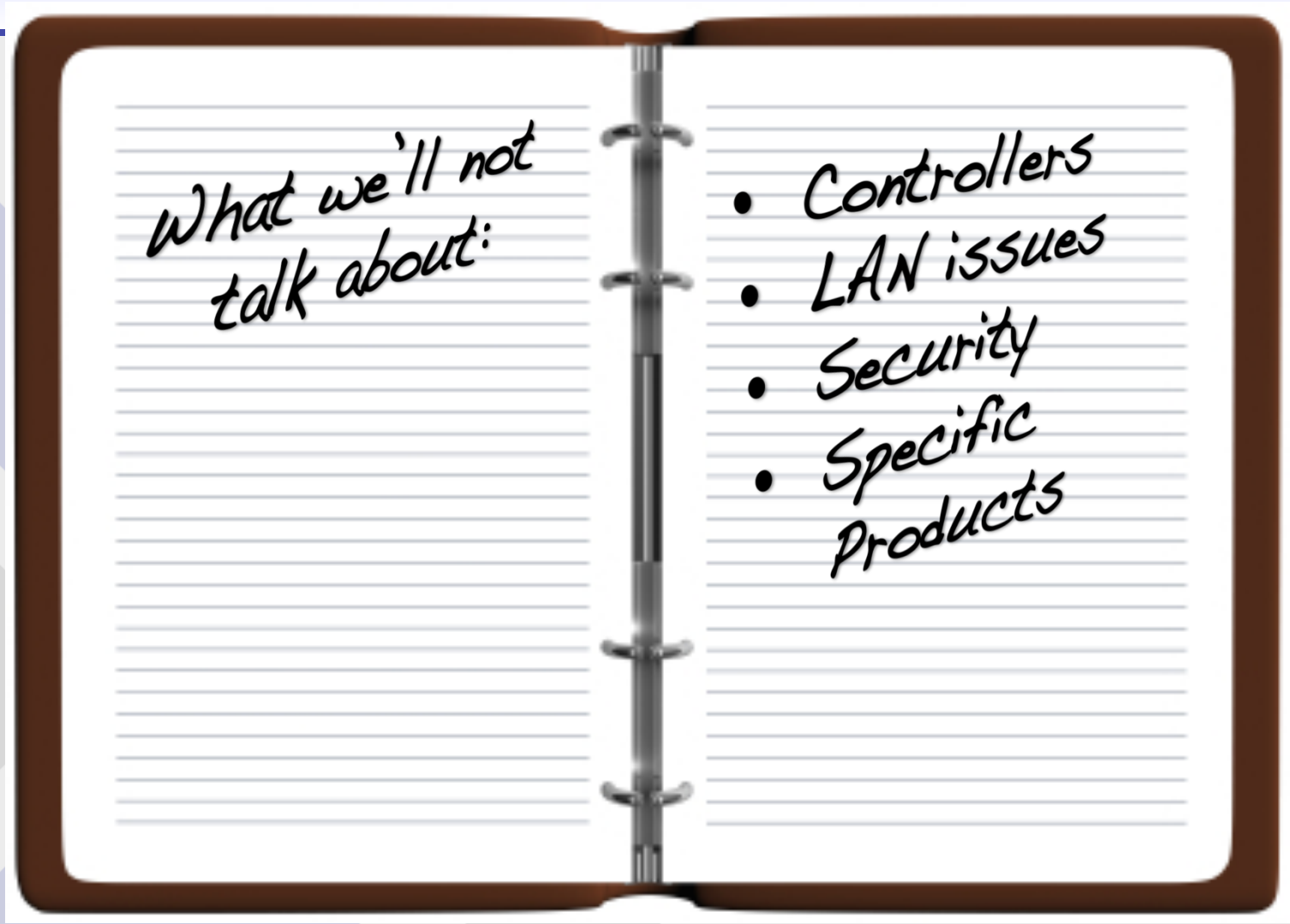
Wireless Fundamentals for Network Engineers

Ron Trunk
Chesapeake Netcraftsmen

Ask me about…Me!

- Ron Trunk, CCIE (10 years+), CISSP
- I help companies deploy secure, high performing networks
- Clients include Federal, State Gov't, Healthcare and Defense industry
- Commonsense, cost effective approach to security and network operations.



What is RF?

- Electromagnetic Energy that can be radiated into space

- Why?
- To transmit information from here to there
- To transmit energy from here to there

- No wires!

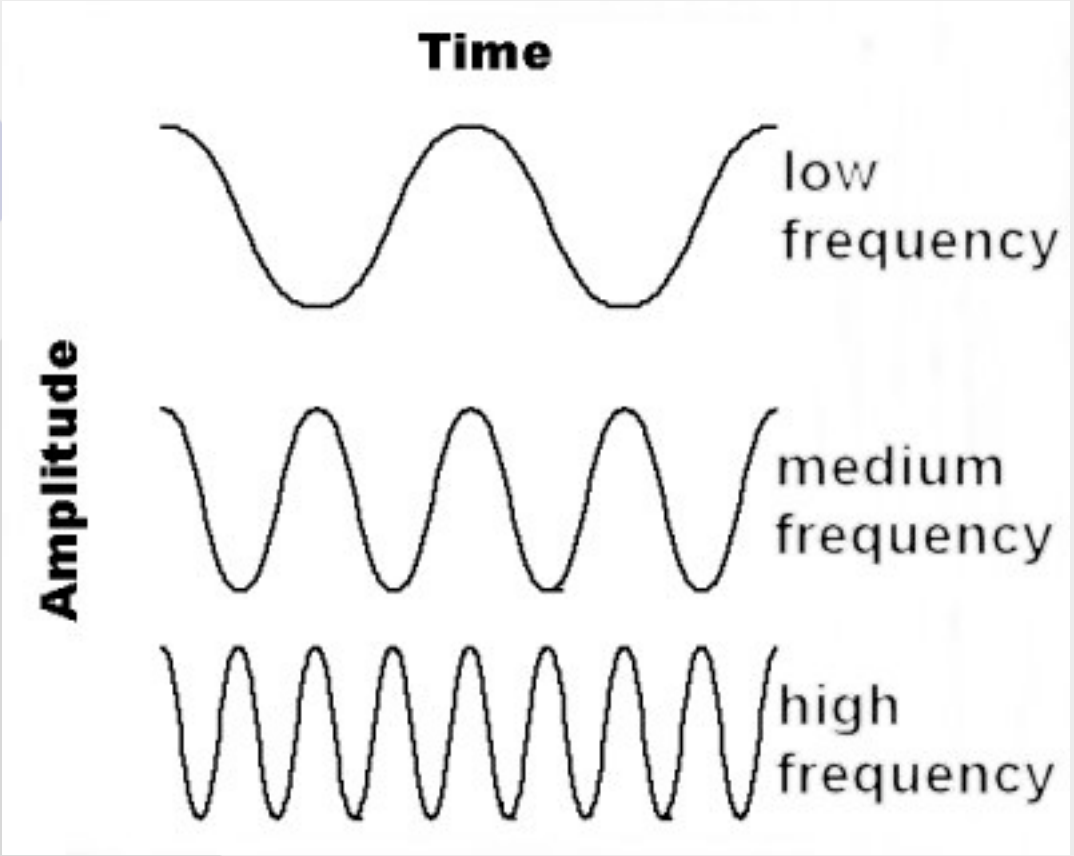
Receiving RF

- The EM energy can induce currents into a conductor, which is then decoded into information
- A receiver is “tuned” to a specific frequency, rejecting information at other frequencies

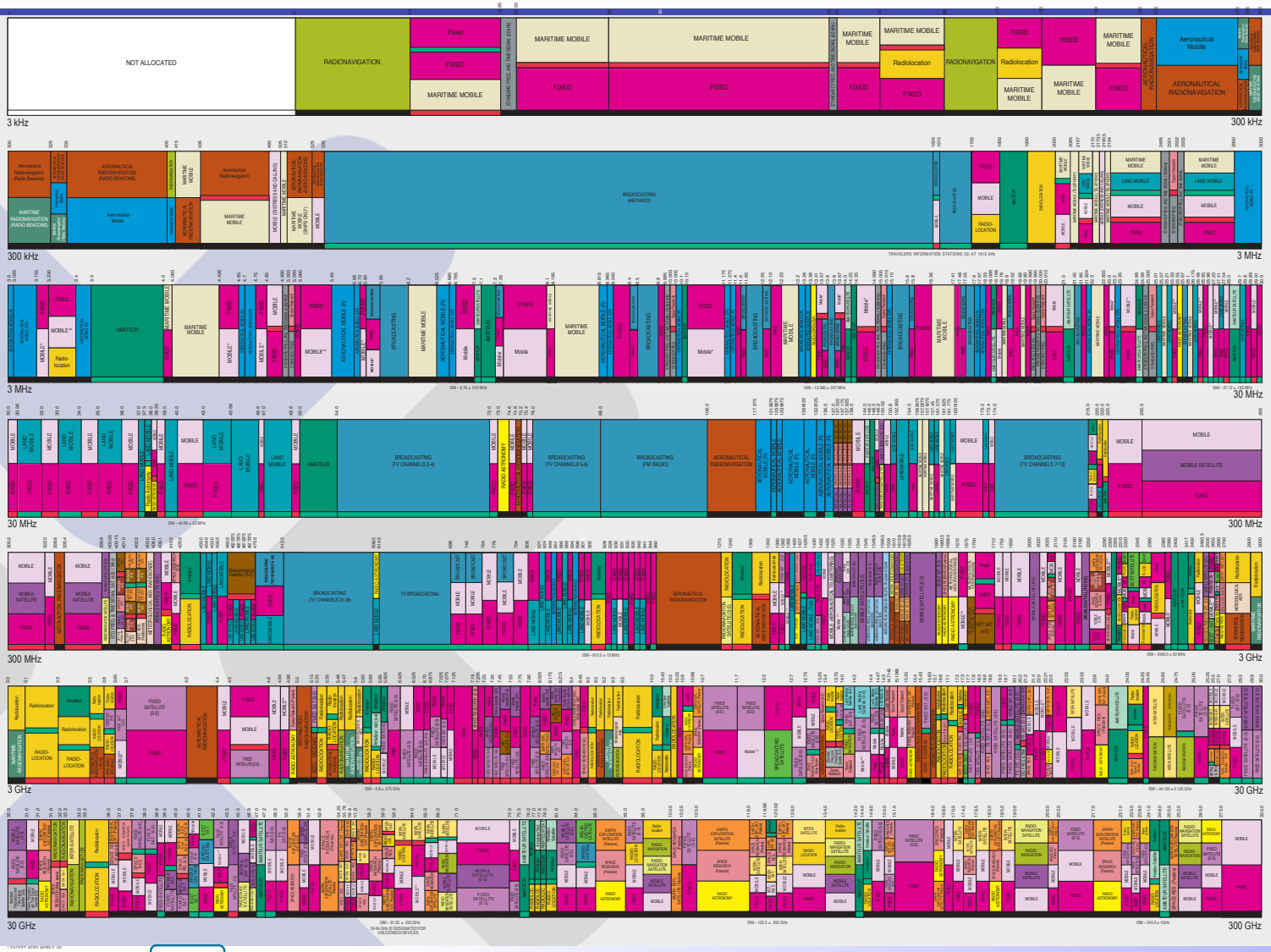
RF is Alternating Current

- Frequency

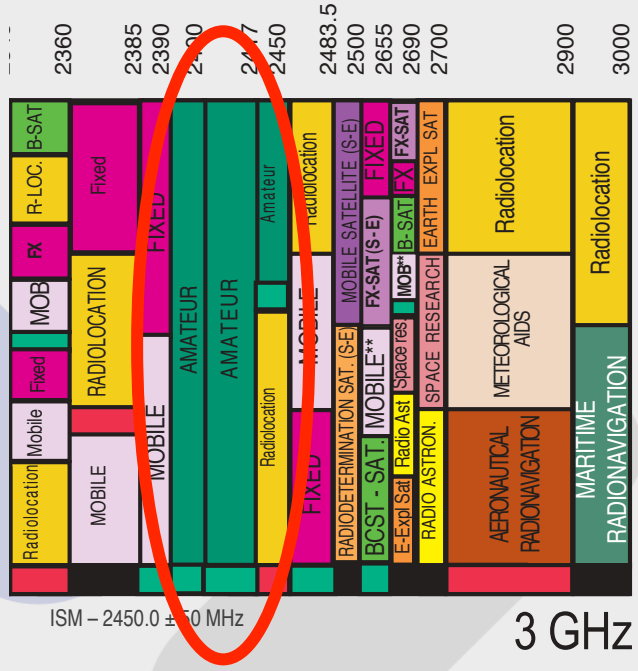
- Hertz (Hz)
- KHz
- MHz
- GHz
- THz

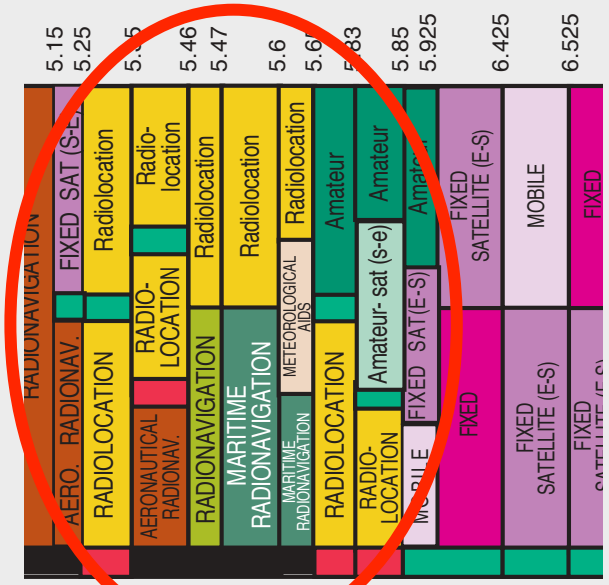


FCC Spectrum Allocation



Wifi Spectrum





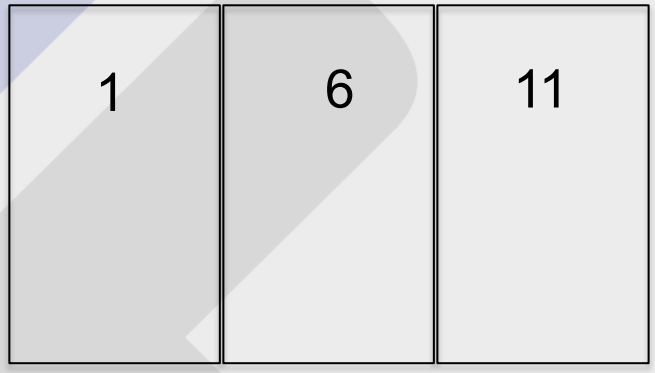
2.4 GHz ISM

5.1 GHz U-NII

Wifi Spectrum

- **Industrial, Scientific and Medical Band (ISM)**
  - **2.412 GHz to 2.472**
  - **3 Channels, 20 MHz wide**
- **Unlicensed National Information Infrastructure Band (U-NII)**
  - **5.15 GHz to 5.875 GHz**
  - **20 Channels (US) 20 MHz wide**

ISM Channels



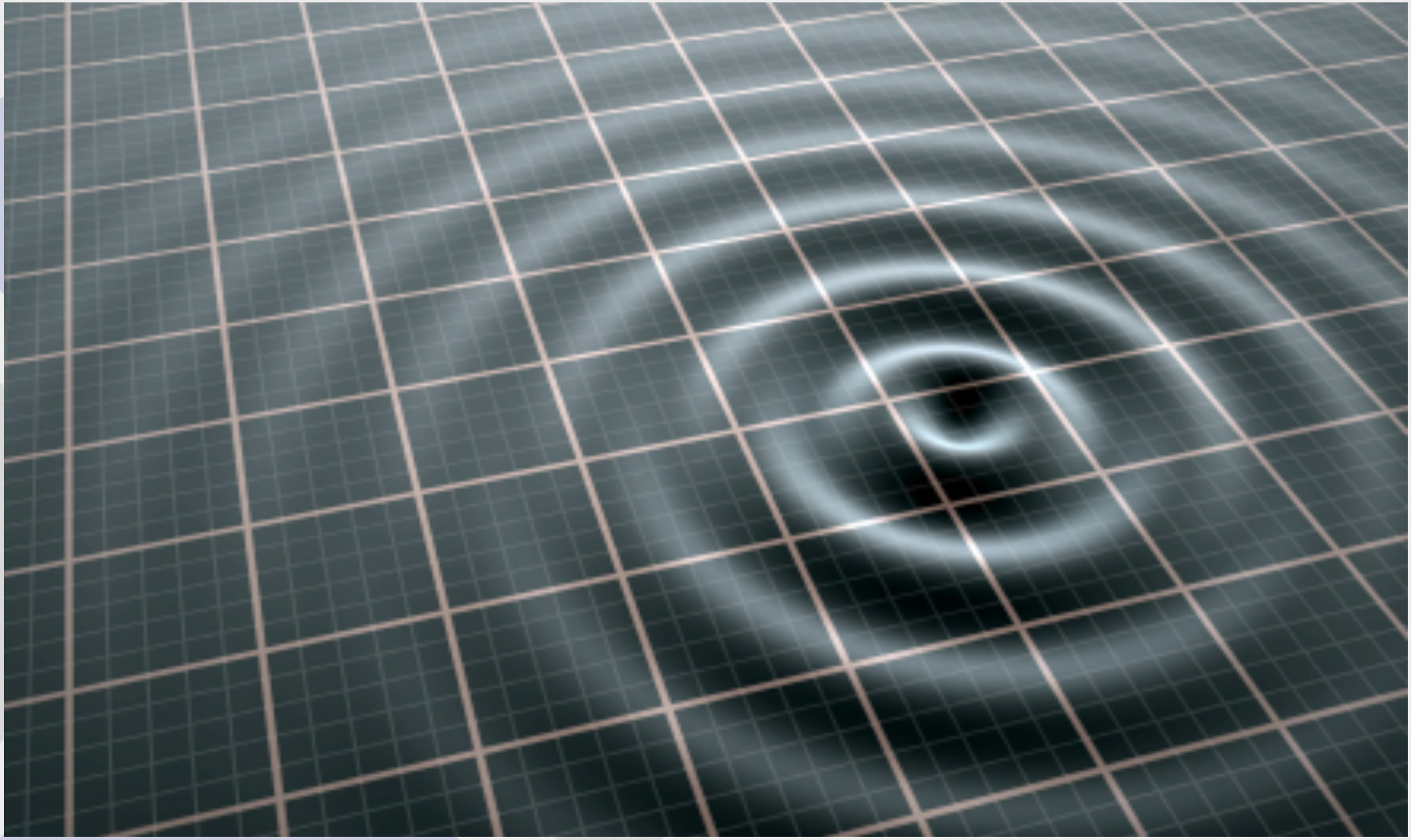
U-NII Channels

nel fier	36	40	44	48	52	56	60	64		149	153	157
r ency	5180	5200	5220	5240	5260	5280	5300	5320		5745	5765	5785
	UNII-1				UNII-2					UNII-3		

Channel Identifier	100	104	108	112	116	132	136	140
Center Frequency	5500	5520	5540	5560	5580	5660	5680	5700
Band	New UNII-2 Channels							

220339

Wavelength



Wavelength

- Wavelength (meters) = speed light (m)/freq(Hz)

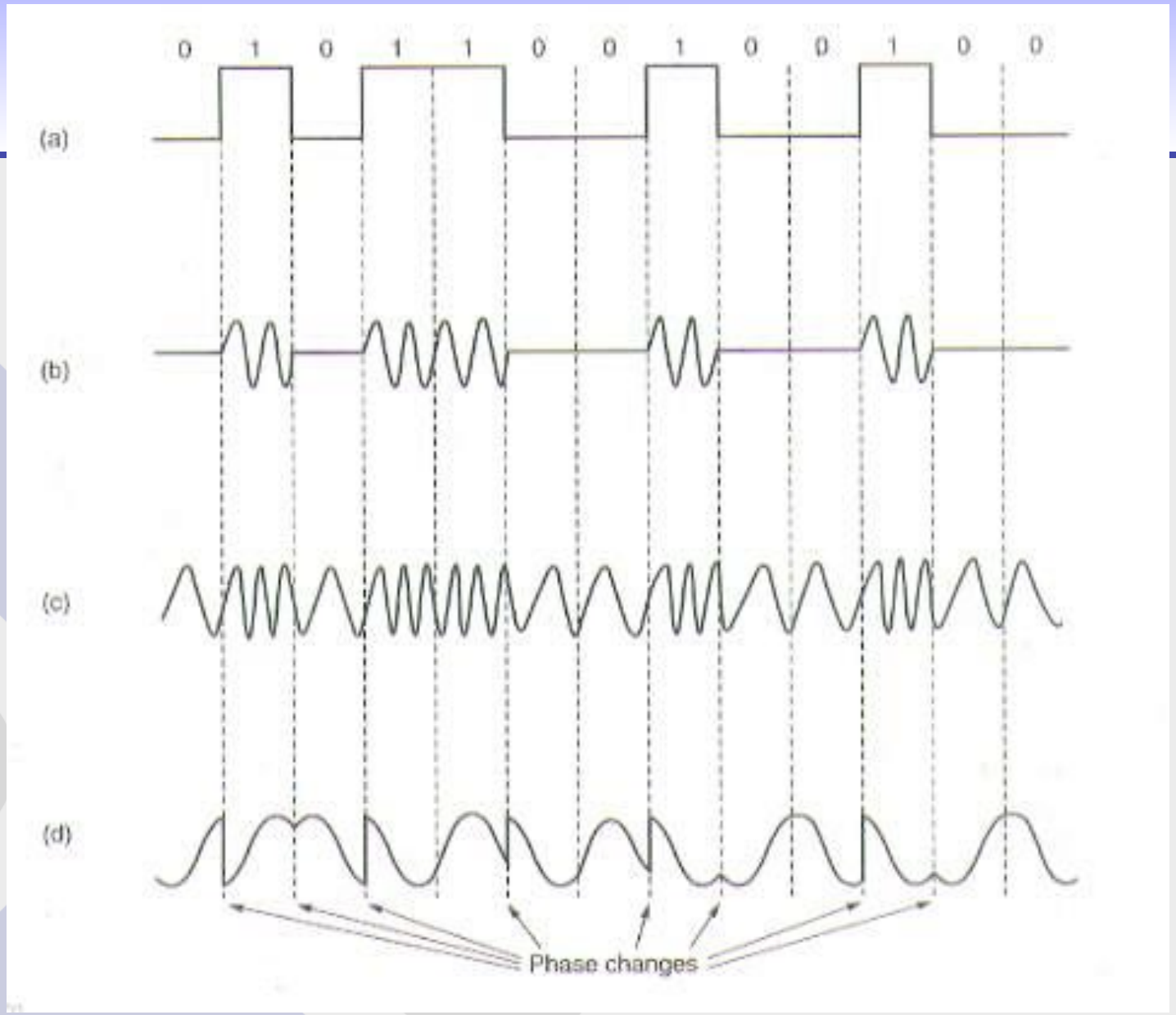
$$\text{Wavelength (m)} = \frac{3 \times 10^8}{\text{Freq (Hz)}} = \lambda$$

- 2.4 GHz = .125m 4.8 in **½ λ dipole**
- WTOP 1580 KHz = 189m (**614** ft.)

Modulation

- Transmitting energy is one thing
- The point is to convey information
- To do this we modulate the energy

- AM and FM
- Amplitude modulation
- Frequency modulation
- Phase modulation



Modulation Increases Bandwidth

- Modulation spreads energy near the carrier frequency
- Generally speaking, the higher the modulation frequency, the wider the bandwidth

Bandwidth and Spectrum

- This is fundamentally why there are only 3 channels in the 2.4GHz ISM (802.11b/g) band
- The channel numbering system was developed before WiFi, so they really have no meaning

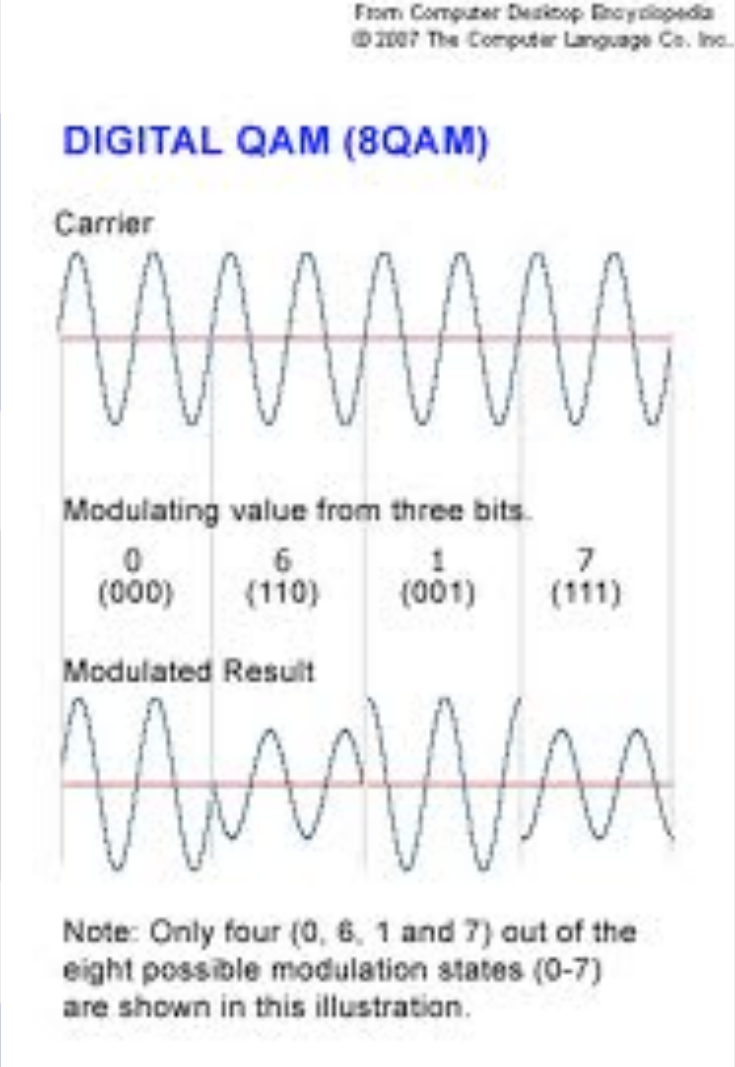
More Data Less Bandwidth

- Various schemes to get more for less

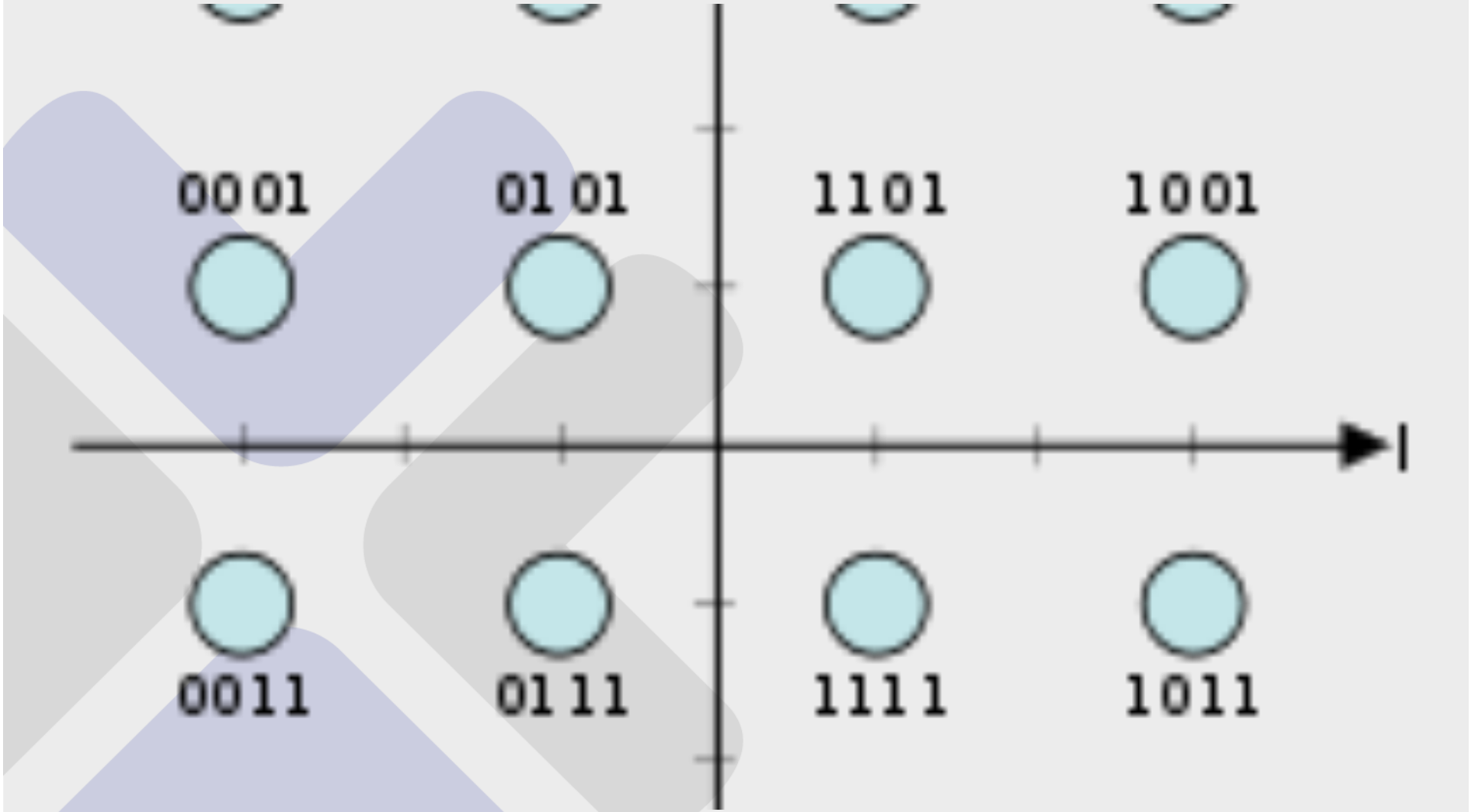
Modulation Tricks

- Use more than two levels (on-off)
  - 0 = 00
  - 1 = 01
  - 2 = 10
  - 3 = 11
- Change more than one thing
  - Amplitude
  - Phase

Quadrature Amplitude Modulation

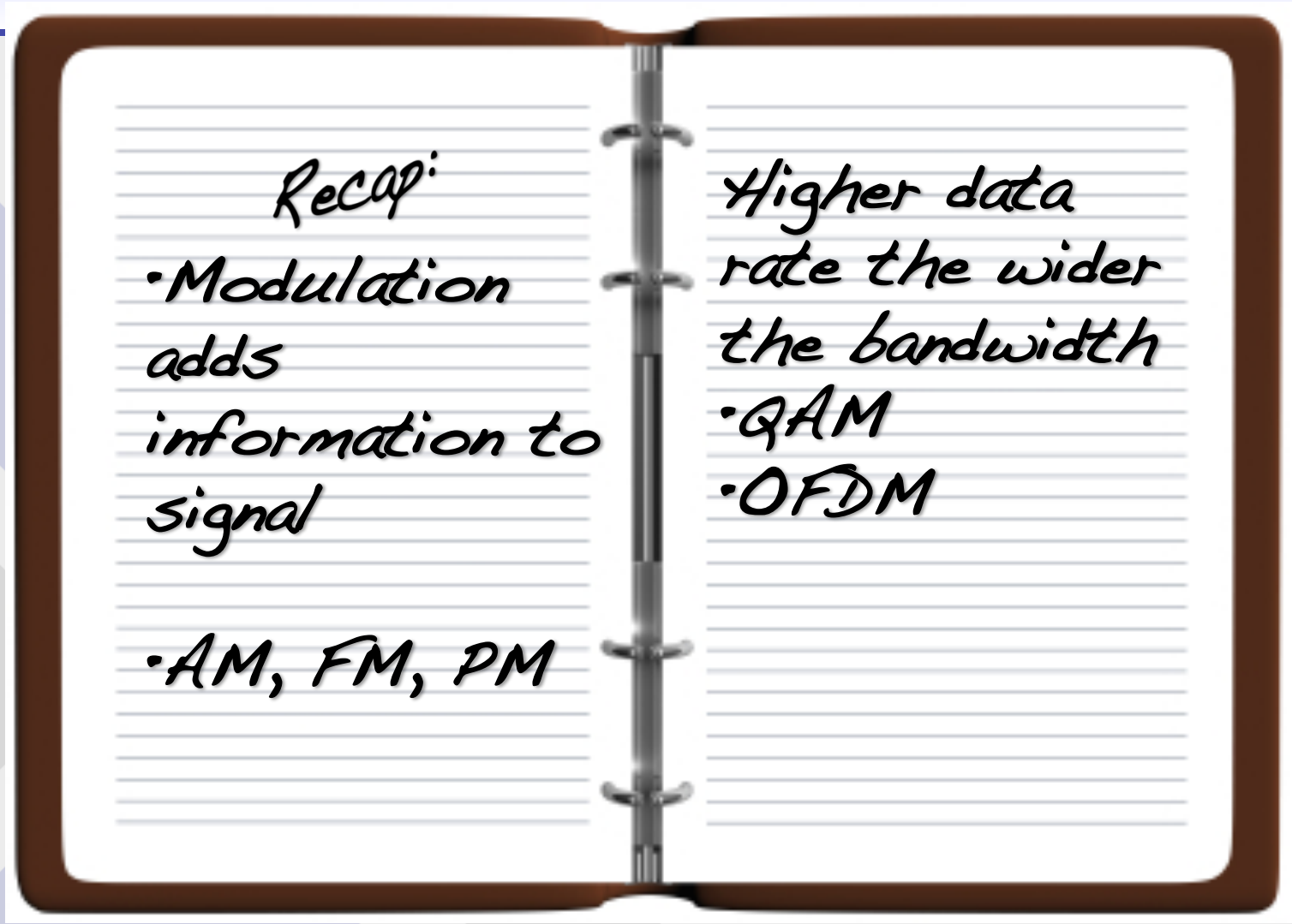


16-QAM



Orthogonal Frequency Division Multiplexing

- Divide channel into subcarriers
- Each subcarrier is 90^{o} out of phase (orthogonal)
- Divide information into multiple streams
- Each subcarrier is modulated by stream using QAM



Measuring RF

- Electrical Power is measured in Watts
- Transmitters are rated by output power to antenna
- In our case, it's milliWatts

Decibel

- Used to measure large dynamic ranges
- It is dimensionless
- A Decibel is a ratio

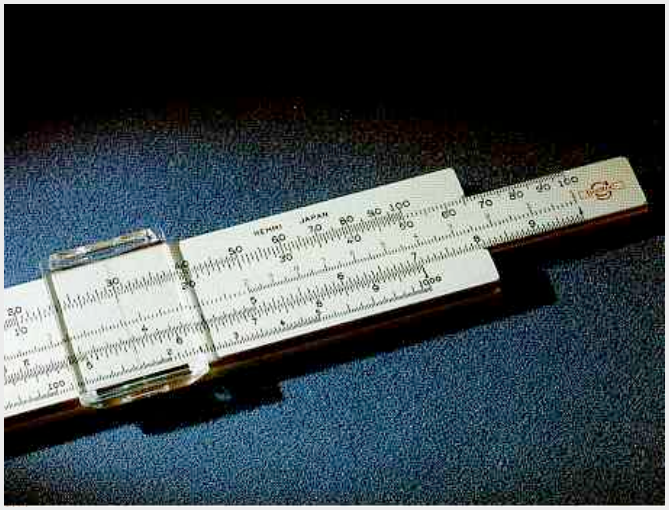
- Decibel is 1/10 of a Bel, but Bel is never used

Decibel

- 10 * log p1/p2
- P1/p2 is
  - Input/Output
  - Value/Reference

Forget Your Slide Rule?

- 3 dB = 2x power
- 10 db= 10x power
- 20 db=100x power



- -3dB = .5x
- -10dB = .1x
- -20 dB = .01x

Decibel Example

- **A**n amplifier with a 16dB gain
- **16 = 10 + 3+ 3**
- = 10 x 2 x 2
- **Gain =** 40x

Decibel

- dB is dimensionless, but references are used
- dBm = 10 log x/1 mW
- 1 mW is 0dBm
- 1 Watt is 30dBm

More References

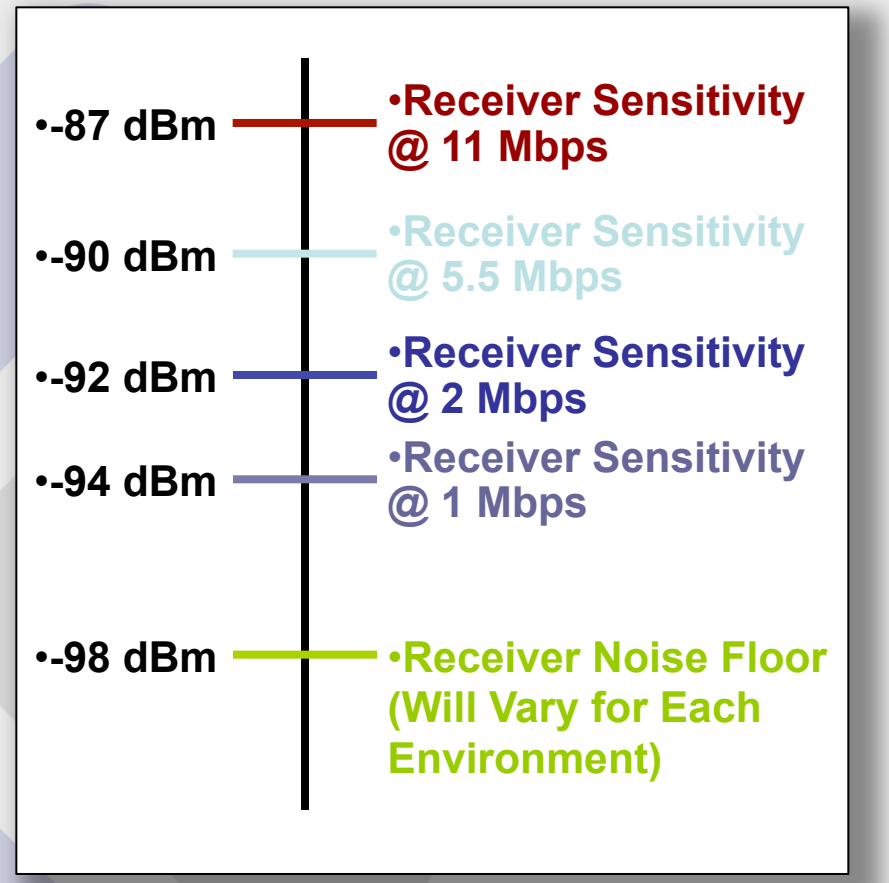
- dBi reference: isotropic (theoretical ideal) antenna
- dBd reference: a standard dipole antenna

- Commercial radio uses dBd, but WiFi uses dBi
- 0 dBd = 1.76 dBi
  - Higher number sounds better?

Receiver Sensitivity

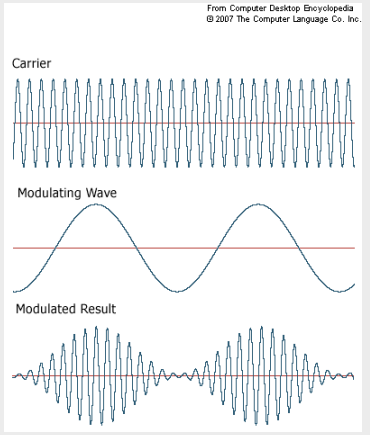
- Receivers rated by minimum power required to excite the decoding circuits
- Rated in dBm
- Lower the better
- Typically in the -80 -90 dBm range
- -90dBm = 1 picowatt

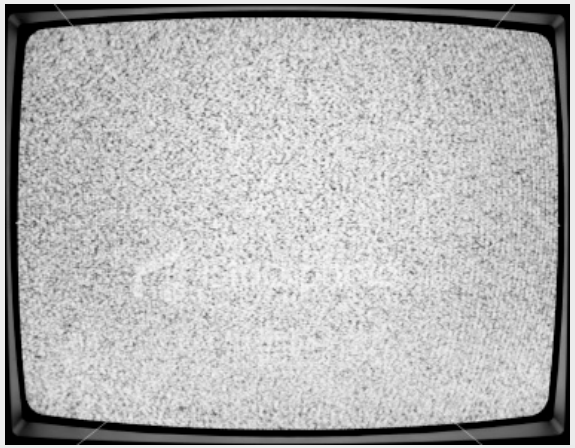
Receiver Sensitivity
Example for 2.4GHz Direct Sequence



Signals and Noise

- If the energy received can be decoded as 802.11 protocol, we call it "Signal."
- Any other energy is called "Noise."





Signal to Noise Ratio

- To reliably decode a signal, it needs to be stronger than the noise
- For a given data rate, there is a minimum signal to noise ratio SNR
  - Expressed in dB

Signal to Noise Ratio

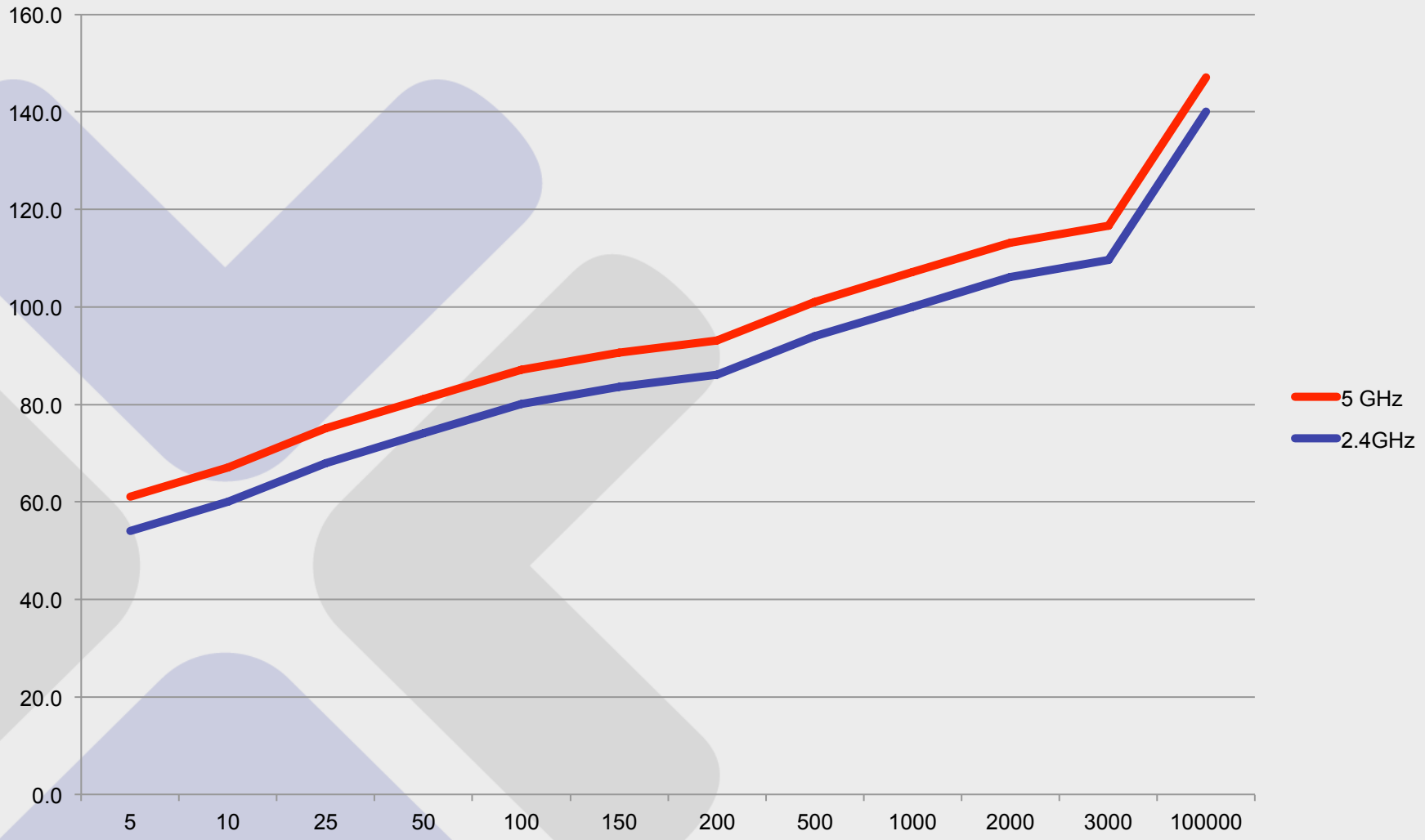
Data Rate	Required SNR (10% PER)
12	5.5
18	7.5
24	10.5
36	12.5
48	17
54	19

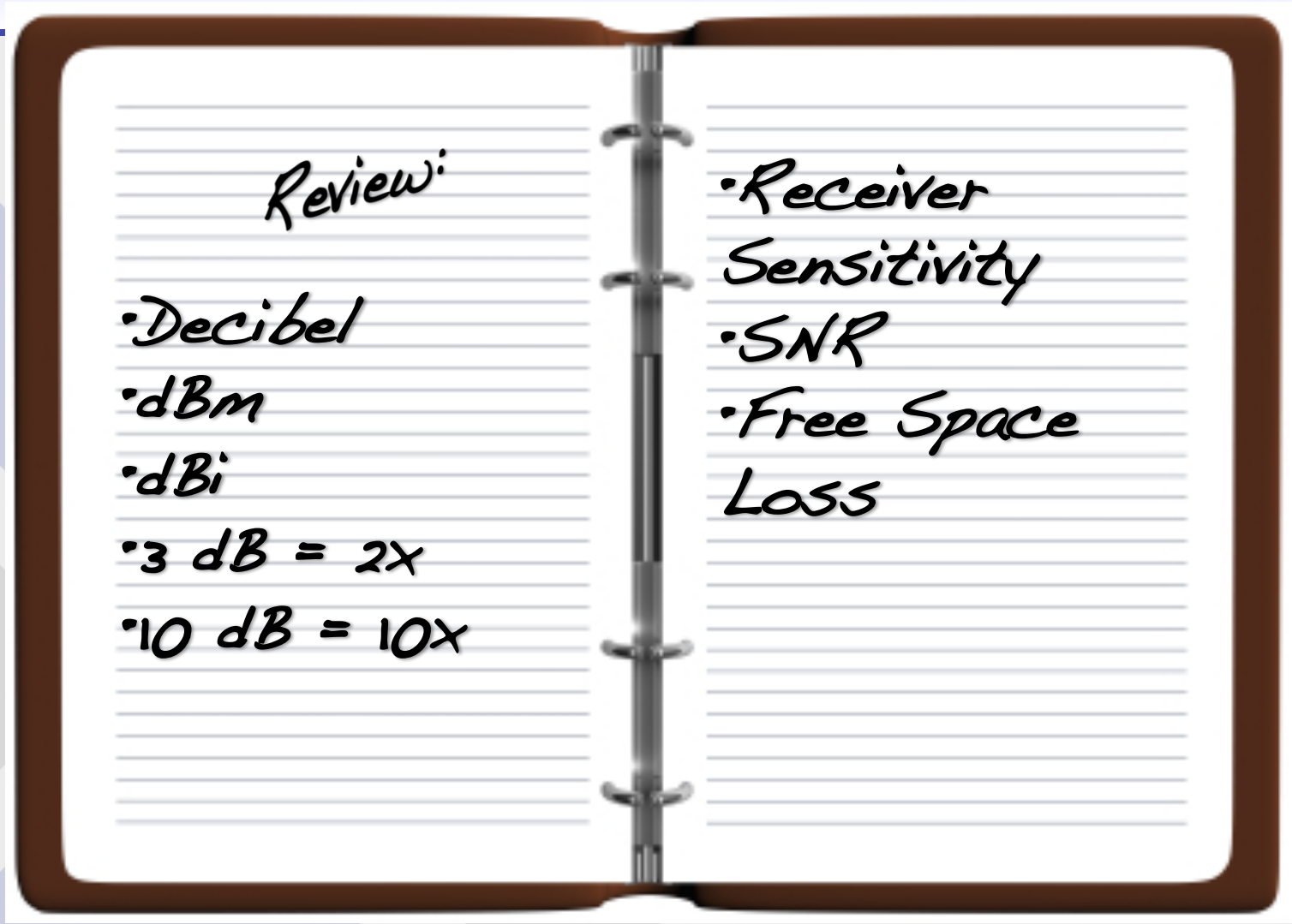
Free Space Loss

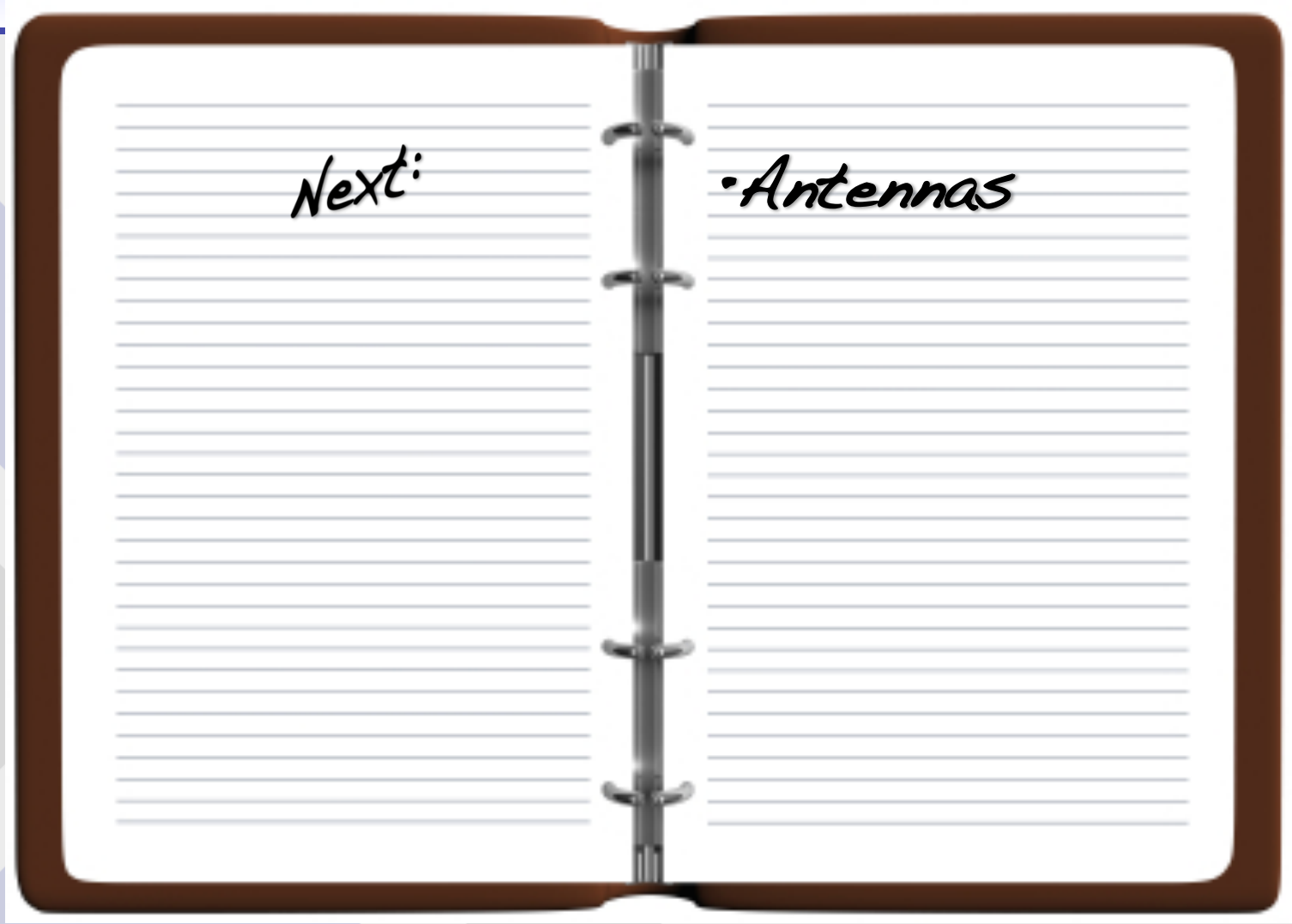
- How much does the signal attenuate travelling through space?
- Proportional to square of distance and square of frequency

$$\mathrm{FSPL(dB)} = 20\log_{10}(d) + 20\log_{10}(f) + 32.45$$

Free Space Loss (Ideal)

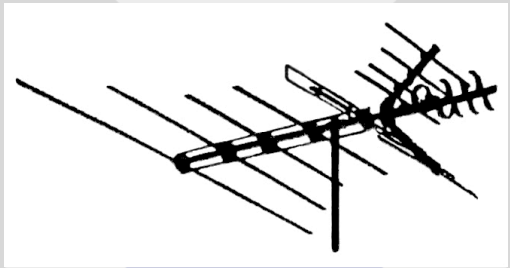






Antenna

- A device that converts conducted energy into radiated energy
- Or vice versa



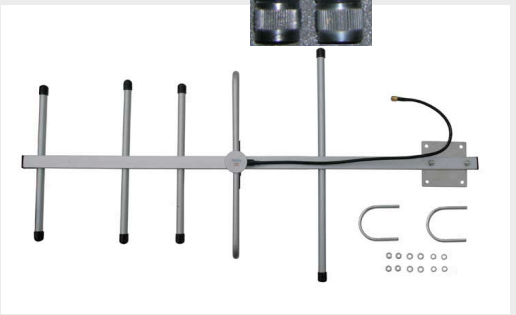
Antenna types

- **Omni directional**

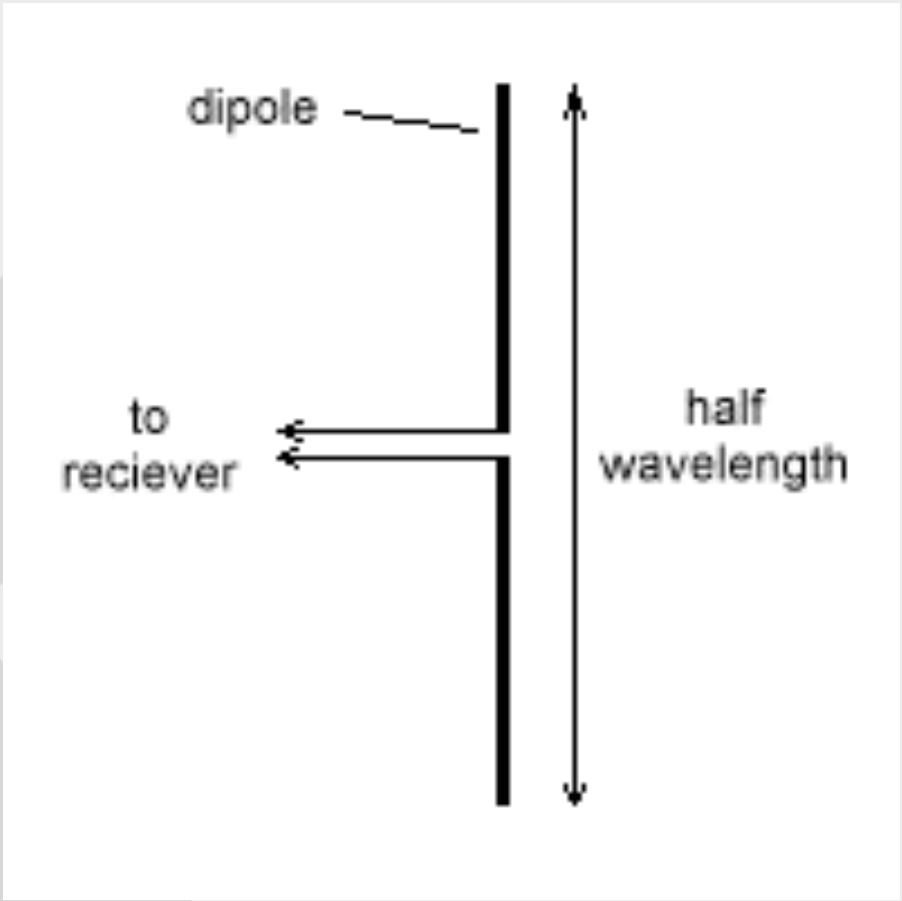
- **Directional**

Antenna Types

- Dipole
- Yagi
- Patch
- Parabolic Antenna



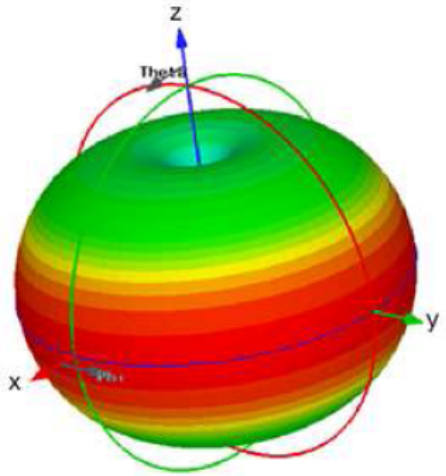
Half-wave Dipole



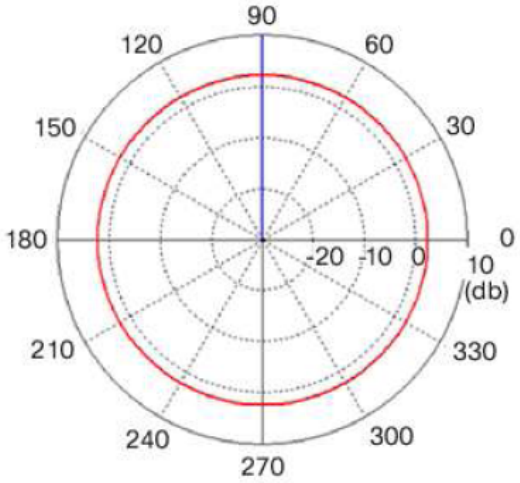
•Understanding antenna patterns

•Dipole (Omni-directional)

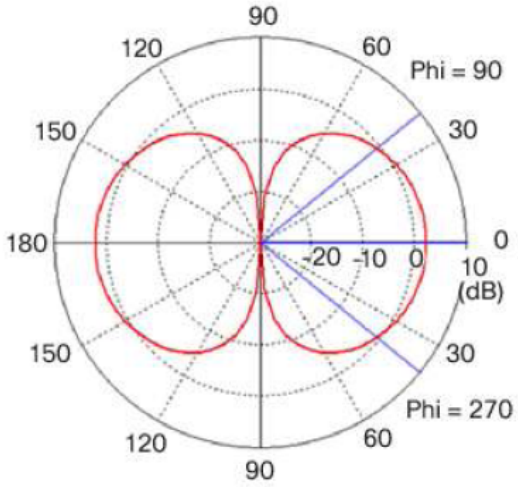
Dipole Antenna Model



Dipole 3D Radiation Pattern



Dipole Azimuth Plane Pattern

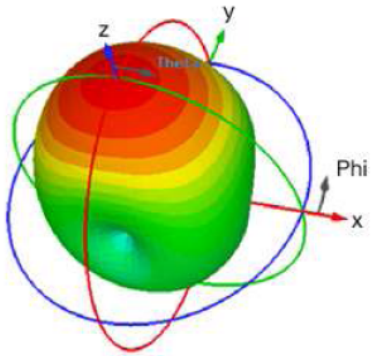


Dipole Elevation Plane Pattern

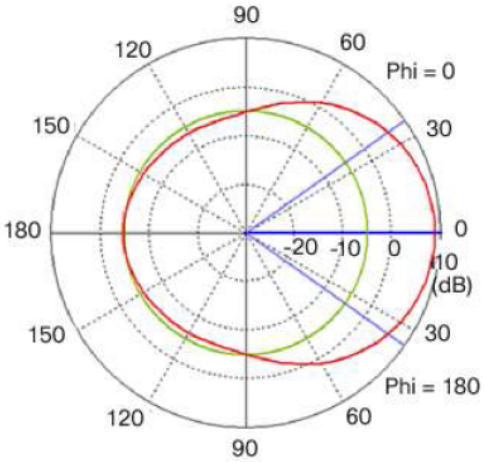
•Understanding antenna patterns

•Patch (Directional)

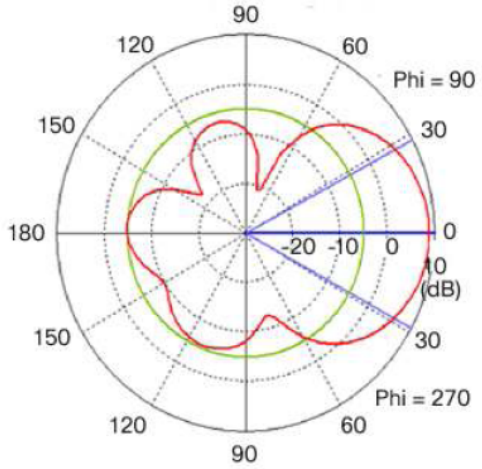
Patch Antenna Model



Patch Antenna 3D Radiation Pattern



Patch Antenna Azimuth Plane Patter

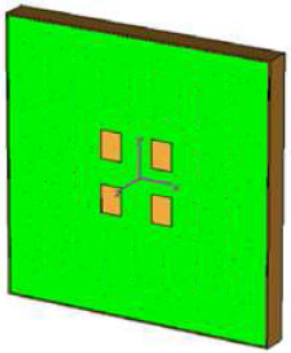


Patch Antenna Elevation Plane Pattern

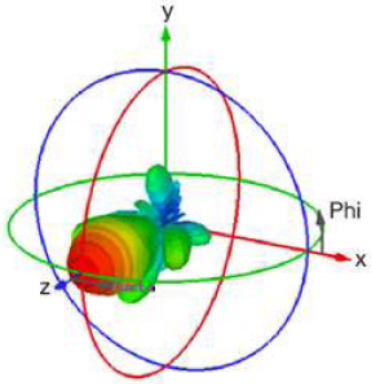
•5 GHz Patch Antenna

•Understanding antenna patterns

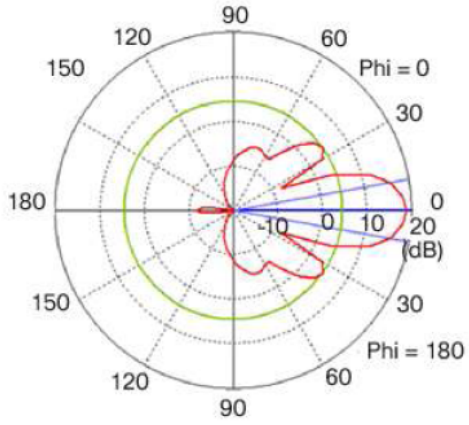
•Patch (Higher Gain Directional)



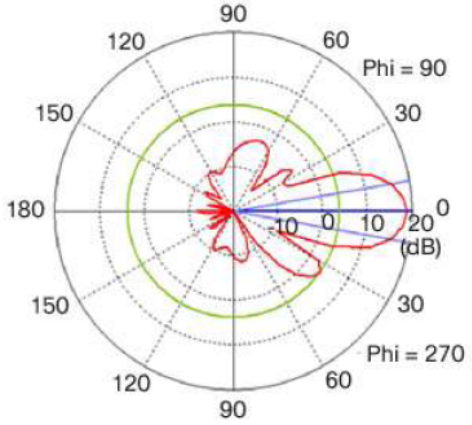
4x4 Patch Array Antenna



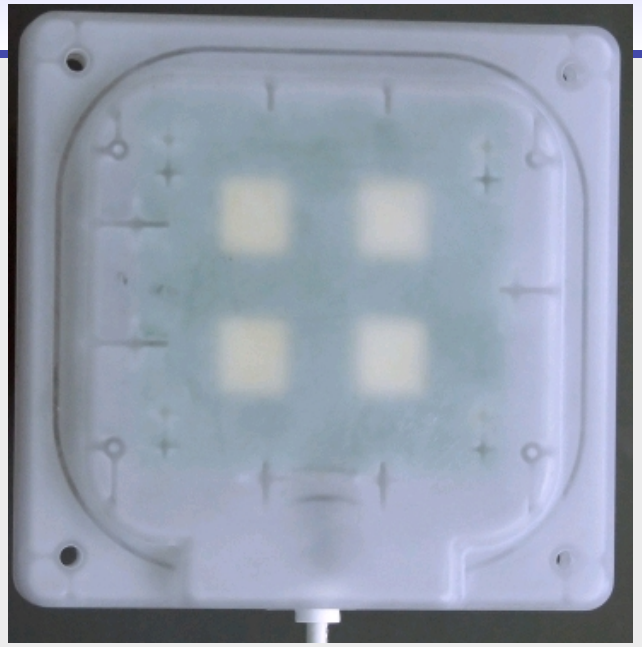
4x4 Patch Array 3D Radiation Pattern



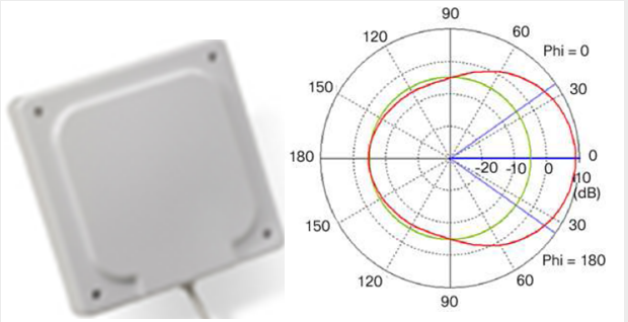
4x4 Patch Array Azimuth Plane Pattern



4x4 Patch Array Elevation Plane Pattern



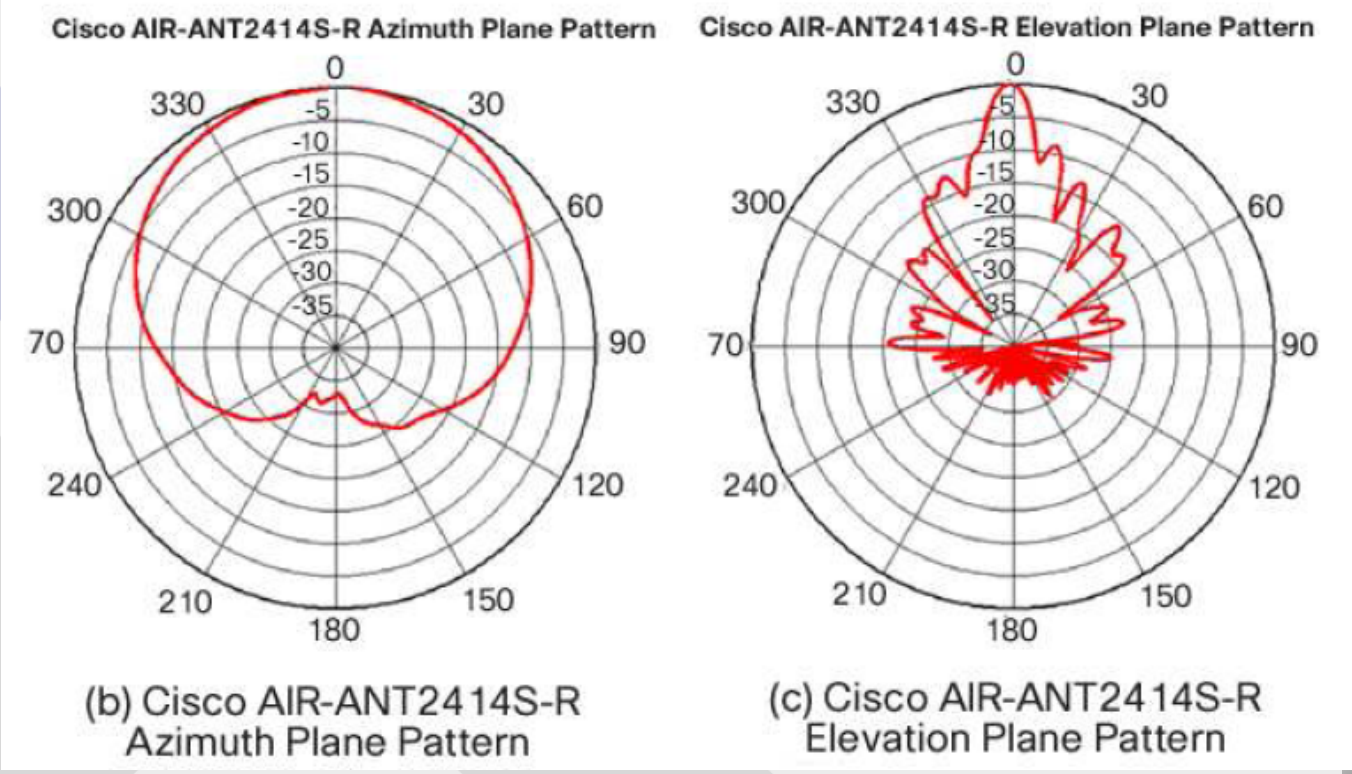
•Four element Patch



•Single Patch Antenna

•Understanding antenna patterns

•Sector (Higher Gain Directional)



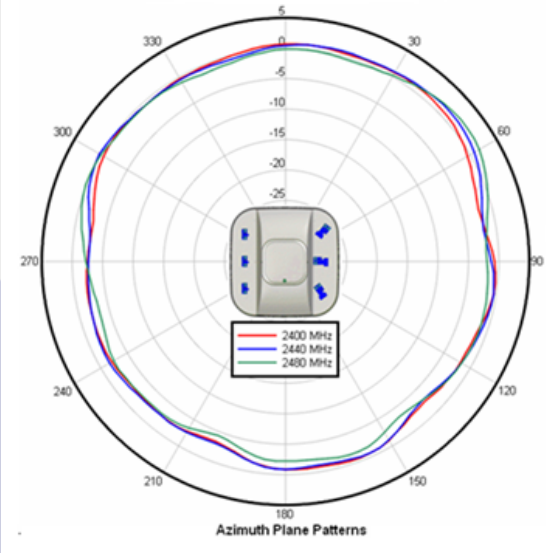
•Elevation plane has nulls due to high gain 14 dBi

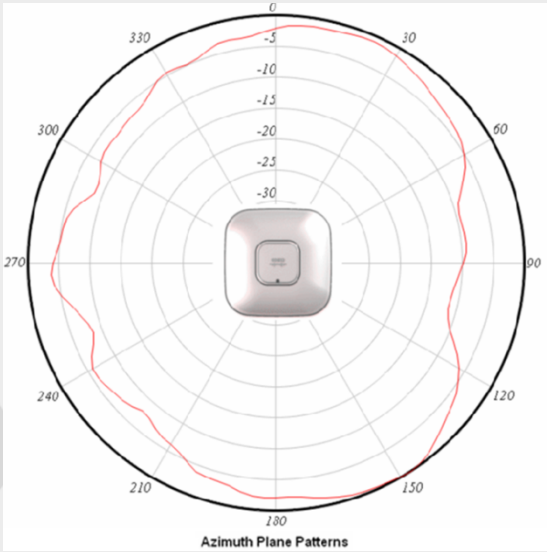
•AIR-ANT2414S-R
•14 dBi Sector 2.4 GHz

Antenna Patterns

Azimuth and Elevation Patterns for 2.4 GHz & 5 GHz

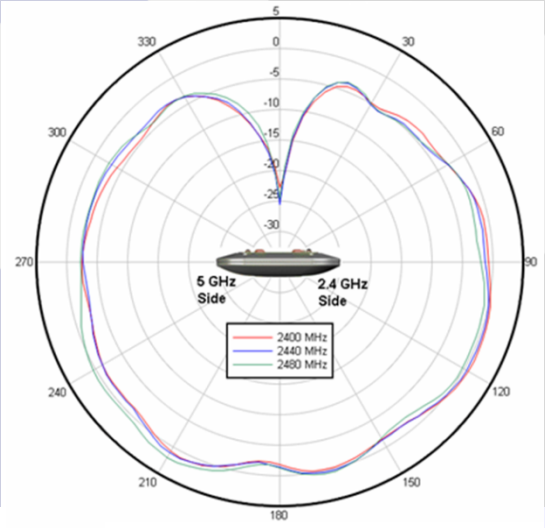
•2.4 GHz
•Azimuth

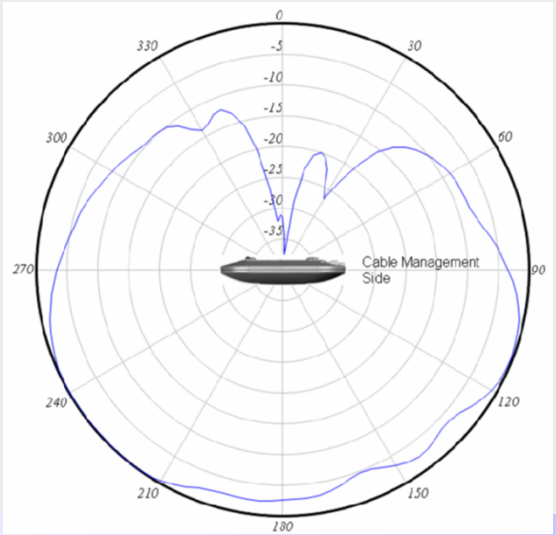




•5 GHz
Azimuth

•2.4 GHz
•Elevation

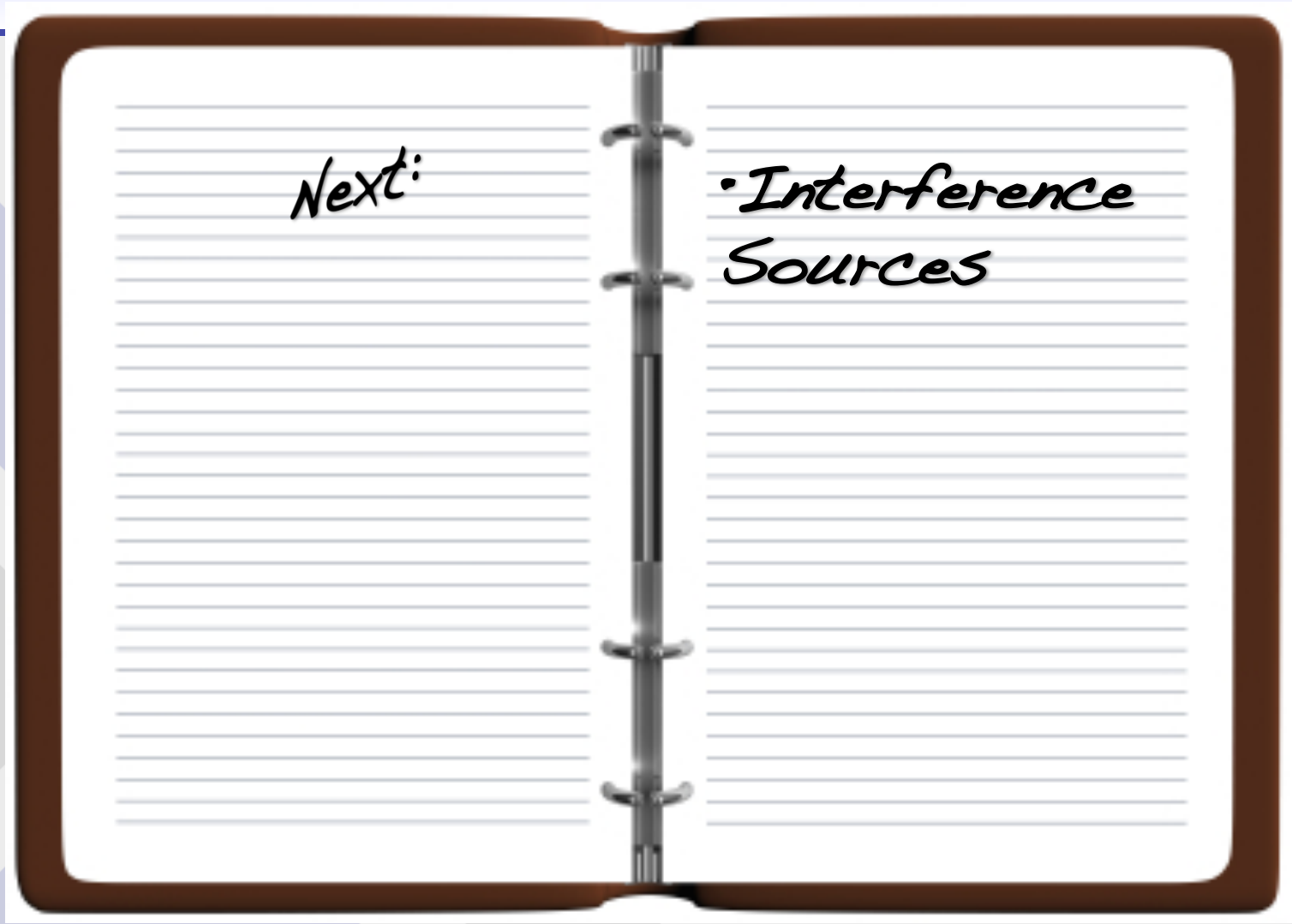




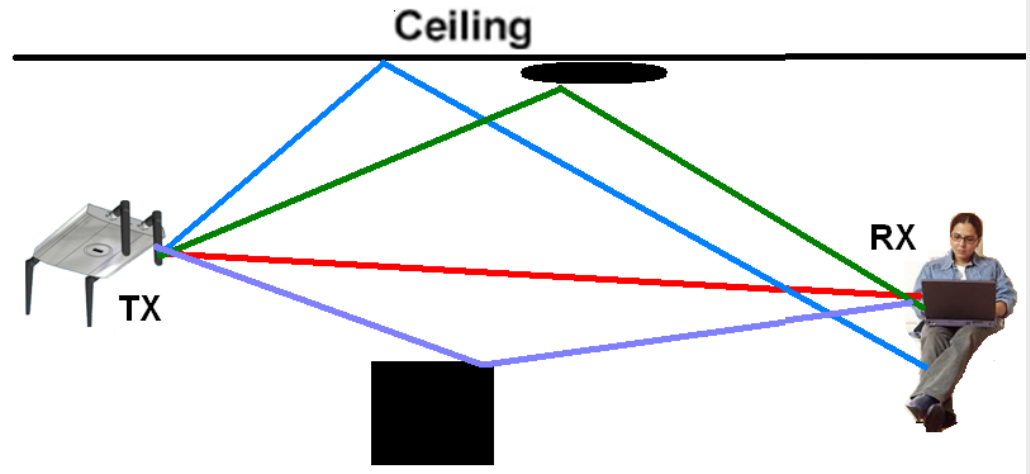
•5 GHz
•Elevation

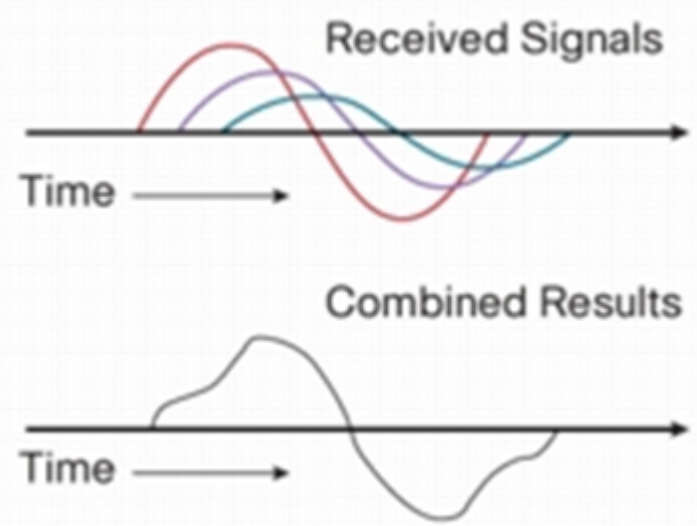
The Accidental Antenna

- Currents can be induced in many metallic materials
- At 2.4 or 5 GHz, a screw can be a fractional wavelength
- Energy induces current in the antenna, which in turn creates a magnetic field
- Can reflect signals (like a mirror)



Multipath



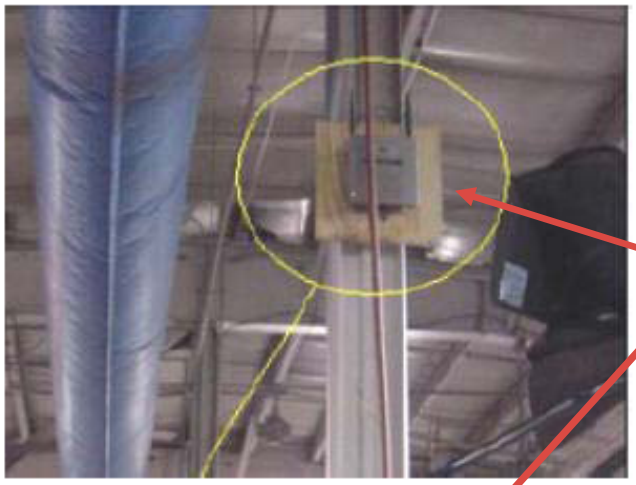


- Reflected signals arrive at different phase
- Cause distortion and fading

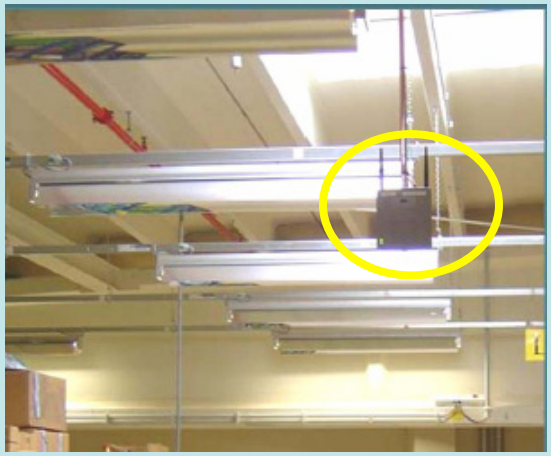
802.11n with more receivers can use destructive interference (multipath) as a benefit.

Multipath TV Ghost

Minimize the Impact of Multipath



- Temptation is to mount on beams or ceiling rails
- This reflects transmitted as well as received packets
- Dramatic reduction in SNR due to high-strength, multipath signals

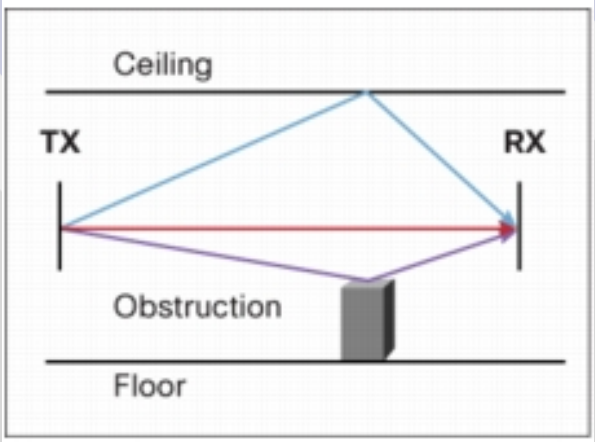


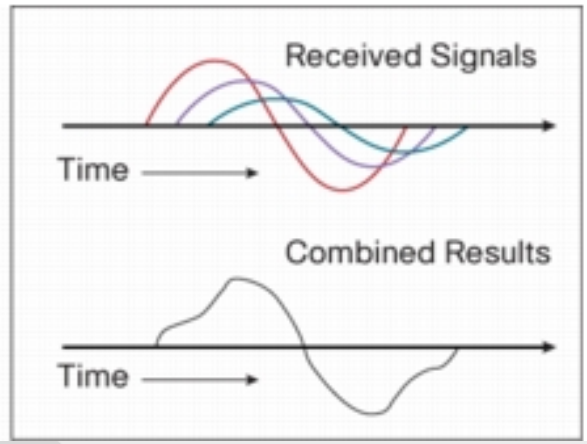
•Minimize Reflections When Choosing Locations

Multipath and Diversity (SISO)

802.11a/b/g diversity has just one radio

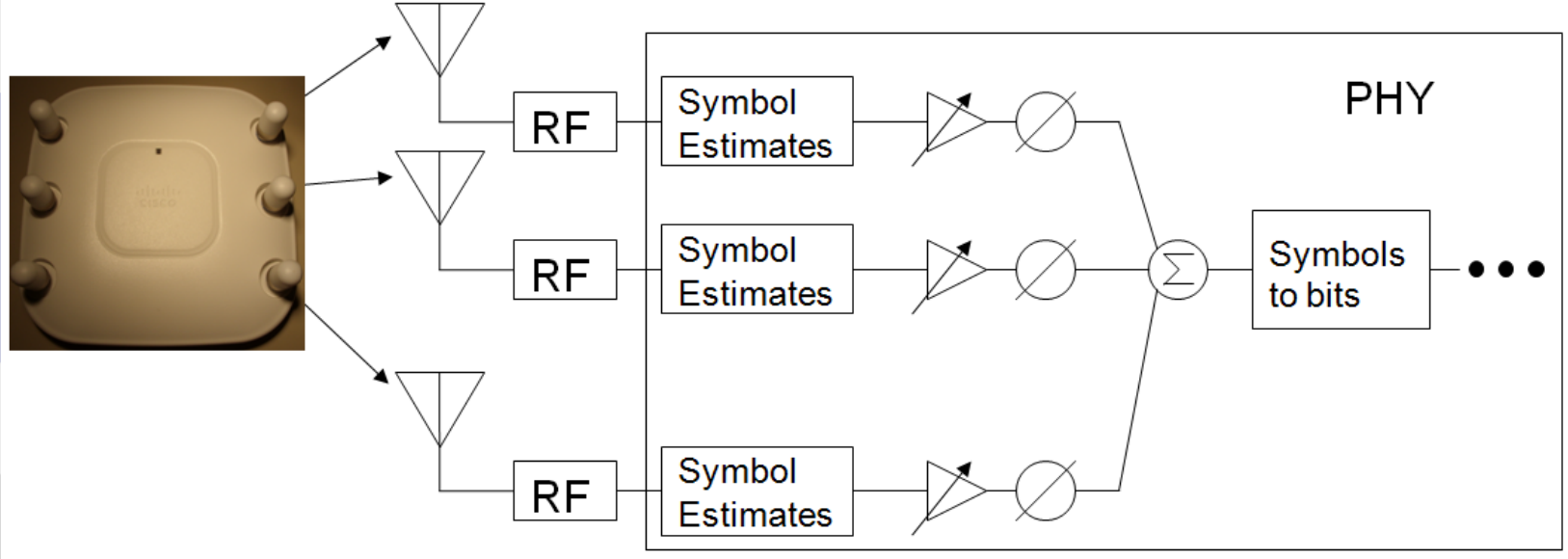
Non-802.11n diversity Access Points use two antennas sampling each antenna choosing the one with the least multi-path distortion





Multipath and Diversity (MIMO)

MRC Maximal Ratio Combining (three radios)



- Multiple antennas and multiple RF sections are used in parallel
- MRC uses DSP techniques to increase SNR
- This is a significant benefit over traditional 802.11a/b/g diversity where only one radio is used

Interference Sources

Microwave Ovens

- 2.450 GHz
- Channel 9

Wireless Cameras

- Operates on any channel
- Best jamming device invented

Cordless Phones

Radar

- S Band Radar
- 1.55 to 5.2 GHz
- Used by
  - Weather radar
  - Ship radar
  - Space Shuttle Communications

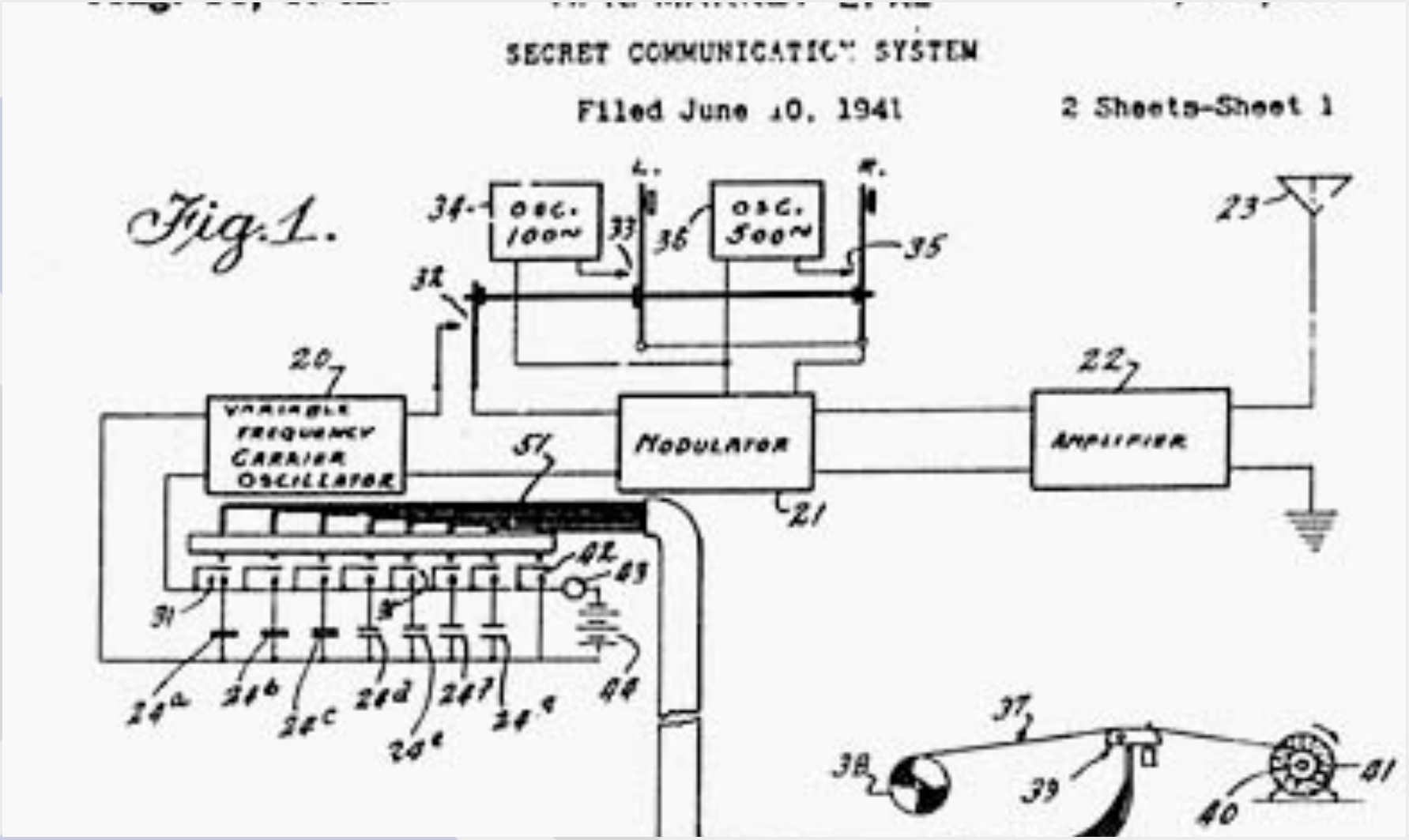
Bluetooth

- 802.15
- 2.402-2.480 GHz
  - All ISM Channels
- 79 channels (each 1 MHz wide)
- Changes channels up to 1600 times per second.

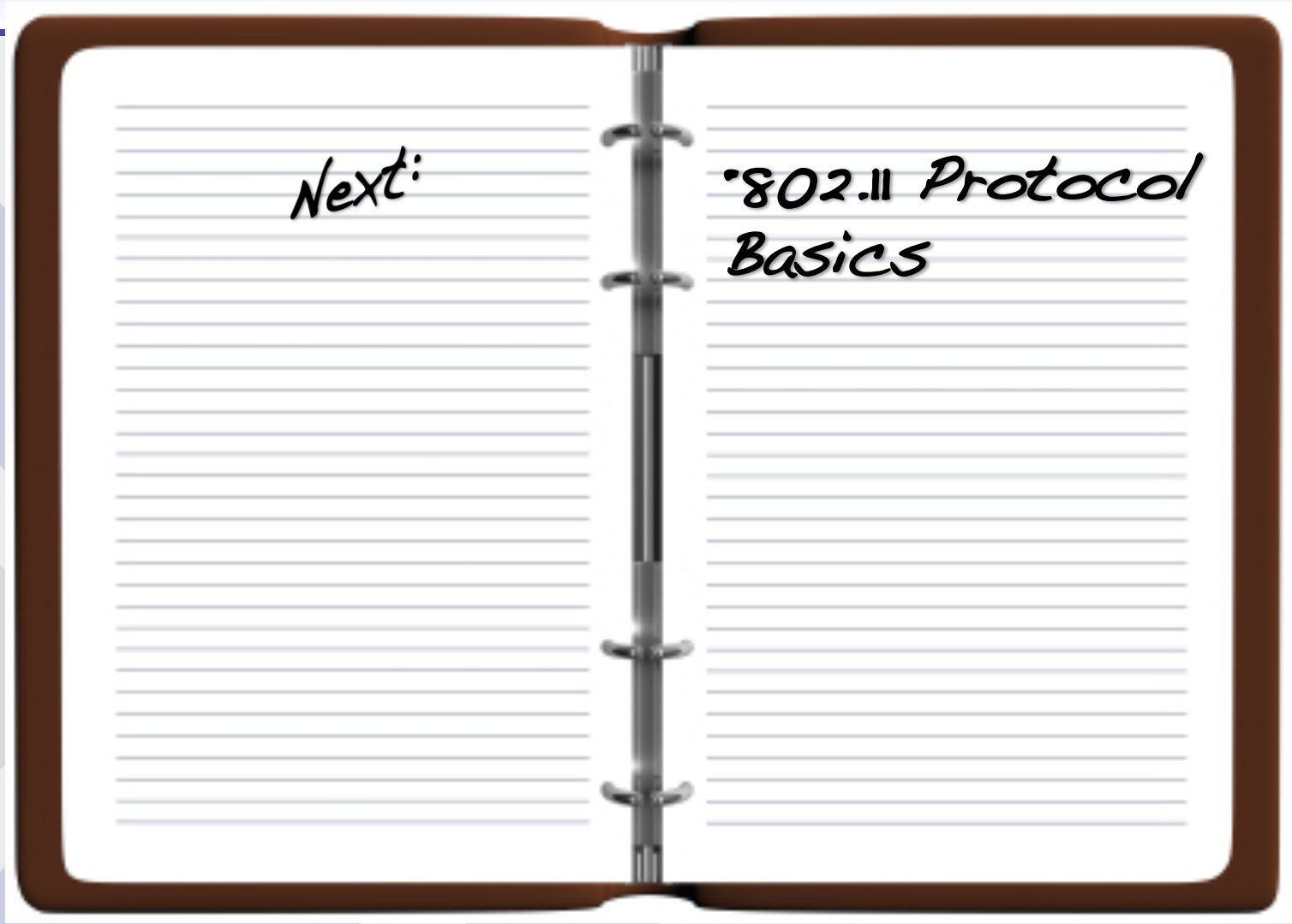
Do You Know This Woman?

- Hedy Lamarr
- 1913-2000
- Austrian-born Actress
- Hollywood Star

She Invented Frequency Hopping Radio



- The Antheil–Lamarr version of frequency hopping used a piano-roll to change among 88 frequencies
- **Frequency hopping was never implemented until 1960's**
- **Now prevents interference for Bluetooth**



802.11 is CSMA/CA

- In contrast to Ethernet (CSMA/CD)
- Differences
  - Wifi is always half duplex
  - Stations may not hear each other
  - All data frames are acknowledged

Collision Avoidance Mechanisms

- Carrier Sense
- Request To Send / Clear To Send
- Distributed Coordination Function
- ACK Frames

Carrier Sense

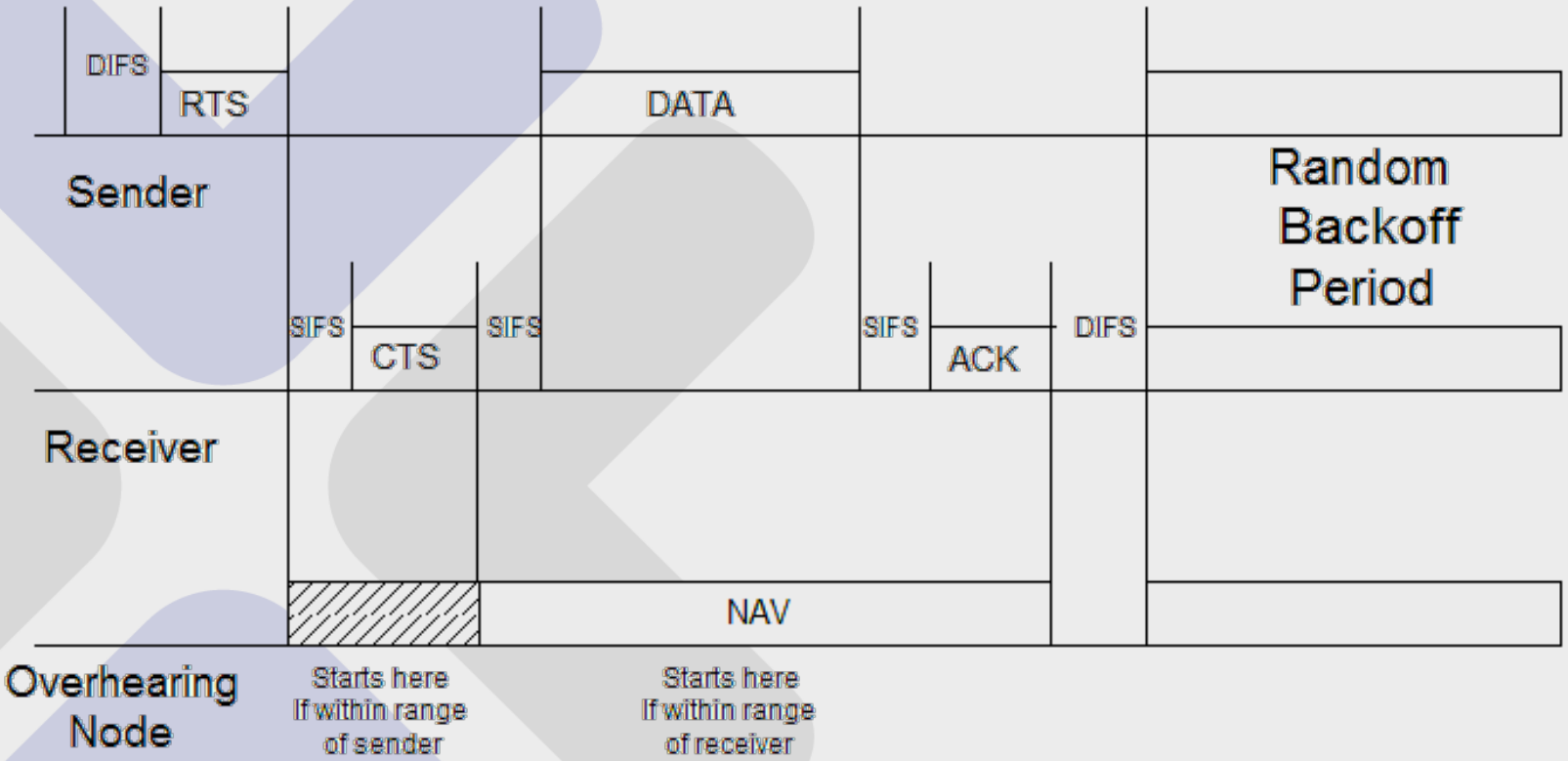
- **Do I hear a carrier?**
  - **-65 dBm for 11b/g**
- **Important that you minimize co-channel interference**

RTS/CTS

- May I talk?
- Yes, you have the floor
- RTS includes Network Allocation Vector (NAV)
  - Other stations wait this duration before attempting to transmit
  - A Sending station includes the duration in the message and the ACK response

Distributed Coordination Function

- **Random backoff period, similar to Ethernet**



Distributed Coordination Function

- Frame Spacing
  - DIFS – Data Frames
  - PIFS – Priority Frame
  - SIFS – Control Frames

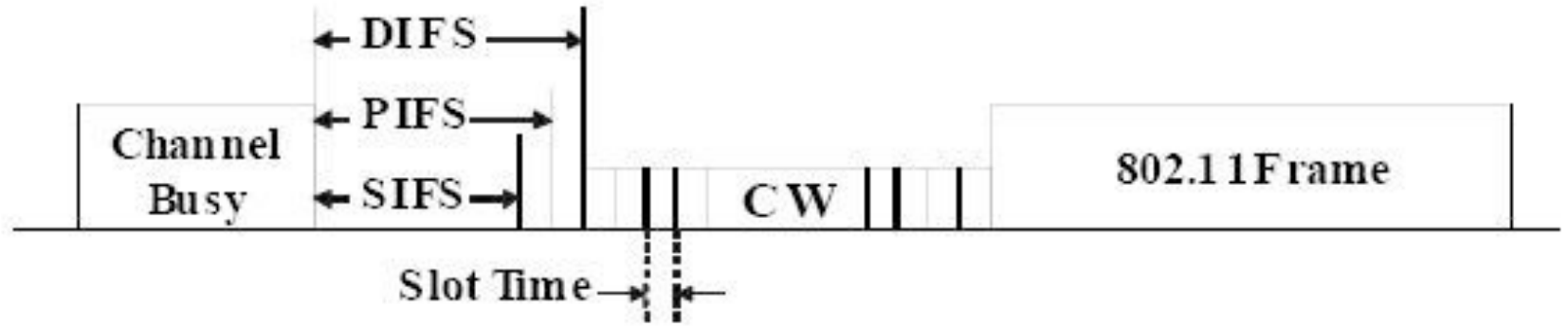


Figure 1. Illus tra tion of the inter-frame spacing in 802.11

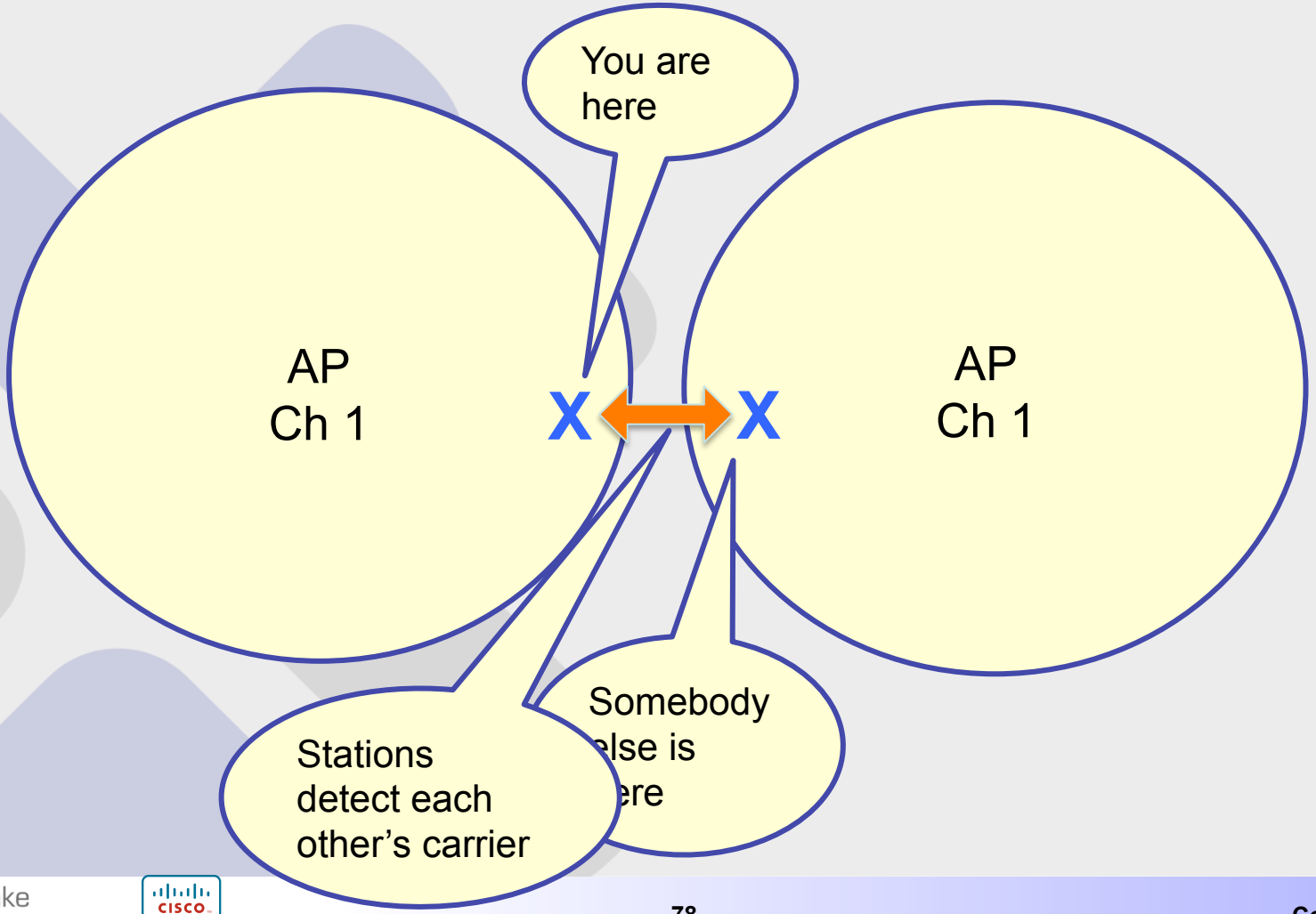
ACK Frames

- Every frame is acknowledged.
- No ACK, then must be a collision
- Backoff and retransmit

Beacons

- Sent by AP every 100mS
- Keeps everyone in sync
- Identifies WLAN (SSID)

Carrier Sense Problems



Channel 1
SSID = Cisco

Channel 1
SSID = Acme

No synchronization between users on different APs

Deploying Wireless

- We'll just talk about the planning and RF aspects
- Controller placement and configuration will be another topic.

High Level Plan

- Gather Requirements
- Initial Survey
- Calculate AP placement
- Spot check design
- Install APs
- Verify Coverage
- Adjust APs

Requirements

- Application
- Bandwidth Requirements
- Coverage Area
- Mobility
- Power
- Aesthetics

Application

- Guest Only?
- LAN replacement?
- Voice?
- Streaming Video?
- Interactive Video?
- Handheld Devices?

Bandwidth Planning: The Engineering Approach

- It is most likely that you won't be supporting just one application
- Design for the highest bandwidth demand that you intend to support
- Multiply this number by the number of connections/seats that you need to support
- This is the aggregate bandwidth you will require in your space

Design Criteria

- **User Density**
  - 100 sf / user in cubicle farms
- **VoIP bandwidth**
  - 20 calls / AP
- **Client Power**
  - Power level 13 dBm (20mW)

Bandwidth Planning: The Real World Approach

- Budgets are the usually the constraining factor

- Bottom Line: How fast do you want to spend?

WLANs are a Shared Medium

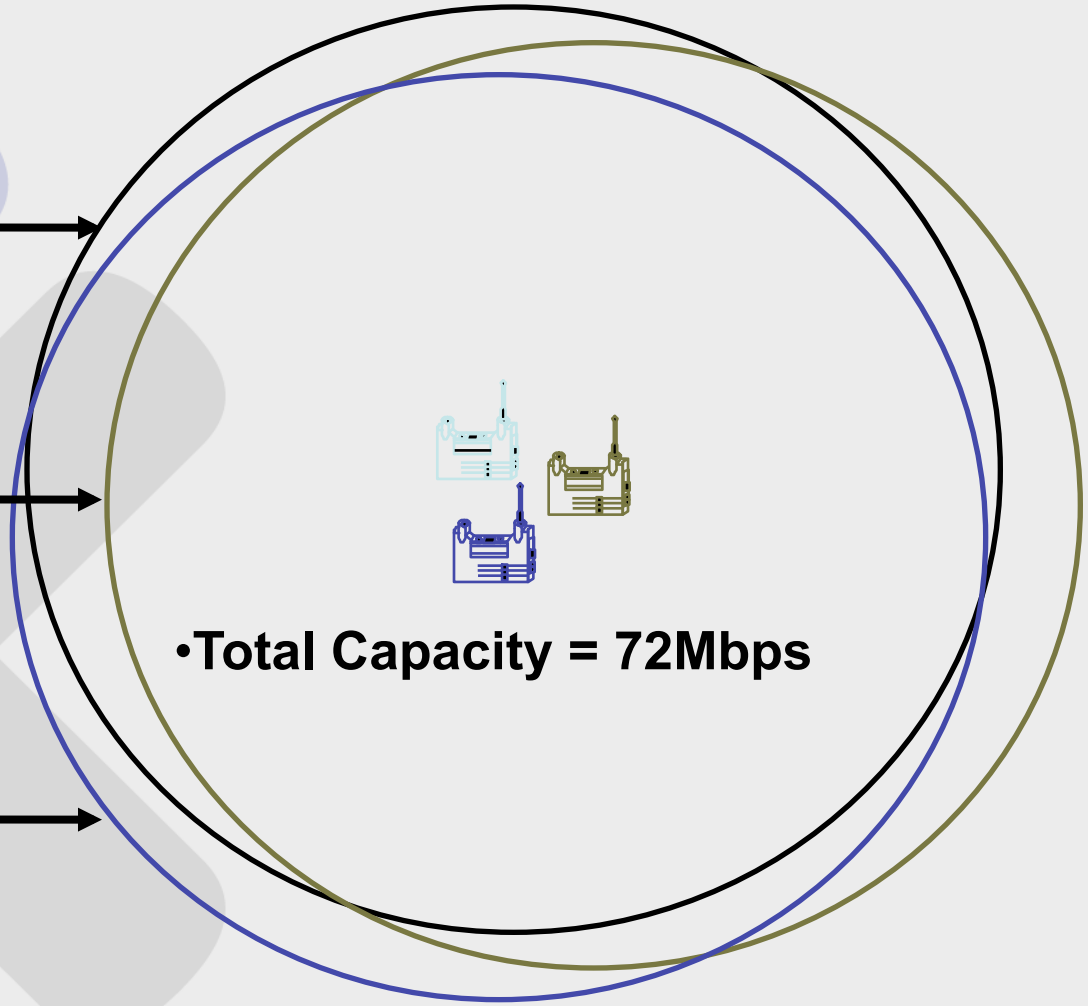
- Available Throughput is shared among users
  - Per AP
- 802.11n max throughput (laptop)
  - 1 user 150 Mbps
  - 5 users 30 Mbps
  - 10 users 15 Mbps

802.11g Scalability

•Blue = 54Mbps Data Rate, 24Mbps Throughput

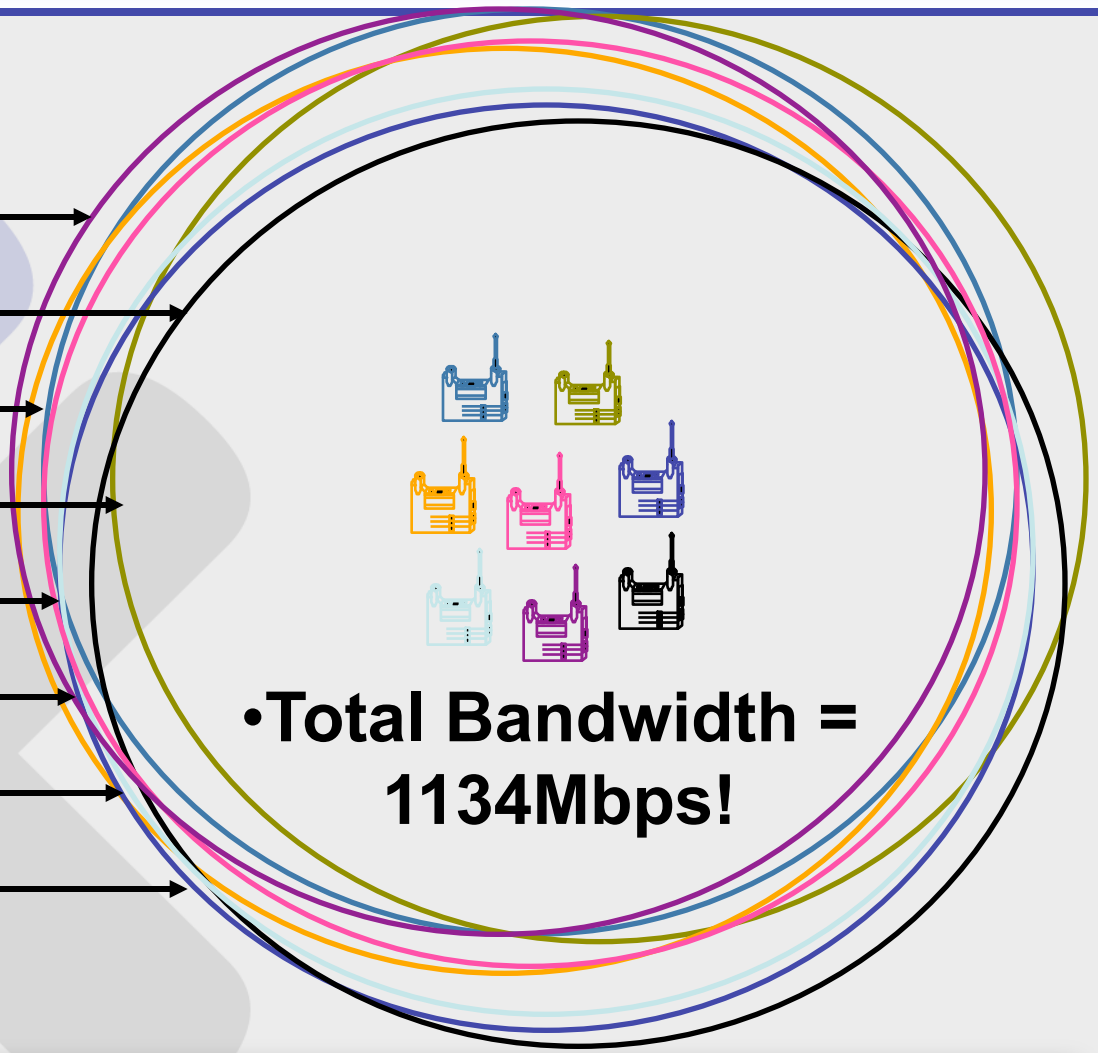
•Green = 54Mbps Data Rate, 24Mbps Throughput

•Red = 54Mbps
•Data Rate, 24Mbps Throughput



802.11a Scalability

- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps
- 54/25 Mbps



What about 11n? 9-bonded channels

Cell Size and Capacity

- For wired LANs, if you need more capacity, add more bandwidth.
- For wireless LANs, adding more APs can reduce capacity.
- Goal: Minimize, not maximize coverage
- The smaller the cell, the fewer users, therefore the more capacity.

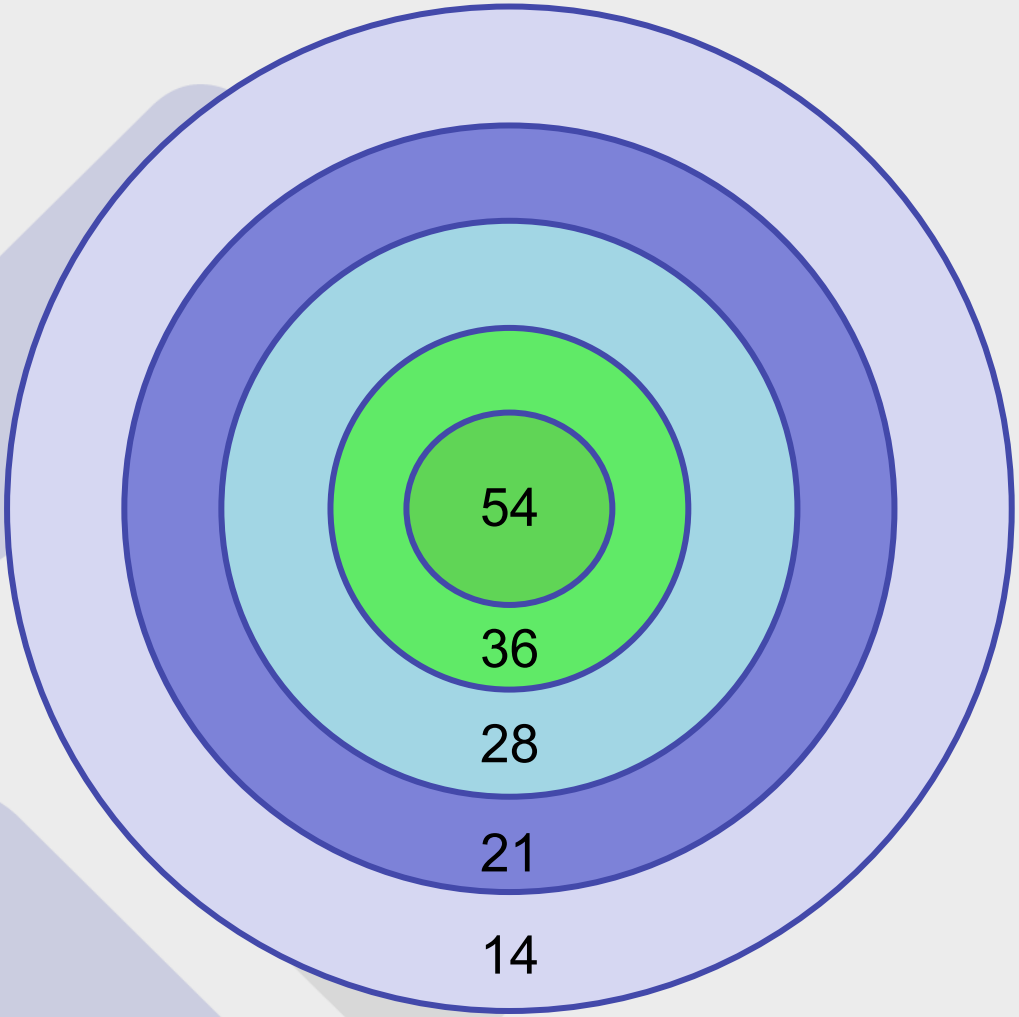
How Big Should A Cell Be?

- -67 dBm cell boundary for voice
- -71 dBm for data only
- The distance from the AP where the received power level drops to -67dBm is considered the edge of the cell

Controlling Cell Size

- Transmitter power
- Antenna
- Data rate

Range vs. Data Rate

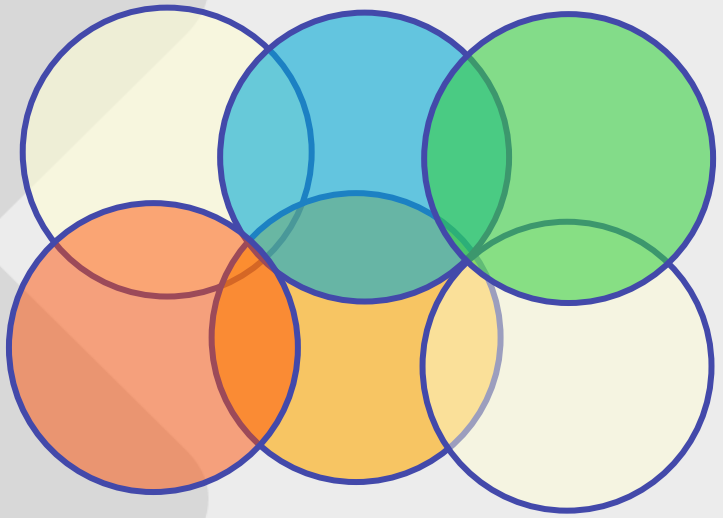


Cell Size and Data Rate

- Lower rates mean lower channel capacity
  - Broadcast/multicast/beacons always sent at lowest rate
- The weaker the signal, the lower the usable data rate
  - Low data rates makes cell too big

Cell Overlap

- Cells should have 10-20% overlap (20% for voice)
- Co-channel cells must be at least -85dBm at the cell edge



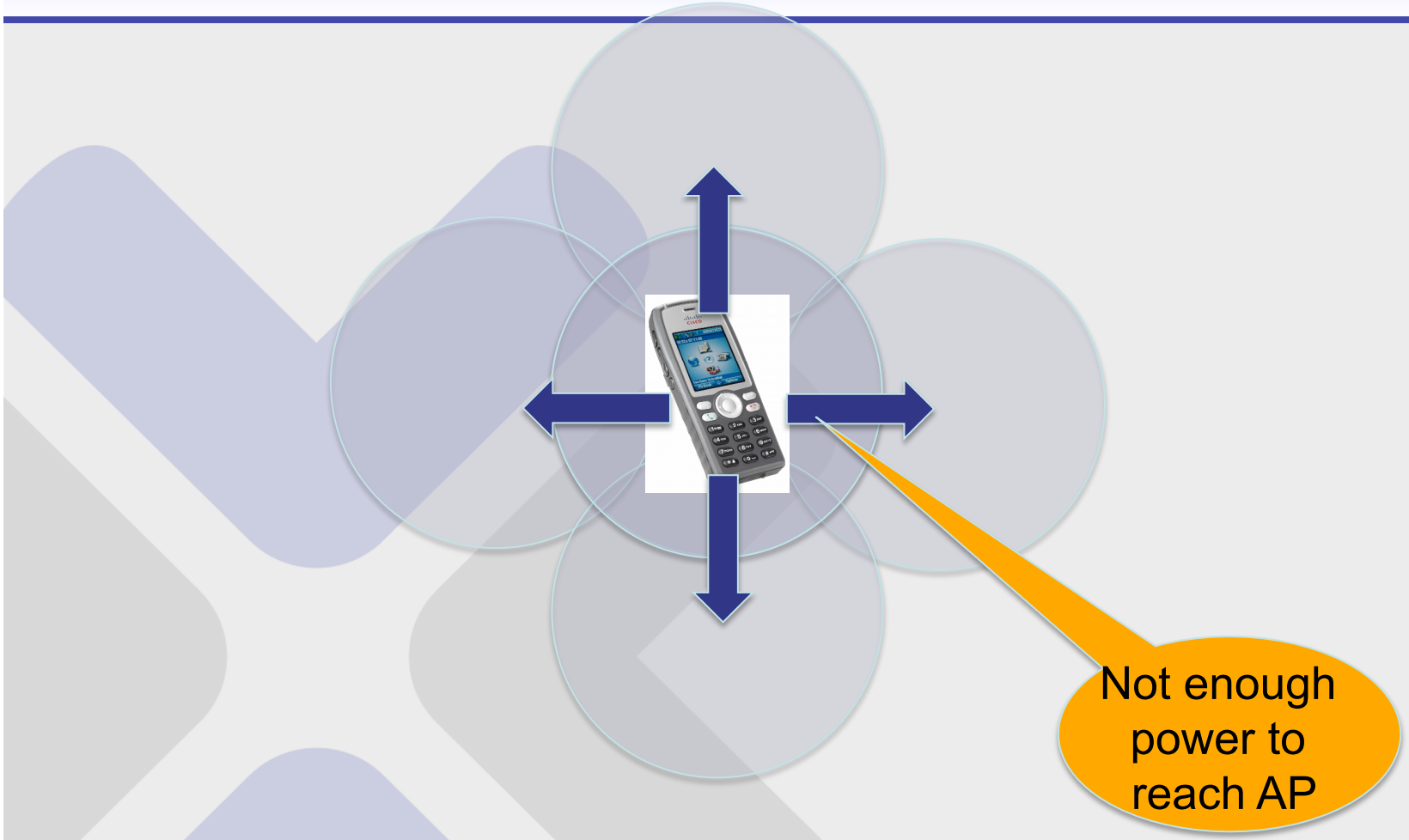
High Availability Requirements

- Hole Detection
- If AP fails…
- 80% is already covered due to overlap
- Neighboring APs increase power to cover hole

High Availability Requirements

- But…
- The client also has to increase power to reach the AP
- APs usually have more power than handsets
- Cisco Handset 7925G 40 mW
- So planning should be based on 13dBm (20 mW) or less

10 dBm



What Band Should I Use?

- Any laptop mfg in last 3-5 years is at least 11g.
- Newer supports 11a and 11n
- iPads are dual band (11a/g/n), but iPhone 4 is 2.4 GHz only (11g/n)
- Don’t support 11b unless you have specific hardware (scanners, etc.).
- Windows and Mac search for 5GHz (ch. 36) first, then switch to 2.4 GHz (ch. 1).

What Band Should I Use?

- Dense deployments, use 5 GHz
- VoWLAN, use 5 GHz
- Video, use 5GHz
- Save 2.4 GHz for guests
- Disable 11b unless absolutely required

Tradeoff

- High Density
- Higher throughput
- Small Cells
- More Bandwidth per User
- More APs

- Low Density
- Lower throughput
- Larger Cells
- Less Bandwidth per User
- Fewer APs

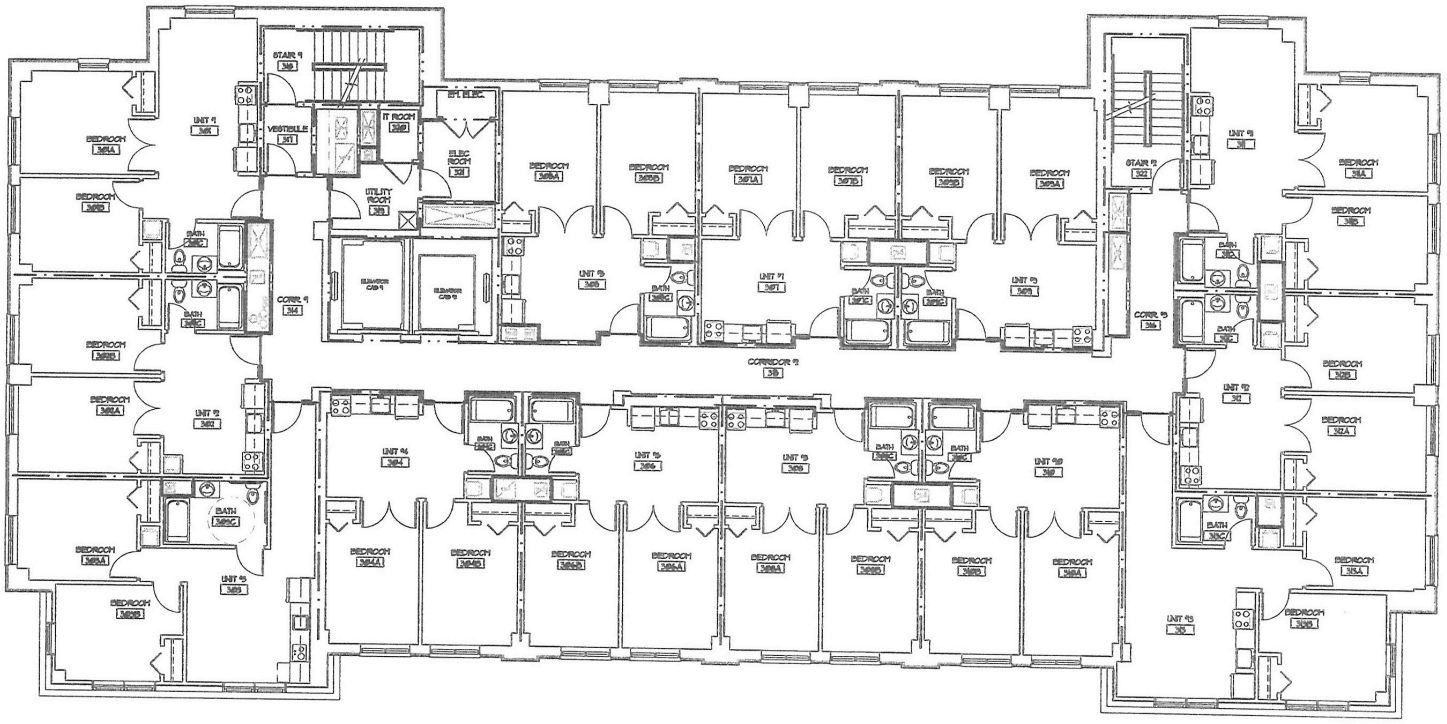
How Many APs Do I Need?

- **Rules of Thumb:**
  - **(Your thumbs may be different)**
- **1 AP/1500 sq ft (Dense)**
- **1 AP/2500 sq ft (Average)**
- **Approximately 27 ft between APs (Dense)**
  - **20% overlap**

AP Spacing

- 1500 sf 30’ spacing 39’ diameter
- 2000 sf 35’ spacing 44’ diameter
- 2500 sf 38’ spacing 50’ diameter
- 3000 sf 42’ spacing 55’ diameter

Coverage Area



Mobility

- Mostly fixed users?
- VoWLAN?
- iPad applications?
- Conference rooms only?

Power

- PoE requirements?
- UPS requirements?

Aesthetics

Survey Equipment

- Two carts (one for AP, one for laptop)
- AP Holder
- AP (autonomous) or small controller
- UPS with long extension cord
- Laser distance tool or roller wheel
- Step ladder
- Floor plans
- Digital Camera
- Stick on dots/labels
- Laptop with long extension cord or UPS

Survey Laptop

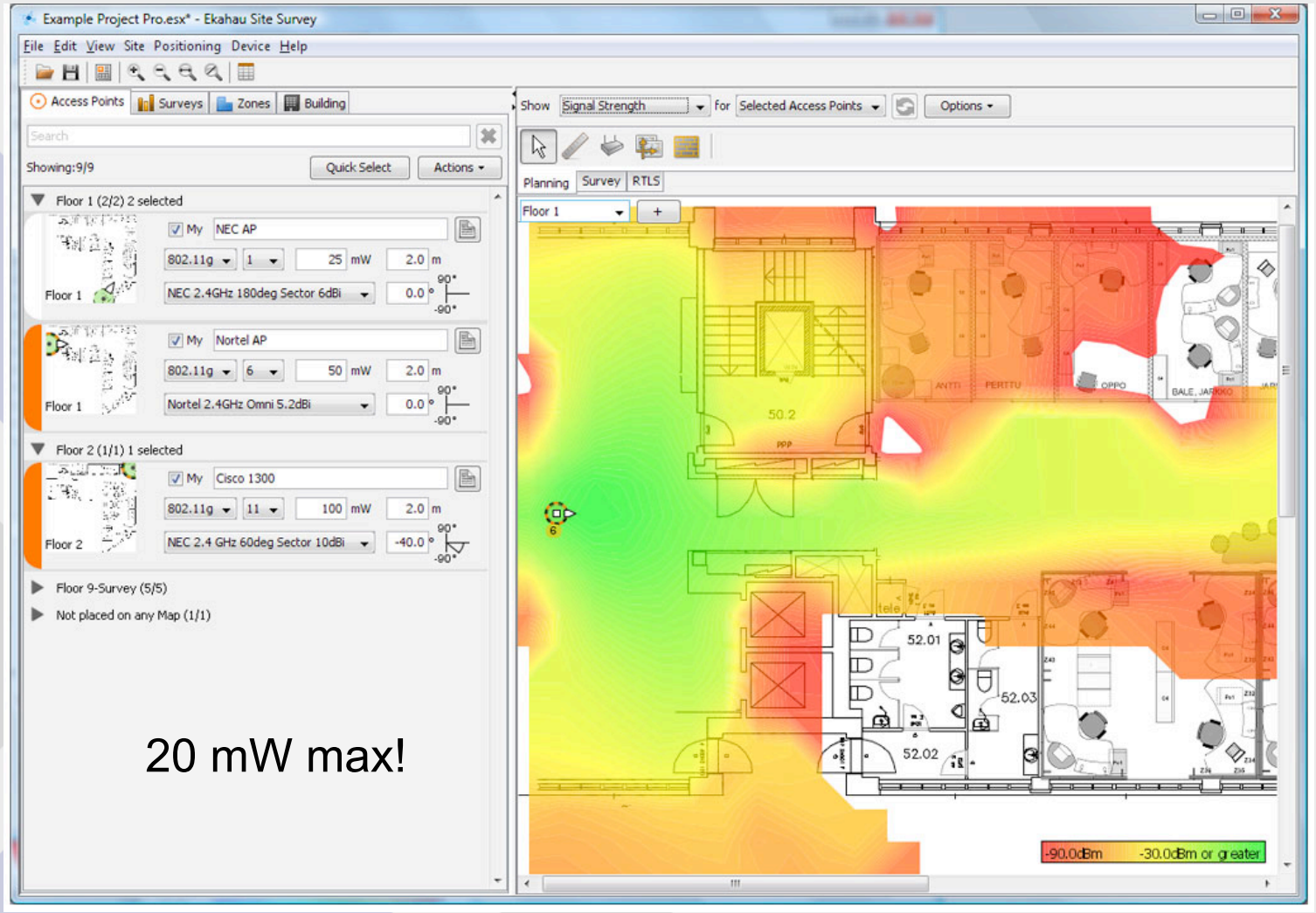
- **Survey software**
  - **Air Magnet**
  - **Ekahau**
- **Spreadsheet of AP locations, name, MAC, notes, oddities, etc.**

First Survey

- Find Interference Sources
- Other wireless networks
- Measure signal in unusual areas

Use Same Model Of AP and Antenna that you plan to buy!

Calculate AP Placement



20 mW max!

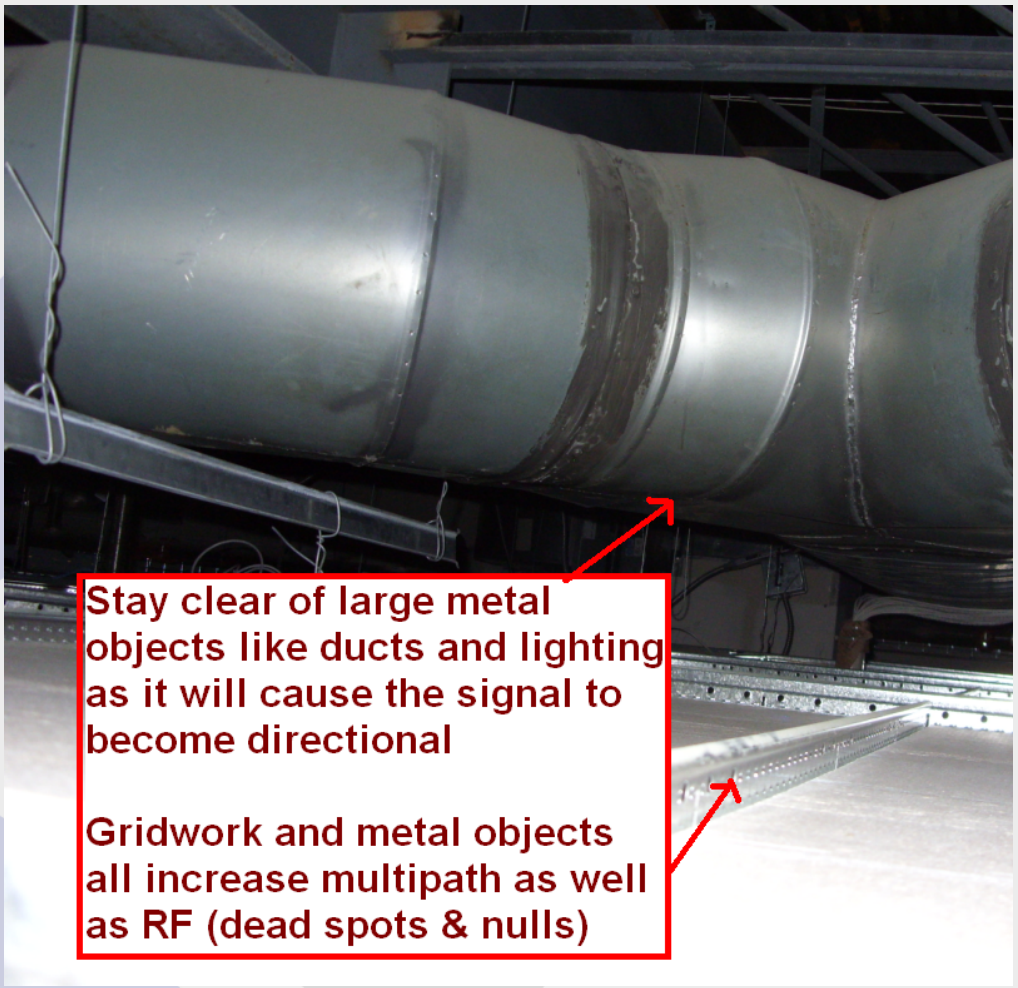
Second Survey

- Spot check AP placement.
- Don’t forget about other floors

Install APs

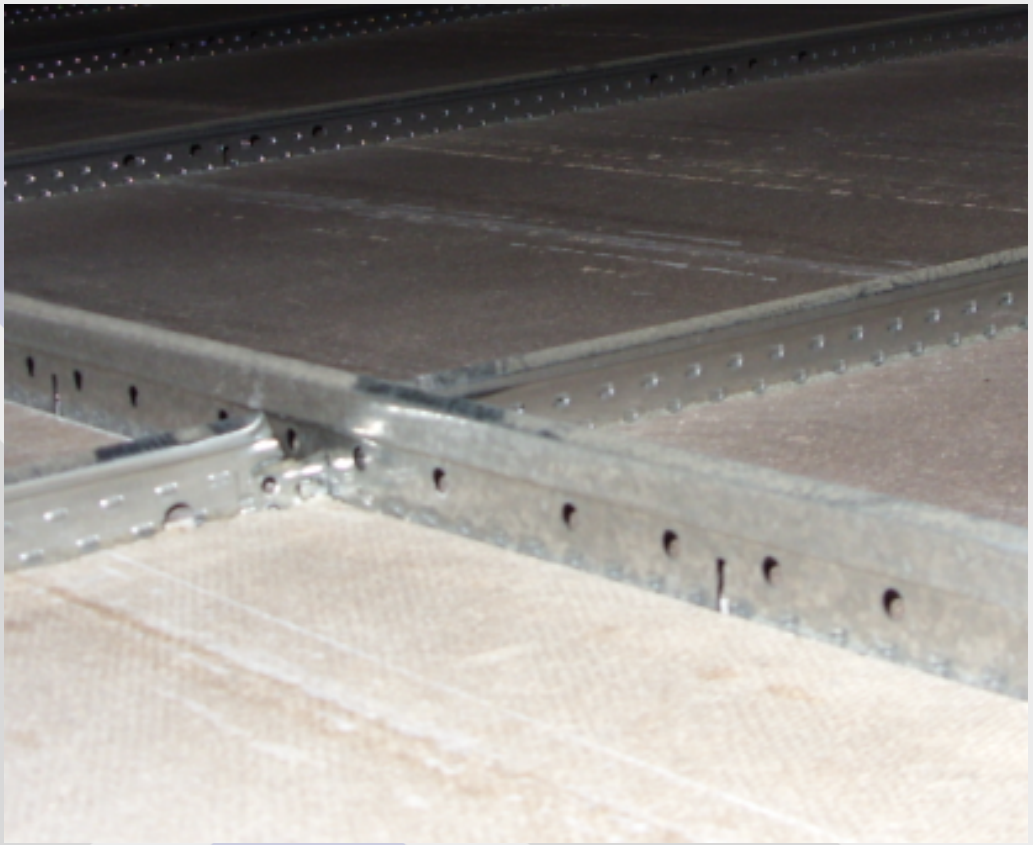
- For above ceiling, leave 10 ft of extra wire
- Mark locations with adhesive dots/ tape.
- Take pictures of each location
  - With enough visual context

AP Placement in Plenum Areas



•Installation above the ceiling tiles

Mount AP close to the tiles and away from objects



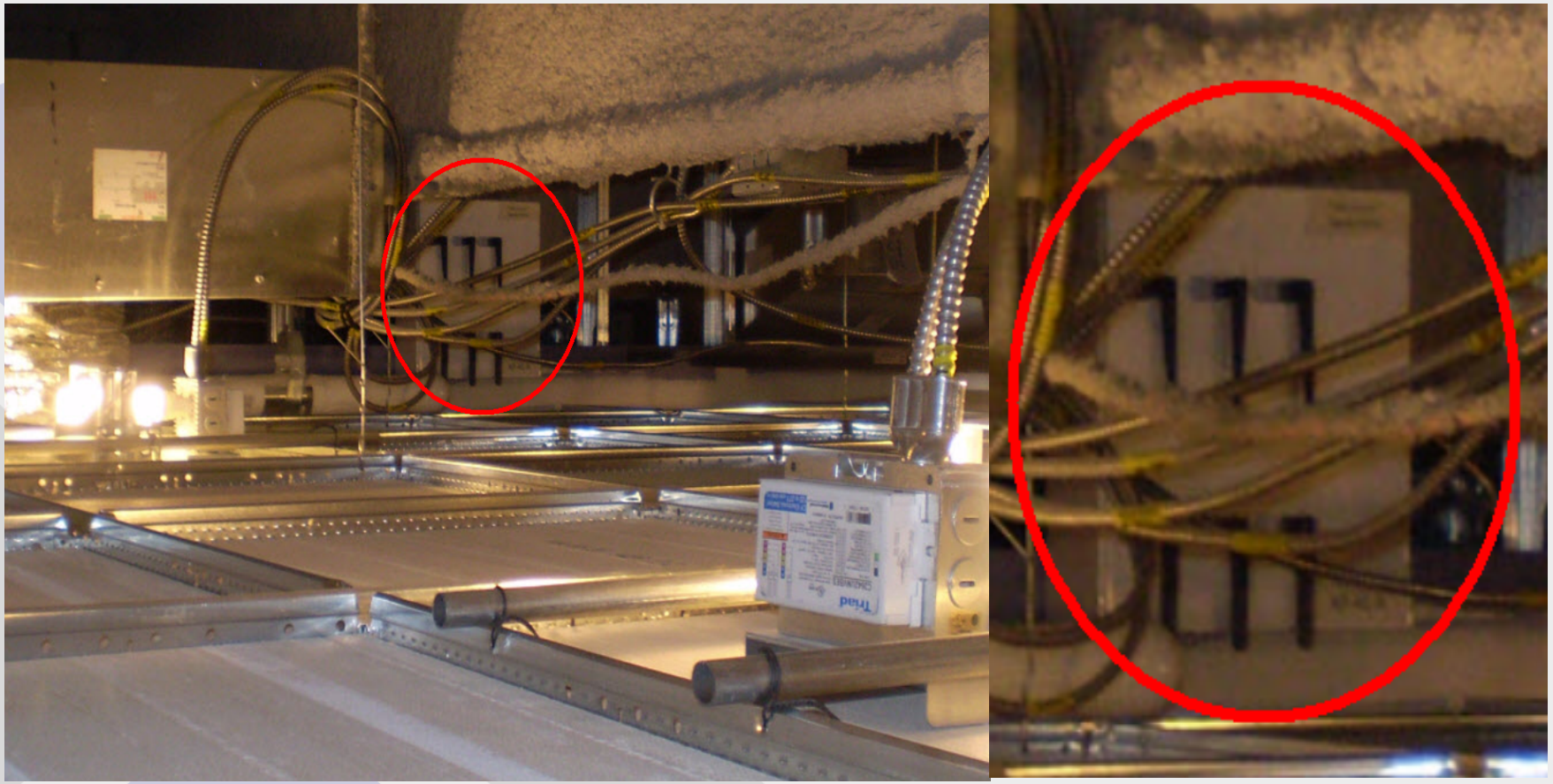
•Try to find open ceiling areas away from metal obstructions (use common sense)

•Tip: Mount antennas either below ceiling tile or the AP as close to the inside of the tile as possible

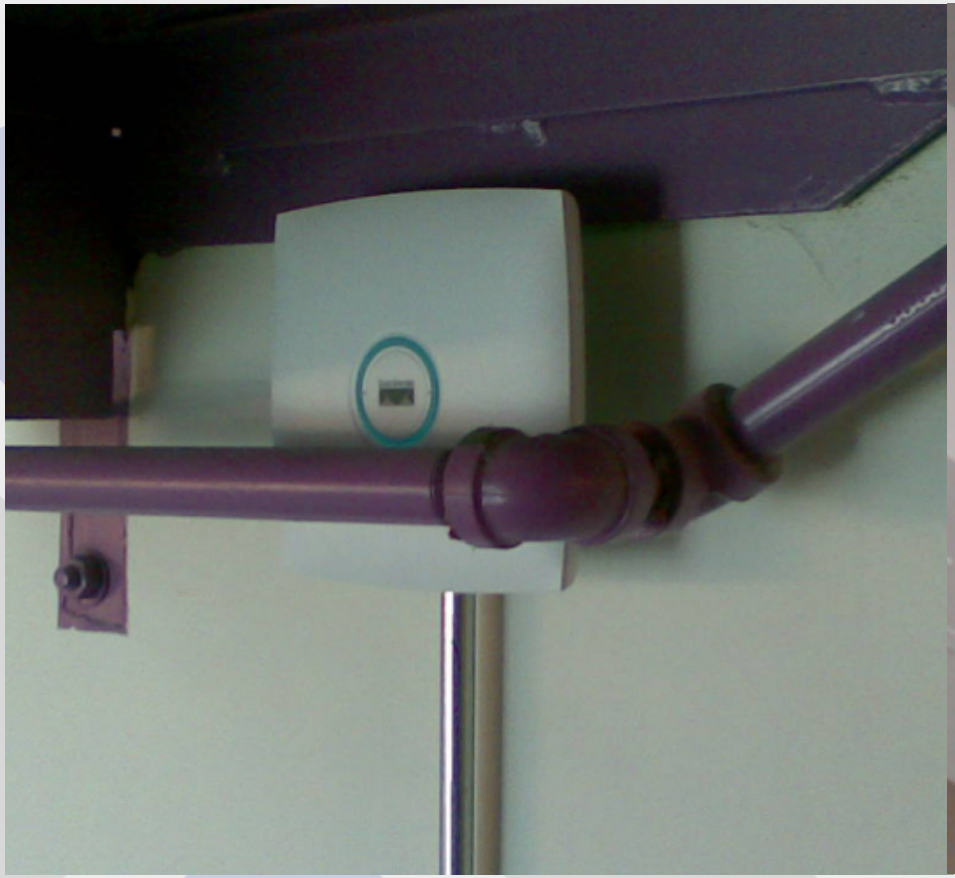
Installs That Went Wrong

- Dipole antennas up against a metal box create a patch like antenna - that plus metal pipes create unwanted **Multipath Destructive Interference**

Installs That Went Wrong



Installs That Went Wrong



- Ceiling mount AP up against pipe
- Antennas are obstructed

- Metal duct blocking antenna causing
- Multipath interference

Installs That Went Wrong

•Patch antenna - Shooting across a metal fence – Put it on a cross arm away from fence or find a better location

•Mount the box “lid down” with the antennas pointing downward – Tip: Antennas do not work well against metal

Ummm…

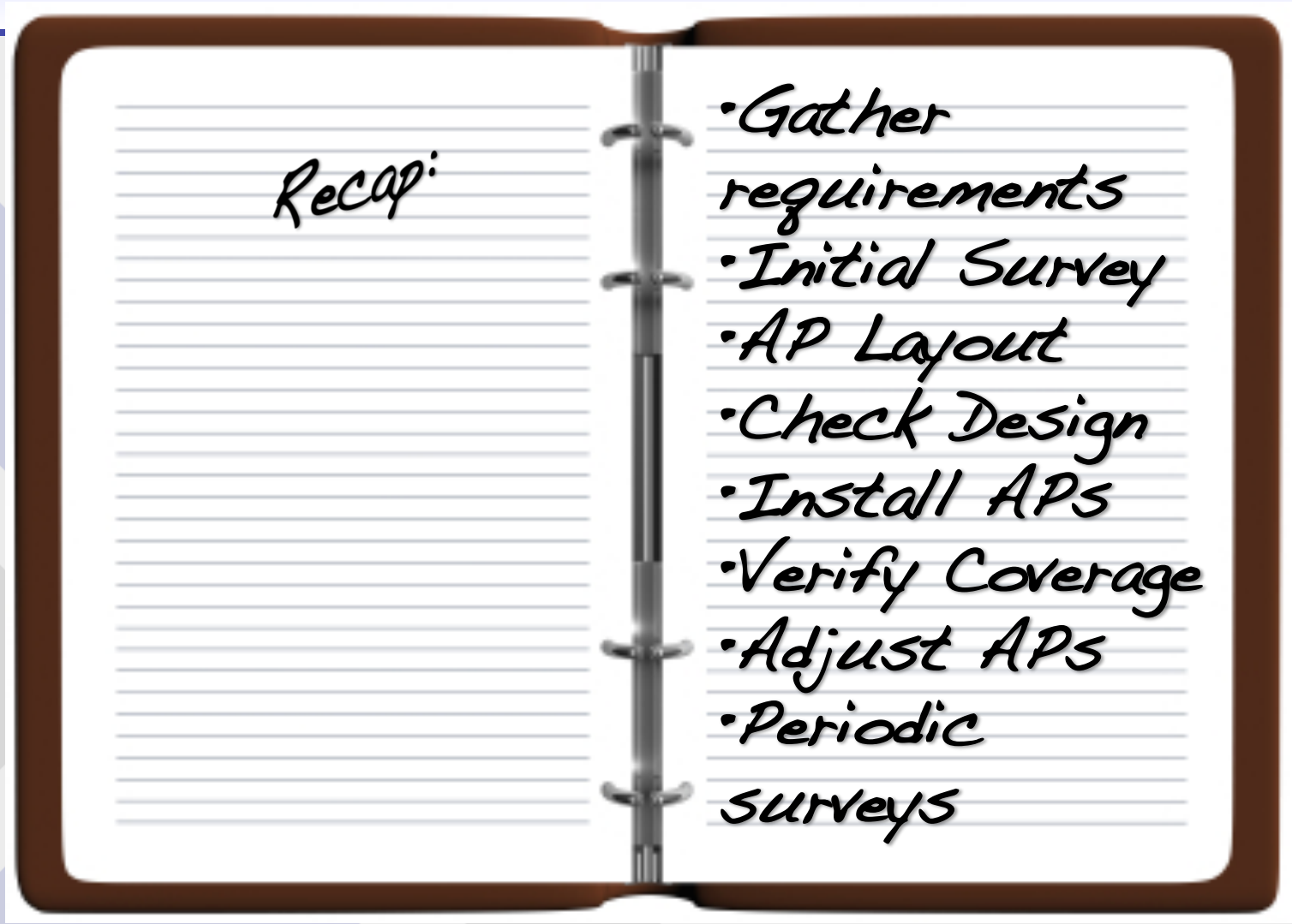
Final Survey

- Verify placement
- Verify roaming
- Verify unusual coverage

- Adjust APs if necessary

Periodic Surveys

- Spot check coverage on a regular basis
  - 3 – 6 months
- New construction
- New equipment
- New applications
- New devices



Hooray! The End!

Questions?

- Rtrunk (at) netcraftsmen.net

- Yes, slides will be posted on our website
- www.netcraftsmen.net/cmug