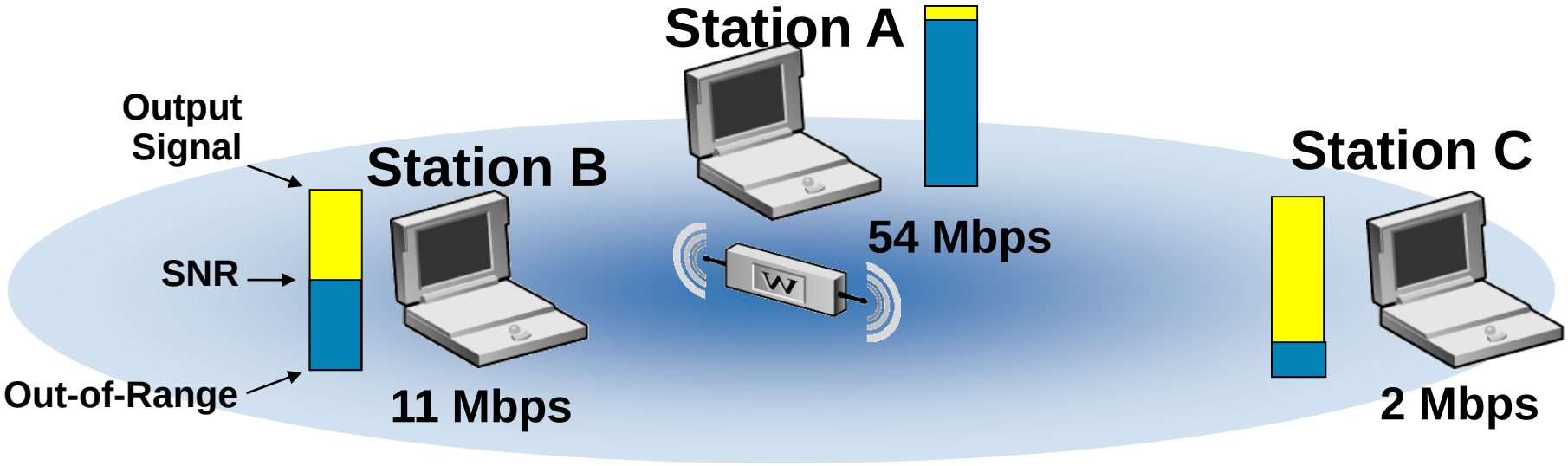
ARCHITECT A DESIGN

- Describe the interconnection of wireless and related wired components
- Identify RF coverage areas
- Identify physical connections required for equipment
- Outline the project plan for deployment
- Administrative characteristics including naming and addressing
- Identify maintenance requirements
- Identify user station and/or software requirements



DESIGN CONSIDERATIONS - RANGE

- Inversely proportional to data rate
- Affected by noise and interference
- Obstructions affect range or shape of coverage area



DESIGN CONSIDERATIONS - ANTENNAS

- Antennas affect the shape of the coverage area
  - Better manage coverage around obstacles
  - To isolate adjacent coverage areas such as outdoor access
- May boost the signal strength increasing data rate and range
- Can be used to correct RF signaling impairments such as multipath and reflection

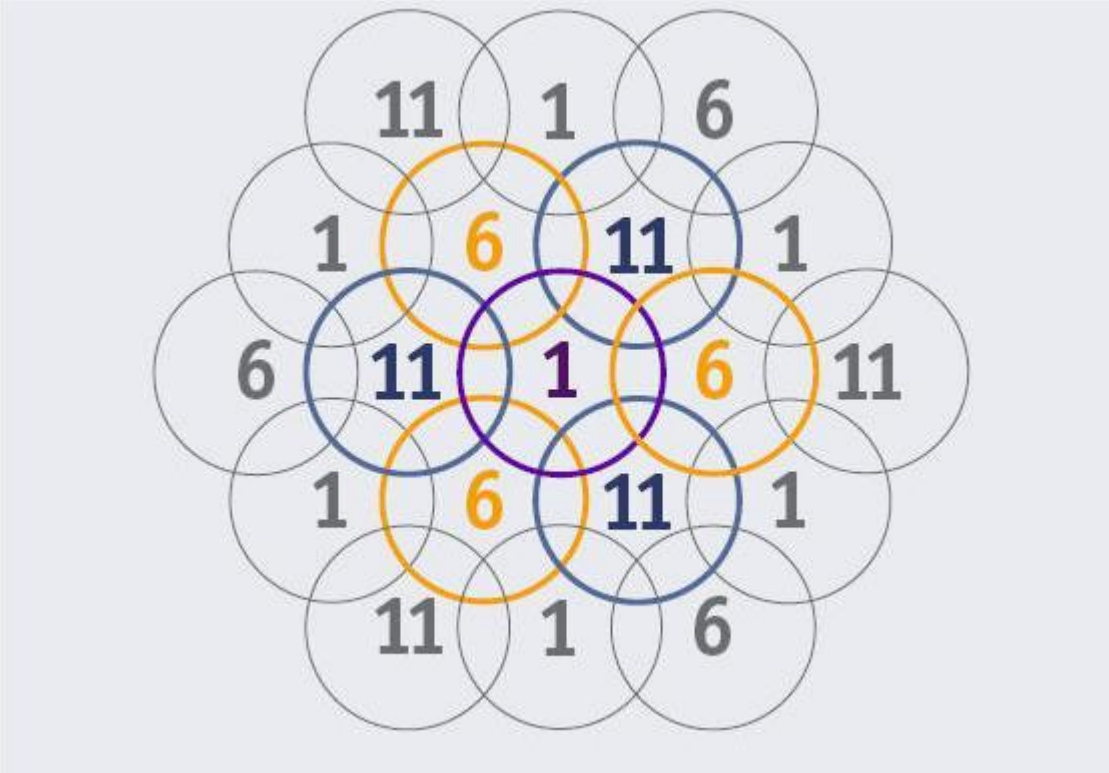
Omni

Dipole

Patch

Yagi

DESIGN CONSIDERATIONS - CHANNEL ALLOCATION



Cisco | Networking Academy®
Mind Wide Open™

MUCHAS GRACIAS

CONSTRUIMOS FUTURO