

The Wi-Fi Boom

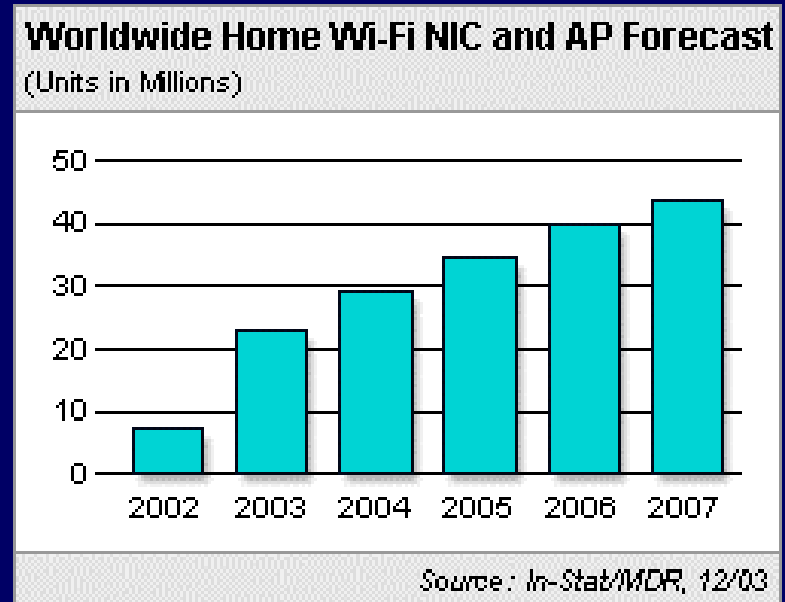
Dr. Malik Audeh
Tropos Networks
March 13, 2004

Outline

- **Wi-Fi has gone mainstream**
- **Background of Wi-Fi/802.11**
- **Technical Details of Wi-Fi**
 - **Physical Layer(s)**
 - **MAC Layer**
 - **Security**
 - **Wi-Fi in different environments**
- **The Future of Wi-Fi**
- **Trends**

Wi-Fi is Everywhere

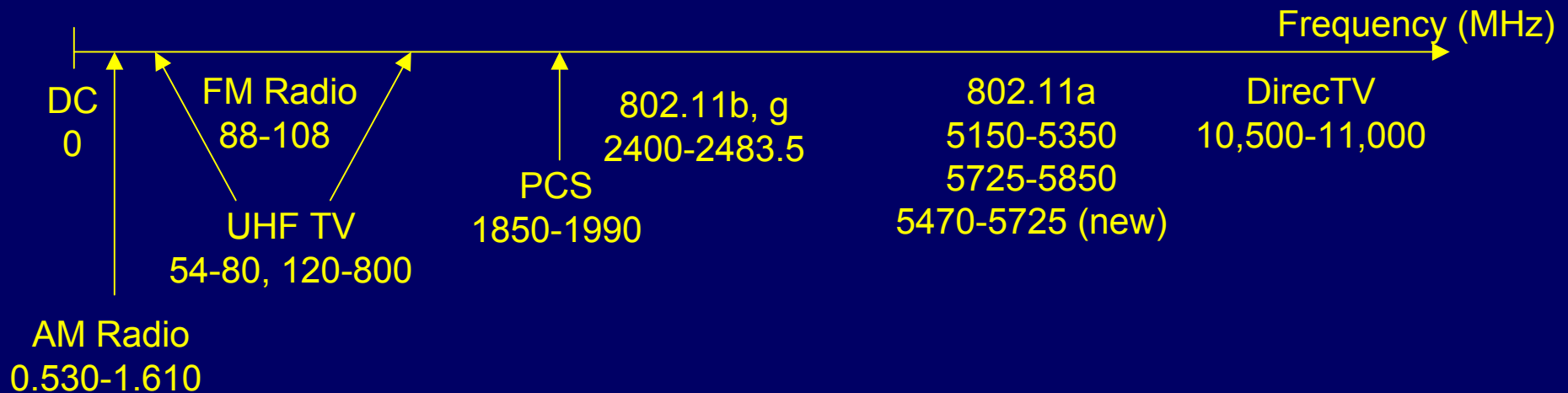
- In the early 90s, the hockey stick curve for WLAN growth was in every publication
- Took until late 90s and early this decade
 - Completion of 802.11 standard
 - Industry alliances (Wi-Fi Alliance, HomeRF)
 - Interoperability
 - The name “Wi-Fi”
 - Component costs
 - End-user need/demand
- Warchalking
- Centrino



Wi-Fi everywhere

- Every major news/business magazine seems to talk about Wi-Fi
 - USA Today Feb. 19, 2004 – once you've used it you'll never go back
- Even with some warts, Wi-Fi is here to stay
 - It's cheap
 - It's easy
 - It's mass-market
 - Everyone loves it
 - It's got room to grow

Electromagnetic Spectrum (not to scale) (not complete)

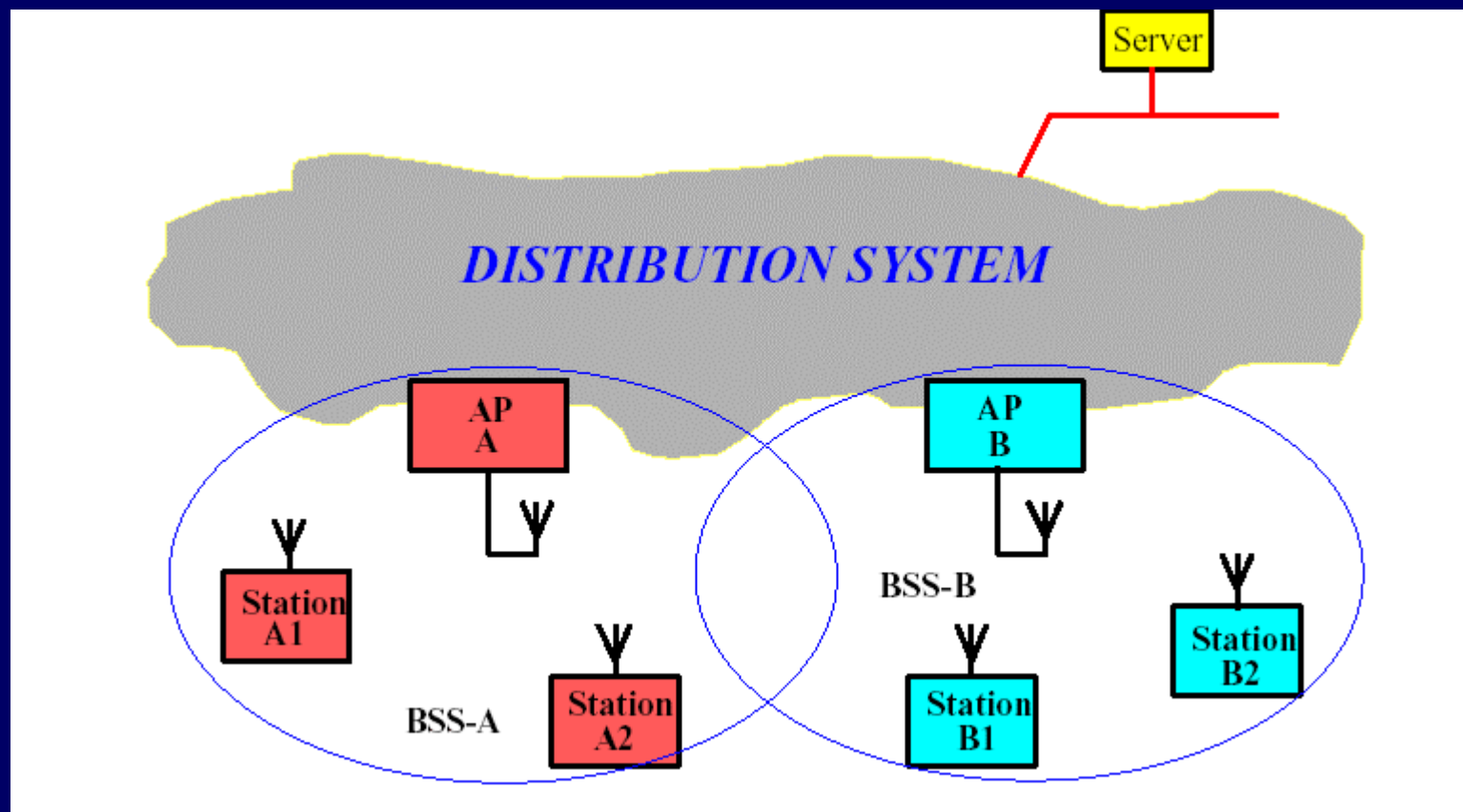


Interference

- Rules of unlicensed band say you cannot CREATE interference beyond legal limits
 - Maximum power allowed differs throughout the world
- But you must ACCEPT any interference that exists in the band
- Examples
 - Other 802.11 traffic
 - Microwave ovens (2.4 GHz)
 - Cordless phones
 - Point-to-point links

Basic Network Topology

- Access Point (AP) and client (a.k.a. end-user, station)



Background of 802.11

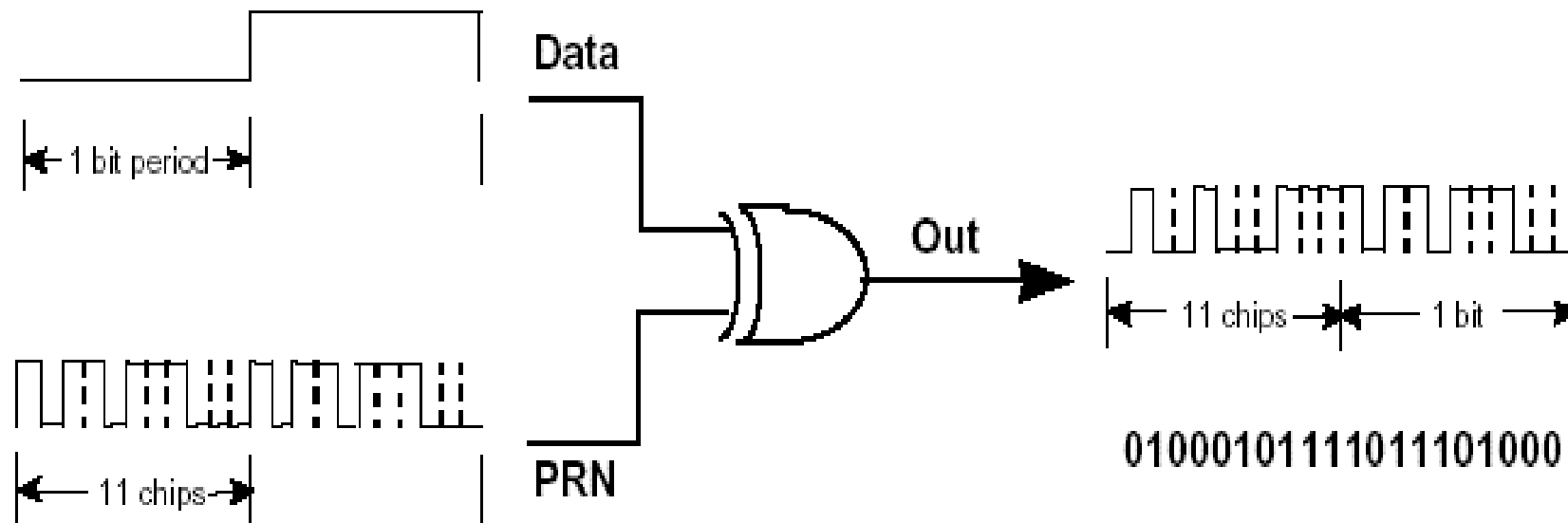
- IEEE standardizes layer 1 and 2 of OSI model
- Creating the first 802.11 standard out of IEEE took 9 years
- Original [“base”] standard 802.11-1999 had the MAC and *two* spread spectrum physical layers with data rates of 1 Mb/s and 2 Mb/s
- Use the same spectrum for transmit and receive
- Amendments since 1999 have added new physical layers, internationalization, operational recommendations

802.11 Physical Layer #1

- **Frequency-hopping spread spectrum**
 - 1 Mb/s and 2 Mb/s data rate (NOT throughput)
 - Signal hops through 26 of 78 possible 1 MHz wide carriers in a pre-determined algorithm throughout the band

802.11 Physical Layer #2

- **Direct-sequence spread-spectrum**
 - 1 Mb/s and 2 Mb/s data rate (NOT throughput)



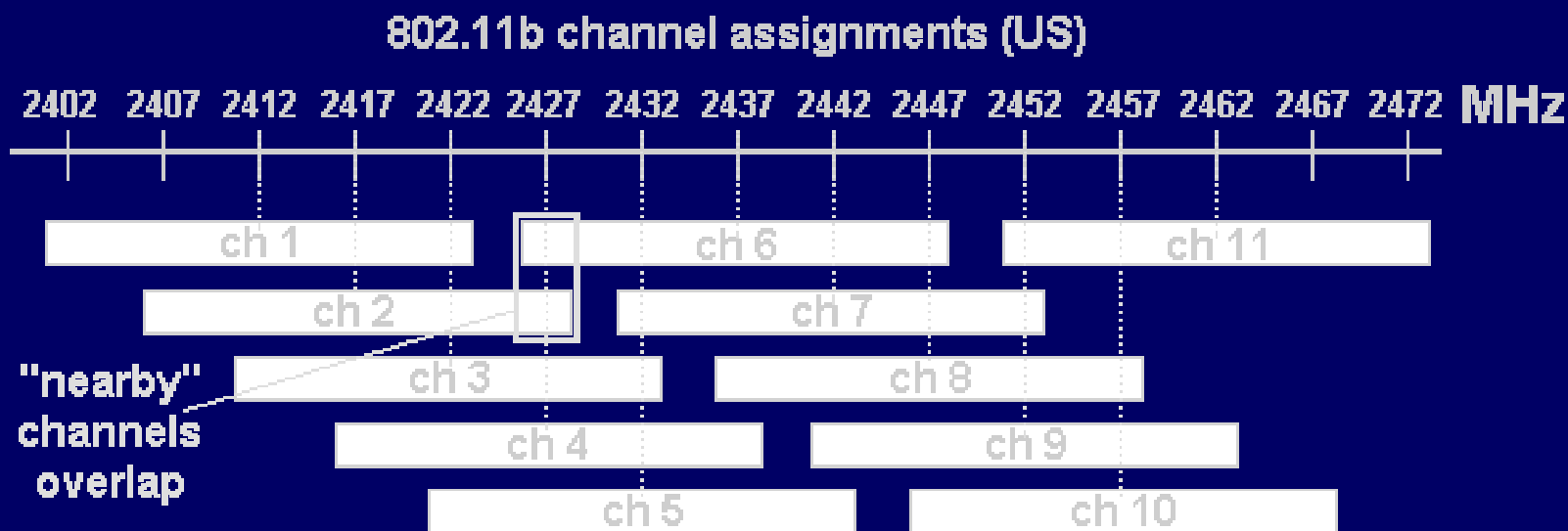
11 Bit Barker Code (PRN):

1 0 1 1 1 0 1 0 0 0

01000101111011101000

802.11b (Today's Majority)

- Also finalized in 1999
- Direct sequence spread-spectrum with data rates of 11, 5.5 Mb/s over 22 MHz channel bandwidth
- Three total non-overlapping channels in 83.5 MHz



Other Physical Layers

- **802.11a**
 - 1999
 - Uses Orthogonal Frequency Division Multiplexing (OFDM)
 - 5 GHz spectrum, can vary widely around the world
 - Channel bandwidth of 20 MHz
 - Data rates of 54, 48, 36, 24, 18, 12, 9, 6 Mb/s
 - Has not achieved popularity of 802.11b
 - Propagation difference
 - Cost
 - 802.11b is good enough for many applications today
 - Advantageous in business applications

802.11g

- **Finalized in June 2003**
- **Same spectrum (2.4 GHz) and channels as DSSS and 802.11b**
- **Uses OFDM to achieve improved throughput**
- **Fully backward compatible w/ 11b**
- **Shared networks are allowed**
 - **Interleaved operation**
 - **Major throughput impact --- a single 11b client cuts 11g throughput by 50%**

802.11 Media Access Layer (MAC)¹⁴

- **Carrier Sense Multiple Access with Collision Avoidance**
 - Collision detect not possible
- **Access point or client senses the medium before transmission**
- **If collision, device waits a random amount of time within an exponential time window before retransmitting**
- **“Hidden Node” problem when clients cannot hear each other**
- **No idea of prioritization for quality of service**

Security

- **Most prevalent negative issue in popular media**
- **Makes corporations nervous about using Wi-Fi**
- **But the troubles are overblown (my opinion)**

What's the problem?

- The original 802.11 security protocol was called **Wired Equivalent Privacy (WEP)**
- Consists of a 10- or 26-byte password (“key”) attached to a 6-byte initialization vector through an encryption algorithm
- Unfortunately, these keys were easy for a listener to decode
- Numerous freeware tools can sniff out the keys
- Many users (e.g., homes) did not even bother setting the WEP key anyway
- Sounds pretty bad....

What's the fix?

- **Rotate the WEP keys**
 - Takes time to figure out the WEP key
 - Even if someone hacks your key, you change it fast enough – takes effort
 - Snooper will move on and look for a wide open AP
 - Business needs to add extra layer of defense
- **Wi-Fi Protected Access (WPA)**
 - Generated by the Wi-Fi Alliance as a framework of dynamic keys and 802.1X authentication
- **Advanced Encryption Standard (AES)**
 - Based on government encryption standard DES
 - So far, has not been cracked

802.11 alphabet soup

- **802.11d: Internationalization [completed]**
- **802.11e: Quality of Service (voice) [ongoing]**
- **802.11f: inter-access point protocol [completed]**
- **802.11h: 5 GHz for Europe [completed]**
- **802.11i: Improved over-the-air security [ongoing]**
- **802.11j: 4.9 GHz for Japan [ongoing]**
- **802.11k: Radio Resource Measurement [ongoing]**

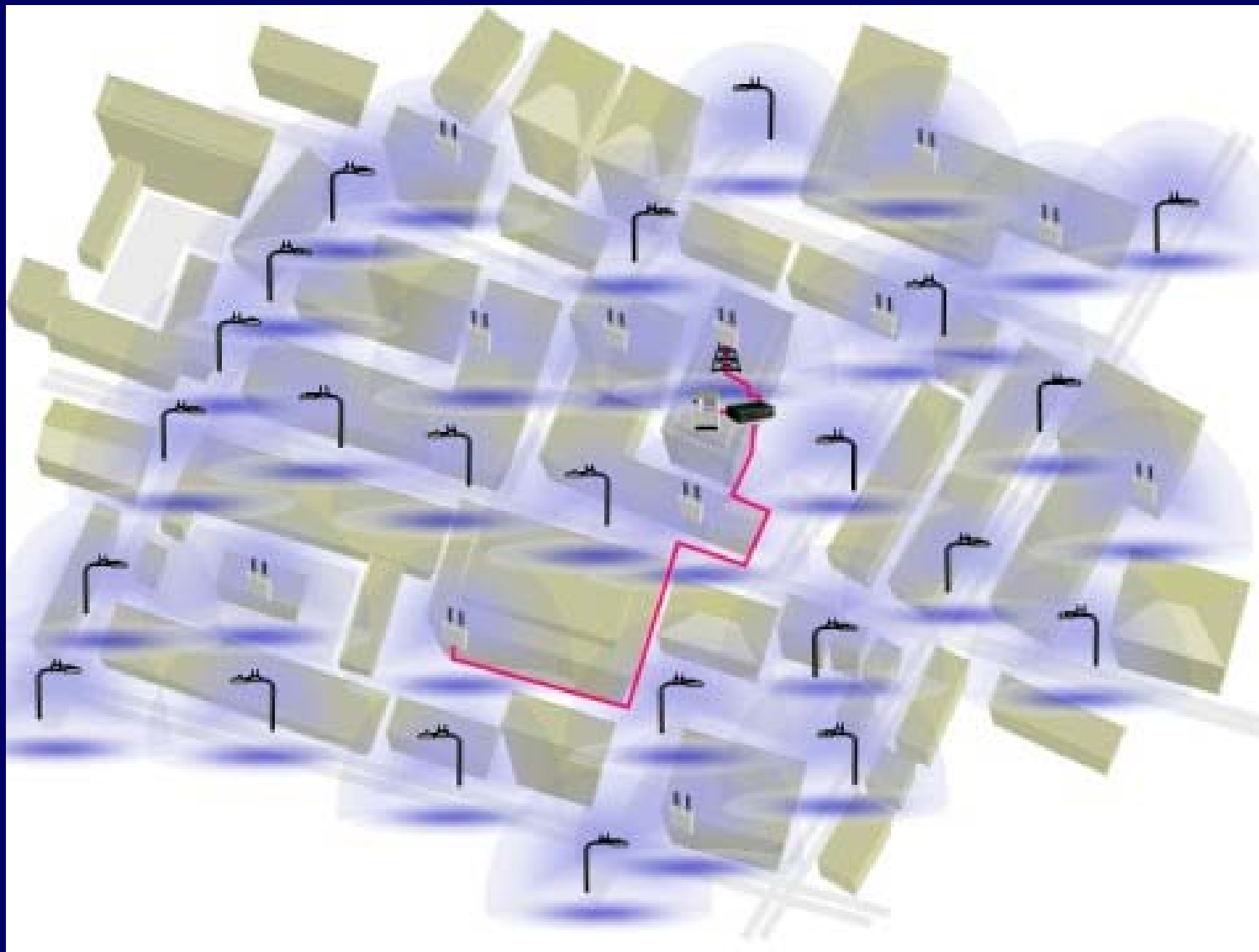
Wi-Fi at home

- **Generally a single AP <\$200**
- **Basic firewall and WEP key is good enough security**
- **Even with wide-open AP, person in street can get access but that's it**
- **802.11g is a good candidate for new install or upgrade, best propagation, unlikely to be concerned with mixed 11g/11b network**

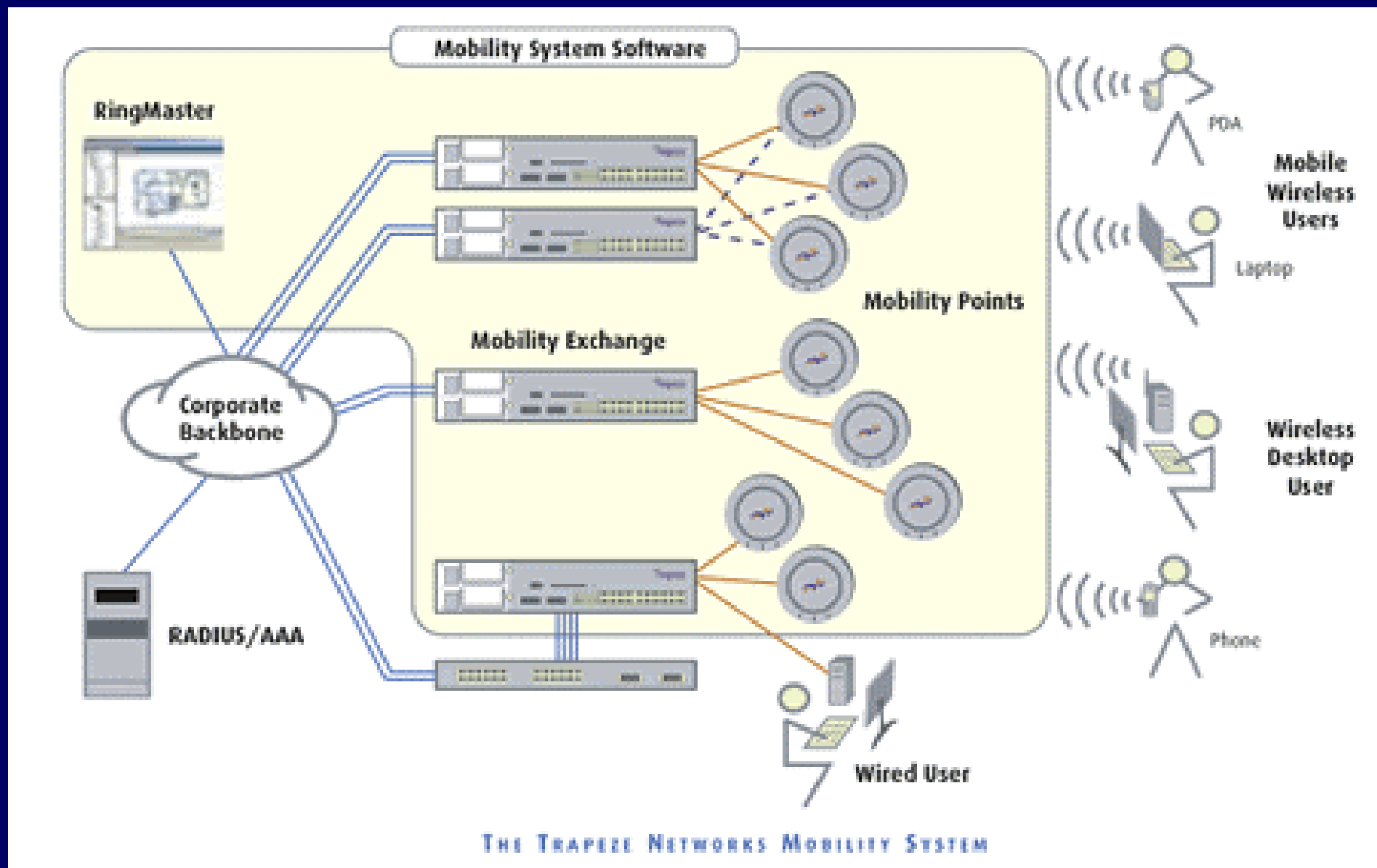
Wi-Fi Hotspot

- **Examples: Starbucks, Hotels**
- **Provides access to individuals who bring 802.11 enabled device to the (generally) small area**
- **Often run w/ no security (no WEP)**
- **Users are directed to a captive portal to subscribe to a service plan**

Citywide Wi-Fi

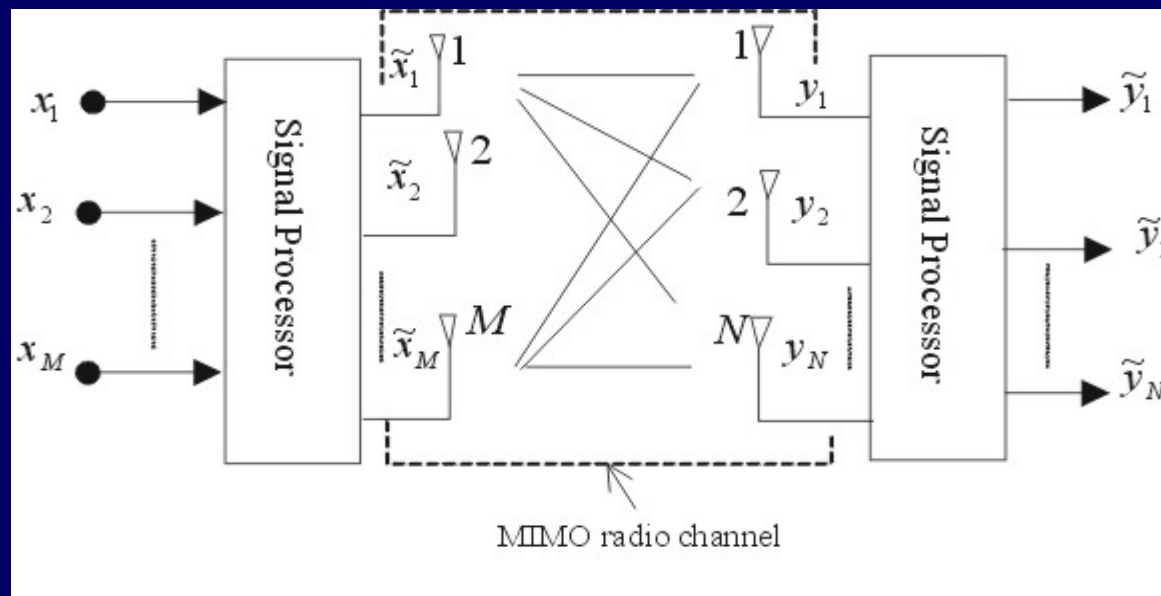


WLAN at the office



Future of Wi-Fi technology

- 802.11n: higher throughput, make 802.11 better suited for even wider applicability



- 802.11p: Wireless Performance Prediction
- 802.11r: Short-Range Communications
- 802.11s: Mesh Networking

Future Trends

- **Wi-Fi has seen phenomenal growth and is here to stay**
- **Wi-Fi is pervasive**
- **However, this is just the beginning:**
 - **Much more room for PHY innovations**
 - **Much more room for MAC innovations**
 - **Billions more worldwide WLAN devices will be used**
- **Enormous opportunity**

References

- ***802.11 Wireless Networks* by Matthew Gast**
- **IEEE 802.11 website <http://ieee802.org/11>**
- **Wi-Fi Alliance website <http://www.wi-fi.org>**
- **Websites of companies in the industry**
 - **Chipsets: Intel, Broadcom, Atheros, TI**
 - **Business Wi-Fi: Airespace, Aruba, Trapeze, Legra, Cisco**
 - **Mesh Networking: Tropos, BelAir, MeshNetworks**
 - **Hotspots: Boingo, T-Mobile**
 - **Home Access Points: D-Link, Linksys, Proxim**