IEEE 802.11 Tutorial

Dave Smith
Timothy P. Wakeley PE

Terminology

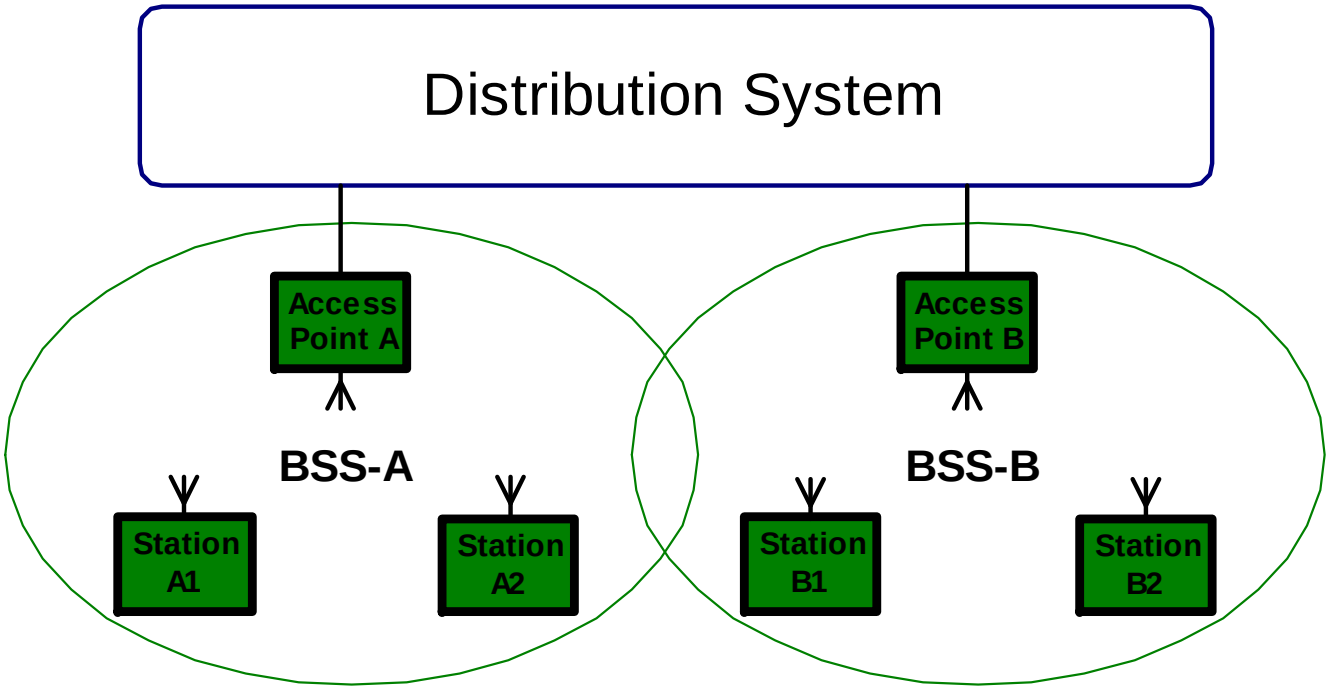
- WLAN – wireless LAN
  - Simply an extension of a wired LAN
  - Completely different protocol from Bluetooth other than they share the same frequency spectrum
- Access Point
  - Central control and distribution point of an WLAN
- Station
  - WLAN node
- WLANs only have APs and Stations

Terminology

- BSS – Basic Service Set
  - One AP and all the stations associated with it
- ESS – Extended service set
  - A collection of BSSs that share the same network settings
  - A mobile station (laptop) can move from one AP to another AP within an ESS
- Infrastructure Mode
  - Stations are associated with an AP

Terminology

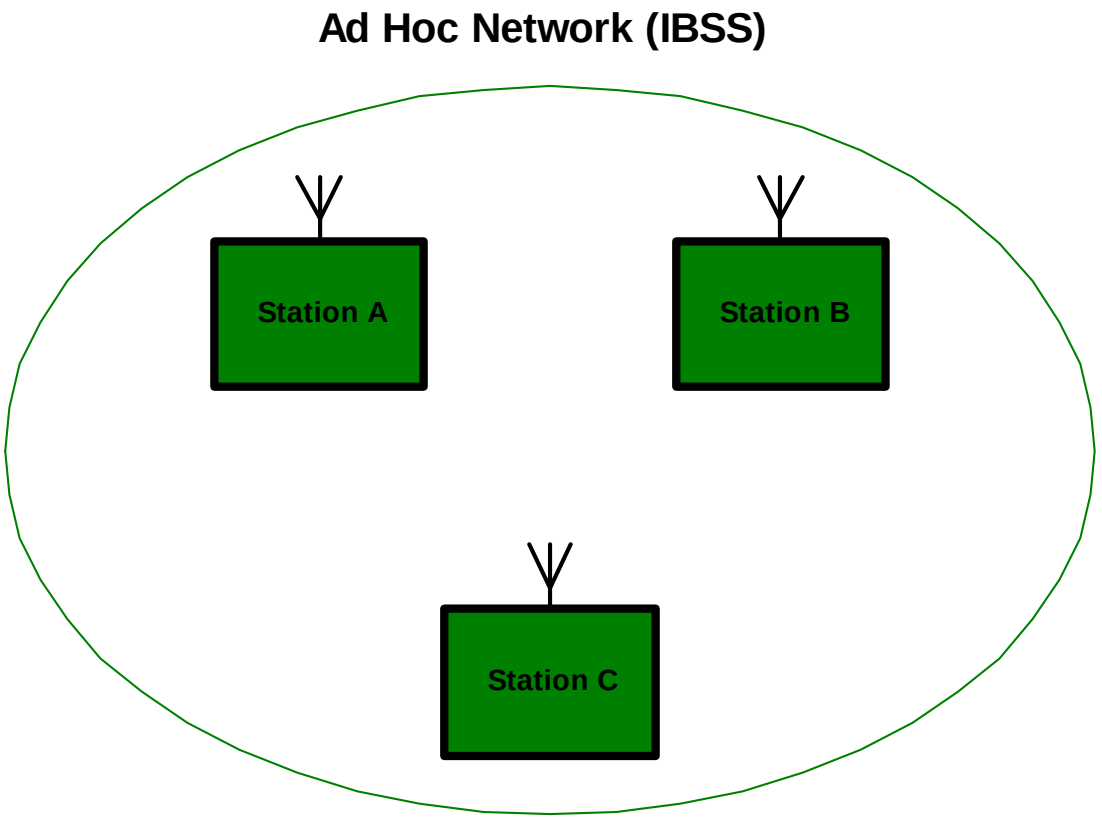
Extended Service Set (ESS)



Terminology

- IBSS – Independent basic service set
  - Stations are not associated with an AP
  - Stations are associated with each other
  - The initiating station is the pseudo-AP
- Ad-hoc Mode
  - Another name for an IBSS network
- SSID – Service Set ID
  - The name of a given BSS or ESS
  - Some call it Network ID

Terminology



Terminology

- WEP - Wired Equivalent Privacy. Uses RC4 as the encryption algorithm
- WPA – Wireless Protected Access
  - WEP with many software enhancements
- WFA – Wi-Fi Alliance – industry interoperability testing body

Terminology

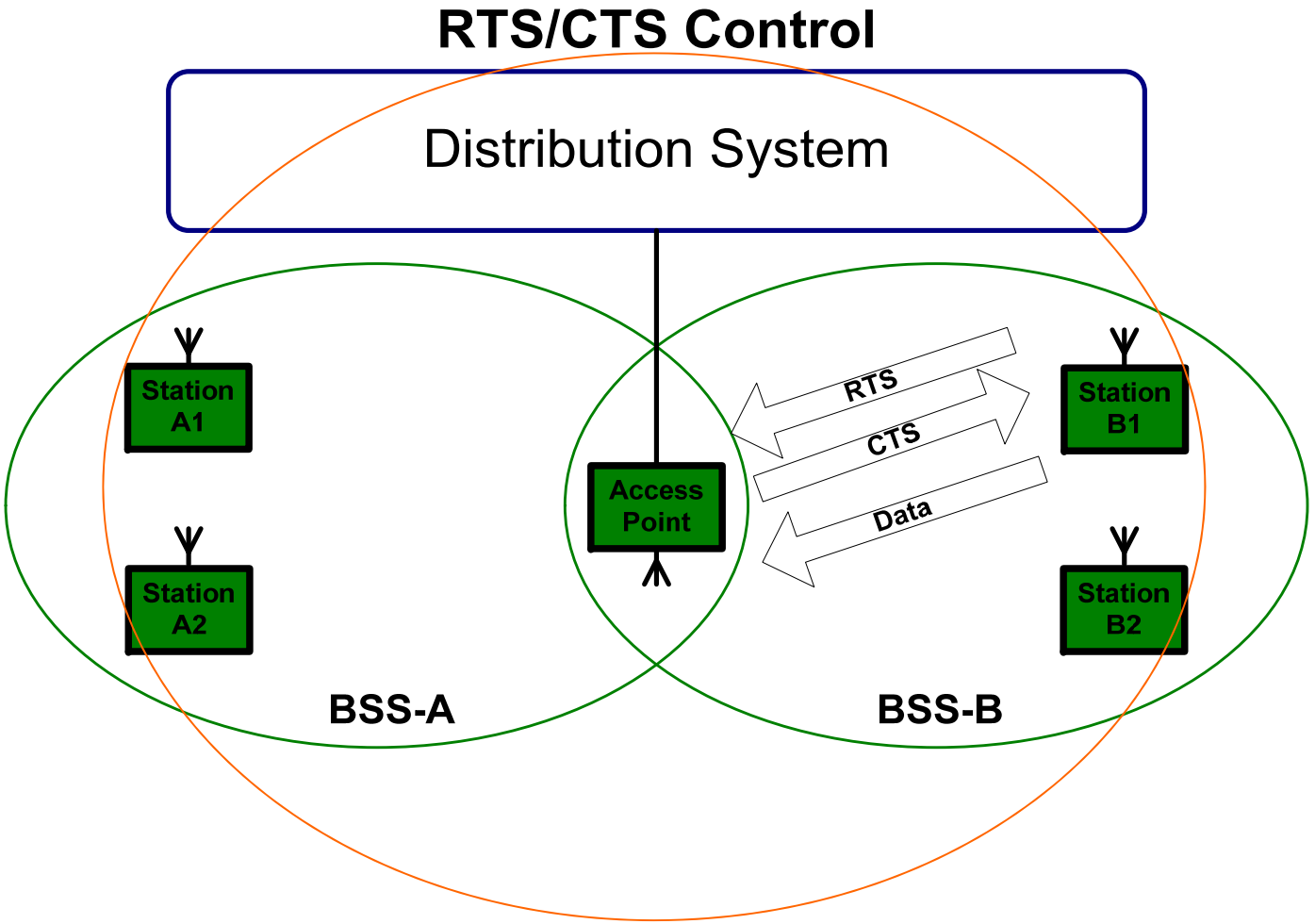
- WI-FI - Wireless Fidelity -
  - Logo owned by Wi-Fi Alliance
- AES-CCM – New 802.11i Hardware encryption engine
- 802.1X - Authentication protocol

Terminology

- DS - Distribution System
  - network used to connect AP's together in an ESS
- RTS - Request to Send
  - Request access to the medium
- CTS - Clear to Send
  - Signals access to the medium
- Hidden nodes
  - Clients that can be seen by one station but not another

Terminology

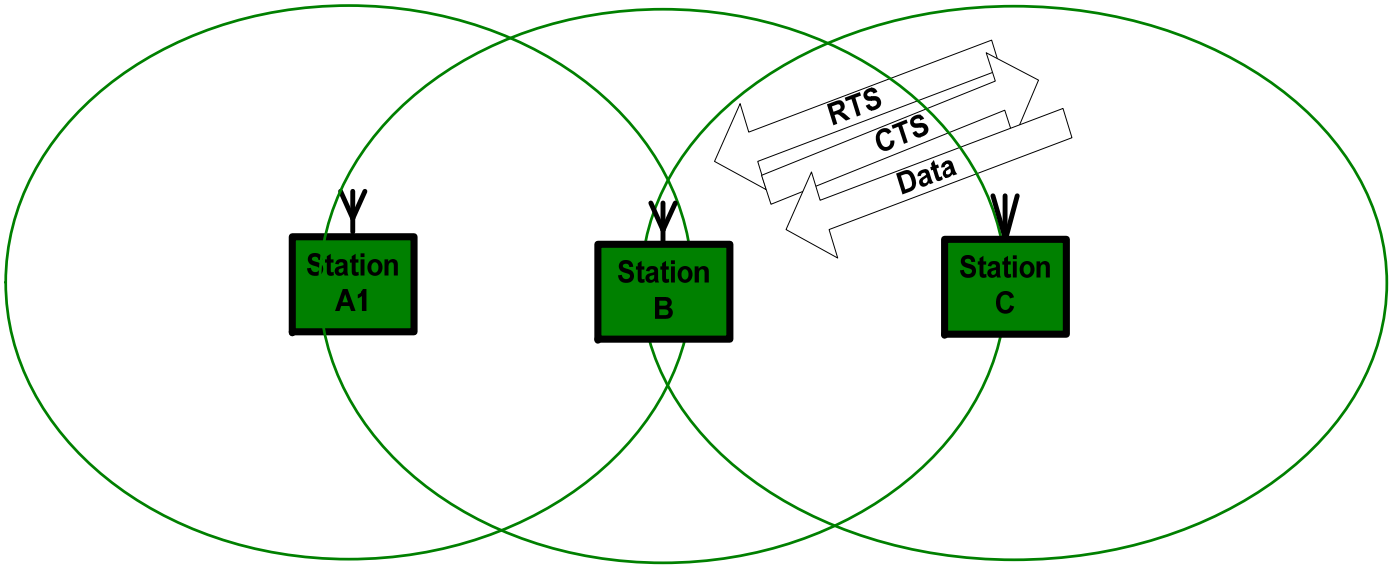
Hidden Node with Access Point



Terminology

Hidden Node Problem

- Adhoc Network

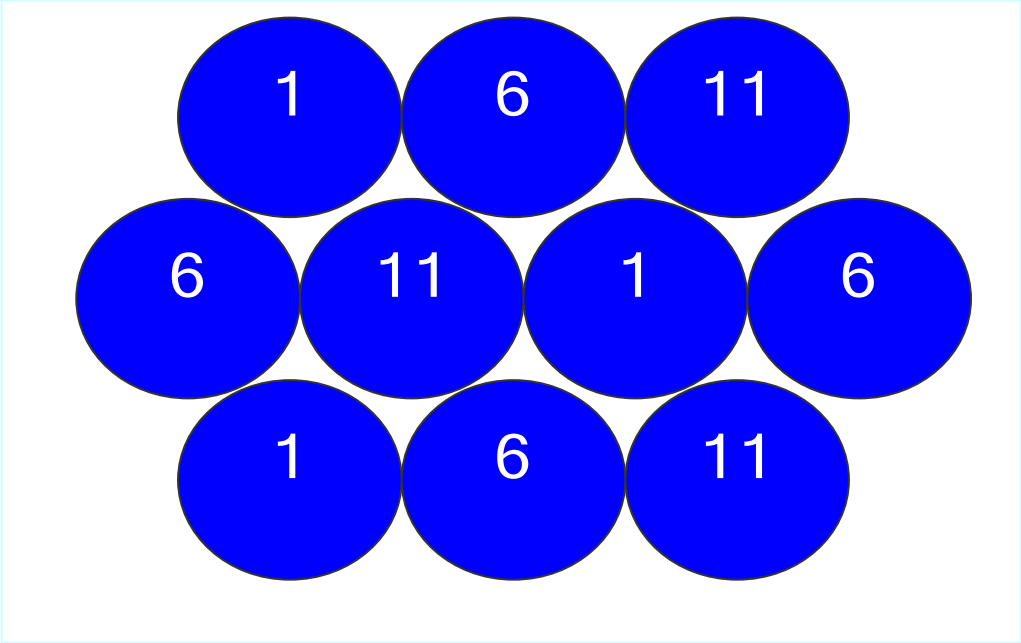


Terminology

- Channels
  - 802.11b/g divides 2.4GHz spectrum into 11 Channels in the USA.
  - 802.11a divides 5-6GHz spectrum in 111 channels in USA
- Channel separation - 5MHz
- Channel bandwidth
  - 20MHz for 11g OFDM
  - 25MHz for 11b DSSS/CCK
- Channel overlap – 15 or 20MHz

Terminology

Non Overlapping Channel Deployment



Terminology

- FHSS – Frequency hopping Spread Spectrum
  - Used in 802.11-1999: 1 and 2Mb/s
  - Same as used in BT
  - Randomly hopping channels to lower interference to other users of the band
- DSSS – Direct sequence spread spectrum
  - Used in 802.11b – 1, 2, 5.5 and 11Mb/s
  - A method of spread the energy of a transmitted signal over a wider band than necessary to lower the level of interference to other users of the band

Terminology

- FSK Modulation – frequency shift keying (same as FM)
  - Used in 802.11 FHSS - 1 and 2 Mb/s
- CCK Modulation – Complimentary Code Keying
  - Used in 802.11b – 1, 2, 5.5, 11 Mb/s
- OFDM Modulation – Orthogonal Frequency Division Multiplexing
  - Data is divided into 48 separate sub-carriers
  - Used in 802.11a/g

Terminology

- BPSK – Binary Phase Shift Keying
  - Digital one and zero are represented by 0 and 180 degrees on polar plot
  - Used in 802.11b – 1 and 2 Mb/s rates
- QPSK – Quadrature Phase Shift Keying
  - Two bits of data are represented by +/- 45 degrees and +/- 135 degrees on polar plot
  - Used in 802.11b – 5.5 and 11 Mb/s rate

Theory of Operation

- How does one connect to a wired LAN?
  - Plug in the cable
- How does one connect to a Wireless LAN?
  - The “plug” is the SSID – network name
  - Every WLAN has an SSID
  - Infrastructure and Ad-hoc WLANs must have an SSID
  - Once the SSID is entered the Station scans the different channels looking for it

Theory of Operation

- How does one connect to a Wireless LAN? – cont
  - If a Station has the SSID of "any" and an AP allows it, then it will lock onto the first WLAN it finds
  - Most NIC card utilities will allow one to scan for all WLANs within range (some APs may not advertise their SSID)
- Once "plugged in" a WLAN is the same as a wired LAN, ex. MAC addresses and IP addresses are required

Theory of Operation

- What does the AP do?
  - It connects the WLAN to the wired LAN
  - It associates and disassociates Stations
  - All data flowing within an WLAN goes through it, Stations do not communicate directly with each other
  - It selects the channel for the BSS
  - It controls the timing of the BSS
  - It manages the BSS, ex. Selects data rate

Theory of Operation

- Infrastructure
  - Access point controlled network
  - Allows for roaming
  - Gives access to the sites infrastructure
  - Anyone can join, provided that they know the SSID, encryption keys if enabled, and are authorized if authentication is enabled
  - A list of SSIDs can be obtained by scanning
  - scanning can be passive or active

Theory of Operation

- Infrastructure (continued)
  - All nodes must adopt the parameters of the AP, such as channel, beacon interval, DTIM and other timers
  - scanning can be passive or active
  - All nodes must be authenticated and associated with the AP before being allowed to access the WLAN

Theory of Operation

- Infrastructure (continued)
  - All communication is between the Client and the AP
    - The AP relays data from one WLAN node to another WLAN node. In this scenario, only half the bandwidth is available between two WLAN nodes vs. WLAN node and another node in the infrastructure
  - In infrastructure mode only the AP generates beacons

Theory of Operation

- Ad-hoc network, IBSS, or peer-to-peer.
  - This is a group of nodes that decide to form a local network, e.g a couple of laptops
  - Anyone can join. All they need to know is the SSID of the network and the encryption keys if enabled.
  - A list of SSIDs can be obtained by scanning
  - scanning can be passive or active
  - All nodes adopt the parameters of the node that created the ad-hoc network

Theory of Operation

- Ad-hoc network or peer-to-peer (continued)
  - All nodes generate beacons
  - All nodes can talk to each other directly
  - Ad-hoc mode supports only Association
    - There is no authentication supported

Theory of Operation

- Channelization
  - 802.11 and 802.11b/g use the ISM band
    - 2.402 – 2.4835 GHz in USA
    - Different countries have slightly different bands
    - 11 channels in USA, each 5 MHz wide
    - DSSS takes 25MHz of spectrum, OFDM takes 20MHz
    - 3 non-overlapping channels: 1,6,11
    - 3 WLANs may operate in the same area if they use the non-overlapping channels

Theory of Operation

- Channelization
  - 802.11a uses the UNII bands in USA
    - 5.150 – 5.350, 5.470 - 5.825 GHz
    - Different countries have slightly different bands
    - 111 channels in USA, each 5 MHz wide
    - OFDM takes 20MHz of spectrum
    - Many non-overlapping channels
    - Many WLANs may operate in the same area if they use the non-overlapping channels

Theory of Operation

- Data Transfer
  - All data, either management or information, is transferred by packets
  - A packet is divided into a Preamble, Header, and Payload
  - The Preamble contains the SYNC bits that enable a station receiver to lock onto the packet
  - The Header contains management bits and information about the Payload
  - The Payload contains the information data and CRC

Theory of Operation

- Data Transfer – cont
  - The 802.11b/g Preamble and Header always occur at 1 or 2 Mb/s rate and is AP selectable
  - The Header contains a series of bits telling the receiver the data rate of the Payload
  - The Payload for 802.11b can be delivered at 1, 2, 5.5, 11Mb/s and can be permanently set or allowed to change dynamically
  - The Payload for 802.11g can be delivered at 6, 9, 12, 18, 24, 36, 48, or 54Mb/s

Theory of Operation

- Data Transfer – cont
  - The 802.11a Preamble and Header always occurs at 6 Mb/s rate
  - The Header contains a series of bits telling the receiver the data rate of the Payload
  - The Payload for 802.11a/g can be delivered at 6, 9, 12, 18, 24, 36, 48, or 54Mb/s and can be permanently set or allowed to change dynamically

Theory of Operation

- How do packets get transmitted?
  - WLAN uses a Distributed Coordination Function (DCF) – all stations and AP contend for the medium
  - The function is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Ethernet uses CSMA/CD – collision detect
  - Each station or AP wishing to transmit senses the medium to determine if it is free
    - If free it will transmit
    - If busy it will use an exponential back-off time and then re-sense the medium

Theory of Operation

- History and Alphabet Soup
  - 802.11 – FHSS @ 1 and 2 Mb/s
  - 802.11b – DSSS @ 5.5 and 11Mb/s
  - 802.11a – OFDM @ 6 to 54 Mb/s
  - 802.11d – Regulatory Domain Enhancement
    - The Station does not transmit until it receives a beacon from the AP telling it what channels and transmit power are allowed

Theory of Operation

- Alphabet Soup - cont
  - 802.11e – Quality of Service (QOS)
    - Enhancement for Isochronous data transfer
    - Point Coordination function with reserved time slots
  - 802.11f – Inter Access Point Protocol
    - Protocol to allow stations to migrate between Aps
  - 802.11g – Higher data rate 2.4GHz PHY
    - Uses 802.11a modulation in 2.4GHz band
    - Raw data rates up to 54Mb/s

Theory of Operation

- Alphabet Soup - cont
  - 802.11h – European Regulatory Enhancements
  - 802.11i – Security Enhancements
    - Replace WEP with AES-CCM
    - Add 802.1x authentication
  - 802.11j – Japanese Regulatory Enhancements
  - 802.11k – Radio Resource Measurement
    - Allows MAC to have access to PHY specific parameters
  - 802.11n – Next Generation 100Mb/s WLAN Standard

Software

Dave Smith

- Management frames
- Software Development

Software

- Management Frames
  - Beacons are used to advertise the service set. They are sent at 1 or 2Mbs data rates. Sent by only the AP in infrastructure mode and by all nodes in Ad-hoc
  - Probe requests are used to actively scan the network for SSIDs.
  - Probe responses are returned from the AP in infrastructure and the last beacon sender in Ad-hoc.
  - Authentication frames are used to authenticate both stations to each other

Software

- Management Frames - Cont
  - De-authentication frame is used by one station to terminate the authentication with another
  - Association request and response frames are used by a station to request an association with a BSS
  - Re-association request and response frame are used by station that was associated with a BSS and is now associating with another BSS with the same SSID.
  - Disassociation frame is used by one station to terminate an association with another.

Software

- Software Development
- 802.11 is not as reliable as Ethernet. Packets can be expected to be lost.
- Applications will have to be able to accommodate a larger amount of data loss then Ethernet.
- Except for Authentication, configuration, packet loss Encryption and the 802.11 device driver, wireless is transparent to the upper layer protocols.
- The driver must convert Ethernet, 802.2, 802.3, and SNAP frames to 802.11 wireless frames and vice versa.

Software

- Software Development - Cont
- If authentication is used, such as 802.1X, the driver or 802.1X layer blocks all packets except EAP packets until authenticated
- Most 802.11 MACs have some form of Microcode that is loaded for handling some or all of the Management packets.
    - Most require Microcode to be downloaded on reset

Software

- Software Development - Cont
- Whatever the Microcode does not handle, the device driver must pick up. For instance, PCMCIA cards handle more than USB devices handle.
- Configuration Issues
  - How does one get an embedded device configured with usernames, passwords or certificates?
  - Most embedded devices do not have keyboards where the information can be easily entered.
  - Remote UI's cannot easily get access without first getting configured on the LAN.

Software

- Software Development - Cont
- Even with Wi-Fi Certification there still are compatibility issues with some devices that will have to be handled in software
  - for instance short and long pre-ambles
  - disassociations without notification
  - MD5 and TLS authentications with Radius Servers.
  - Residential Gateways vs Access Points
  - Ad-hoc networks (Wi-Fi is beginning to address this issue)
  - WEP Encryption Key UI's (ASCII,hex or both or pass phrase

802.11 Design Considerations

Timothy P. Wakeley PE

-Link Budget

-Range vs. Data Rate

-Antenna Design

-Transmit Power

Design Considerations

- Link Budget Theory
  - Link Budget = TX power – RX sensitivity
  - Link Budget = Path and element loss between Transmitter and Receiver
  - Measurement units – 0 dBm = 1mW

Design Considerations

- Link Budget Theory (caution – radio vendor talking)
  - Starting point – Transmitter output power = 100mW (20dBm)
  - End Point – Receiver sensitivity = - 80dBm
  - Path loss over 100 meter @ 2.4GHz ($1/r^2$) = 80 dB
  - What's left: TX-RX-path loss = 20dB (lots to play with)

Design Considerations

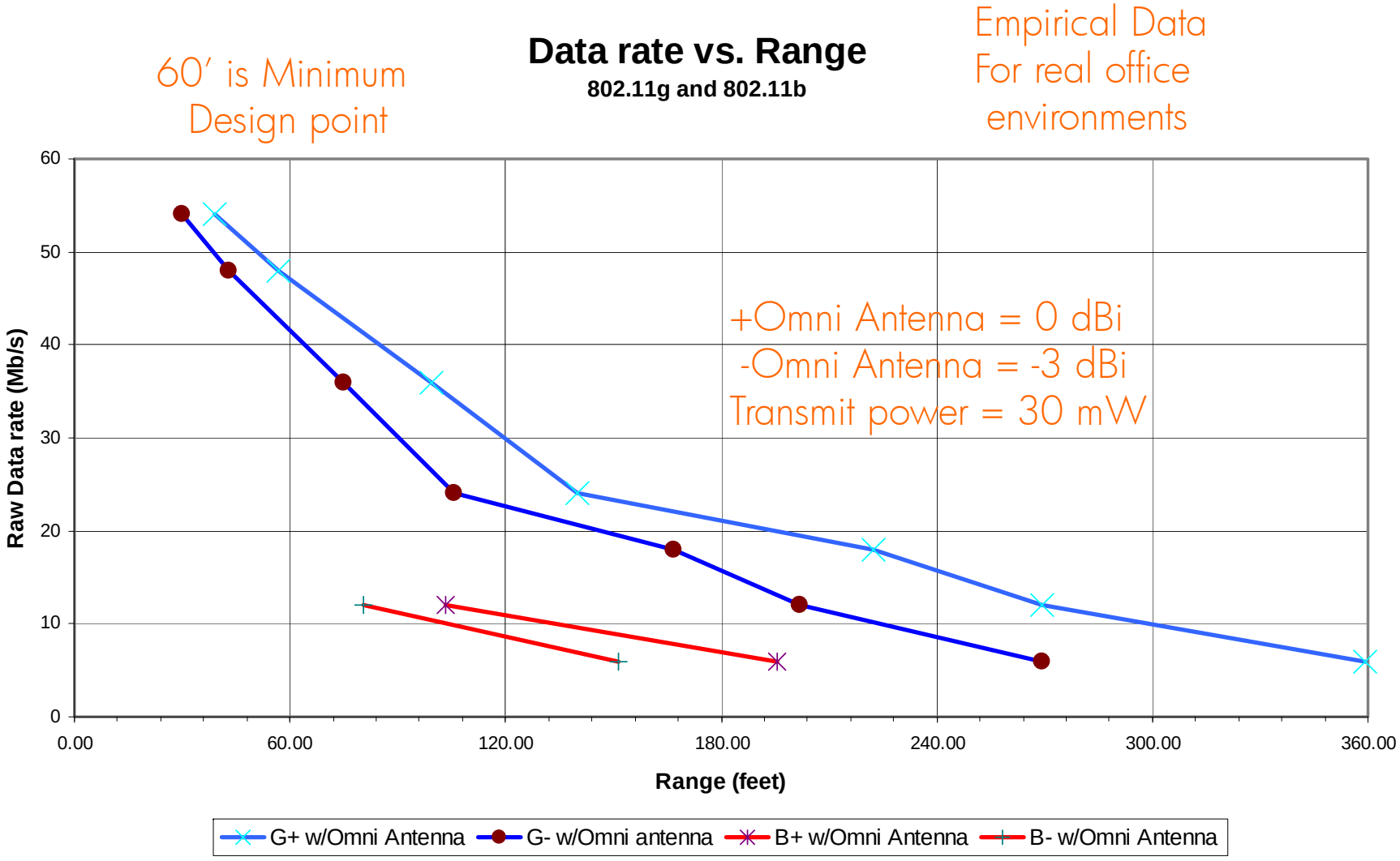
- Link Budget Theory (caution – radio vendor talking)
  - What elements are left? Antenna nulls
  - We can have antennas with 10dB nulls – great!

- For Reality Check please turn the page

Design Considerations

60' is Minimum Design point

Empirical Data For real office environments



Design Considerations

- Don't Vendors advertise 100 meters ??
  - Doubtful even at 1Mb/s rate, but slow data rates will get low customer satisfaction
  - Multi-path – it helps and hurts
    - Helps – Signal bounces around and can help overcome nulls
    - Hurts - Echoing of same signal into the receiver
  - Real office environment effective path loss
    - Absorption, etc: $1/r^{2.7}$ instead of $1/r^{2}$

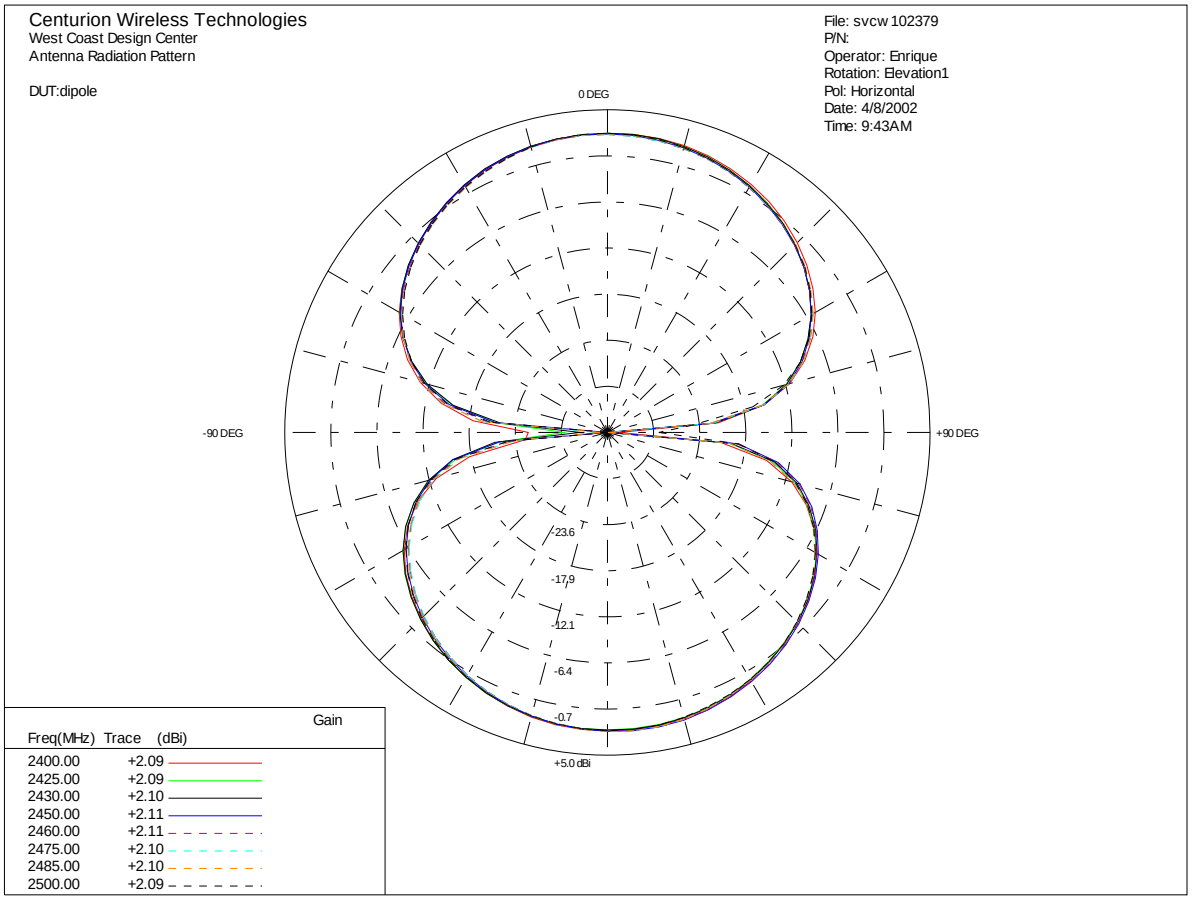
Design Considerations

- I thought 100mW was the power limit ??
  - Please wait a few slides

Design Considerations

- Antenna Measurements
  - dBi – antenna referenced to isotropic (point) radiator
    - A point radiator has a gain of 0 dBi
    - A reference dipole has a gain of 2.2 dBi
  - Antenna radiation is polarized
    - Horizontal and Vertical
  - Antenna plots are measured in vertical and horizontal polarization
    - In far field (few meters outside an anechoic chamber) the two combine

Design Considerations

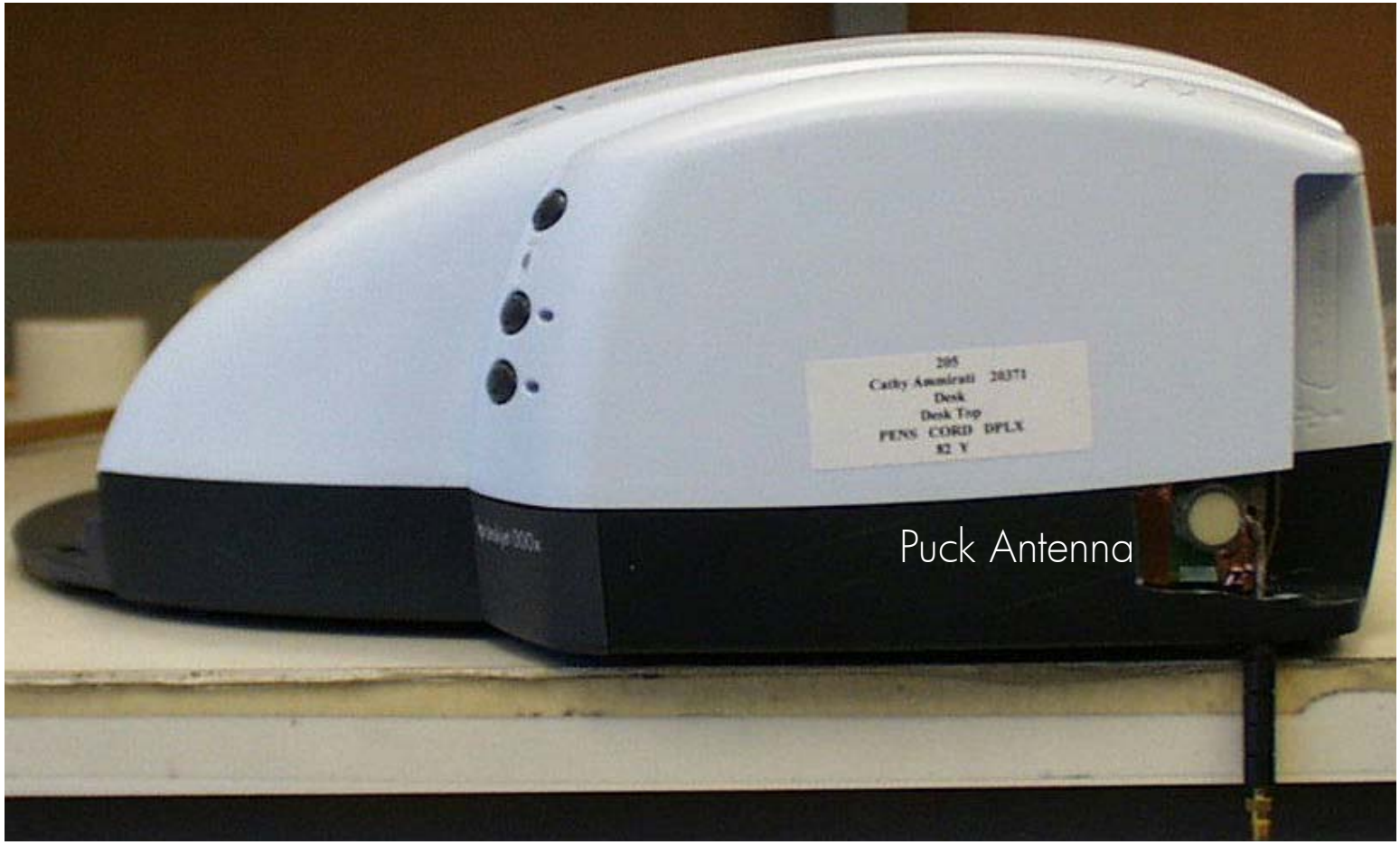


Horizontal Radiation Pattern of Dipole

Design Considerations

- Antenna Measurements – cont
  - Radiation plots are taken in the 3 mutually perpendicular axis in both horizontal and vertical polarizations
    - Azimuth, Elevation 1, and Elevation 2
    - A clear description of E1 and E2 is always needed
  - 6 total plots
  - The H and V plots are then added together

Design Considerations

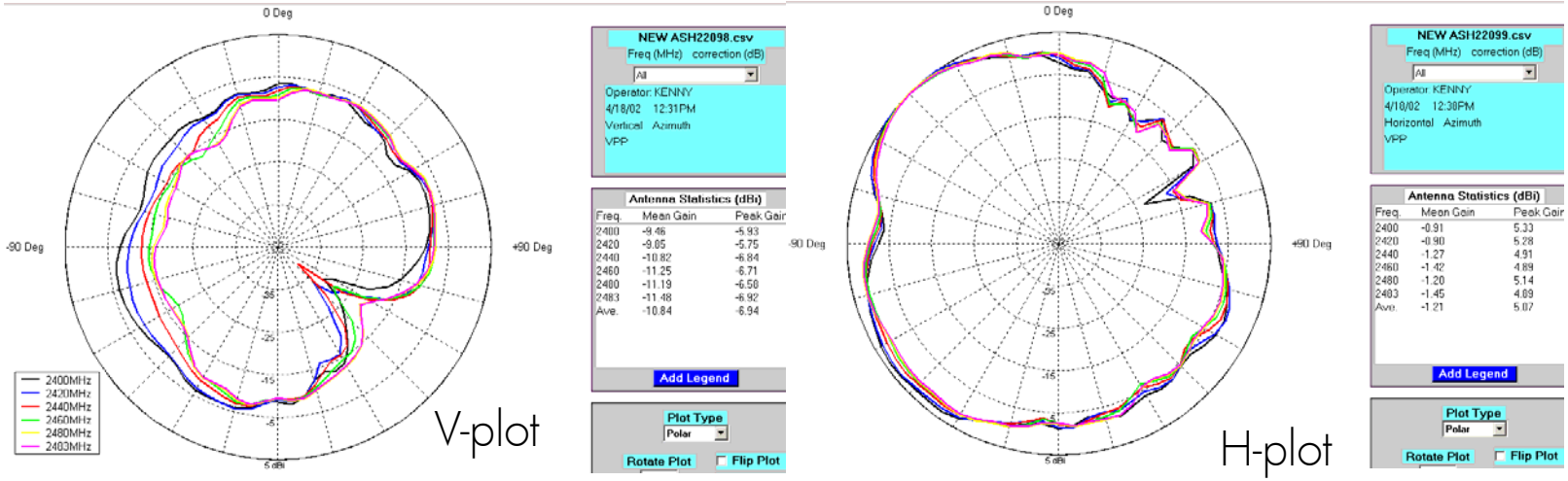


Gepetto Printer

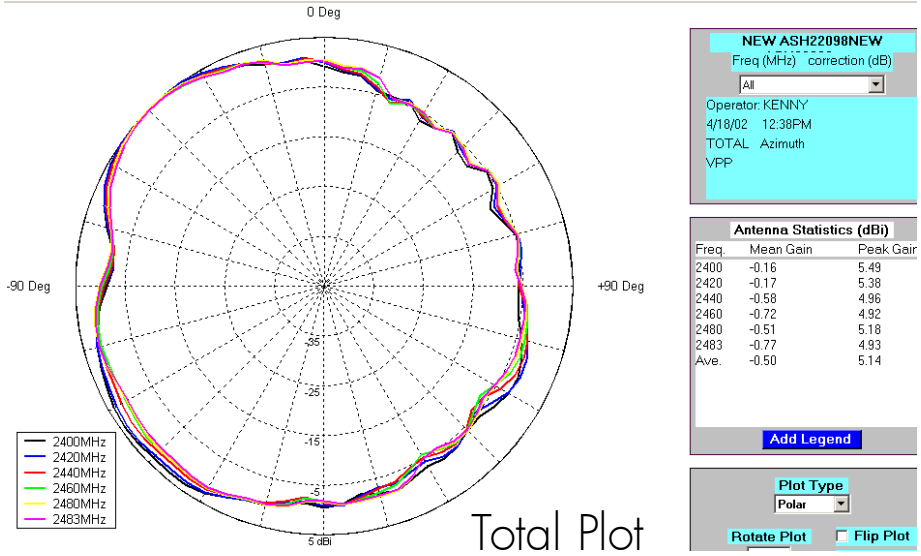
Design Considerations

Gepetto Printer

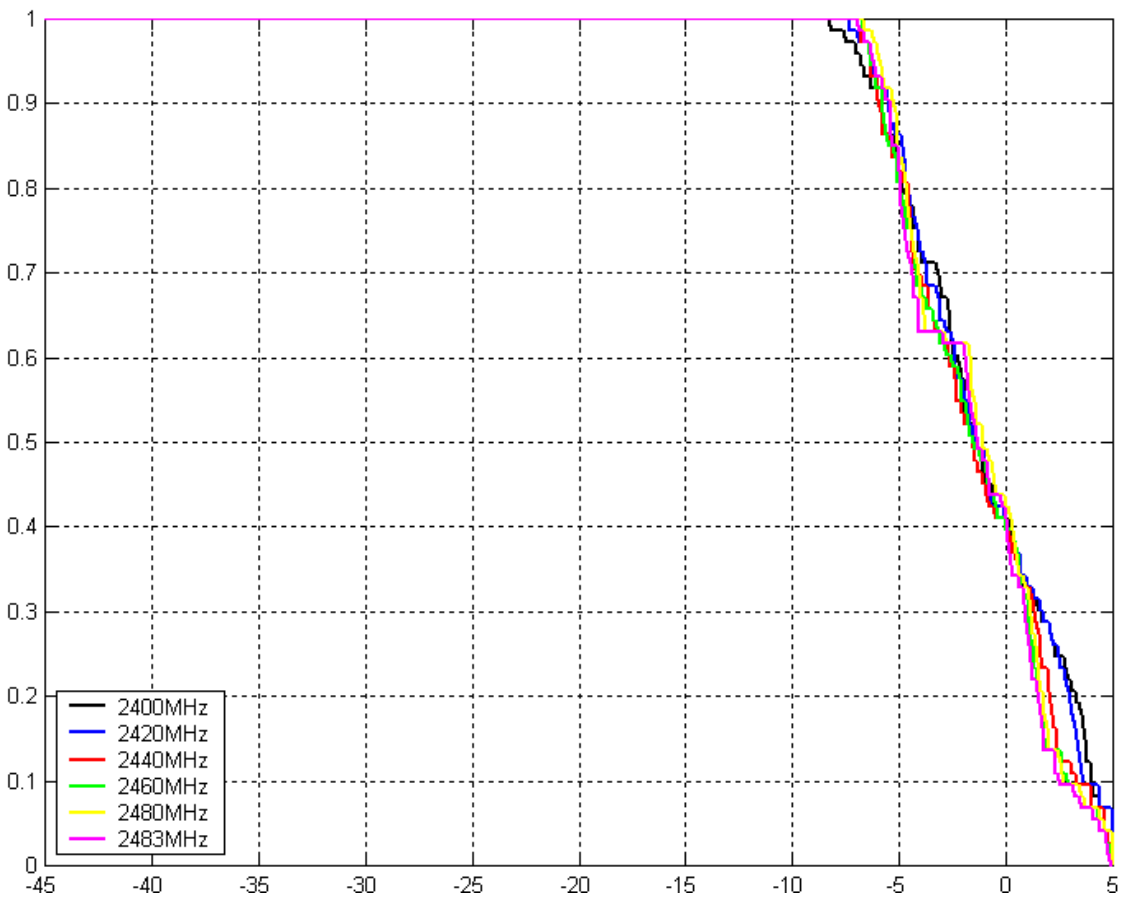
Design Considerations

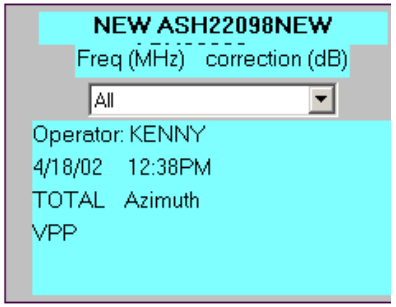


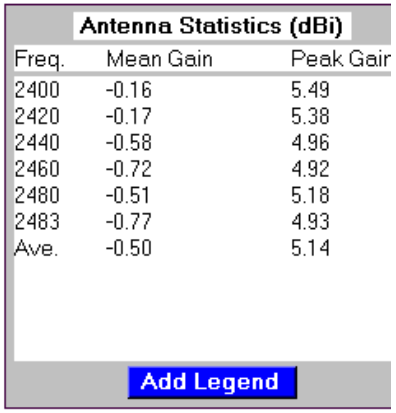
Gepetto Azimuth Orientation

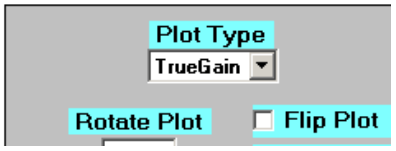


Design Considerations









Azimuth Waterfall Plot

Design Considerations

- Transmit Power
  - Measured in dBm (dB milliwatts)
    - 1 mW = 0 dBm
  - How much Transmit power can we have?
    - Limited by USA (FCC) and European (ETSI) regulations
    - USA limit is 1000mw or 30dBm average
    - European limit is 100mw or 20 dBm EIRP PEAK!!!

Design Considerations

- Transmit Power - cont
  - EIRP: effective isotropic radiated power
    - Isotropic means the antenna gain is included
  - Which antenna gain?
    - If one is certifying a radio module with an antenna, then it is the gain of the antenna while the module is being tested BY ITSELF
    - If one is certifying a product, then it is the gain of the antenna with the radio IN THE PRODUCT

Design Considerations

- Transmit Power - cont
  - Peak power kills us!!!
    - Peak to average ratio for 802.11b waveform is ~ 3dB (1/2 lost!)
    - Average power is used to calculate link budgets
    - Average power is specified in 802.11b data sheets

Design Considerations

- Transmit Power - cont
  - Allowable Average Conducted Output Power
    - = 20dBm Peak – max antenna gain – temp offset (is radio linear over temp?)
    - = 17dBm – max antenna gain – temp offset

Design Considerations

- Transmit Power - cont

  Example – HP Rubicon print server radio

  - Max antenna gain = 1.1 dBi
  - Max power offset over temperature = 1.2 dBm @ 10C
  - Conducted limit = 17– 1.1- 1.2 = 14.7dBm
  - 14.7 dBm = 30mW

Design Considerations

- Conclusions
  - Omni antenna pattern is best (0 dBi)
    - Nulls will reduce range
    - Peaks will reduce allowable transmit power level
    - If one has nulls, one will have peaks (conservation of energy)
  - Temperature compensation circuits are needed in the radio

Design Considerations

- Business 101 decisions
  - Europe restricts us to 30mW and USA is 1W
    - One SKU or 2 ??
  - Do we certify at the product level or module level?
    - Certification cost ~$125K
    - Module certification can be transferred between products
    - Product level certification allows antenna pattern customization

IEEE 802.11 Security

Dave Smith

Security

- Why is security such a big deal in WLANs?
  - The medium for Ethernet is wire – physical barriers to entry
  - The medium for WLAN is the Air – it goes everywhere
  - Using a hand built “Pringle Can” high gain antenna students were able to drive around NYC and tap into corporate WLANs
  - Since WLANs are just an extension of the wired LAN and it is “easily” accessible, WLANs can compromise the entire corporate intraNET

Security

- What Security mechanisms are there now?
  - WEP RC4 over-air encryption
    - 64 bit or 128 bit stream Cypher – more later
  - Security key – 64 bit or 128 bit
    - Once one has "plugged" into a WLAN by entering the SSID an additional requirement of the correct KEY is required before the AP will allow informational data transfer
    - With just the correct SSID management data is allowed

Security

- Current Security Mechanisms - cont
  - MAC address authentication
    - The AP will only allow stations with approved MAC address to transfer informational data
  - APs do not advertise the WLAN SSID
    - AP configuration option
    - Station scanning only shows that the WLAN is operating on a particular channel

Security

- Authentication Modes
- Open System
  - No verification of the identity of either station is conducted. Can connect with or without encryption.
- Shared Key
  - Verification of identity is conducted with use of a shared 'WEP' key. Both stations must utilize the same shared key.
- Closed System
  - Proprietary method used by some vendors to hide the SSID of the BSS requiring the joining station to know the SSID in order to join. (Additional level of security).

Security

- Authentication Types
  - EAP - Extensible Authentication Protocol
    - Protocol used for Authentication
  - EAP-MD5
    - Username and Password authentication with Radius server
  - EAP-TLS
    - Certificate based authentication with Radius server
  - EAP-Others
    - There are many others that can be used, for instance TTLS, Kerberos etc.

Security

- What is WEP?
  - WEP – wired equivalent privacy
  - Meant to prevent casual eaves dropping
  - RC4 is a stream cypher that uses static encryption keys and predictable initialization vectors
  - With the advances in computer power a sniffer can easily find out the IV and then get the Key

Security

- How is Security going to be improved?
- IEEE 802.11i Standard
  - Short term software fix called WPA (Summer'03)
    - WPA changes the key automatically every 50K packets
  - Hardware encryption fix – AES-CCM block cypher
    - Spring'04
  - 802.1x – Port Based Network Access Control
    - Allows use of Upper Layer Access Protocols (ULAP) to authenticate users
    - ULAP example: Radius, Kerberos, TLS

Security

- Security improvements – cont
- Industry Initiatives – propietary, etc
  - CISCO LEAP – proprietary authentication
    - Default corporate standard
    - HP print servers will support LEAP in Future release

Security

- Methods of Attack
- There have been several methods of attack ranging from hacking the key to denial of service
- Hacking the key
  - several programs are available on the net such as 'Air Snort' which monitor a period of traffic (~1hour), then analyze the data and within 15-18 minutes are able to recover the key.
  - Use of certain IV's result in the key being somewhat exposed (Weak Key) enabling the key to be compromised.
    - One example is the re-use of an IV within a traffic session by any node. Some vendors always started with the same IV (zero) at power up, thus creating 'Weak Keys'

Security

- Methods of Attack – Cont
- Bit flipping attacks
  - These attacks work on the fact that once a connection is established very little changes in the IP header and because of the RC4 stream cypher, the IP header is in a known location.
  - With this kind of attack, a captured packet is used and the destination IP address is changed to an address outside the firewall. The bogus packet is then injected back into the network with a correct CRC which the AP then dutifully decrypts the packet and sends it to the router to route outside the firewall
  - With the original encrypted packet and the unencrypted packet, the key can be derived

Security

- Methods of Attack – Cont
- DHCP and Bootp can also be attacked because of predicatable packet headers
  - There are other protocols that are susceptable to this kind of attack
- XOR attack - with this attack one captures some packets and XOR's the packets together to derive a third packet.
  - This third packet is then used to XOR against new packets
  - As a result, some of the packet data will drop out, thus being exposed
  - From multiple attempts, eventually the key can be determined

Security

- Methods of Attack – Cont
- Replay Attacks
  - These attacks capture network traffic and then modify some of the traffic and replay the traffic, injecting it back into your network.
- Denial of Service
  - This attack overpowers the node under attack

Security

- Methods of Attack – Cont
- Packet injection attacks
  - These attacks try to get some node on the network to respond to the data for example, injecting email into the network and getting a client to respond to it.
  - Packets are injected via wireless and the client responds via the infrastructure, again sending the injected frame outside the firewall.

Security

- Methods of Attack – Cont
- Client identity theft
  - This method of attack results in a bogus client being given access to the network because of false or stolen credentials.
  - This is often used with a denial of service attack against the node that had its credentials stolen.

Security Solutions

Dave Smith

Some material from Rabah Hamdi PSG Mobile Group

Security Solutions

- Place network outside firewall
- Use VPN to tunnel through firewall
- Use 802.1X with EAP-TLS and Radius
  - Change Encryption keys often
- Use proprietary solution from one vendor
- Wait for IEEE 802.11i standards

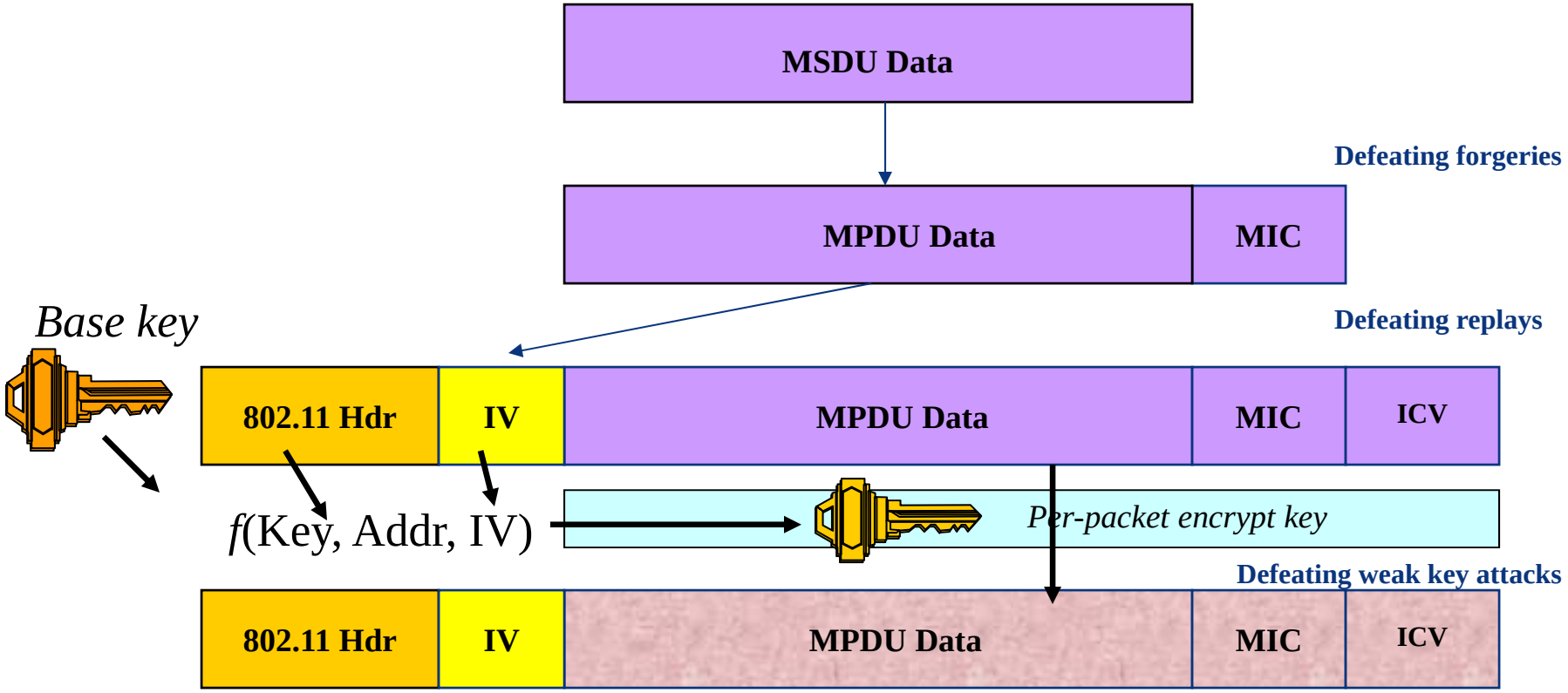
Security Solutions

- Current WEP-based solution is “broken”, 802.11i Task Group is chartered to fix it.
- Current Security is at MAC layer, independent of PHY (a/b/g) variations
- IEEE 802.11i is currently at draft standard level – 2-pronged approach:
  - “Interim”: WPA with 802.1x-based authentication
  - “Best”: AES-CCM encryption w/802.1x-based authentication
- Many players are implementing interim proprietary solutions
  - Gets them time-to-market/market leadership
  - All are converging on 802.11i-based standard implementations

Security Solutions

- WPA enhances WEP encapsulation:
  - Message Integrity Code (MIC) over MSDU
    - Defeating forgeries
  - Packet sequencing counter (16 bits) for each MPDU
    - Defeating replay
  - Cryptographic key mixing function & RC4 key as the WEP seed
    - Weak Key avoidance
  - WPA requires IEEE802.1x authentication and key management
  - Rapid Rekey - 2^{15}
    - EAPOL-Key - Change encryption key frequently
  - Per-link keys
    - Unique key per STA

Security Solutions



Evaluation Tests

Timothy P. Wakeley PE

Evaluation Tests

- IEEE 802.11b Standard Requirements
- Transmit Requirements
  - Power on/off ramp – 10-90% time of 2 uS
  - Frequency tolerance of +/- 25ppm
  - RF Carrier Suppression of 15dB below spectral peak

Evaluation Tests

- Transmit Requirements – cont
- Spectral Mask – frequency domain envelope
  - The transmitted spectral products shall be less then –30 dBr for:
    - fc-22 MHz < f < fc-11MHz; and
    - fc+11 MHz < f < fc+22 MHz;
  - and shall be less than –50 dBr for
    - f < fc-22 MHz; and
    - f > fc+22 MHz.

Evaluation Tests

- Transmit Requirements – cont
- Modulation Accuracy - informational
  - Ideal BPSK modulation in 1 and 2 Mb/s mode
    - In phase diagram this is shown by a unit vector from the origin with an angle or either 0° or 180°
  - Ideal QPSK modulation in 5.5 and 11 Mb/s mode
    - In phase diagram this is shown by a unit vector from the origin with an angle or either 45°, 135°, 225°, or 315°

Evaluation Tests

- Transmit Requirements – cont
  - A real modulation vector will have a slightly different magnitude and angle
  - The difference between ideal and real is called the Error Vector
  - For 802.11b the normalized error vector can have any angle and a maximum magnitude of 0.35 or 35% - EVM

Evaluation Tests

- Receiver Requirements
  - Adjacent Channel (Interference) Rejection
    - 35dB of rejection 25MHz away, 8% FER, 1024 byte packet
  - Receiver Minimum Sensitivity of –76dBm
    - 8% FER with 1024Byte packet at 11Mb/s rate
    - No channel conditions given
  - Receiver Maximum Input Level of –10 dBm

Evaluation Tests

- Additional Tests for Quality and Vendor Comparison
  - Transmit Tests
    - The rms EVM should be below 10% for BPSK
    - The rms EVM should be below 12% for QPSK

Evaluation Tests

- Additional Tests - cont
  - Receiver Tests
    - Receiver sensitivity of –76dBm with perfect TX waveform is meaningless
  - Measure Receiver Sensitivity with these test cases for 8% FER
    - TX modulation with uniform EVM distribution; max EVM=0.35, rms EVM=0.20
    - TX modulation with normal EVM distribution; max EVM=0.35, rms EVM=0.12

Evaluation Tests

- Additional Tests – cont
  - Additional receiver test cases – cont
    - Inter-symbol interference; 133nS of delay spread at 11Mb/s
    - Carrier frequency offset of -25ppm to +25ppm.