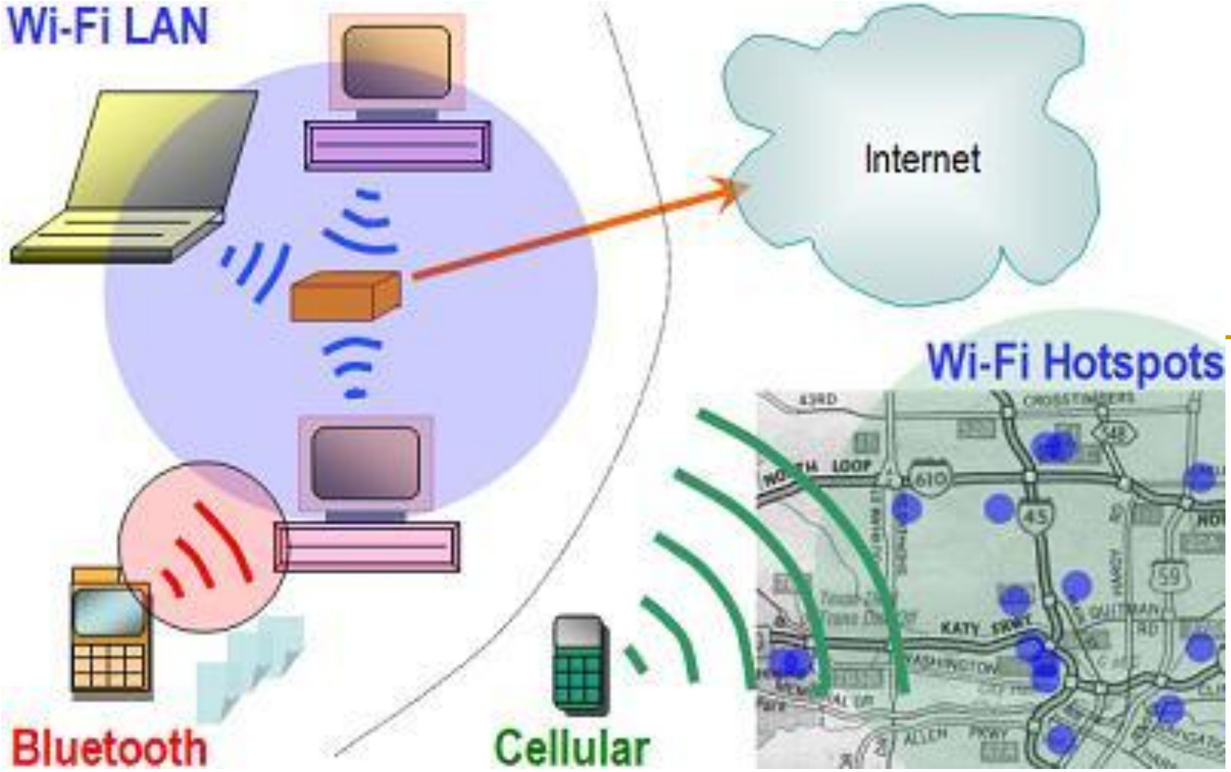
Wireless Networking Basics



Ed Crowley

2017

Today’s Topics

- Wireless Networking
  - Economic drivers & Vulnerabilities
- IEEE 802.11 Family
  - Operational Modes
  - Wired Equivalent Privacy (WEP)
  - WPA and WPA2
- Authentication Protocols
- WLAN Threats
- Wireless Auditing (Hacking) Tools
- Securing WLANs
- Bluetooth and Infrared Overview
- WiMax IEEE 802.16

Wireless Communications

Information transmission without physical cables.

- Radio
- Microwave
- Infrared
- Laser
- Other

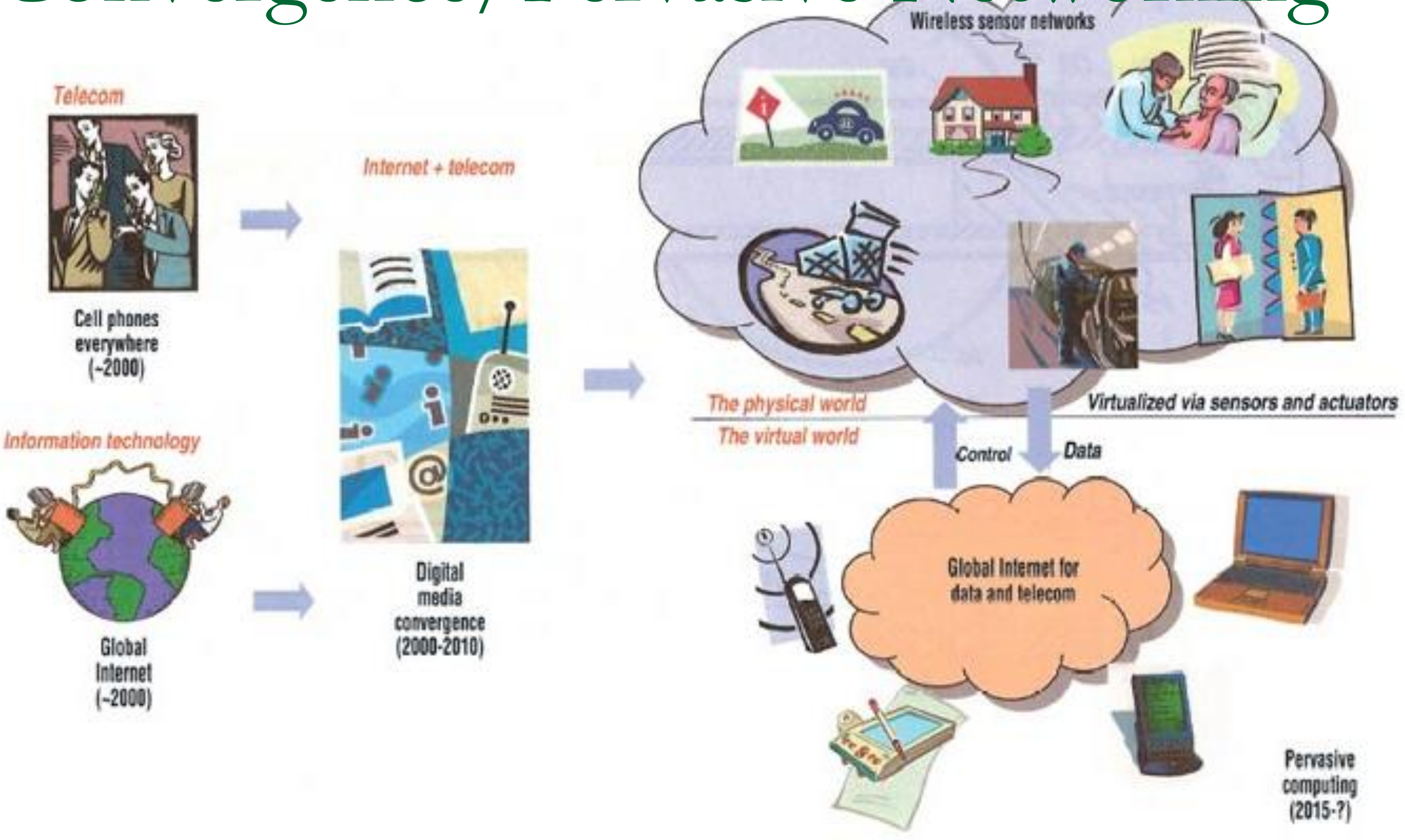
Common examples include

- Cell phones…
- 802.11 networking …

In the future, will they merge into one pervasive network?

- Any difference between a TCP/IP packet from a cell phone and a TCP packet from a computer?

Convergence/Pervasive Networking


Telecom
Cell phones everywhere (~2000)
Information technology
Global Internet (~2000)
Internet + telecom
Digital media convergence (2000-2010)
Wireless sensor networks
The physical world
The virtual world
Virtualized via sensors and actuators
Control
Data
Global Internet for data and telecom
Pervasive computing (2015-?)

1. Global use of cell phones and the Internet will converge to deliver wireless sensor networks that tie the physical and virtual worlds with pervasive computing.
(Courtesy of Rutgers University's WINLAB)

Wireless Growth Drivers

1. Convenience
2. Cost

Dynamic Attributes

- Gilder's Law
  - Total bandwidth of communication systems triples every twelve months.
- Metcalfe's Law
  - Value of a network is proportional to the square of the number of nodes.
    - As a network grows, the value of being connected to it grows exponentially, while the cost per user remains the same or reduces.
- Moore’s Law
  - With time, hardware gets faster, cheaper, and more reliable.

Wireless Vulnerabilities

- At home, your next door neighbor, with a UHF scanner, may listen to your cordless phone calls.[1]
- At the coffee shop, person next to you might sniff your wireless connection. (MiM Attack)
  - Stealing your credit card numbers, passwords, Facebook credentials ...

Conclusion

- Open broadcast infrastructures increase both ease of use and vulnerability.

1. For the last decade or so, it has been illegal for a nongovernmental person to purchase a scanner with these capabilities… Prior to that, these receivers were legal…

Governmental Regulations

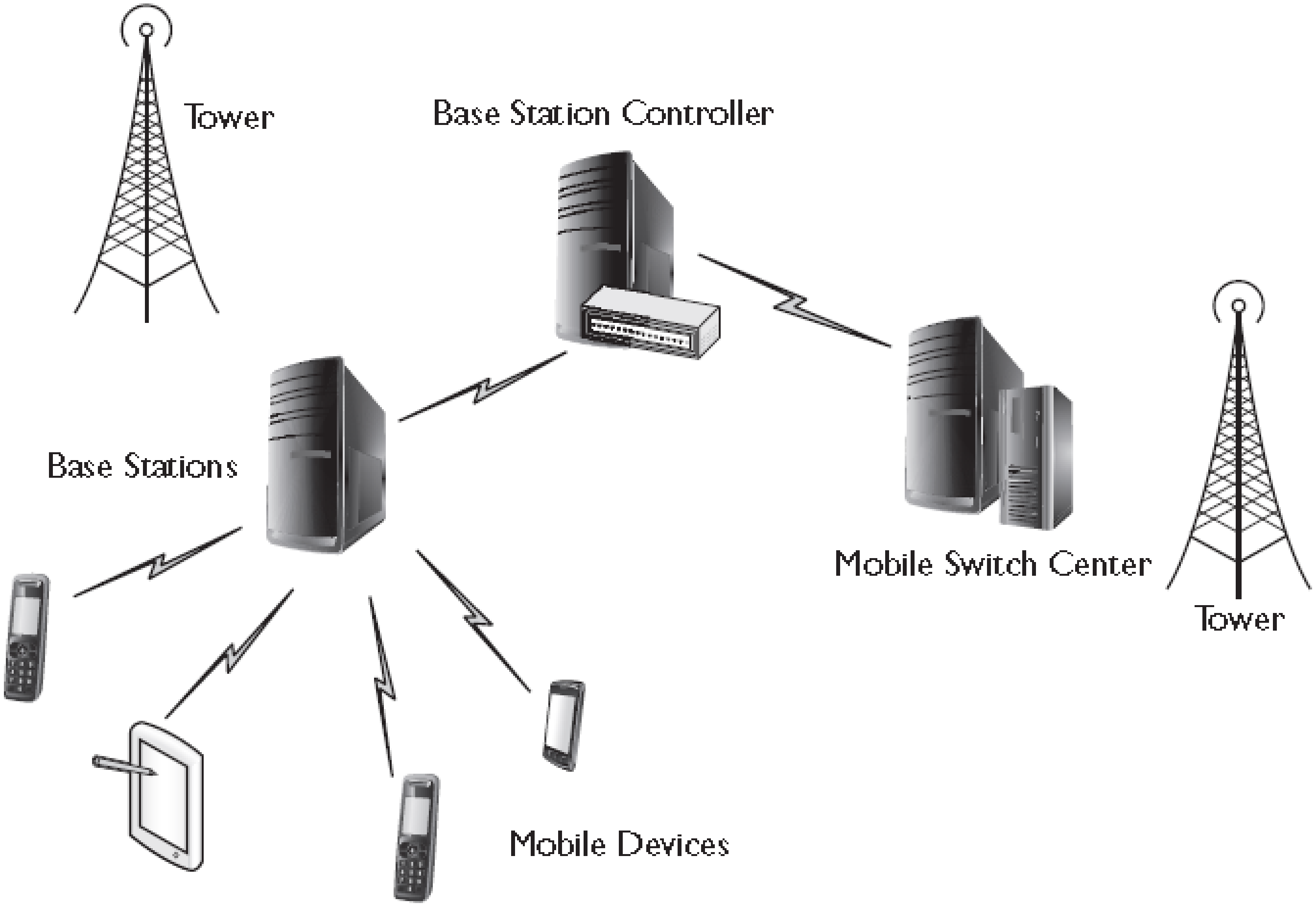
- In US, electromagnetic frequencies used for communications are FCC regulated.

http://wireless.fcc.gov/index.htm?job=rules_and_regulations

- Governmental regulation means:
  - Wireless systems in different countries may operate on different frequencies
  - Allocated wireless frequencies in one country may not match allocated frequencies in another country.

802.11 Utilizes ISM & U-NII Bands

- 802.11 b, g, n utilize ISM bands
    1. Industrial
    2. Scientific
    3. Medical
  - In general, communications equipment must accept any interference generated by ISM equipment.
- 802.11a operation falls under the ‘National Information Infrastructure’ (U-NII) mandate
    - 5 GHz

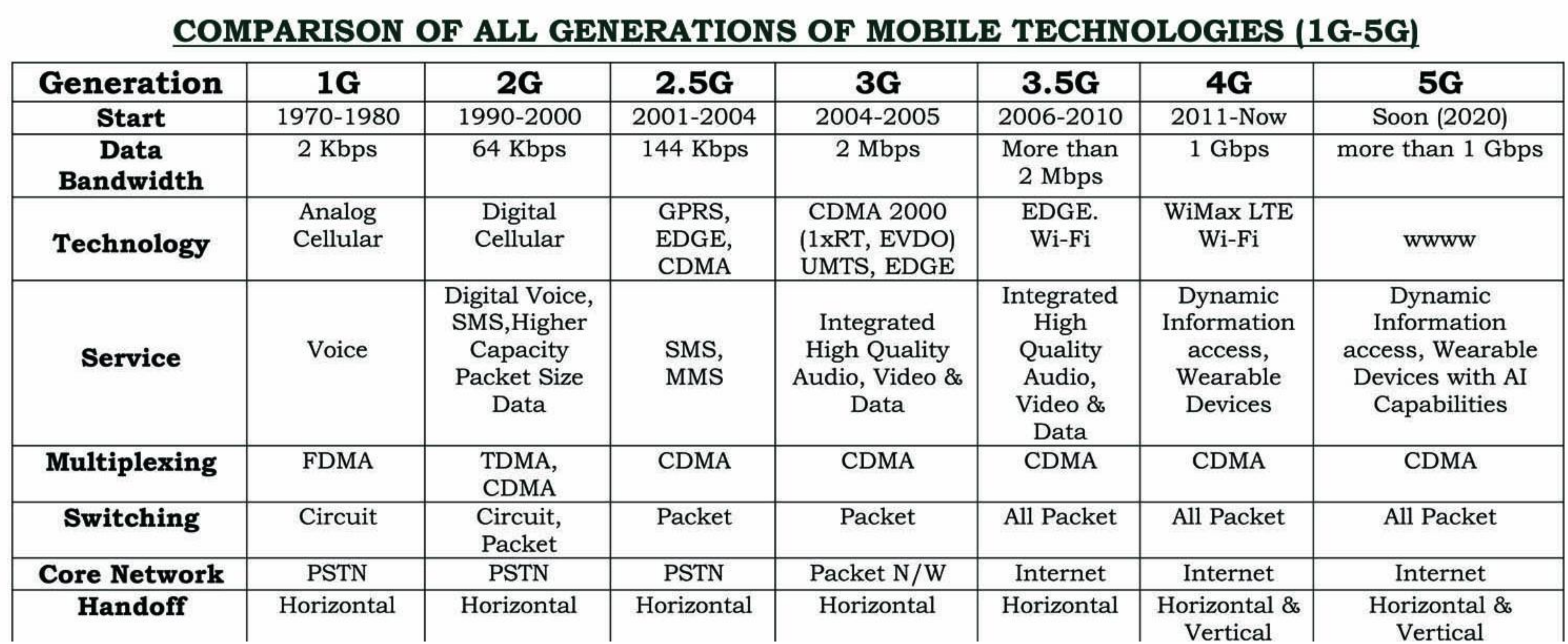


Cellular Infrastructure Components

Cell System Terms

- Base Station
  - Responsible for handling traffic and signaling between a mobile phone and the network switching subsystem.
- Base station controller (BSC)
  - Controls one or more base stations.
  - Functions include radio network management (such as radio frequency control), BTS handover management and call setup.
- Mobile switching centre (MSC)
  - Primary service delivery node for GSM/CDMA.
  - Responsible for routing voice calls and SMS as well as other services (such as conference calls, FAX and circuit switched data).
  - MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during call.

Cell Technology by Generation



COMPARISON OF ALL GENERATIONS OF MOBILE TECHNOLOGIES (1G-5G)

Generation	1G	2G	2.5G	3G	3.5G	4G	5G
Start	1970-1980	1990-2000	2001-2004	2004-2005	2006-2010	2011-Now	Soon (2020)
Data Bandwidth	2 Kbps	64 Kbps	144 Kbps	2 Mbps	More than 2 Mbps	1 Gbps	more than 1 Gbps
Technology	Analog Cellular	Digital Cellular	GPRS, EDGE, CDMA	CDMA 2000 (1xRT, EVDO) UMTS, EDGE	EDGE. Wi-Fi	WiMax LTE Wi-Fi	wwww
Service	Voice	Digital Voice, SMS,Higher Capacity Packet Size Data	SMS, MMS	Integrated High Quality Audio, Video & Data	Integrated High Quality Audio, Video & Data	Dynamic Information access, Wearable Devices	Dynamic Information access, Wearable Devices with AI Capabilities
Multiplexing	FDMA	TDMA, CDMA	CDMA	CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit, Packet	Packet	Packet	All Packet	All Packet	All Packet
Core Network	PSTN	PSTN	PSTN	Packet N/W	Internet	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal	Horizontal & Vertical	Horizontal & Vertical

Millimeter-wave 5G modem coming mid-2018 with 5Gbps peak download
http://arstechnica.com/business/2016/10/qualcomm-5g-x50-modem-millimetre-wave-5g-modem/

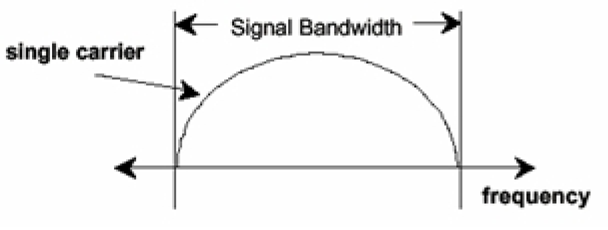
Wireless Networking

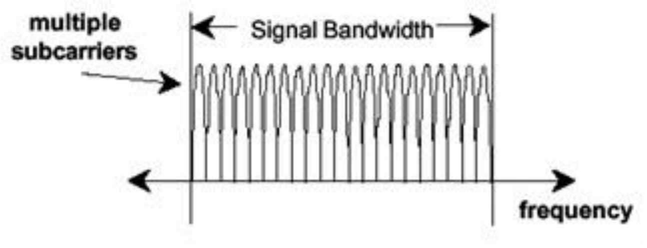
- Spread Spectrum de facto wireless LAN communication standard.
  - Broadcasts signals over a specified frequency range.
  - Originally, military technology developed to provide secure, mission-critical communications.
- Provides limited immunity to interference associated with narrowband systems.

Spread Spectrum RF Technologies

- Different spread spectrum modulation technologies utilized in different Wireless LAN Standards:

1. Direct Sequence Spread Spectrum (DSSS) (802.11b)
2. Orthogonal Frequency Division Multiplexing (OFDM) (802.11 a,g,n) a multi-carrier modulation scheme where data is split up among several closely spaced subcarriers.
3. MIMO--multiple-input multiple-output (802.11 n)





IEEE 802.11 Family

- Wireless LAN (WLAN) standards.
  - 1997, IEEE accepts 802.11 Specification.
  - Specifies an over-the-air interface between:
    - A mobile device wireless client and a base station or
    - Between two mobile device wireless clients.
- Uses Industrial Scientific Medical (ISM) Bands
  - 902-908 MHz
  - 2.4-2.4835 GHz
  - 5.725-5.825 GHz

802.11 Standard Family

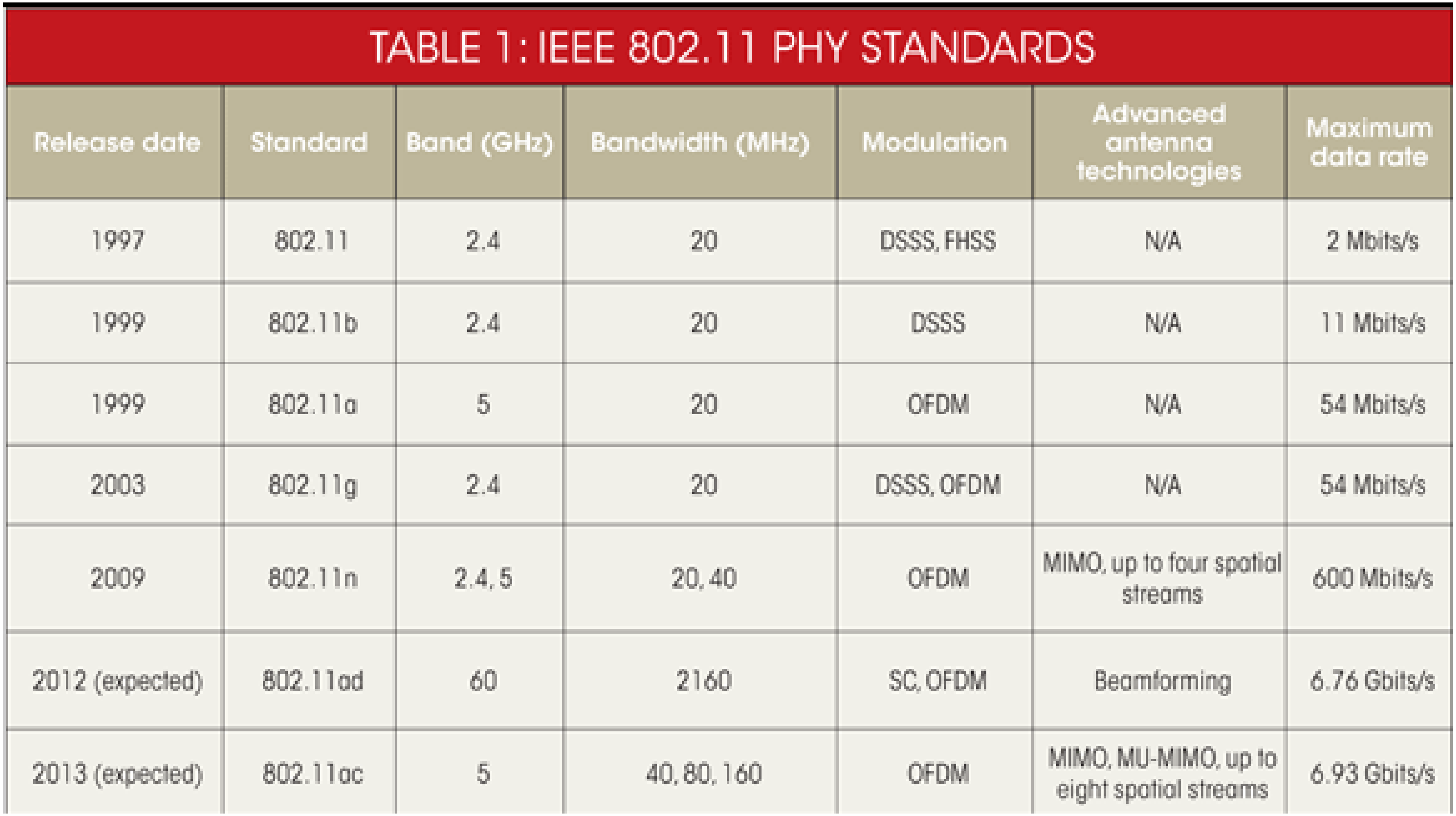
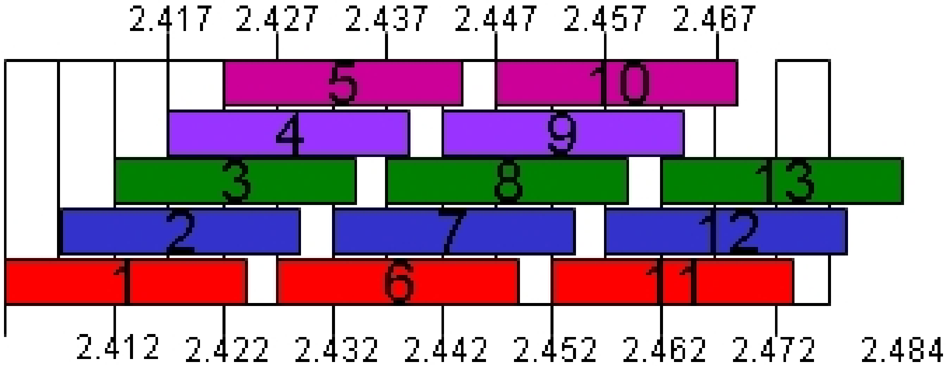


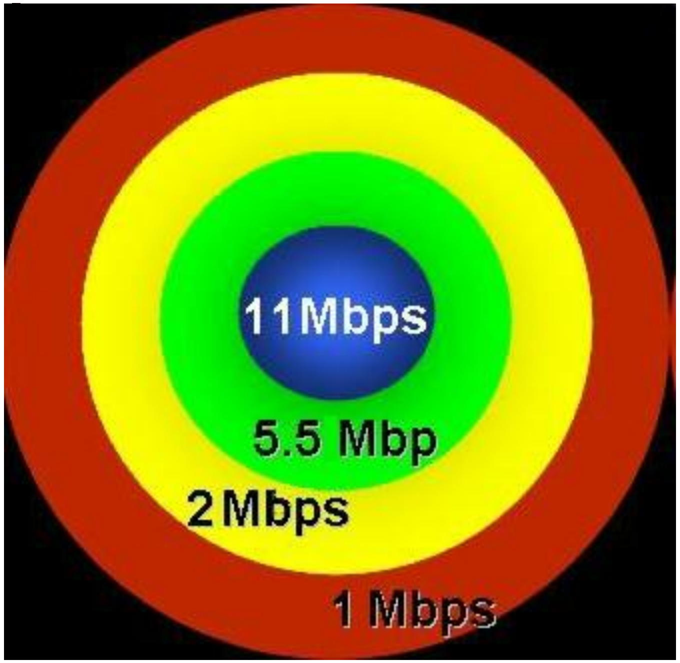
TABLE 1: IEEE 802.11 PHY STANDARDS

Release date	Standard	Band (GHz)	Bandwidth (MHz)	Modulation	Advanced antenna technologies	Maximum data rate
1997	802.11	2.4	20	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4	20	DSSS	N/A	11 Mbits/s
1999	802.11a	5	20	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4	20	DSSS, OFDM	N/A	54 Mbits/s
2009	802.11n	2.4, 5	20, 40	OFDM	MIMO, up to four spatial streams	600 Mbits/s
2012 (expected)	802.11ad	60	2160	SC, OFDM	Beamforming	6.76 Gbits/s
2013 (expected)	802.11ac	5	40, 80, 160	OFDM	MIMO, MU-MIMO, up to eight spatial streams	6.93 Gbits/s

802.11 Channels and Throughputs



Channels



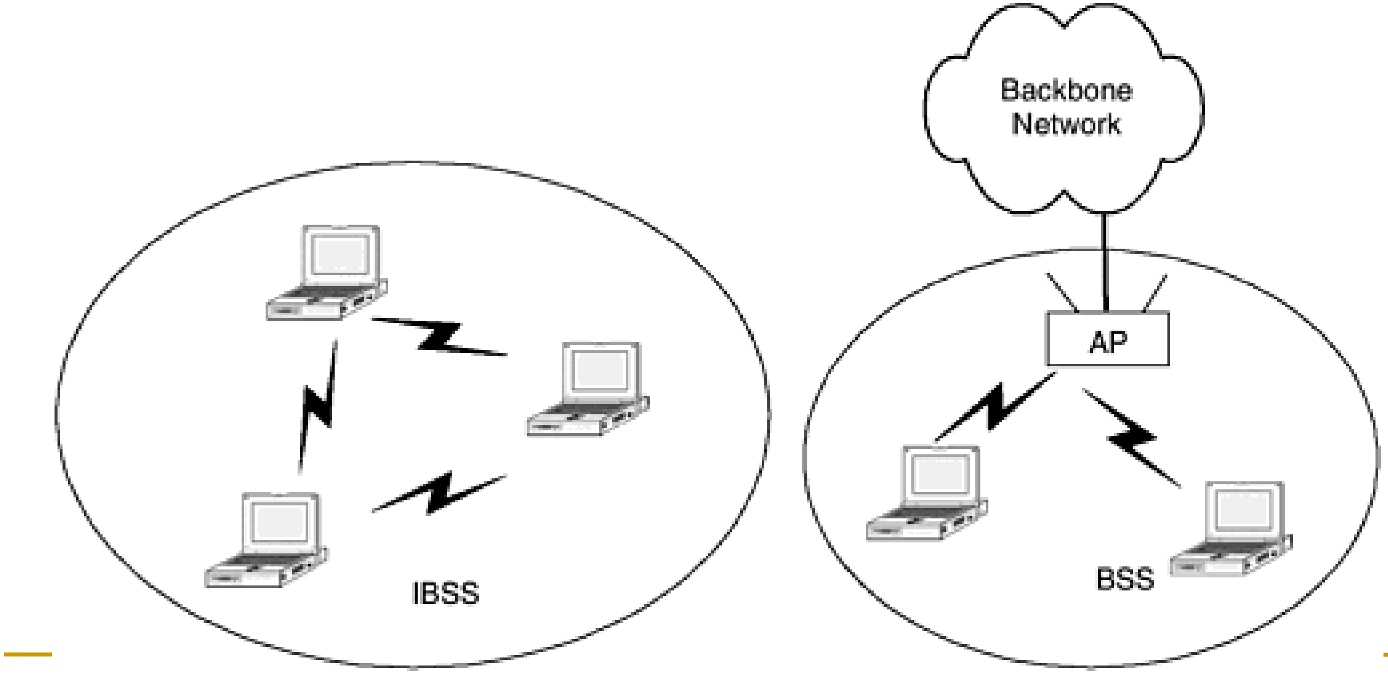
Available Throughputs

IEEE 802.11 Standard

- Specifies physical and data link (media access control (MAC)) network layer attributes.
- Physical layer responsible for transmission of data among nodes.
  - Can use direct sequence spread spectrum, frequency hopping spread spectrum or infrared pulse position remodulation.
- MAC Layer consists of a set of protocols responsible for maintaining order on the shared medium.

Service Sets

- A Basic Service Set (BSS) without an Access Point (AP) called an ad hoc network
- A BSS with an AP is called an infrastructure network.

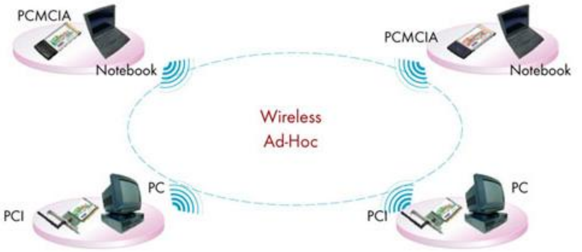


When using multiple APs called an Extended Service Set (ESS)

MAC Layer Services

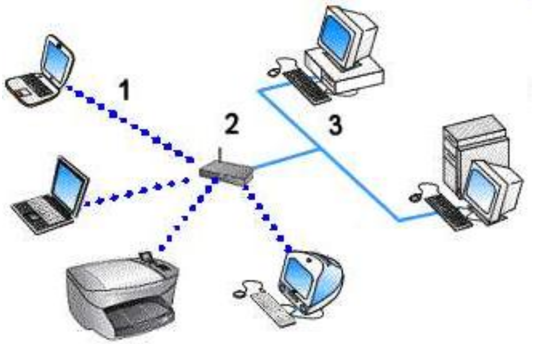
- Data transfer
  - CSMA/CA Carrier Sense Multiple Access/Collision Avoidance
    - Contrast with wired CSMA/CD
- Association
  - In Infrastructure mode, establishes wireless links between wireless clients and access points
- Re-association
  - Takes place when a wireless client moves from one Basic Service Set (BSS) to another
- Authentication
  - Proves a client's identity with 802.11 Wired Equivalent Privacy (WEP)
  - Shared key configured into the access point and each client.

802.11 WLAN Operational Modes



Ad Hoc Mode

- Denotes a mesh wireless network with computers connected as peers.



Infrastructure Mode

- Centered around a wireless access point (WAP).
- A WAP is a centralized wireless device that controls wireless traffic.

Original 802.11 MAC Layer Services

Confidentiality, Privacy???

- By default, data transfers in the clear.
- Optional WEP encryption originally
  - RC-4 in output feedback mode
    - Secret key shared between mobile and base stations …
    - Flawed implementation …
  - Using CRC-32 checksum another vulnerability
  - No protection against replay attacks
    - Aireplay can send fake authentication packets to the AP

Association Frames

- Before communicating, mobile wireless clients and access points must establish a relationship, or an association.

Three Possible States

1. Unauthenticated and unassociated
2. Authenticated and unassociated
3. Authenticated and associated

Service Set Identifier (SSID) and Basic Service Set

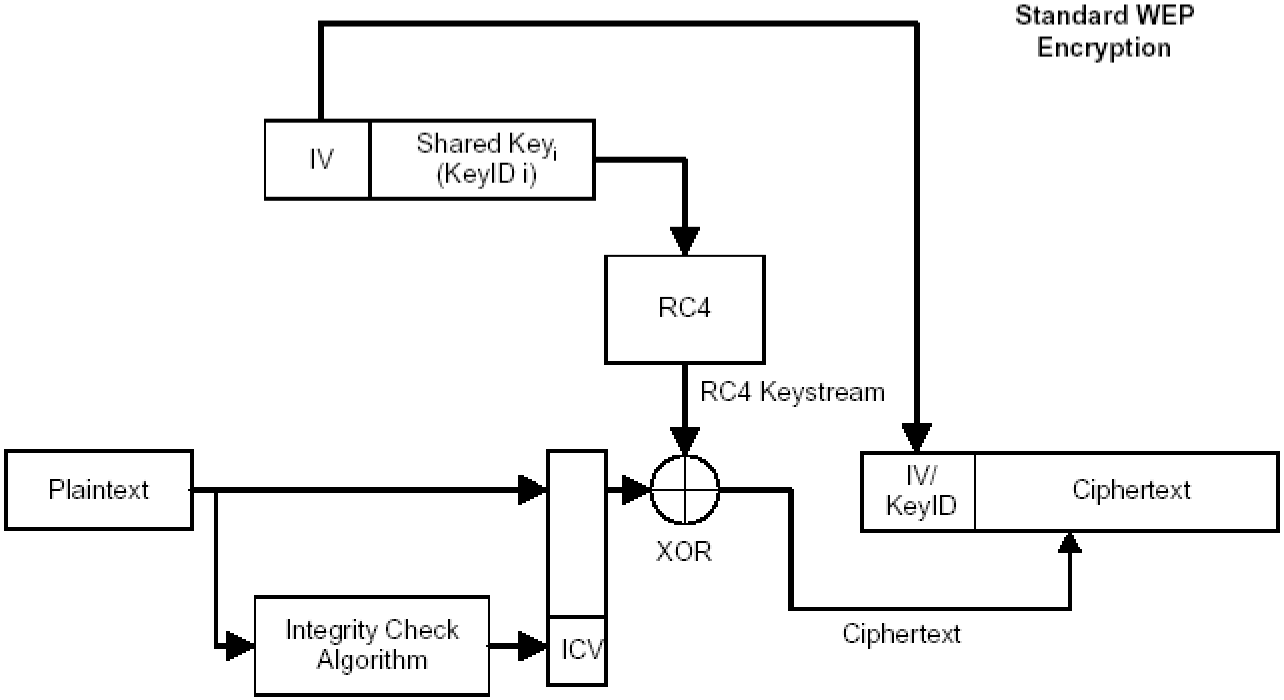
- Channel and service set identifier must be configured for a WLAN to function.
- SSID is an alphanumeric string that differentiates networks operating on the same channel and functions as a unique identifier.
- In infrastructure mode one access point (AP) together with all associated stations (STAs) is called a Basic Service Set (BSS).
  - Each BSS is identified by an BSSID.
  - In infrastructure mode, a basic BSS consists of at least one AP and one STA.....

Wired Equivalent Privacy (WEP)

- Original mechanism for securing wireless LANs.
  - Part of original 802.11 standard.
  - Utilizes RC 4 stream cipher
- Symmetric same key encrypts and decrypts.
  - To encrypt, keystream X0Red with plaintext.

(Flawed) RC-4/WEP Encryption Process

Figure 1. Standard WEP Encryption Process



24 bit IV passed in open

WEP Goals

Access control

- Prevents users lacking WEP key from gaining network access

Privacy (Confidentiality)

- Protect wireless LAN data streams by encrypting them
  - Allowing decryption only by users with correct WEP keys

WEP Authentication Methods

- Client cannot participate in a wireless LAN until after client is authenticated.

Two types

1. Open
   - Open, the default authentication protocol, authenticates any request.
2. Shared Key
   - Considered a null authentication

Shared Key Authentication

- Utilizes shared secret key to authenticate station to AP.
  - Uses:
    - Challenge and response
- Anyone without assigned key is denied access.
  - Same shared key encrypts and decrypts
    - Note, this vulnerability

WEP Key Management

- Shared key resides in each station’s Management Information Database (mib).

Two schemes

1. A set of four default keys are shared by all stations, including the wireless clients and their access points.
2. Each client establishes a key mapping relationship with another station

Popular WEP Cracks

- Passive attacks that decrypt traffic based on statistical analysis
- Active attacks that inject new traffic from unauthorized mobile stations
  - Based on known plaintext (ARPs)
- Active attacks that decrypt traffic based on tricking the access point
- Dictionary-building attacks that, after an analysis of an appropriate volume of traffic, allow real-time automated decryption of all traffic.

WPA and WPA2

- WPA instant response to WEP vulnerabilities
- WPA2 part of 802.11i standard
- Attempts to address WEP’s vulnerabilities
  - Consists of two encryption approaches:
    1. TKIP/MIC
    2. AES-CCMP

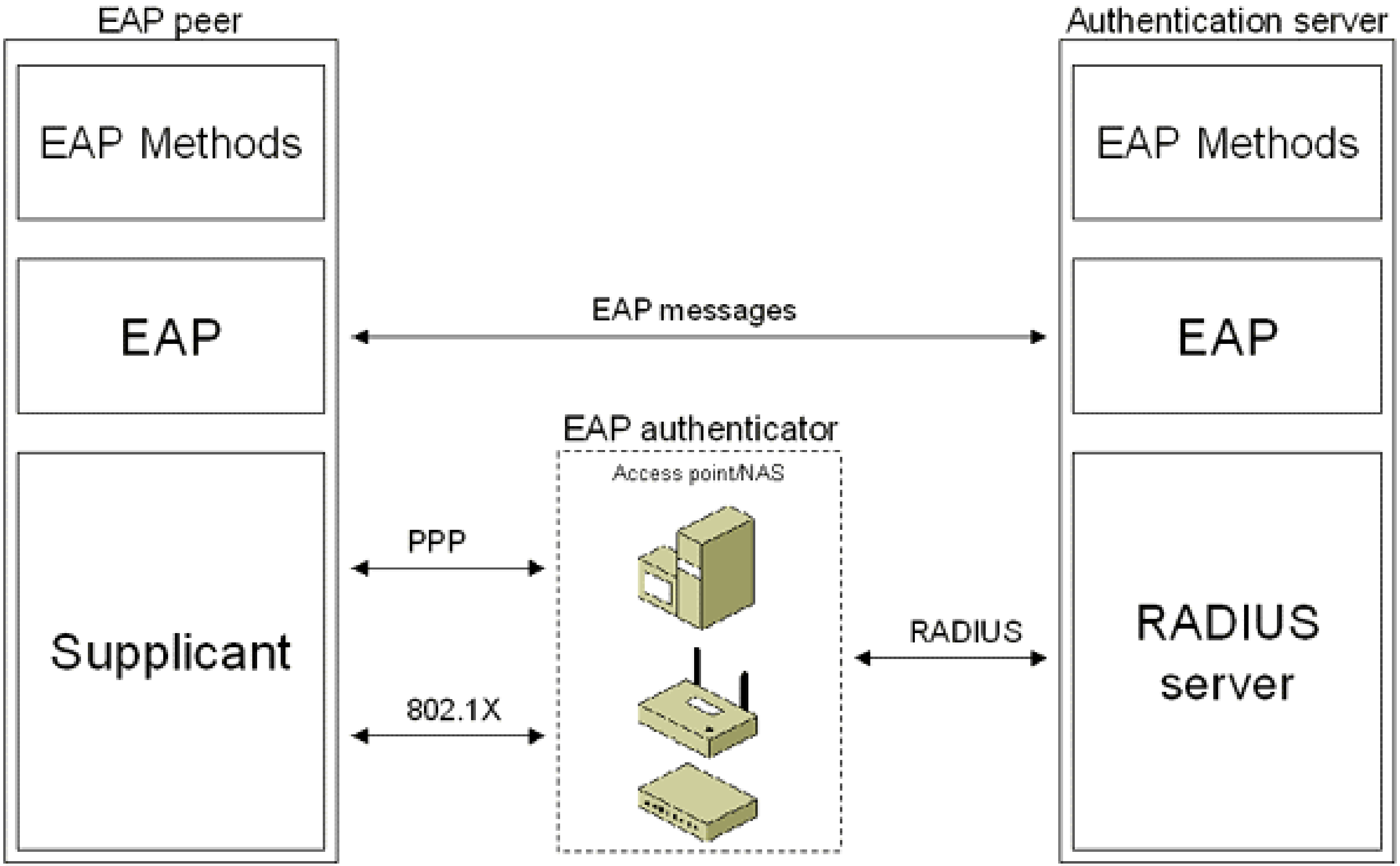
802.11 Supports RADIUS

- Remote centralized authentication, authorization, and accounting (AAA) services.
- Until the client is authenticated, 802.1x allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected.
- After successful authentication, normal traffic can pass through the port.
- Also supports EAP, EAP-TLS, and LEAP.

EAP and LEAP

- Extensible Authentication Protocol (EAP) is an authentication framework that provides some common functions and negotiation of authentication methods (called EAP methods).
- LEAP is a proprietary EAP method that uses a modified version of MS-CHAP.
  - Lightweight Extensible Authentication Protocol (LEAP) developed by Cisco Systems.
  - Cracked early 2004, when Joshua Wright released ASLEAP.

Extensible Authentication Protocol



PEAP

Designed to correct some EAP deficiencies, Protected Extensible Authentication Protocol (PEAP), a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.

- Jointly developed by Cisco Systems, Microsoft, and RSA Security.
  - aka Protected EAP or PEAP

WLAN Threats

- Denial of Service Attacks
  - Many potential vectors.
    - For example, Microwave ovens operate in 2.4 GHz range
- SSID Problems
  - Default
- The Broadcast Bubble
  - Extends past your building
- War Driving
- Rogue Access Points
- MAC Spoofing defeats MAC filtering

Wireless Auditing Tools

Kismet

- Layer 2 wireless network detector, sniffer, and intrusion detection system.
- Sniffs 802.11 a, b, and g traffic

NetStumbler

- Functions as a high level WLAN scanner.

WEPCrack

- Open source tool for breaking 802.11 WEP secret Keys.

Wireless Auditing Tools

AirCrack

- WLAN and WEP auditing tool.
- Fast tool can crack encryption.

- Tools such as Kismet, NetStumbler, and NetSurveyer can also be used to identify rogue access points.

Securing WLANs

- Includes strategies for MAC address filtering, firewalls or a combination of protocol based or standards based measures.

Standards and Policy Based Solutions

- Address ownership and control of wireless

MAC Address Filtering

- Time consuming, limited effectiveness.

Securing WLANs

SSID Solutions

- If the SSID is set to manufacturers default settings, often means other measures are also at default.
- SSID should not reflect company’s name, division, or products.

Antenna Placement

- Should be incorporated into site survey and site updates

Other Measures

- VLANS
- VPNs
- Wireless RADIUS
- Dynamic WEP Keys

Want Security? Don’t use WEP

- Enable WPA2
- For enterprises, employ a AAA server
- Employ regular scans to find rogue access points.
- Consider network based Intrusion detection on the wireless LAN
- Employ secure logging

TKIP

- Temporal Key Integrity Protocol (TKIP) was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware.

CCMP

- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) was created to replace TKIP and WEP.
- Uses Advanced Encryption Standard (AES) algorithm with a 128-bit key and a 128-bit block.

Bluetooth

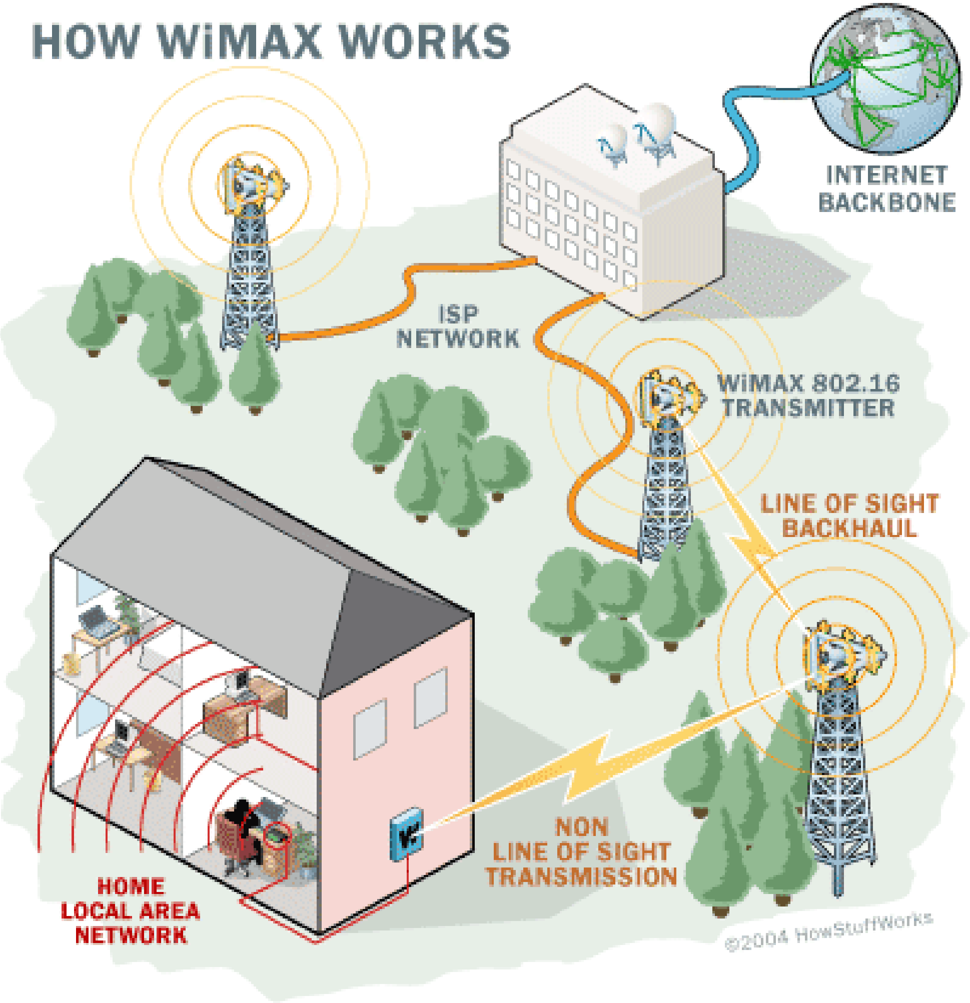
- A simple peer to peer protocol that connects multiple consumer mobile information devices with different functions (cell phones, laptops, printers, cameras,…)
- Whenever any Bluetooth enabled devices come within range, they instantly transfer address information and establish small ad hoc networks between each other.

Bluetooth and Infrared Attributes

- Bluetooth Class 1,2, or 3 creates Personal Area Networks (PANs)
  - Range from 1 to 100 meters…
  - Power from 1 to 100 mw
- Infrared Networking
  - Line of sight
  - Range up to 1 meter
  - Throughput up to 4 Mbps

WiMAX IEEE 802.16

- Worldwide Interoperability for Microwave Access
- Physical and DataLink Standard
- Long (relatively) range system that uses licensed or unlicensed spectrul to deliver network connectivity…



- Complements 802.11

Questions?

Lecture originally based on Chapter 15, Wireless Networking, from the Certified Ethical Hacker Study Guide which you can access online at: http://proquest.safaribooksonline.com.ezproxy.lib.uh.edu/book/certification/ceh/9781118989289

http://proquest.safaribooksonline.com.ezproxy.lib.uh.edu/book/certification/ceh/9781118989289