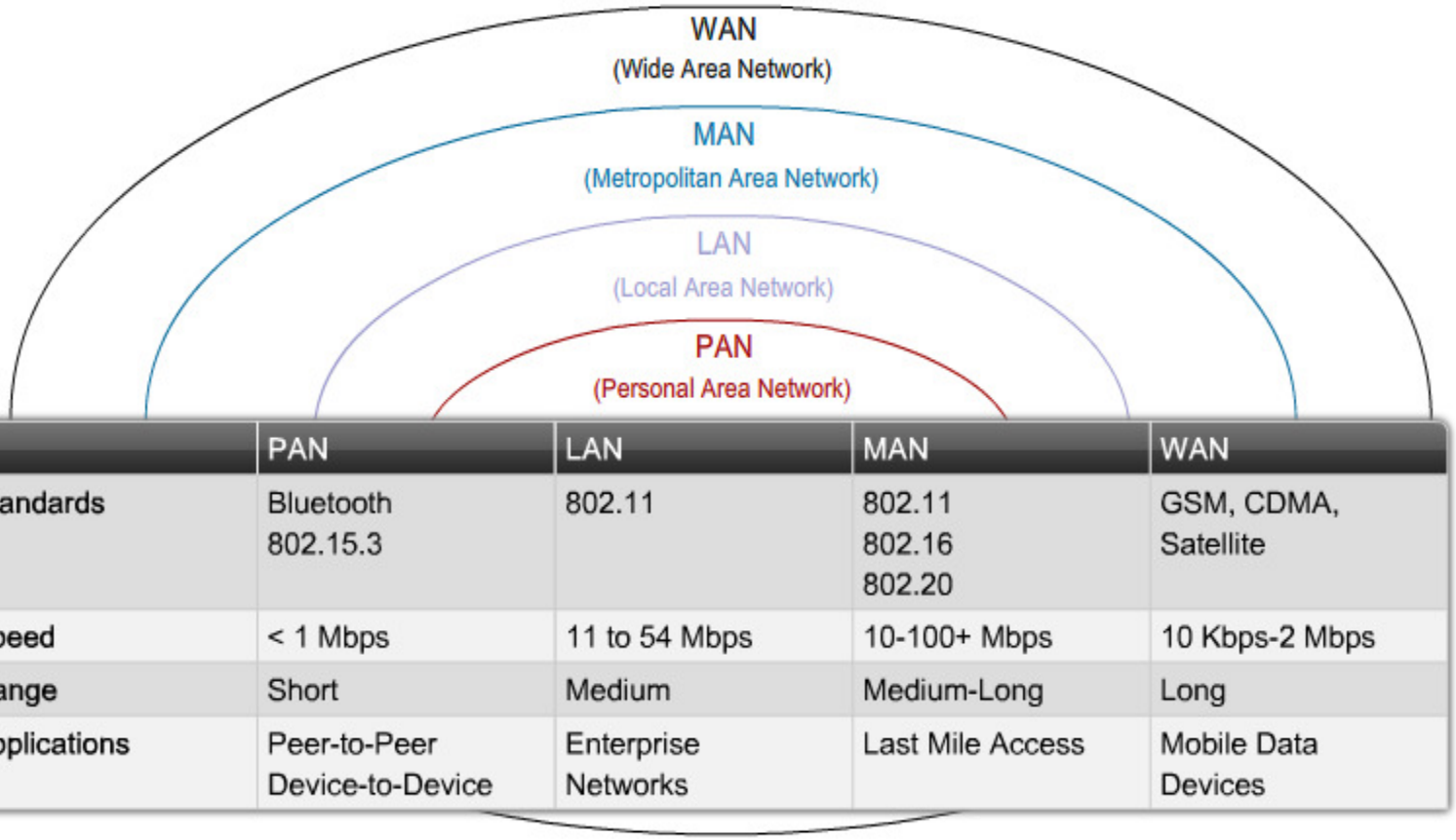
Basic wireless Concepts and Configuration

Chapter 7



	PAN	LAN	MAN	WAN
Standards	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Speed	< 1 Mbps	11 to 54 Mbps	10-100+ Mbps	10 Kbps-2 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise Networks	Last Mile Access	Mobile Data Devices

Orginizations

- ITU-R
  - Regulates RF bands
- IEEE
  - Regulates how RF is modulated

- Wi-Fi
  - Non-profit
  - Ensures vendor interoperability

802.11

	802.11a	802.11b	802.11g		802.11n
Band	5.7 GHz	2.4 GHz	2.4 GHz		Unconfirmed Possibly 2.4 and 5 GHz bands
Channels*	Up to 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Data Rates	Up to 54 Mbps	Up to 11 Mbps	Up to 11 Mbps	Up to 54 Mbps	Speculated to be 248 Mbps for two MIMO streams
Range	~150 feet or 35 meters	~150 feet or 35 meters	~150 feet or 35 meters		~230 feet or 70 meters
Release Date	October 1999	October 1999	June 2003		Expected in 2008
Pros	Fast, less prone to interference	Low cost, good range	Fast, good range, not easily obstructed		Very good data rates, improved range
Cons	Higher cost, shorter range	Slow, prone to interference	Prone to interference from appliances operating on 2.4 GHz band		

- 802.11n – Released October 2009

Modulation

- DSSS
  - Direct Sequence Spread Spectrum
  - 802.11b + 802.11g
  - Simpler than OFDM
- OFDM
  - Orthogonal Frequency Division Multiplexing
  - 802.11a + 802.11g
- MIMO
  - Multi input Multi output
  - 802.11n

Components

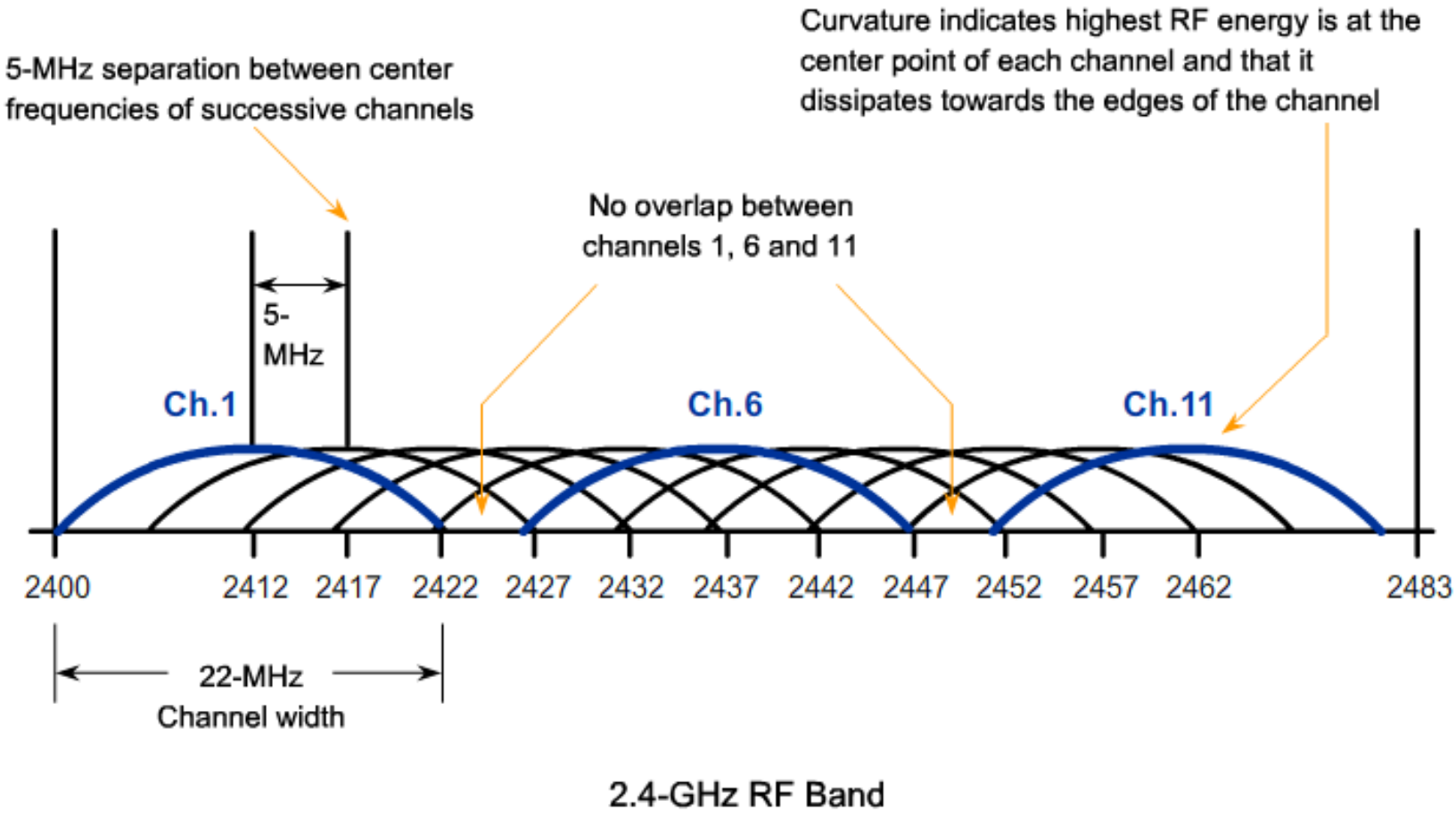
- Wireless NIC
  - Connects to an Access point
- Access point
  - Connects wireless Clients to a LAN
  - Acts like a hub
  - RF is a shared media

CSMA/CA

- Carrier Sence Multiple Access / Collision Avoidance
- Coordinates who can send traffic

- RTS + CTS
  - Request To Send
  - Clear To Send
  - Negotiation between AP and client about when to send
  - Helps with Hidden node problems

Channels


5-MHz separation between center frequencies of successive channels
Curvature indicates highest RF energy is at the center point of each channel and that it dissipates towards the edges of the channel
No overlap between channels 1, 6 and 11
5-MHz
Ch.1
Ch.6
Ch.11
2400
2412
2417
2422
2427
2432
2437
2442
2447
2452
2457
2462
2483
22-MHz Channel width
2.4-GHz RF Band

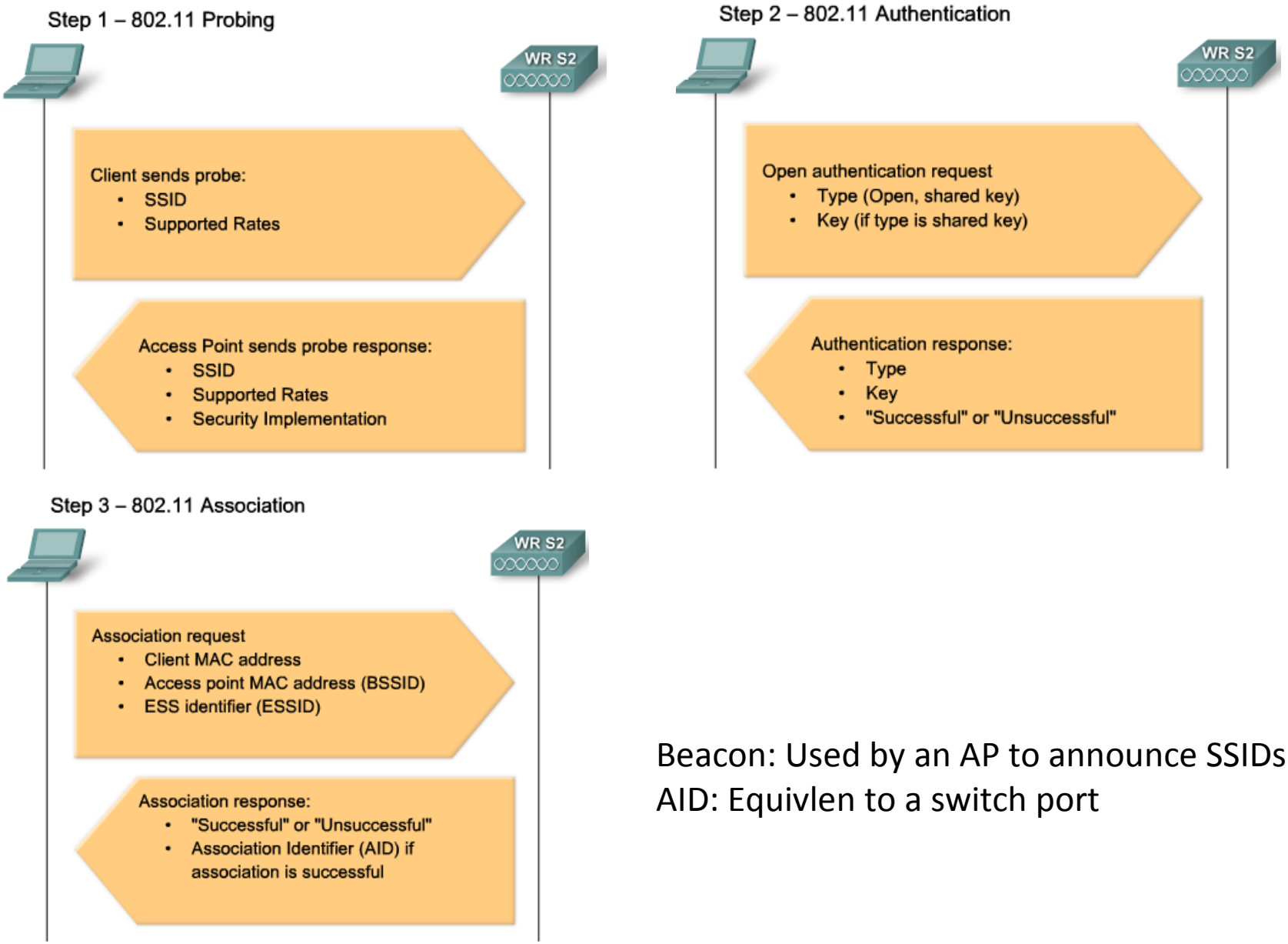
Configuration parameters

- Mode
  - WLAN protocols: 802.11a,b,g,n
  - Mixed mode: 802.11b+g
- SSID
  - Shared Service Set Identifier
  - Identification of wireless networks
  - Broadcast or hidden
- Channel
  - Use non-overlapping channels:

Topologies

- Ad hoc
  - IBSS: Idependent Basic Service Set
  - Client to Client
- Infrastructure mode
  - Single AP
    - BSS: Basic Service Set
    - Coverage area: BSA – Basic Service Area
  - Multiple AP's with the same SSID
    - ESS: Extended Service Set
    - Coverage Area: ESA – Extended Service Area
    - BSSID: The Mac address of the AP is used to differentiate between them
    - 10 – 15 % overlap in AP coverage, non-overlapping channels

Association



Beacon: Used by an AP to announce SSIDs

AID: Equivlen to a switch port

Authentication

- Open authentication
  - No authentication
- Shared key
  - WEP: Wired Equivalency Protection
  - Not recommended

Design

- Position access points above obstructions.
- Position access points vertically near the ceiling in the center of each coverage area, if possible.
- Position access points in locations where users are expected to be.
- Use non-overlapping channels
- 10-15% overlap in coverage area
- AP power settings towards outside walls

Threats

- War drivers
  - People who use open networks
- Hackers(Crackers)
  - People who crack WEP keys
- Rouge Access points
  - Unathorized Aps
  - Usually installed by users

- MITM
  - Man in the Middle
  - Attacker inserts himself between the target and the gateway
  - Mitigation:
    - IPS: Intrusion Prevention system
      - Identifies abnormal traffic
    - Authentication of users

- DoS
  - Denial of Service
  - Flooding of CTS
  - Massive amounts of disassiociate commands

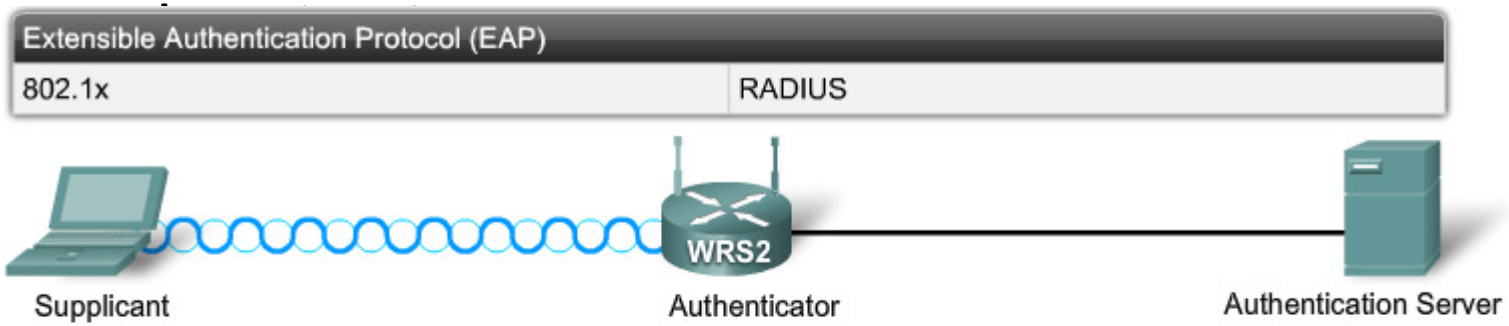
Security protocols

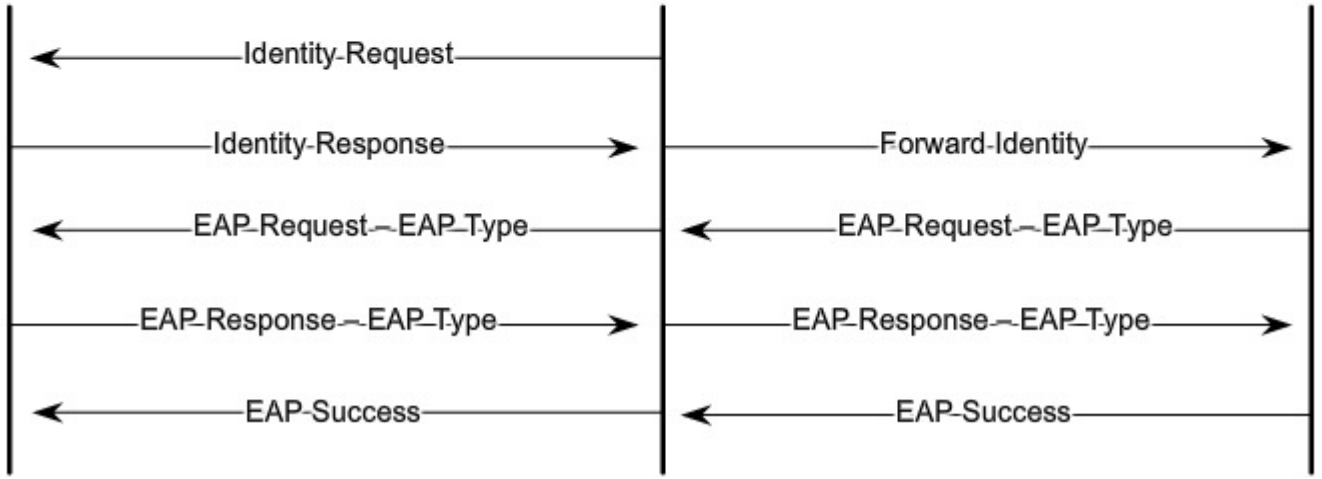
Open Access	First Generation Encryption	Interim	Present
SSID	WEP	WPA	802.11i/WPA2
• No encryption • Basic authentication • Not a security handle	• No strong authentication • Static, breakable keys • Not scalable	• Standardized • Improved encryption • Strong, user-based authentication (e.g., LEAP, PEAP, EAP-FAST)	• AES Encryption • Authentication: 802.1X • Dynamic key management • WPA2 is the Wi-Fi Alliance implementation of 802.11i

Mac address filtering and SSID cloaking is not considered secure by them selves

EAP

- Extensible Authentication protocol
  - Blocks all traffic, except Eap until successful





Encryption

- TKIP
  - Temporal Key Intergrity Protocol
  - WPA
  - Encrypts layer 2 payload
  - Integrity check
- AES
  - Advanced Encryption Standard
  - WPA2
  - Adds to the functionality of TKIP
    - Sequence numbers
    - Detection of nonencrypted data