



Long Distance Wireless Networking

Using Non-licensed Radios

Tim Pozar

Late Night Software

www.lns.com

Bay Area Wireless Users Group

www.bawug.org



The Lofty Goals...

- ⇒ A general knowledge of what can & can't be done.
 - ⇒ “10,000 foot view” as details can't be covered in 1 hour.
 - Would need at least a 3 day course
 - ⇒ I will be touching on a number of subjects.
 - ⇒ Pointers to details as we go along and at the end.
 - ⇒ Should get you started in design of your network.
 - ⇒ Better idea of when a consultant is steering you straight.
- ⇒ What issues are there in deploying a long distance link or network.
 - ⇒ Technical – RF
 - ⇒ Some Regulatory
 - See my paper at: <http://www.ins.com/papers/part15>
 - ⇒ Security

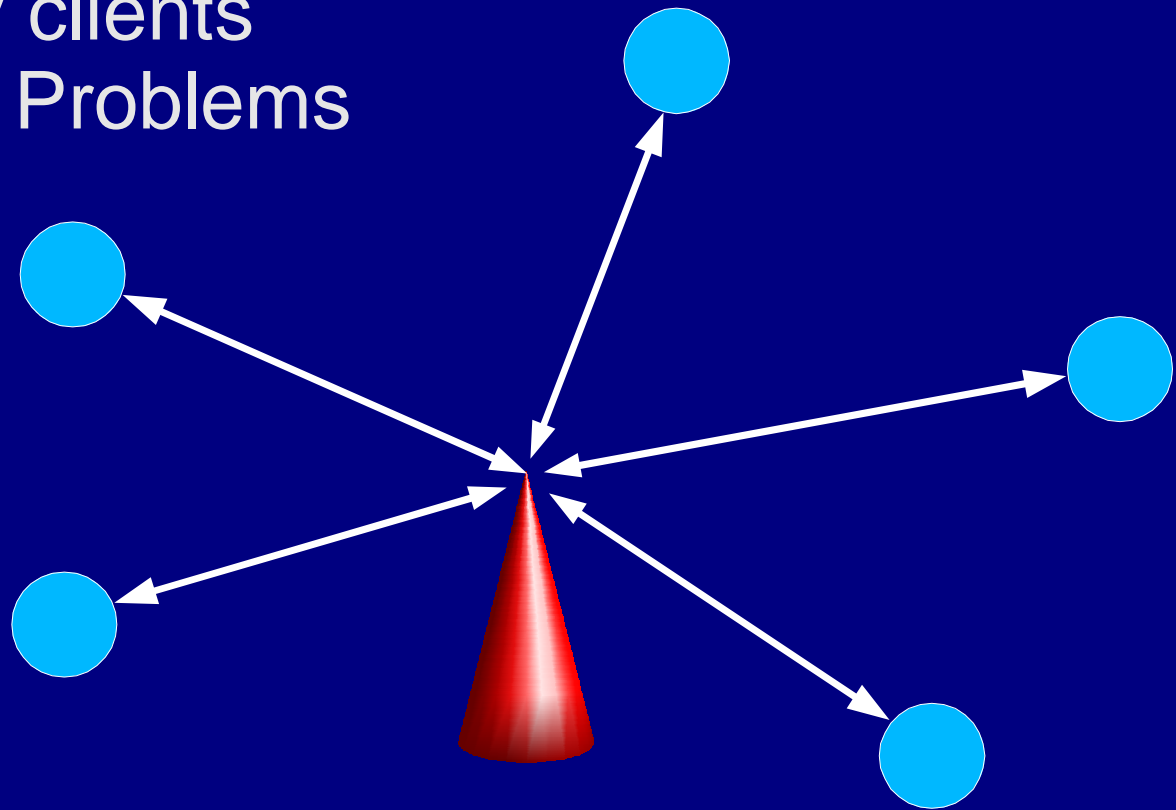


Applications

- ⇒ Home/Office (LAN)
 - ⇒ Originally designed for and the traditional use.
- ⇒ Campus Area Network (CAN)
 - ⇒ How do you get across the street or a city?
- ⇒ Wireless ISPs (WISPs)
 - ⇒ WISPs will try to cover a small area (Hot Spot) such as a store or cafe all the way up to a rural or metropolitan area (MAN).
 - ⇒ One Access Point (AP) can do about a 10 mile radius legally.

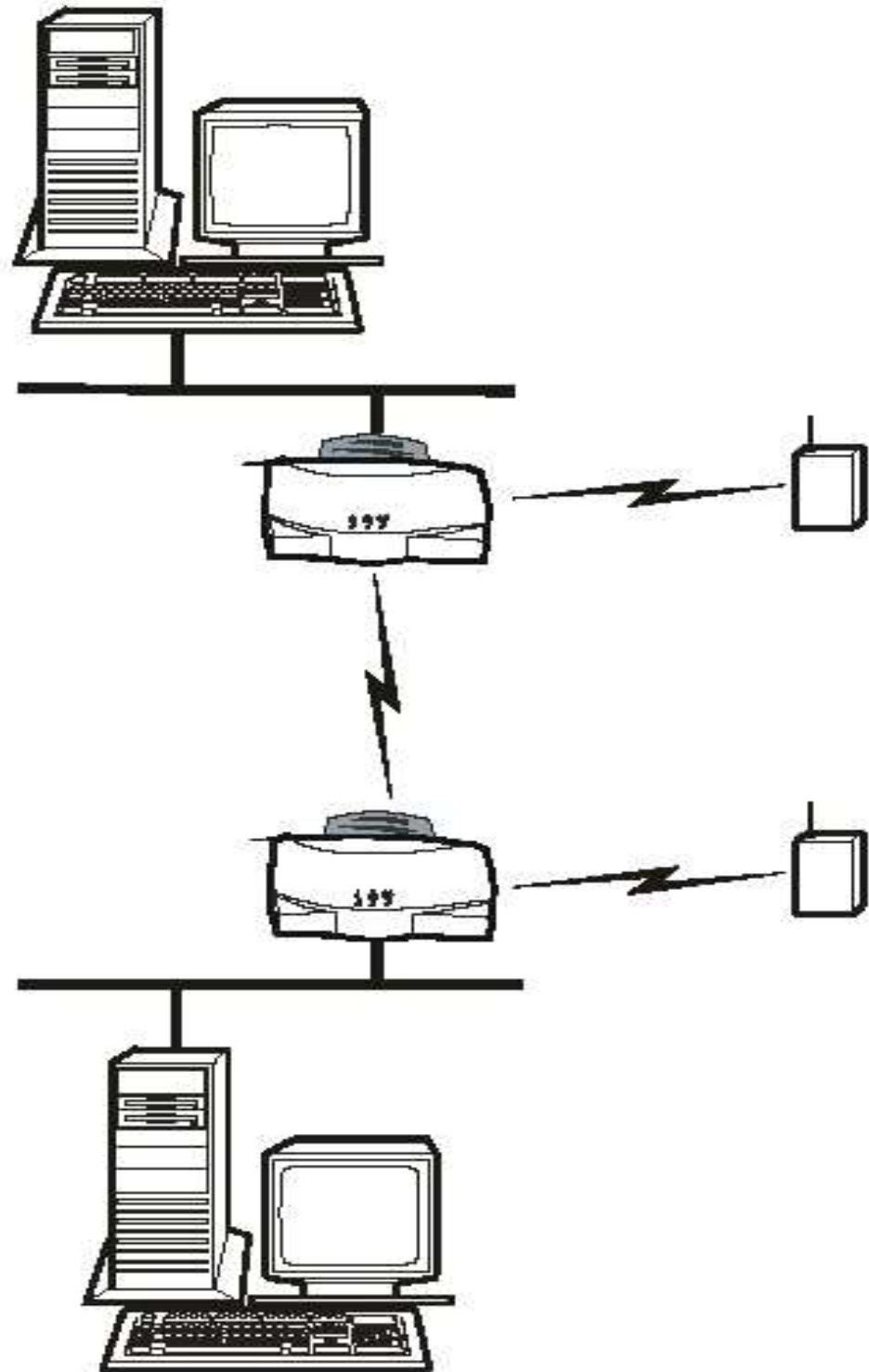
Topology - Star Mode

- ⇒ Traditional Design
- ⇒ One AP / Many clients
- ⇒ Hidden Xmitter Problems



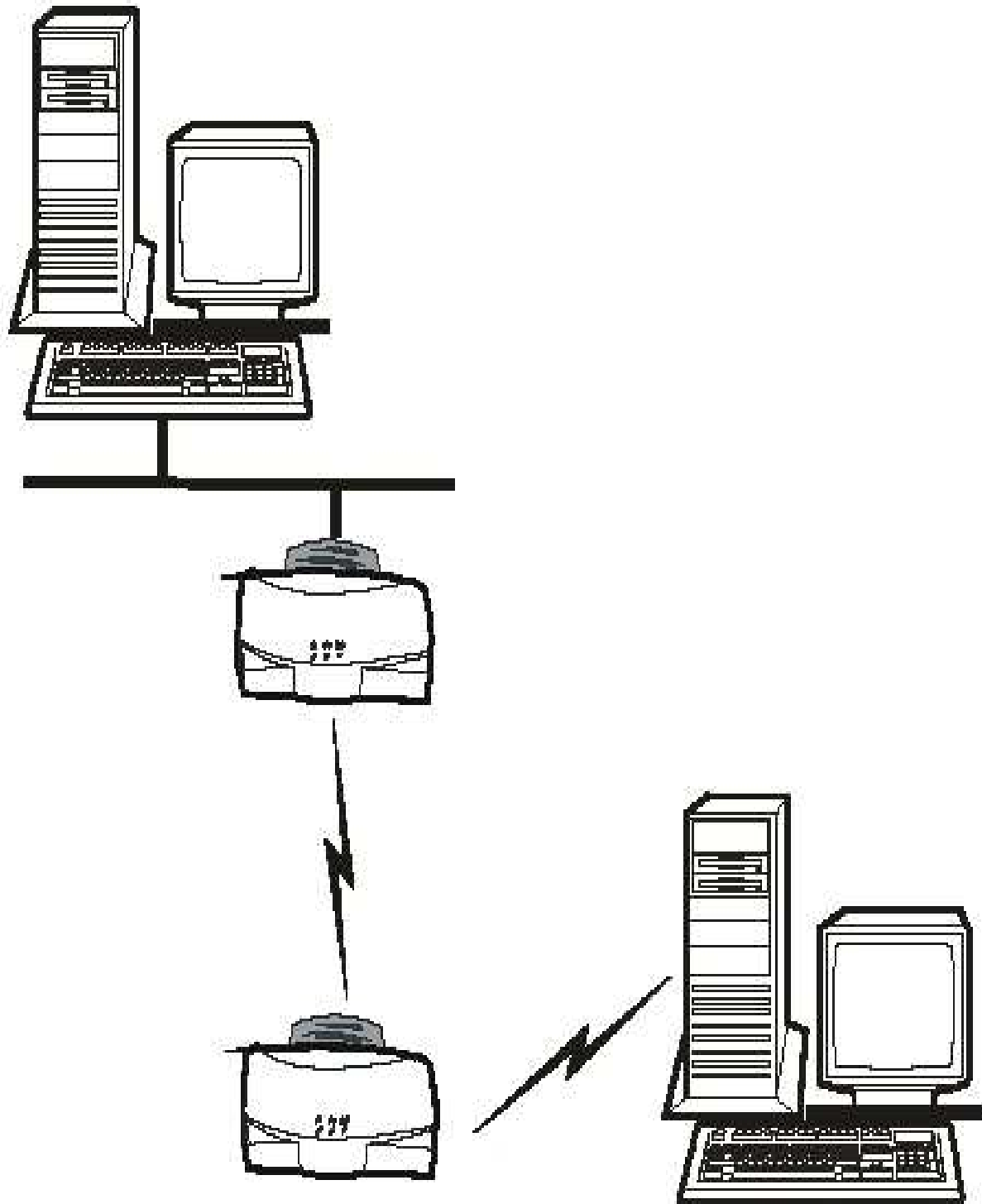
Topology - Bridging

- ⇒ Used to link two Ethernet Segments
- ⇒ If designed properly it can go 10s of miles.
- ⇒ Traffic is unencrypted unless you run additional software or hardware.



Topology - Repeater

- Extends the wireless range.
- Getting around obstacles





Applications - Community Networks

- ⇒ The ones that are stretching the limits of the technology.
 - ⇒ Uses much of the same technology and layout.
 - ⇒ Just more power and slightly more expense.
- ⇒ Co-operative in nature
- ⇒ Defined to be “free” within a network co-op.
- ⇒ Examples:
 - ⇒ Neighborhood Area Networks (NAN) and Hot-Spots
 - Early example of a community network
 - Short range - ~1 mile diameter
 - NYC Wireless - Bryant Park in NYC...
 - Coverage Map of PozarLAN...

Bryant Park

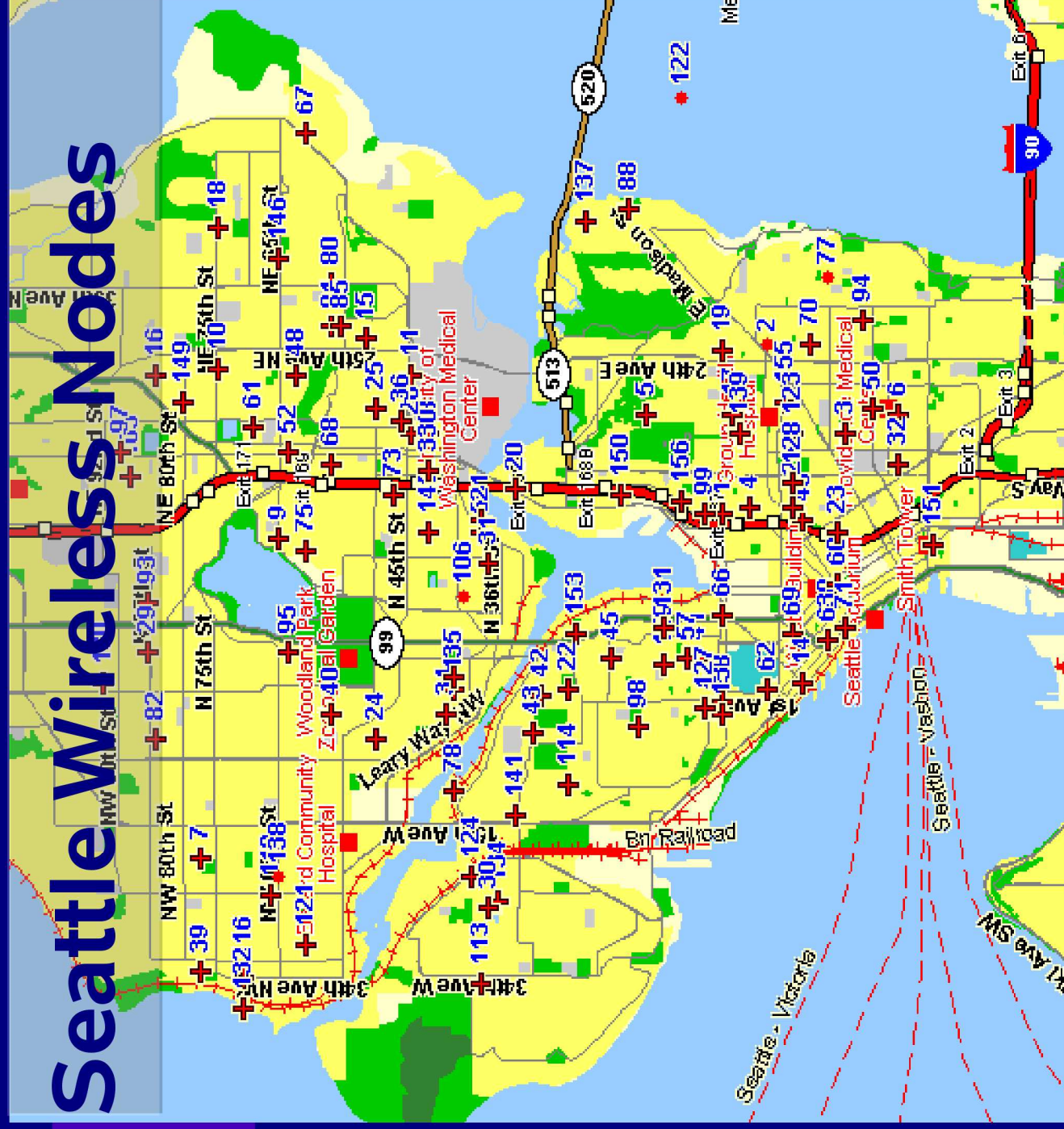




Community Networks

- ⇒ MAN sized:
 - ⇒ San Francisco Presidio – SFLAN
 - Point to multipoint
 - ⇒ Seattle Wireless...
 - Mesh Network
- ⇒ Multiple Counties:
 - ⇒ BARWN – San Francisco Bay Area...

Seattle Wireless Nodes



BAWRN Network Map





Why Use 802.11?

- Biggest reason: Non-licensed
 - Significantly less regulatory control
 - No expensive licenses or coordination.
 - The arcane regulatory knowledge needed for licensed radios is not needed.
- The hardware cost is magnitudes less than equivalent licensed technology.
 - Client cards are from \$35 to \$150; Access Points are from \$50 to \$500.
 - Even less than (non) unlicensed "carrier class" radios
 - Example: Western Multiplex/Proxim Tsunami point-to-point radios are \$12,000 per end not including the thousands of \$ for antennas, coax, installation, etc.



Why Use 802.11? (cont.)

- ⇒ Speeds range from 11Mb/s to 54Mb/s
 - ⇒ Another magnitude jump of low-cost networking hardware from a couple of years ago. (2Mb/s) or even 2 to 3 magnitudes of amateur packet radio (1.2-56Kb/s).
 - ⇒ Real world speeds about 5Mb/s to 20Mb/s
- ⇒ Plug and play
 - ⇒ Most modern operating systems support 802.11
 - i.e. Mac OSX, *BSD, Linux, MS-Win 95 to XP.
 - ⇒ Depending on implementation, it can be as easy to set up as standard Ethernet and in some cases easier.



Why Use 802.11? (cont.)

- ⇒ A significant number of manufactures are putting money and releasing hardware that are compatible with 802.11 standards.
 - ⇒ Cisco, Agere, Breezecom, Symbol/3com, Xircom/Intel, Intersil/Prism, Atheros, Proxim/ORiNOCO, etc.
- ⇒ Of course its wireless
 - ⇒ Good solution for older installations/buildings
 - ⇒ Roaming of laptops



Why Not Use 802.11?

- ⇒ Biggest reason: Non-licensed
 - ⇒ Non-existent coordination facilities.
 - ⇒ Other users on the bands.
 - Folks with large organizations that lobby (ie. ARRL, SBE)
 - ⇒ “Regulations Affecting 802.11 Deployment”:
<http://www.ins.com/papers/part15>
 - ⇒ You have no legal priority or recourse over any other user of the spectrum...



FCC R&R Part 15.5

General Conditions of Operation

(b) Operation of an intentional, unintentional, or incidental radiator is subject to the conditions that no harmful interference is caused and that interference must be accepted that may be caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

(c) The operator of a radio frequency device shall be required to cease operating the device upon notification by a Commission representative that the device is causing harmful interference. Operation shall not resume until the condition causing the harmful interference has been corrected.



Why Not Use 802.11? (cont.)

- ⇒ The protocols have problems scaling.
 - ⇒ Companies like Etherlinks are trying to solve it.
 - ⇒ Modifications to the standards will help minimize interference (ie. Automatic Power Control and frequency selection)
- ⇒ Outdoor deployment requires RF engineering knowledge to minimize interference issues.
- ⇒ Other regulatory issues one may have to deal with for outdoor deployment.
 - ⇒ Radio Frequency Radiation standards
 - ⇒ Local ordinances for antennas
- ⇒ Security – (more later on)



Conclusions on issues

- ⇒ Building an expensive network on 802.11 can be risky as you have no rights or priorities.
- ⇒ Coordinate with other users.
- ⇒ A properly designed network will survive longer.
- ⇒ Other issues can affect you like FCC Rules changes or pressure to get the FCC to enforce. Be active in watching and changing the FCC's Rules!



Why Not Use 802.11? (cont.)

What this all means is you should consider getting yourself an expert in the area if you are putting in a sizable investment and want your network to last.
Until then...



How to Design a Network:

⇒ Site Survey

- ⇒ Should be done for every deployment.
- ⇒ Depending on the complexity of the deployment, the engineering study requirements will change.
- ⇒ It gets down to - “Can you get the signal from one antenna to the other so it can be successfully used?”

⇒ Engineering the Link

⇒ Antenna Requirements

- The signal should only go where it is needed to minimize interference to other networks and to your own.

⇒ Signal Requirements

- Transmitter power
- Signal strength needed for the receiver



Site Survey

- ⇒ Short distances (<30meters) can be determined by visual inspection.
- ⇒ Longer distances will likely need to use visual with microwave path engineering software.
- ⇒ Examples:
 - EDX - www.edx.com - 10s of thousands of \$
 - PathLoss - www.pathloss - ~\$4,000
 - Radio Mobile -www.cplus.org/rmw/ - Free (example later)
- ⇒ The more you pay the more accurate the uptime and coverage predictions.
 - Details later



Site Survey (cont.)

- ⇒ Real and potential interference needs to be evaluated.
 - ⇒ Look around. What antennas do you see nearby?
 - ⇒ Objects nearby that will cause multi-path? (future slides)
- ⇒ Non-intrusive testing - sniff around:
 - ⇒ Use dstumbler or netstumbler to see what SSIDs you can see.
 - ⇒ Note channel usage.
 - ⇒ A spectrum analyzer will reveal non-802.11 RF.
- ⇒ Try it out:
 - ⇒ Bring masts and 24 dBi dishes.
 - ⇒ Note signal and noise levels.



Engineering Software Design - Questions:

- ⇒ Overview:
- ⇒ Can the antennas can see each other?
- ⇒ Do objects cut into the Fresnel Zone?
 - ⇒ How high do we need the antennas to clear?
- ⇒ What is the free-space path loss?
 - ⇒ First cut on what size of antennas and transmitter power output (TPO) needed.
- ⇒ What is the predicted up-time of the path determined from frequency, EIRP, distance, weather, type of terrain, etc.
 - ⇒ Final cut before field test of antennas and TPO.

Loss and Gain in a System

⇒ Gain:

- ⇒ Transmitter Output Power (TPO) in dBm or Watts.
 - $\text{dBm} = 10 \cdot \log_{10}(\text{power in milliwatts} / 1 \text{ mW})$
 - 0 dBm/1 mW; 15dBm/30mW; 20dBm/100mW; 30 dBm/1 W
- ⇒ Transmitter and receiver amplifiers
- ⇒ Transmit and receiving antennas.

⇒ Loss:

- ⇒ Coax, connectors
 - ie. LMR-400: 0.22 dB per meter.
- ⇒ Free-space loss
 - $\text{dB} = 92.4 + 20 \text{ Log}_{10}(\text{distance in km}) + 20 \text{ Log}_{10}(\text{freq. in GHz})$
- ⇒ Obstructions and Diffraction (ie. Trees, rain, etc.)
- ⇒ Atmospherics (ie. Snow/Rain, Refraction (ie. Ducting))

Simplified Path Calculation Schematic

Omni-directional
Antenna

Directional
Antenna

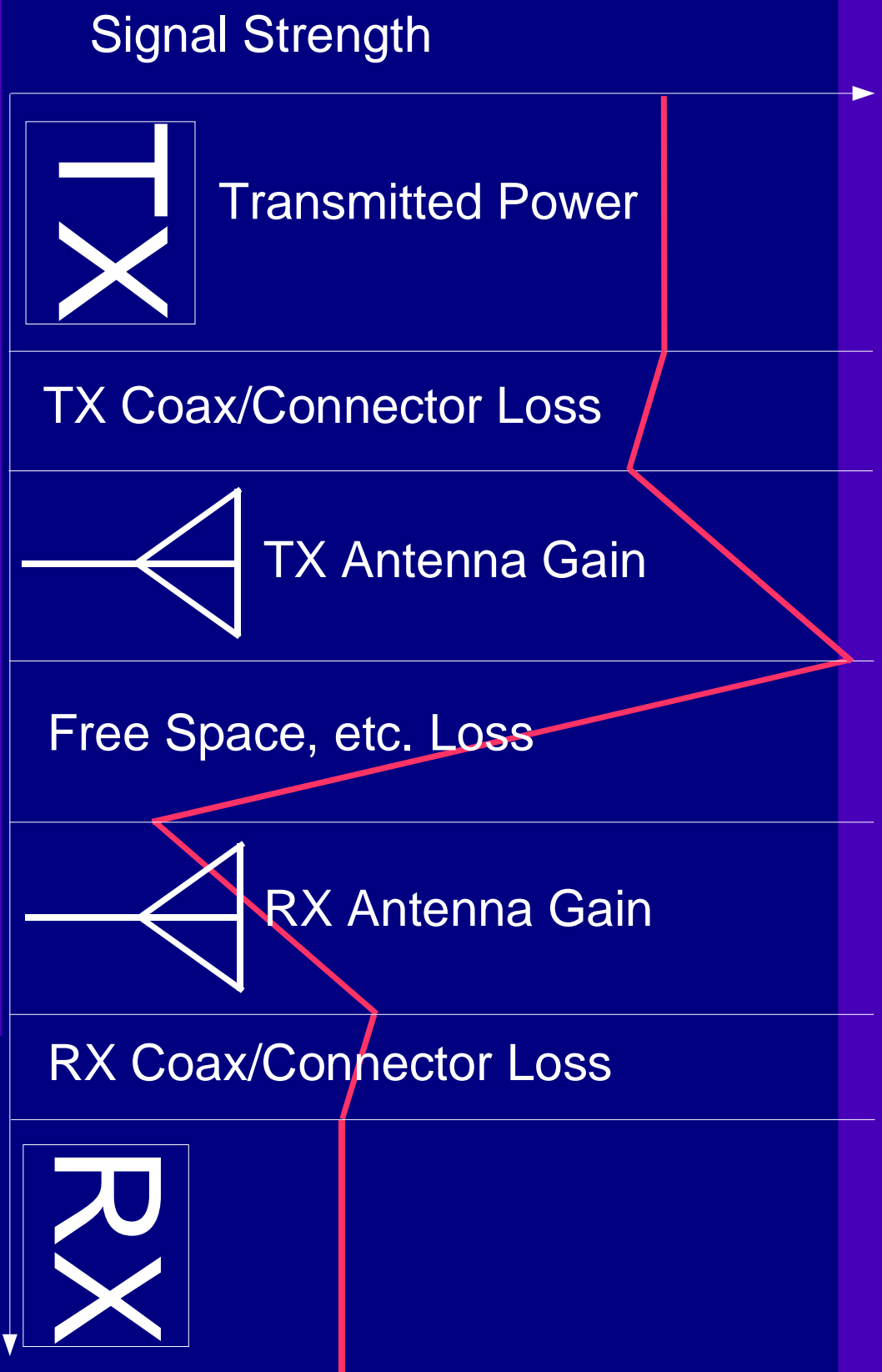
Free-space, etc. loss

Connector and
Transmission Line Loss

TX
Output

RX
Sensitivity

Signal Level Through the Link



Simple Path Calculation -

www.ins.com/pathcalc

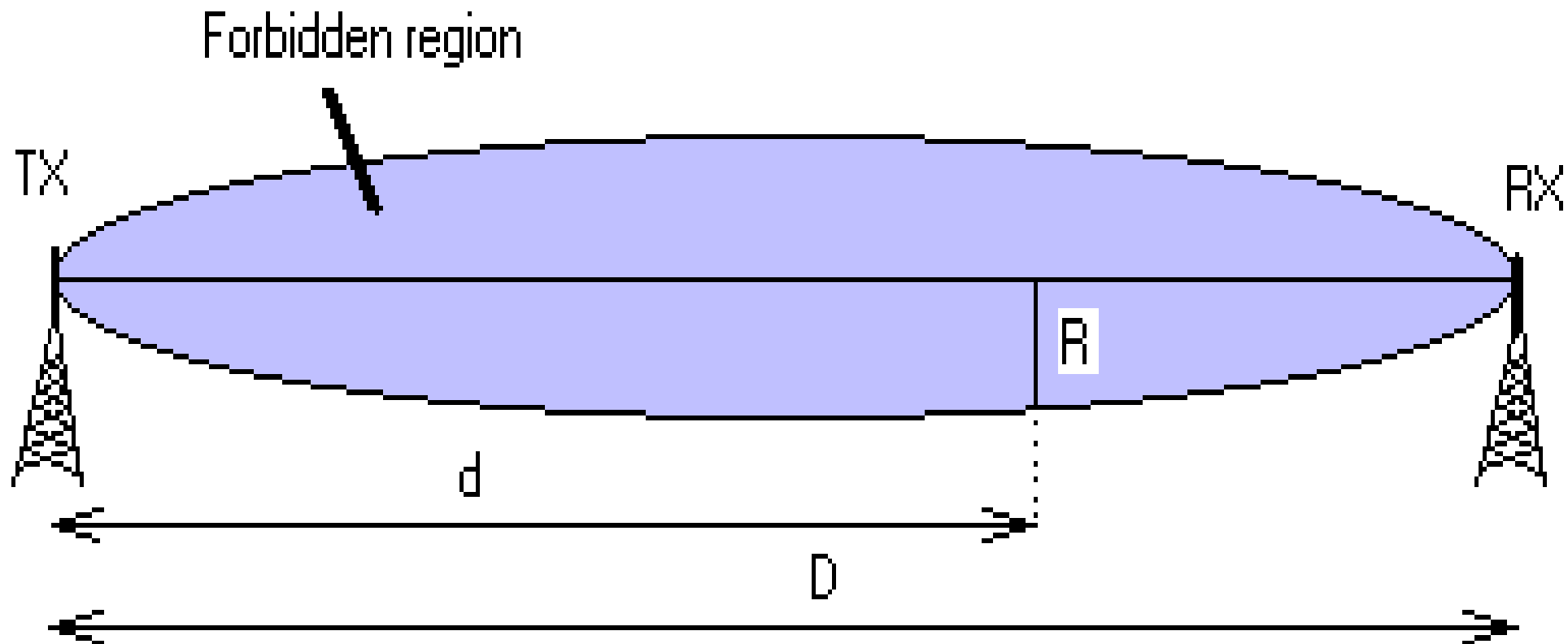
<u>Free Space Loss Path</u>		
Frequency	2.4000	GHz
TPO	1.0000	Watts
TPO dBm	30.0000	dBm
Transmission Line Loss	2.0000	dB
TX Antenna Gain	6.0000	dBi
Path Length	5.0000	miles
Free Space Loss	118.1836	dB
RX Antenna Gain	18.0000	dBi
RX Transmission Line Loss	3.0000	dB
RX Signal	-69.1836	dBm
RX threshold	-80.0000	dBm
Fade Margin	10.8164	dB



Signal Path Loss - Through the aether...

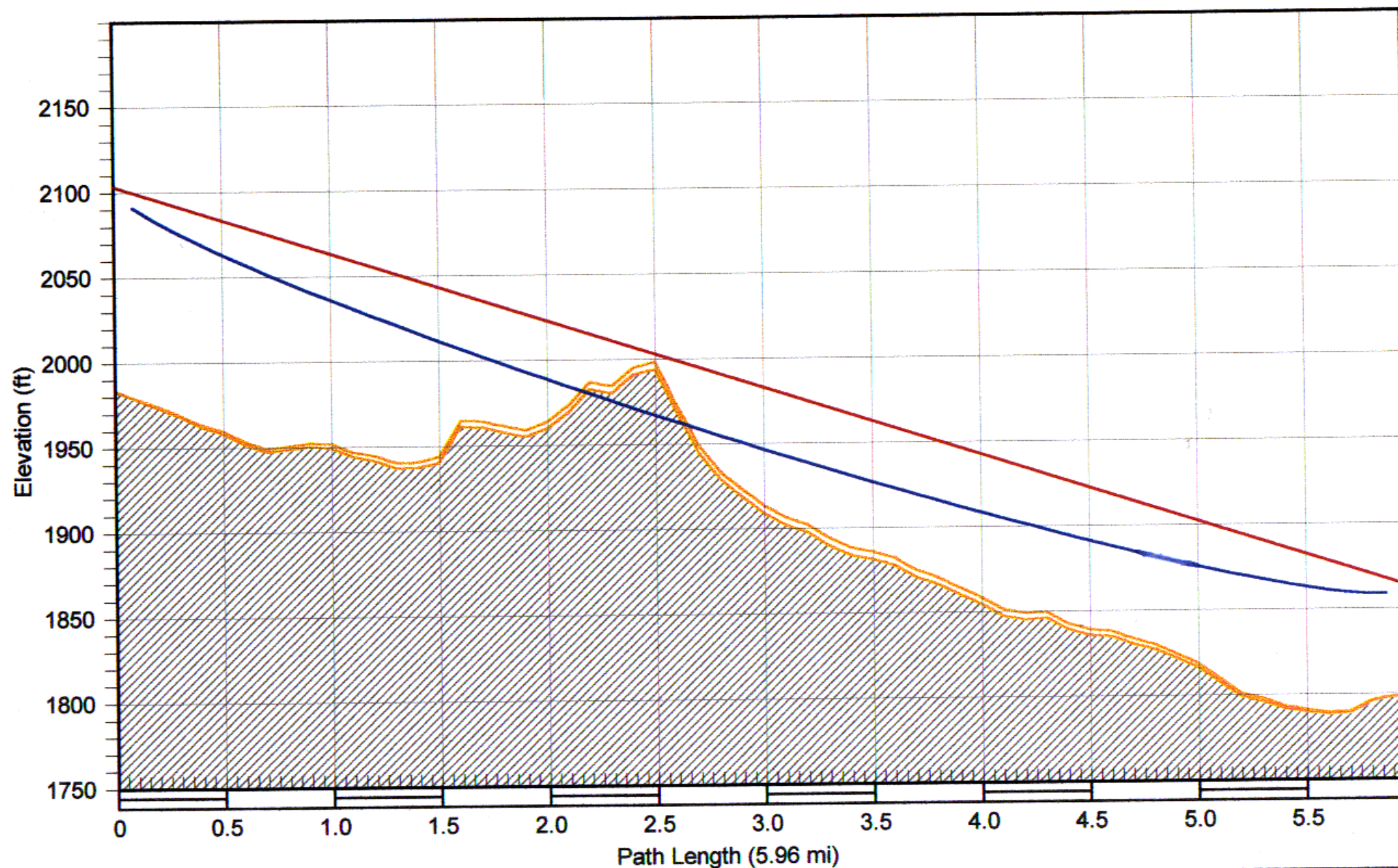
- ⇒ Atmospheric Attenuation
 - ⇒ Rain/Snow
 - ⇒ Trees (Spring/Summer vs. Fall/Winter)
 - ⇒ Typical Solution: Just need to have lots of signal
 - Needed fade margin will increase with distance.
- ⇒ Refraction
 - ⇒ Thermal Ducting
 - ⇒ Marine Layers
 - ⇒ Typical Solution: Diversity Reception
- ⇒ Fresnel Zone Attenuation...

Fresnel Schematic



Fresnel Zones Calculation:

<u>Fresnel Zones:</u>		
Distance from TX to calc point	2.5000	miles
Path Length	5.0000	miles
Distance from RX to calc point	2.5000	miles
Frequency	2.5000	GHz
First Fresnel Zone Radius	50.9117	feet
Second Fresnel Zone Radius	72.0000	feet
Third Fresnel Zone Radius	88.1816	feet
Forth Fresnel Zone Radius	101.8234	feet



KEYAFM
Latitude 48 50 37.00 N
Longitude 099 45 02.00 W
Azimuth 241.42°
Elevation 1983 ft ASL
Antenna CL 120.0 ft AGL

Frequency (MHz) = 5800.0
K = 1.33
%F1 = 100.00

Shell Valley
Latitude 48 48 08.22 N
Longitude 099 51 54.90 W
Azimuth 61.34°
Elevation 1798 ft ASL
Antenna CL 65.6 ft AGL



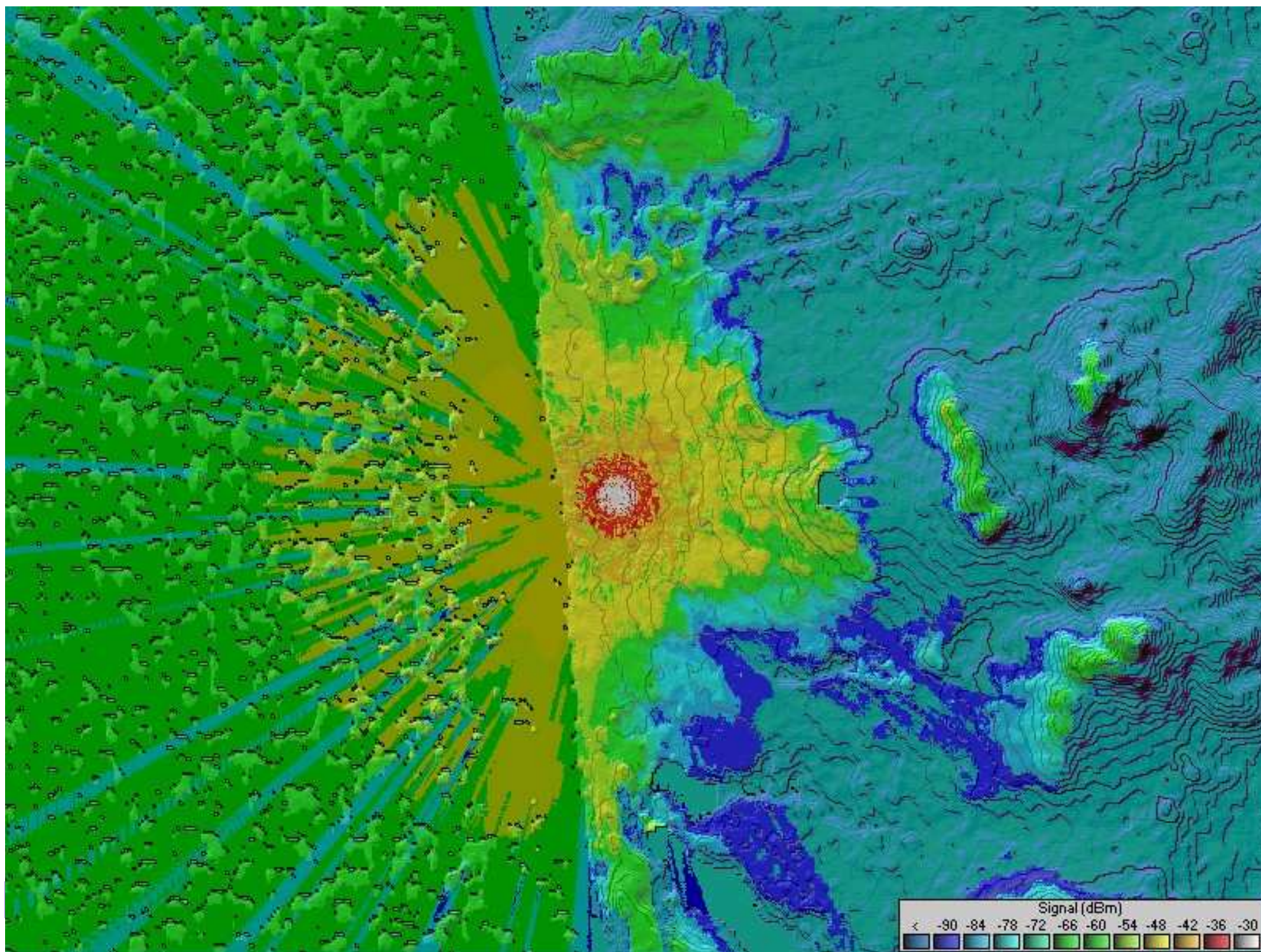
Signal Path Interference - Other Considerations

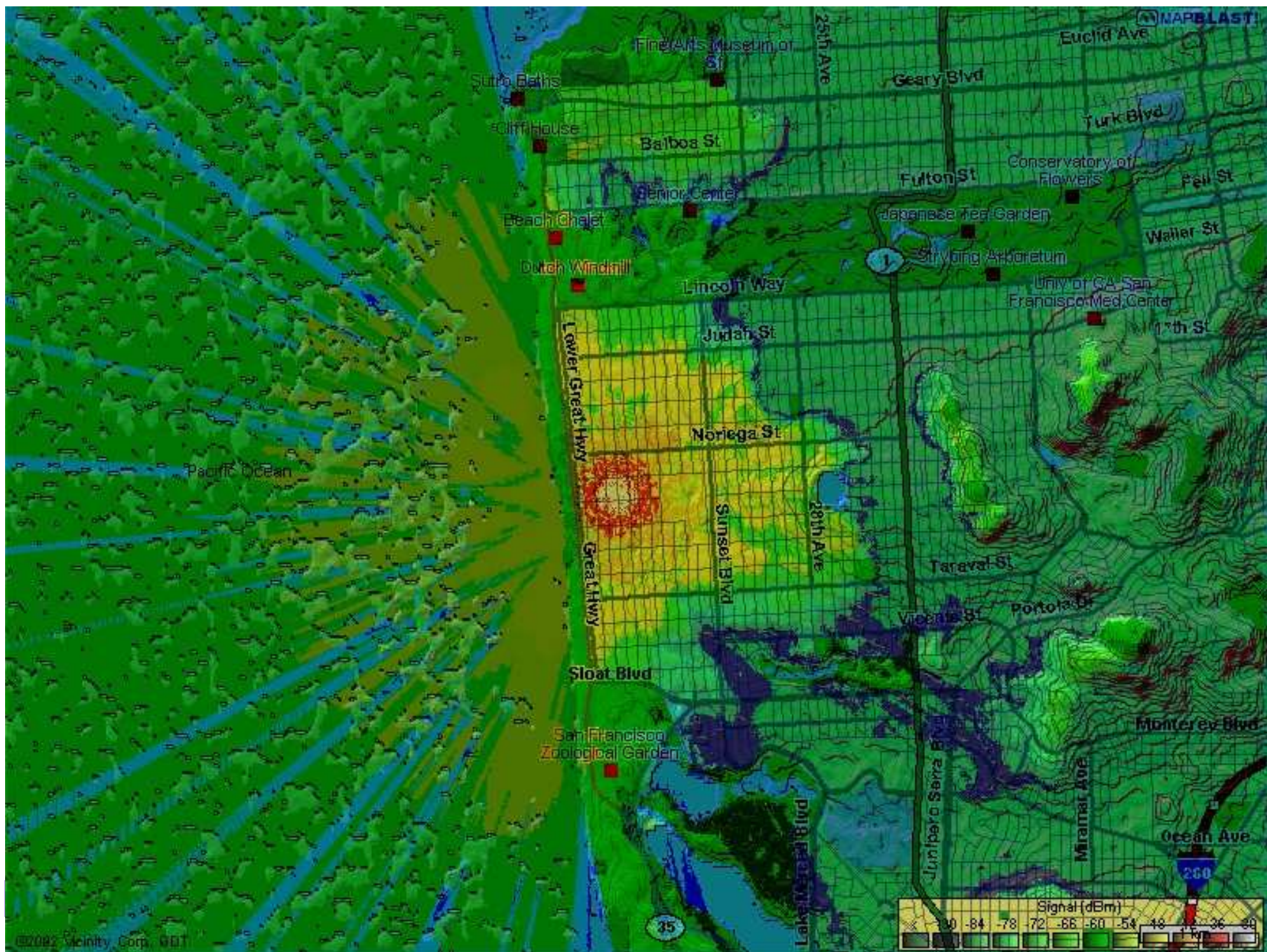
- ⇒ Multi-path
 - ⇒ Buildings likely to create a second path that will cause interference?
 - ⇒ Typical Solutions:
 - Change the polarization of the antenna
 - Change the beam-width of the antenna
 - More gain, tighter beam-width, more expense.
 - Add shielding
- ⇒ Other users of the band?
 - ⇒ Typical Solutions:
 - Change frequency.
 - See above



Coverage Area – Point to Multipoint

- ⇒ Questions:
 - ⇒ How many clients can see your AP?
 - ⇒ What sort of signal strength can the clients expect?
- ⇒ Propagation Prediction Methods:
 - ⇒ An elaborate form of ray-tracing.
 - ⇒ Longley-Rice
 - ⇒ Terrain-Integrated Rough-Earth Model (TIREM)
 - Considered a better method
 - ⇒ Both can over-predict 5-17dB.
 - ⇒ The more expensive software modifies these methods for better accuracy.







Which Antenna for the Job?

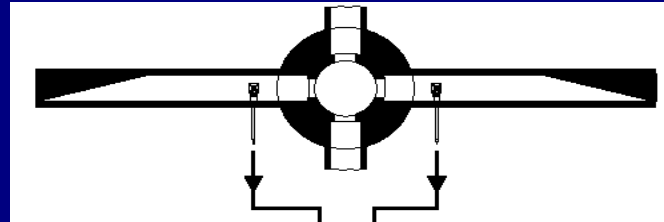
- ⇒ Multi Point to Multi Point
 - ⇒ Omnidirectional antennas on both ends
- ⇒ Point to Multi Point
 - ⇒ Omnidirectional for the "point" or "center", directional for the endpoints.
- ⇒ Point to Point
 - ⇒ Directional for both ends.

Different Antennas for the Job

⇒ Point to Multipoint

⇒ Di-pole

- Typical PC card antenna
- Very low gain, radiates in almost all directions equally
- Horizontal Polarization



⇒ Omni-Directional

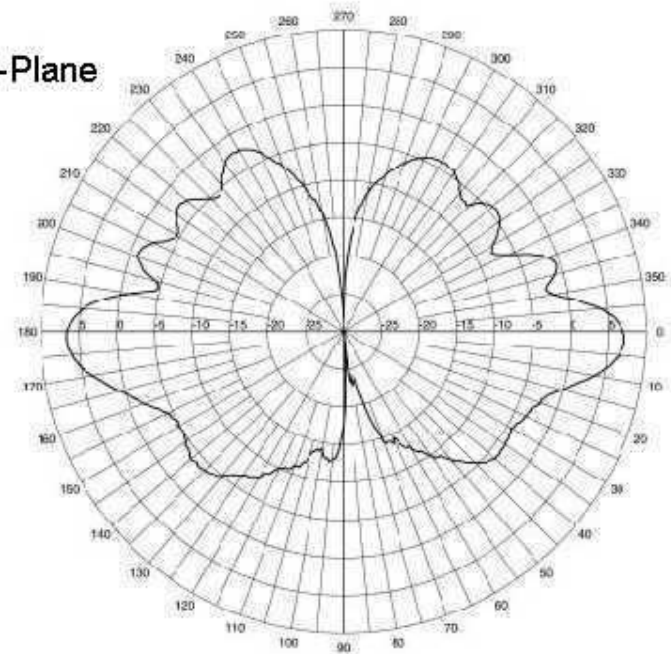
- Usually has gain: 0 to 15 dBi – Lower gain better for tall mounts.
- Typically Radiates equally well on the horizontal plane.
- Vertical Polarization

⇒ Panel or Sector

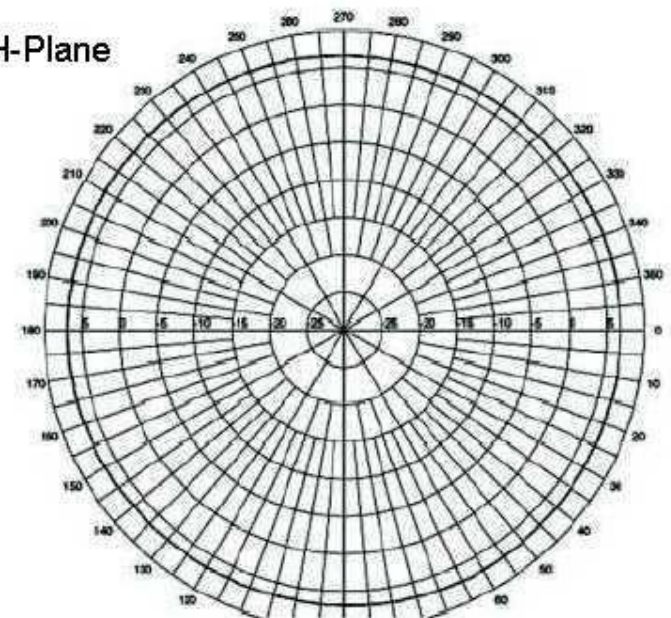
- Used to cover a section of a flat area.
- Has gain: 3 to 18 dBi
- Horizontal beam width is typically 10 to 120 degrees.
- Vertical beam width is typically 10 to 45 degrees



E-Plane



H-Plane

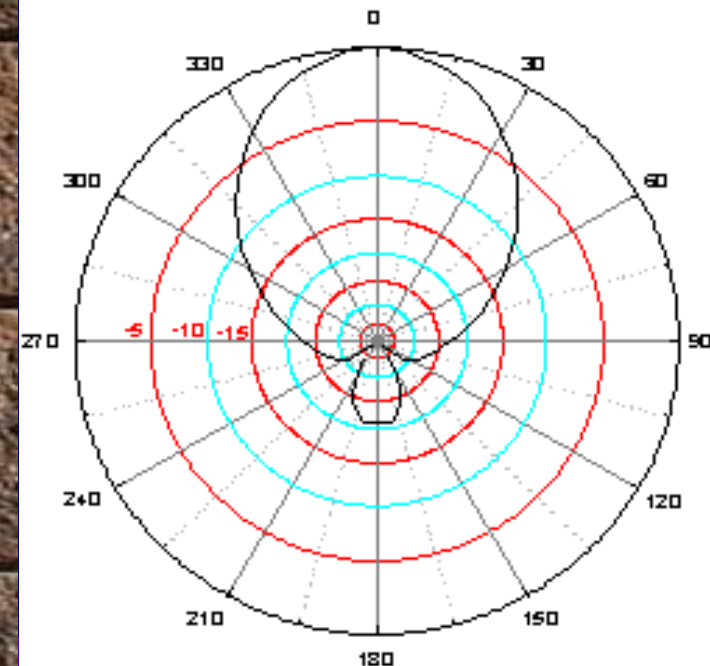
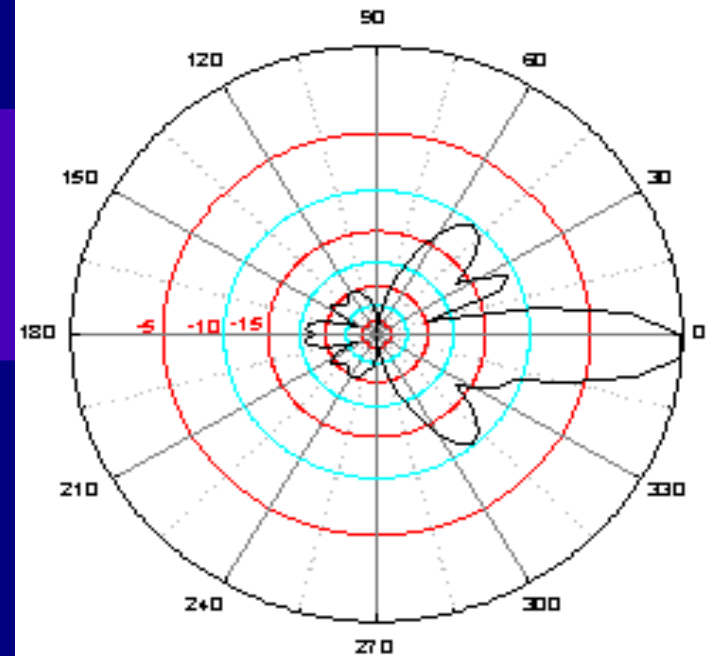


Panel Antennas

- Great for targeting an area to serve.
- Typically put around a tower to segment coverage of an “omni”.

SuperPass
SPFPGH14S
Gain – 14 dBi

Hort. Beam – 60 deg.
Vert. Beam – 18 deg.






Directional Antennas

- ⇒ Does not radiate in all directions
 - ⇒ Typically on the horizontal plane.
- ⇒ The more focused the antenna, the higher the gain.
- ⇒ Will have either vertical, horizontal or circular polarization



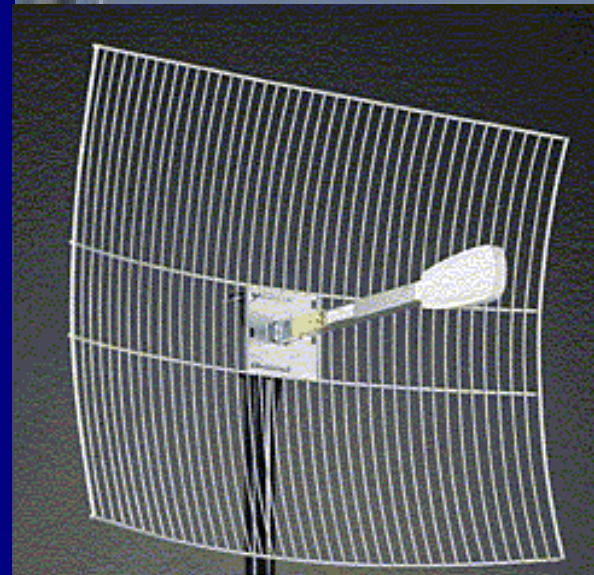
Why Use a Directional Antenna?

- ⇒ Helps your system and be a good neighbour.
 - ⇒ Raise the effective power to the distant point you are trying to serve.
 - ⇒ Helps with the fade margin.
 - ⇒ Reduce interference to the path.
 - ⇒ Your receiving antennas will be less sensitive to off-axis signals (ie. Other transmitters or multi-path).
 - ⇒ Reduce interference to others.
 - ⇒ Transmitting antennas will send less signal to off-axis receivers.
- 

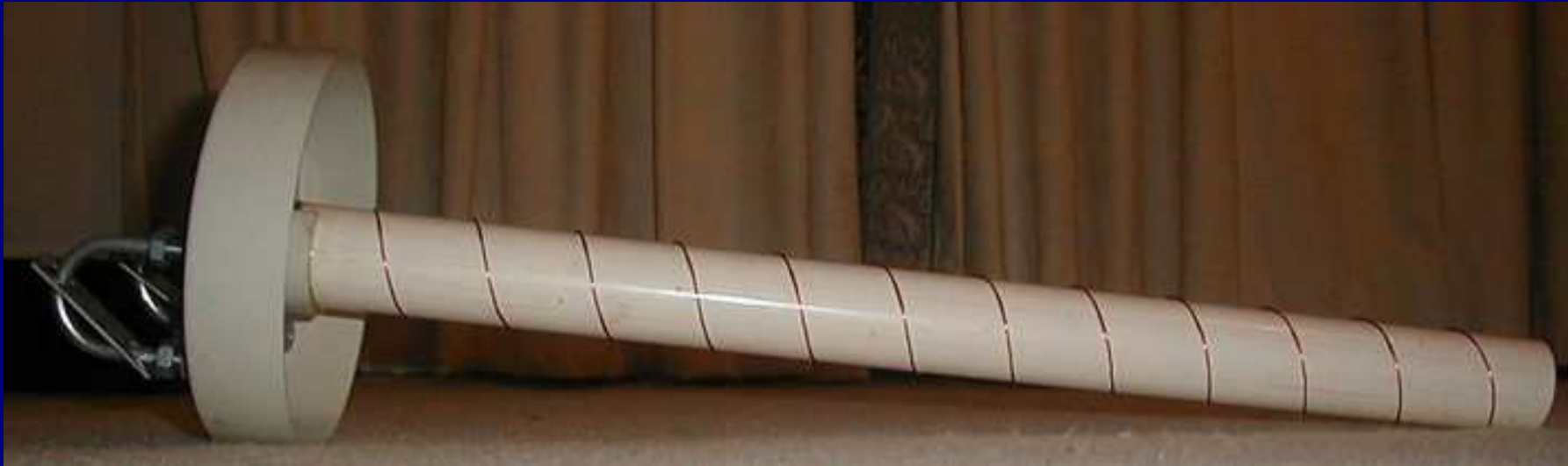
Antennas 101 continued... P2P

- ⇒ Yagi
 - ⇒ 5 – 18 dBi of gain
 - ⇒ Vertical or horizontal polarity

- ⇒ Parabolic
 - ⇒ “Dish” shaped
 - ⇒ Larger than a Yagi
 - ⇒ 15 – 36 dBi of gain
 - ⇒ Vertical or horizontal polarity



Helical Antennas



- ⇒ Has circular polarization
 - ⇒ Left or right handed
 - ⇒ Great for multi-path problems (see next slide)
- ⇒ Gain is 10 – 25 dBi

Antenna Polarity

- ⇒ Polarity is a product of the design of the antenna.
- ⇒ Each end must match.
- ⇒ It can be used to minimize multi-path and interference.
- ⇒ Typical Polarities:
 - ⇒ Horizontal
 - Avoids multi-path from vertical objects like buildings
 - ⇒ Vertical
 - Avoids multi-path from horizontal objects like the ground, bodies of water.
 - ⇒ Circular
 - It can avoid multi-path from “odd-number bounced sources.
 - Left or right handed



Frequency Coordination

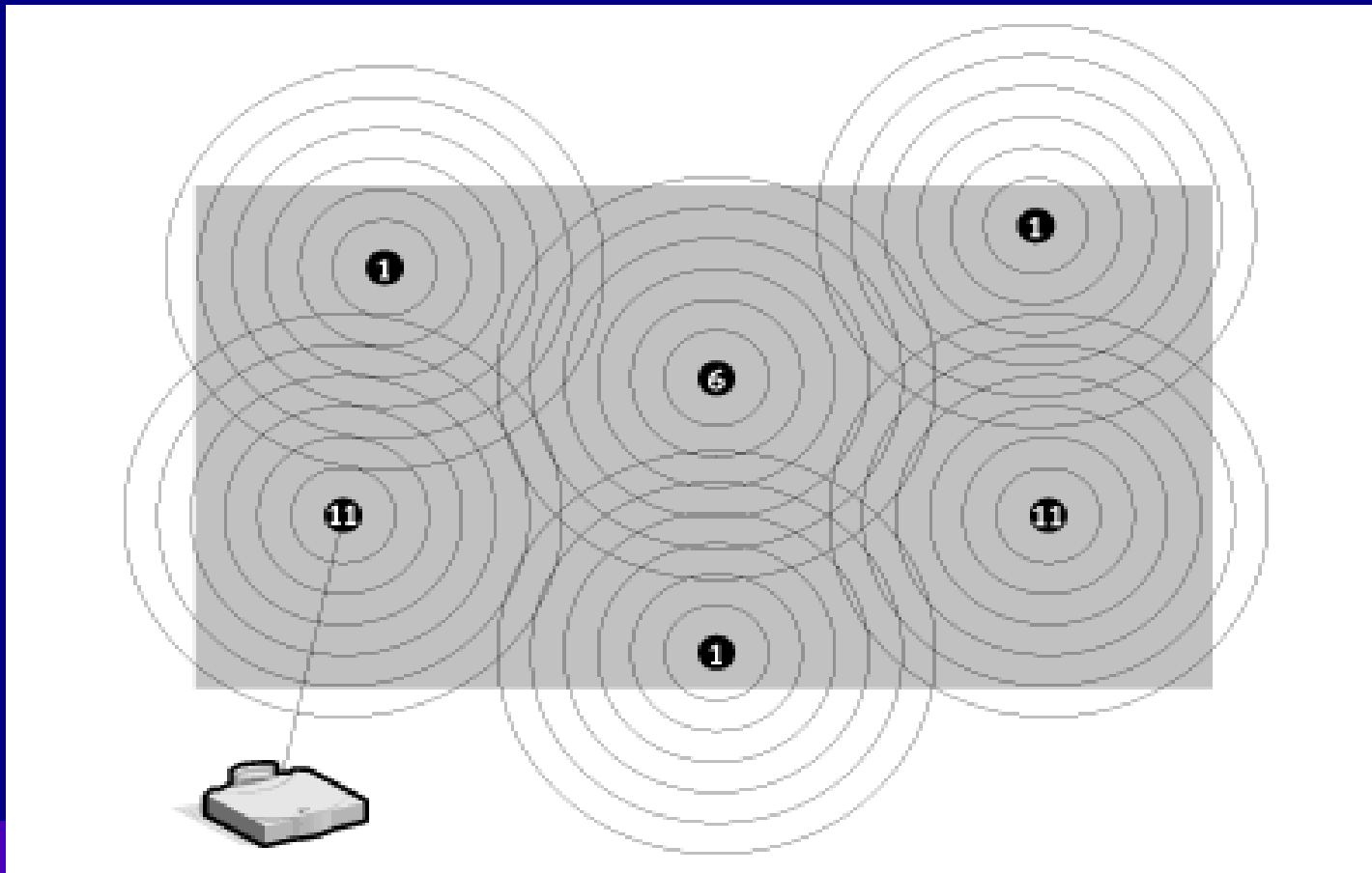
- ⇒ The bands are crowded and the channels overlap.
 - ⇒ @ 2.4GHz only channels 1, 6 & 11 do not overlap.
(next slide.)
- ⇒ Need to coordinate internally.
- ⇒ Need to coordinate with other band users.
 - ⇒ 2.4 is used by non-licensed and licensed users
 - Licensed users are: Amateurs, ENG, Public Safety, etc.
 - ⇒ Find out who may be using the band in your area.
 - I.e. Mountain tops may have licensed users.
 - ⇒ Better would be to use a spectrum analyzer and try to identify the users.
 - ⇒ Worst case: just fire it up and find out what works.

Frequencies of 802.11b Channels at 2.4 Ghz

Channel	Bottom (Ghz)	Center (Ghz)	Top (Ghz)
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

Multiple Aps vs. Frequencies

- ➔ APs should not overlap Channels/Frequencies.





Access Points – Examples...

- ⇒ Range in costs from \$50 to \$1000
- ⇒ High end to low:
- ⇒ Cisco 1200
 - ⇒ Supports 802.11b, 802.11a & 802.11g
 - ⇒ Space for 2,048 MAC addresses
 - ⇒ ~\$600 to \$800
- ⇒ Cisco 350
 - ⇒ Next step in the “Aironet” line from the 340 series.
 - ⇒ ~\$500 to \$1000
 - ⇒ Space for 2,048 MAC addresses

APs – Mid-level \$

- ⇒ Apple Airport 2
 - ⇒ MAC support for 50 users
 - ⇒ Router supports NAT
 - ⇒ Modem for out & inbound PPP
 - ⇒ 15dBm (30mW) TPO
 - ⇒ ~\$300





APs – Low End \$

- ⇒ D-Link AirPlus Enhanced 2.4GHz Wireless Router
 - ⇒ ~\$50 to \$100 (Some \$50 rebates out there)
 - ⇒ Proprietary 22Mb/s protocol using Packet Binary Convolutional Coding (PBCC) – Not accepted by the 802.11g working group.
 - ⇒ 256bit WEP

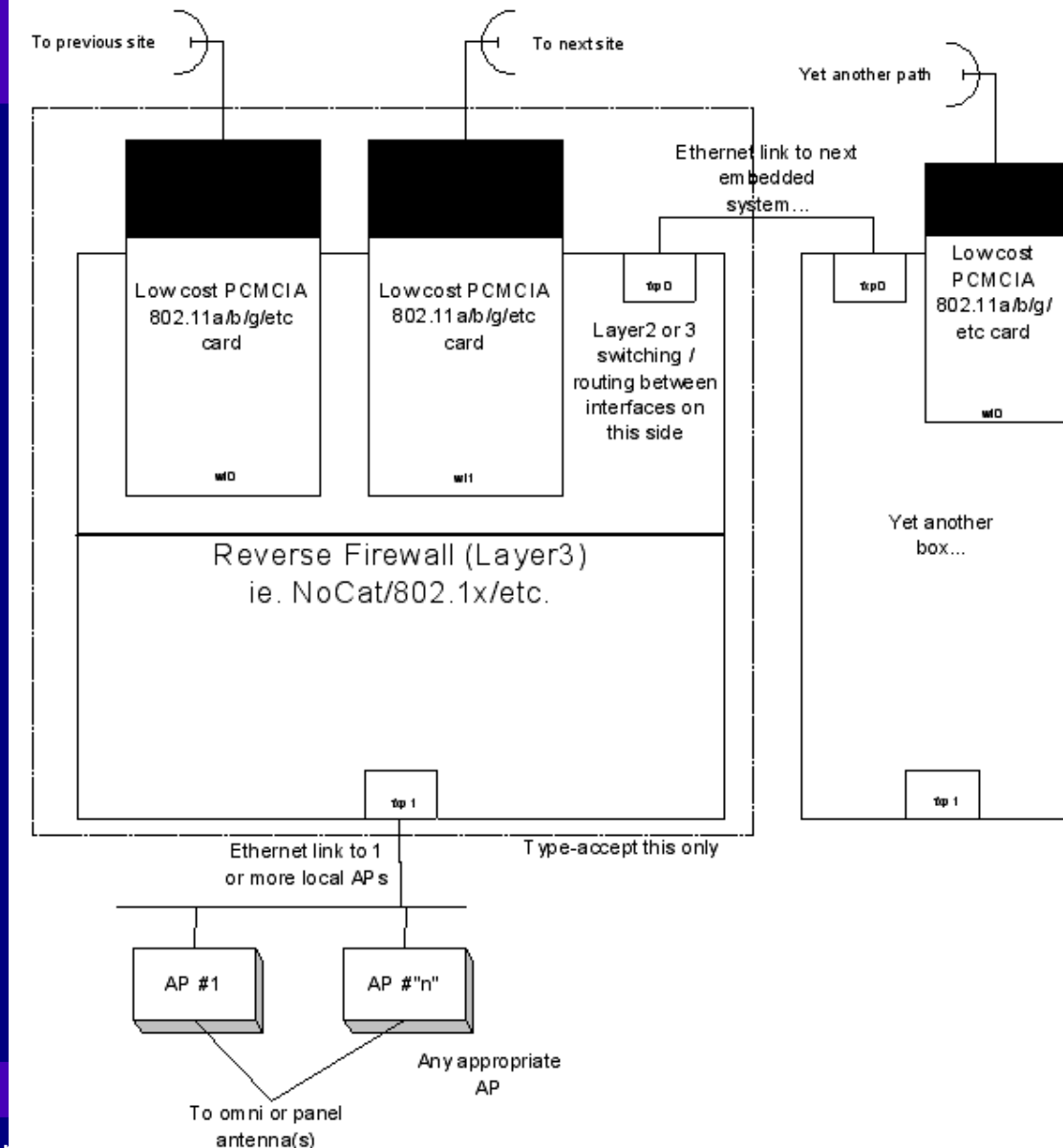
Home-brew APs - Example

- Soekris 4521 - www.soekris.com
- 2 PCMCIA slots and 1 mini-PCI for radios (3 radios total)
- 133MHz – 486
- 2 100base-T
- CompactFlash slot
- FreeBSD 4.5 in < 32 MB
 - IPFW, NAT, NoCat, Open1X (open1x.org), etc.



BAWRN Designed Hardware

- ⇒ Layer 2/3 switching/routing between radios via 802.11 and cat-5.
- ⇒ Layer 2/3 to access points
- ⇒ Can run “fancy” routing protocols such as spanning tree or BGP.
- ⇒ Can also be its own AP.





Other Hardware

⇒ Amplifiers

- ⇒ Great for TX and RX issues if used properly.
- ⇒ Best installed next to the antenna to overcome cable loss.
- ⇒ Can cause more “RF pollution” with excessive power.
- ⇒ Regulation issues – Equipment Certification.

⇒ Cables

- ⇒ Bigger the better for longer runs. ie. LMR-600

⇒ Grounding and Lightning Arrestors

- ⇒ You don't want to keep replacing your gear do you?

⇒ Battery Backup

- ⇒ How critical is it if the power goes out?




Security and Authentication

- ⇒ Current, 802.11 radios do not have either
- ⇒ Security
 - ⇒ All the normal security issues and more.
 - ⇒ Vendor defaults to open.
 - ⇒ The current “security” (WEP), is badly implemented
 - Want to crack WEP? AirSnort - airsnort.shmoo.com
 - WEP key discovery is passive.
 - Only authorizes the clients to the AP. Does not authorize the AP to the clients. No mutual authorization.
 - ⇒ Attackers don't have to be physically connected.
 - So long as they can hear the AP and the AP can hear them.




Security Needs

- ⇒ Determine what the real threat is.
 - ⇒ What are your security policies and incident response procedures?
 - ⇒ Terms of service for open and semi-open APs
- ⇒ Access Monitoring and Accounting
 - ⇒ Who is logging in and what are they doing?
- ⇒ Firewalling
 - ⇒ Minimizing attacks
 - ⇒ Preventing access to “internal” resources
 - ie. Account lists, AP software
- ⇒ Resource Allocation
 - ⇒ ie. Bandwidth hogs



Security in the near future – 802.11i

- ⇒ Potential approval for 802.11i in early 2003
 - ⇒ Replacement for WEP
 - ⇒ Two steps:
 - ⇒ Temporal Key Integrity Protocol (TKIP) (aka WEP2 or WPA)
 - ⇒ Still uses RC4 but keys will not be shared between clients.
 - ⇒ TKIP changes temporal keys every 10,000 packets
 - ⇒ May only require a firmware upgrade to existing APs.
 - ⇒ The Wi-Fi Alliance is suggesting TKIP as a stop gap until...
 - ⇒ Advanced Encryption Standard (AES)
 - ⇒ Designed to replace TKIP
 - ⇒ Requires a co-processor or built into the radio silicon.
 - ⇒ APs and clients will need to be replaced.
- 



Security – 802.11i (cont.)

- ⇒ Atheros Communications and Resonext Communications are shipping chips now that support WEP, TKIP, and AES. Nokia is shipping hardware.
- ⇒ Further reading:
 - ⇒ Intel white papers 802.11 key management -
 - ⇒ http://cedar.intel.com/media/pdf/wireless/80211_1.pdf
 - ⇒ http://cedar.intel.com/media/pdf/security/80211_part2.pdf



Access, Authentication and Accounting

- ⇒ Beacon Frames
 - ⇒ Closed networks do not advertise; turn off the beacon.
 - ⇒ Good 802.11 sniffers can pick up the SSID (network name) anyway.
- ⇒ MAC Address Filtering
 - ⇒ Static lists (lots of work) or via Radius servers.
 - ⇒ Trivial to clone a MAC address



AAA cont...

- ⇒ WEP uses a shared password
 - ⇒ No individual responsibility
 - ⇒ Every device will need to be changed if they key is discovered outside of authorized users
 - ⇒ Can be discovered through software.
 - AirSnort is an example.
 - AirSnort does require 5-10 million packets to crack a key. This could be up to 15GB of traffic.



Security/AAA Solutions

- ⇒ AP outside the firewall
 - ⇒ Or integrated into the AP
 - Soekris and Musenki SBCs
 - Open802 Linux on an AP
- ⇒ Bandwidth Limiting
 - ⇒ Bandwidth based on access
- ⇒ Some type of AAA logging
 - ⇒ ie. To a remote SYSLOG server (perhaps tunneled)

Security/AAA Solutions (cont.)

- ⇒ NoCat - www.nocat.net
 - ⇒ Captive Portal
- ⇒ Use external encryption
 - ⇒ End to End
 - ⇒ IPsec, SSH, SSL, etc.
- ⇒ 802.1X just coming out
 - ⇒ Can use multiple authorization schemes with PPP's Extensible Authentication Protocol (EAP) (RFC 2284/2484) such as EAP-TLS, EAP-TTLS
 - ⇒ Individual keys required for access
 - ⇒ Per-session WEP key.
 - ⇒ Dynamic WEP key for 802.1X is still being hammered out.
 - ⇒ Cisco 350 APs & WinXP have it built in.



Future...

- ⇒ 802.11e – MAC layer QoS
 - ⇒ Should be out soon
- ⇒ 802.11f – Inter-Access Point Protocol (IAPP)
 - ⇒ Roaming between all access points.
 - ⇒ Troubles getting vendors to agree.
- ⇒ 802.11g – 22Mb/s at 2.4GHz
 - ⇒ OFDM
 - ⇒ Should be seeing hardware soon
- ⇒ 802.11H – Spectrum Managed 802.11a
 - ⇒ Automatic power control
 - ⇒ Automatic frequency selection
 - ⇒ Needed for EU and something 802.11b should have.



Future (cont.)

- ⇒ 802.11i – Security
 - ⇒ WEP2 out first
 - ⇒ New hardware needed

- ⇒ How do we increase bandwidth while still addressing the physics (turf and spectrum)?
Possible Solutions are:
 - ⇒ Mesh
 - MeshNetworks, et. al.
 - ⇒ Phased-Array Antennas
 - Vivato, et. al.

Resources

⇒ Books

- ⇒ “Building Wireless Community Networks” - Rob Flickenger – O'Reilly
- ⇒ “802.11 Wireless Networks” - Matthew Gast – O'Reilly

⇒ <http://www.freenetworks.org>

- ⇒ The “meta” site for the community groups such as:
 - Bay Area Wireless Users Group - <http://www.bawug.org>
 - Great mailing list.

⇒ <http://nocat.net>

- ⇒ AAA open-software for *NIX

⇒ <http://www.ieee.org>

- ⇒ The standards body for 802.(n)(x)



Thank You and Q&A

⇒ Bay Area Wireless Users Group:

www.bawug.org

⇒ Tim Pozar:

pozar@lins.com