SystemEXPERTS

Practical Wireless IP:
Concepts, Administration, and Security

Brad C. Johnson &
Philip Cox
SystemExperts Corporation

Just checking...

- This is a top level bullet
  - This is the next level in
    - this would be level 3
      - this would be level 4
- Can you hear?
  Check 1…2…3…Check
- **Is it too hot?**
  Too cold?

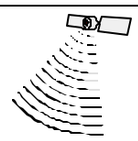
Course Contents

- What is is
  - Wireless, focused on
    - IP services for laptops
      - and a little on handheld and cell-phone Internet access
  - Wireless, for understanding
    - Security, configuration, and usage
- What it isn't
  - A Radio Frequency Primer
  - An *in-depth* analysis of Cellular Wireless protocols
  - An exhaustive list of wireless providers and devices

Course Objectives

- When you leave this course, you should be able to:
  - Identify major protocols and standards used by, first and foremost, wireless LANs as well as PDAs and cell-phones
  - Identify important features and configuration options associated with Access Point and client cards
  - Understand major threats to wireless IP networks

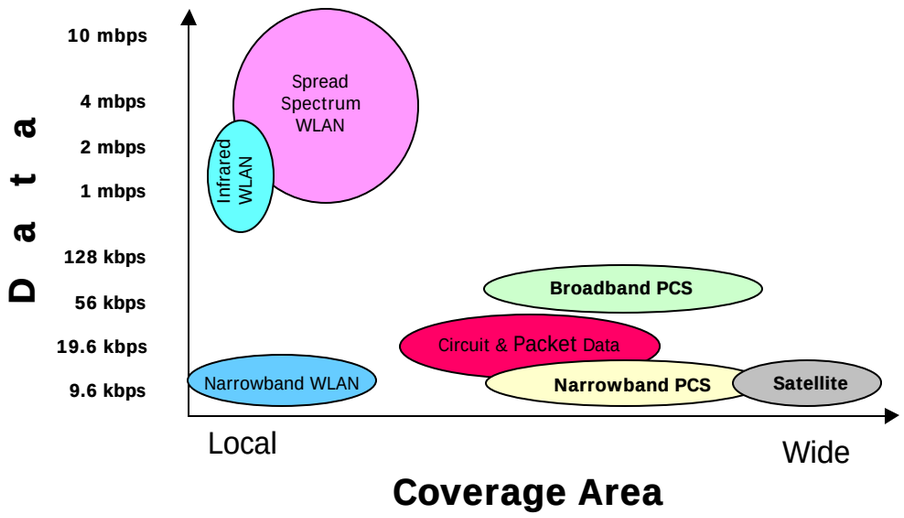
Where are We?



- **From 50,000' to 5' in about 24 slides**
  - **Threats**
- Handheld Practicals
- LAN Practicals
- *NIX and Wireless
- Currents
- Antennas

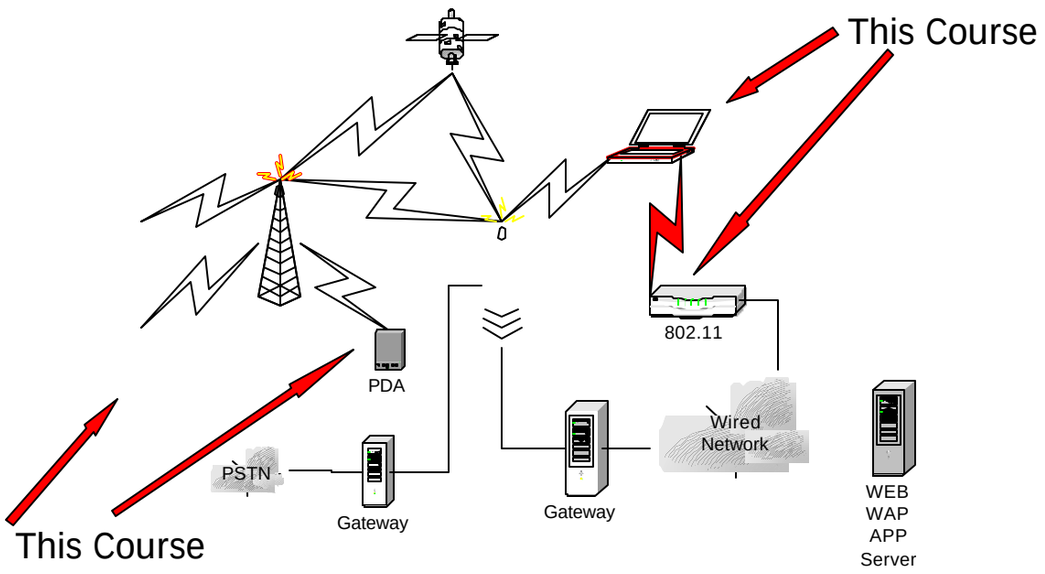
SystemEXPERTS

What is Wireless



SystemEXPERTS

Wireless Component Overview



Wireless Devices

- Historically
  - Single function device (very small)
    - use a phone to talk
    - use a pager to get a phone call notification
    - use a PDA to load appointments
  - General purpose devices (small)
    - desktop or laptop for “anything”
- Now and moving into the future
  - Simple devices becoming more flexible
  - General purpose devices becoming (almost) as small/light as the single function devices

Single Function Device Migration

- Handheld
  - Cellular Phone
    - voice and data
    - increasing speeds
    - more complex displays
  - PDA
    - viable as stand-alone wireless device (without requiring desktop download first)
  - Pager
    - interactive

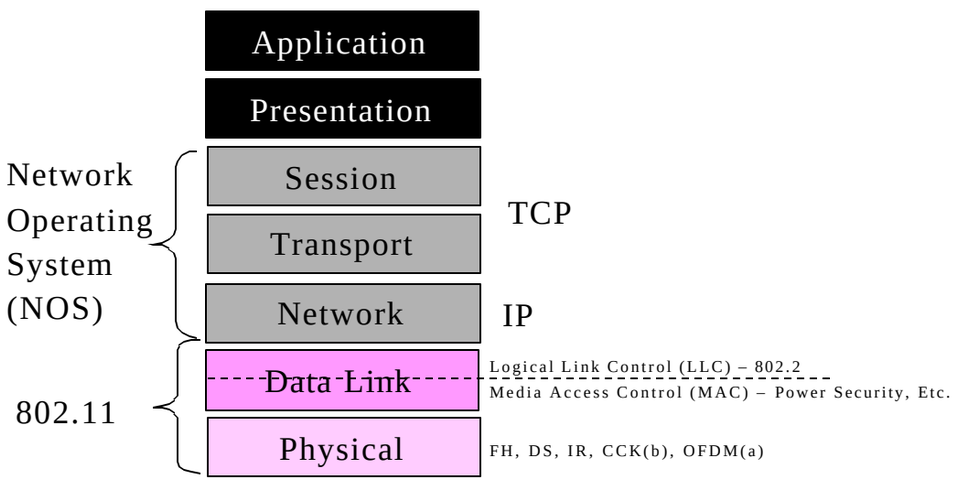
General Purpose Devices

- HomeRF
  - 2.4 GHz band
  - 1.6 Mbps from a distance of about 150 feet
  - Residential market
- Bluetooth
  - 2.4 GHz band
  - Creates Personal Area Networks (PANs)
  - Up to 780 Kbps within a 10-meter range
  - “Appliance” market

802.11b

- Unlicensed 2.4 GHz band
- Uses direct-sequence spread-spectrum (DSSS)
  - Frequency-Hopping FHSS can only be used for 1 & 2 Mbps in US because of FCC regulations
- 1 - 11 Mbps from a distance of about 150 to 2000 feet (without special antenna)
  - …more on this later
- Home business and business markets

802.11 Plain and Simple

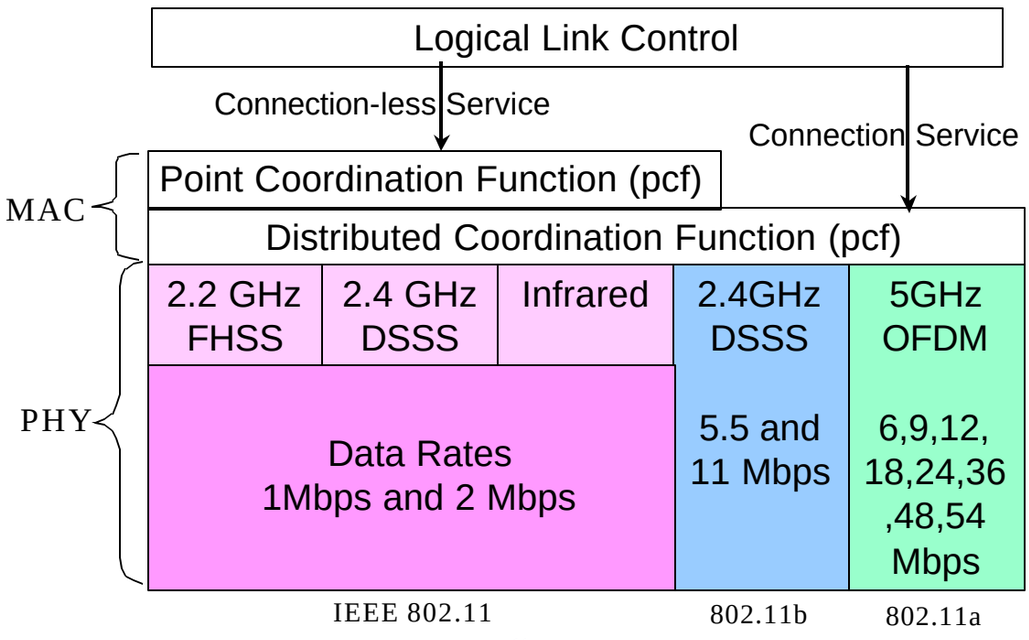


802.11b

- Physical Layer
  - Physical Medium Dependent (PMD) – wireless encoding
  - Physical Layer Convergence Protocol (PLCP) – common interface
    - long preamble for all 802.11b systems
    - short preamble for special case: e.g., streaming video, Voice-over IP
- MAC Layer
  - Inter Frame Space (IFS)
  - Physical Carrier Sense
  - Virtual Carrier Sense
    - e.g., hidden-node
  - Frame Control
  - Power Management
  - Fragmentation

SystemEXPERTS

802.11 A Little Less Plain & Simple



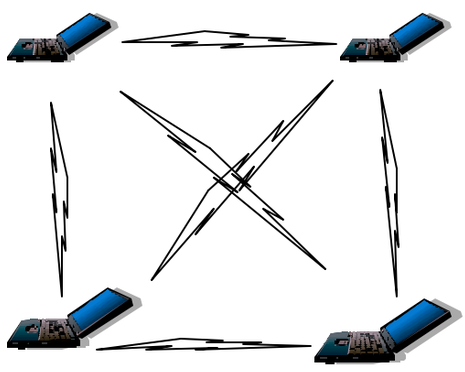
SystemEXPERTS

802.11b Frame Control

- 3 types of 802.11b packets
  - Management (type 00)
    - {association, re-association, probe} {request, response}
    - authentication, de-authentication, & disassociation
    - beacon
      - e.g., time-stamp, traffic indication map, supported rates
    - ATIM – Announcement Traffic Information Message
      - sent after each frame
  - Control (01)
    - RTS, CTS, ACK, CF*, PS-Poll
  - Data (10)
    - ok, data! plus
    - CF-ACK/Poll, etc.

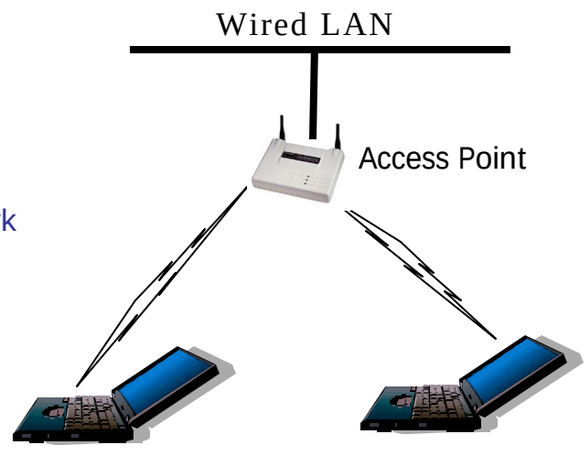
802.11b IBSS

- Independent Basic Service Set (IBSS)
  - Ad-Hoc mode
  - Often called peer-to-peer
  - No Access Point (AP)
    - i.e., with just your client cards
  - No wired connections, only link wireless clients



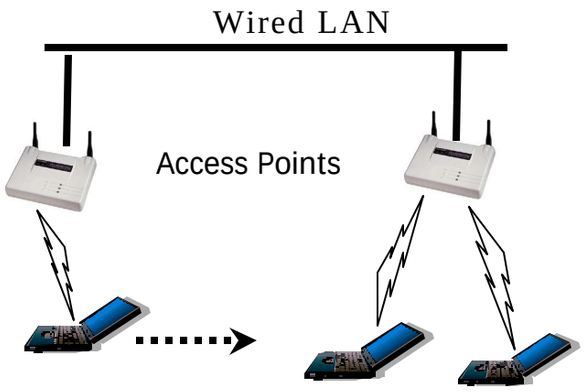
802.11b BSS

- Basic Service Set (BSS)
  - Infrastructure mode
  - Uses an AP to connect clients to a wired network



802.11b ESS

- Extended Service Set (ESS)
  - Infrastructure mode
  - Uses multiple APs
  - Clients may roam between APs
    - …more on roaming later



Exposures

- Technology problems
- Theft of hardware
- Insecure configuration information
- Masquerading
- Virus
- Eavesdropping
- Authorization

Technology Problems

- What does “technology” mean?
  - The current state of common hardware and software solutions, examples include
    - protocol issues
      - the raging debate over WEP
    - specification issues
      - WEP doesn’t encrypt the SSID and, in general, management packets
    - configuration issues
      - default AP is WEP disabled, open authentication, default SNMP community string
    - interoperability issues
      - the Gap in WAP

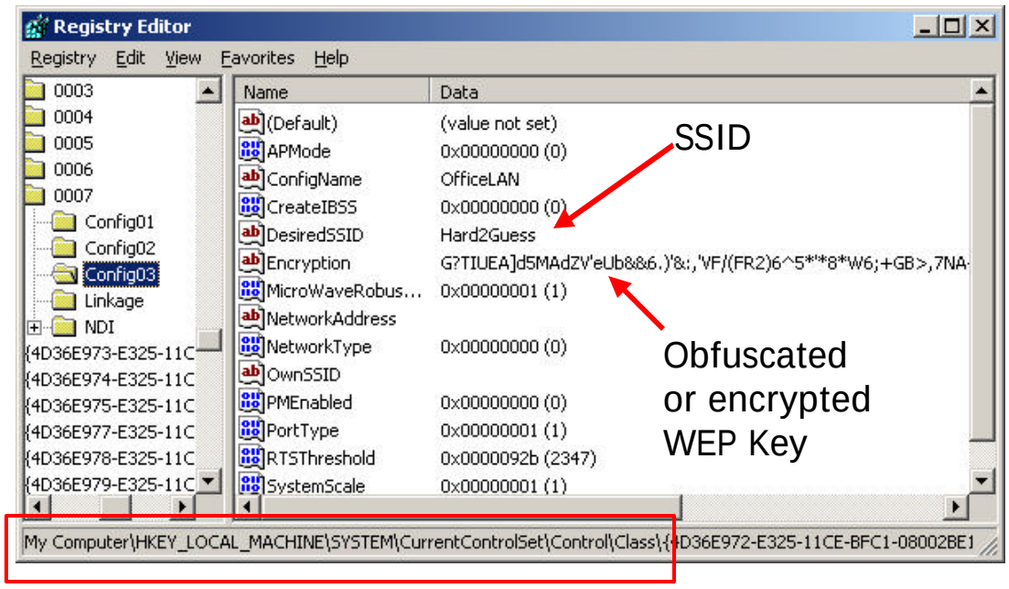
Theft of hardware

- Wireless stuff is small
  - Wireless cards fit in a shirt-pocket
  - Most of the APs fit in a jacket pocket or are easily hidden in any kind of bag
    - should they be tagged like clothes in a store?
- Cisco 340 cards write WEP keys to the card
- If a laptop were stolen, how long would it take to re-key your Wireless network?
- APs have WEP Keys in them
  - Data is stored locally

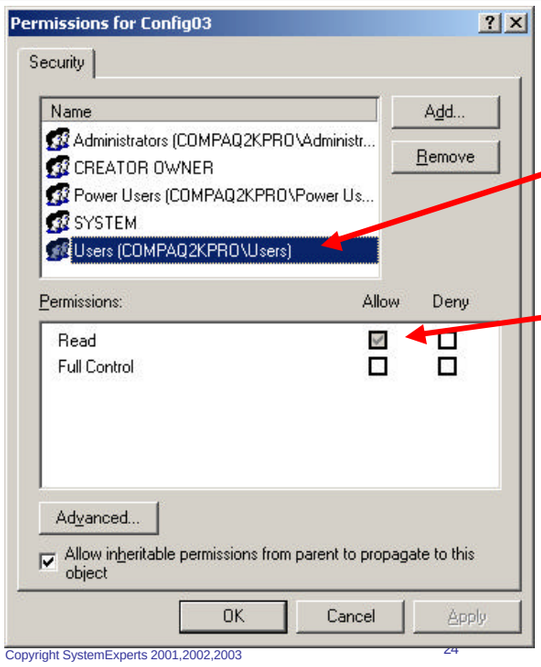
Insecure Configuration Information

- Where does the client store the information?
  - Cisco: On the card
    - so steal it
  - Lucent:
    - on Windows, it's in a world-readable registry key: so copy the values and import them into your configuration
    - on other OSs, it's stored in a file
  - Other cards are storing the data someplace too ☺
- Let's take a closer look at the Lucent Windows example

Lucent Client Registry Entries



Registry Permissions



Any authenticated user

Can read and copy this data ☹

Masquerading

- Client side
  - AP identifies system, not user
  - System may be used by more than one user
  - No authorization schemes for different user groups
- Access Point
  - Clients don't authenticate AP's
- Solution
  - Per user authentication: EAP

Virus

- Various ways that virus can "get" to your wireless device
  - Host based that is carried forward on a PDA (HotSync) or phone (TrueSync) sync
  - PDA passes on through infrared
  - Web phone downloads
    - examples include the European EPOC OS

Courtesy of Information Security

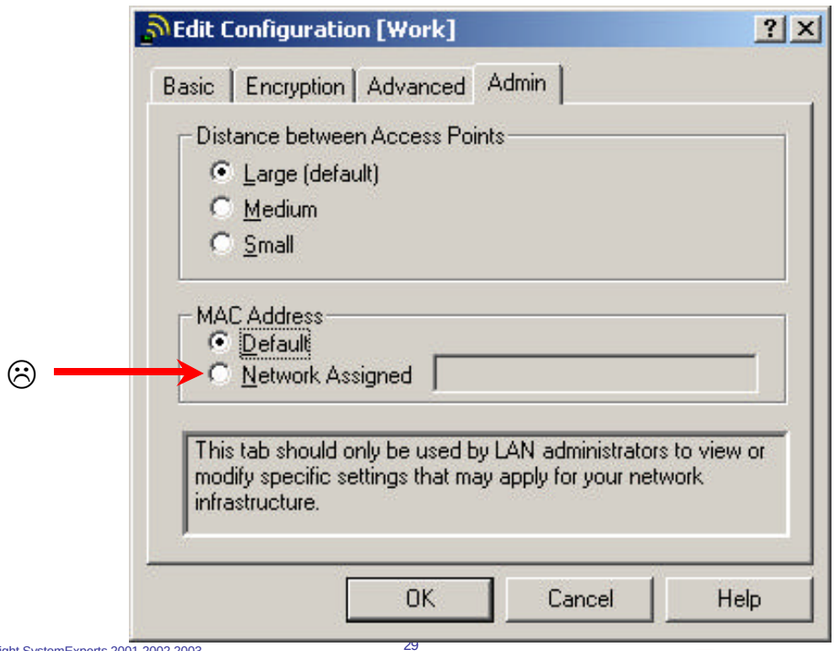
Eavesdropping

- Indirect: listening to the network that the wireless access point is connected to (PROMISC)
  - Remember: WEP only encrypts data between the client and the access point!
  - Quite frankly, this is what most people are doing when they talk about “sniffing wireless”
- Direct: listening to the airwaves (RFMON)
  - Sender can not detect eavesdropping
  - Frequency band largely determines range
    - it is quite possible that it goes outside the building
    - special electromagnetic shielding is needed to “stop” leakage

MAC Layer

- Can configure the AP to talk to specific Media Access Control addresses (MAC, a.k.a. hardware address)
  - Not to be confused with Message Authentication Code (MAC)
- Controls access to wired network not wireless
- Some APs will use RADIUS to get the information
- Problem:
  - MAC addresses can be manually set very easily (see next slide)

MAC address configuration



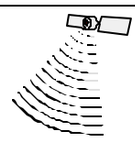
☹

Notes:

Notes:

Notes:

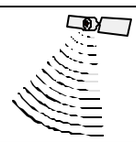
Where are We?



- From 50,000’ to 5’
- **Handheld Practicals**
- LAN Practicals
- *NIX and Wireless
- Currents
- Antennas

SystemEXPERTS

Section Contents



- **Transports**
- Mobile Data Services

SystemEXPERTS

Key Factors in Technology

- Regulation
  - Determines who gets what and how
- In US "competition" was king
  - Regional Bell's and one other (1/2 each)
- In Europe "interoperability" was king
  - Government owned "*Bells*", so no competition, so let's interoperate
  - Need to exchange billing and accounting information
- Security was designed to protect against fraud
  - As opposed to protecting your data

Cellular Basics

- Two Connections Types
  - Circuit Switched
  - Packet Switched
    - More efficient (~10x) than circuit switched
- Transmission techniques
  - Frequency Division Multiple Access (FDMA)
    - Frequency range is divided into channels
    - Dedicated channel/frequency per call
  - Time Division Multiple Access (TDMA)
    - Each call gets a "timeslot" of time on a certain frequency
  - Code Division Multiple Access (CDMA)
    - Uses spread spectrum techniques (i.e., is spread over the available frequencies)
    - Each call has a unique code

Major Cellular Systems

- Advanced Mobile Phone System (AMPS)
- IS-54/IS-136
- IS-95
- Global System for Mobile Communications (GSM)
- Integrated Digital Enhanced Network (iDEN)
- PCS

Note Telecommunications Industry Association (TIA) is the main standards carrier for the Interim Standards (IS)

GSM

- "THE" system outside of the US
- A digital system using a modified version of TDMA
- Data at 9.6k
  - No modem needed for circuit or packet switched data
- 900 MHz (GSM800) and 1800 MHz (GSM1800) in Europe and Asia, 1900 MHz US (GSM1900)
  - They are **not** compatible
- Use Subscriber Identification Module (SIM) cards to store all the connection data and identification numbers you need to access a particular wireless service provider

GSM Security

- International Mobile Equipment Identity (IMEI) for each device to determine if device is allowed on the network
- Shared secret: Stored in the Authentication Center (AuC) and subscriber's SIM card
  - Authentication: The AuC generates a random number sends it to the mobile. Mobile uses A3 cipher and shared key to generate a signed response sent back to the AuC
  - Encryption: Use a key derived from A8 cipher using the same pseudo random number+subscriber-key as above. Cipher key is used with the TDMA frame number, in the A5 cipher to create a value to XOR with data
    - same process in IS-54/136 & PCS1900

Today's Data Systems

- Primary mobile wireless data services are…
  - Cellular Digital Packet Data (CDPD)
  - iDEN packet service
  - Circuit-switched data service for CDMA networks (e.g., SprintPCS)
  - Circuit-switched data services for GSM networks
  - Modems and analog phones
- All of these services offer speeds in the 9.6 Kbps to 19.2 Kbps range
- How they deliver…
  - Smart phones (phones with micro-browsers)
  - Wireless modems (PC card or cable with phone)

CDPD

- IS-732
  - Uses idle voice channel or dedicated data channel depending on network configuration
- It enables analog AMPS networks to carry packetized data alongside voice
  - CDPD is to AMPS what D-AMPS+ is to TDMA (IS-136/D-AMPS) a way to do Packet Data vice Circuit Data
- Operates on the 800 MHz frequency
- Data only, up to 19.2k
- Requires a modem to convert analog

CDPD Security

- Clone prevention: Asks 2 questions
  - How many times have you accessed the network?
  - What was the last password you used?
- Network level security based on RC4
  - Diffie-Hellman to get session key

Other Popular Systems

- Cingular (a.k.a. Mobitex)
  - Operated by Bell South and RAM Mobile Data
  - Data up to 8k
  - Wide coverage
    - Australia, Belgium, Canada, Korea, Netherlands, Sweden, United Kingdom, United States
  - Used by PALM VII and Blackberry
- ARDIS (DataTAC)
  - Connection oriented
  - Two versions: MDC4800 and RD-LAP
  - Most widely used version is Radio Data Link Access Protocol (RD-LAP)
    - used by Motient for Blackberry

What is 3G?

- Generic term covering a range of future wireless network technologies
- a.k.a. IMT-2000
- Includes …
  - cdma2000
  - UMTS (Universal Mobile Telecommunications System)
  - GPRS (General Packet Radio Service)
  - WCDMA (Wideband Code Division Multiple Access)
  - EDGE (Enhanced Data rate for GSM Evolution)
- Focus is to combine high-speed mobile access with Internet Protocol (IP) based services

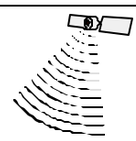
In a box …

Network Type	Technology	Provider	Speed
Packet (data)	Mobitex	Cingular	8k
	CDPD	*AT&T*, Verizon, BC TEL Mobility, TELUS Mobility	19.2k
	RD-LAP	Motient	19.2k
	iDEN	*Nextel Online*	9.6k
Circuit (voice and data)	CDMA	*Verizon*, *Sprint PCS*, Bell Mobility & Clearnet PCS, Airtouch, GTE, Bell Atlantic, Primeco, others	14.4k
	GSM	*Cingular* (old PacBell), Voicestream, Omnipoint, BellSouth Mobility, Sprint, others	9.6k
	TDMA	*AT&T*, BellSouth, Southwestern Bell	9.6k
	AMPS	*AT&T*	19.2k
	iDEN	*Nextel* (voice)	9.6k

Observations

- A lot of things are changing quickly here, and it's hard to keep them straight
- Watch IMT-2000 and your wallet ☺
- IS-54, IS-136, and IS-95 will default to AMPS when their signal cannot be detected
- Arguably the best site to find technical information
  - www.privateline.com/Cellbasics/Cellbasics.html
  - www.howstuffworks.com/cell-phone.htm
- As time passes, we'll watch and see what actually shakes out

Section Contents



- Transports
- **Mobile Data Services**

SystemEXPERTS

Mobile Data Services

- Currently there are three main services provided:
  - Messaging
  - Wireless Web
  - Proprietary applications
- As time goes on, specific applications will be written or ported to provide mobile services

SystemEXPERTS

Mobile Data Services: Messaging

- Short Messaging Service (SMS)
  - Available on all digital technologies
  - 140-260 byte messages, store and forward
- Cell Broadcast Service (CBS)
  - Available on GSM only
  - 1,395 byte messages
  - Limited deployment: No way to bill, it's broadcast ☺
- Unstructured Supplementary Services Data (USSD)
  - Connection oriented, GSM based (also UMTS, GSM successor)
  - 182 bytes, uses control channel

Mobile Data Services: Wireless Web

- Factors: speed, screen size, and CPU/memory
- Uses a micro-browser
- Popular delivery standards
  - Compact HTML (C-HTML)
  - Web Clipping
  - Wireless Application Protocol (WAP)

C-HTML

- Created by W3C
- Simplified version of HTML
- Heavily used in Japan via i-mode service
  - Virtually unknown elsewhere
- Advantage: Displays equally well on regular browsers
- Disadvantage: Not optimized for handheld limitations

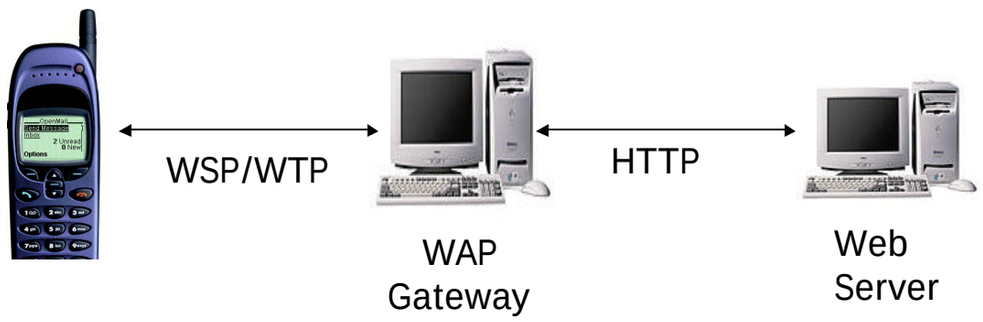
Web Clipping

- Palm proprietary
  - Palm VII (US only)
- Palm Query Application (PQA) loaded on each server interprets HTML and tell the PALM which parts of the page to download
  - A separate PQA must be installed for each site
  - Downloaded to Palm from desktop
- Uses Mobitex and OmniSKY networks
- Advantage: Fast access and off-line browsing
- Disadvantage: Need to have PQA on each system

Wireless Application Protocol (WAP)

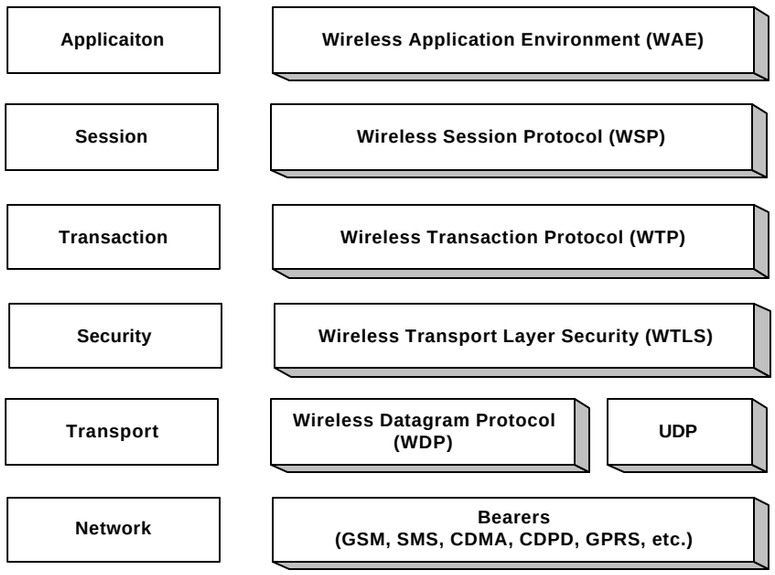
- An application environment
- A set of communication protocols for wireless devices
- Derived from Handheld Device Markup Language (HDML) by Phone.com (a.k.a. Unwired Planet)
- Client/server philosophy
- Uses a micro-browser and a WAP Gateway connected to the mobile network

WAP Architecture



Note: WAP Server = WAP Gateway + Web Server

WAP Protocol Layers



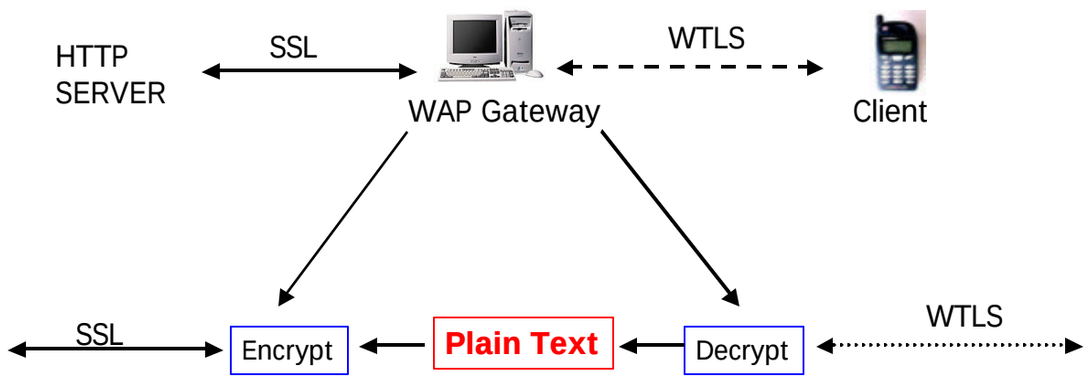
SystemEXPERTS

The Gap in WAP

- Not to be confused with WAP Gap
  - …which is hundreds of millions of devices that are NOT using WAP
- What is the Gap in WAP?
  - WAP handset to WAP server handled by WTLS
  - WAP server to Internet handled by SSL
  - Once decrypted by WTLS, data is exposed until it is re-encrypted by SSL
    - this of service providers, like PalmNet

SystemEXPERTS

Gap in WAP



VPNs

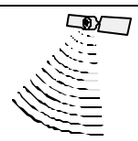
- Certicom's movianVPN
  - Basis for iPassConnect PDA service
    - requires a modem and two pieces of software on the PDA
    - lightweight version of iPass' dialer, called iPass Synch and movianVPN
      - users dial up an iPass-affiliated ISP, then establish a VPN
  - Cisco VPN concentrators will support the client
- Texas Instruments/SafeNet VPN

What Really Matters?

- Security
  - Encryption options by…
    - the Bearer
    - the Application
    - WTLS
- Device cost
  - Phones
    - constantly changing options and services
  - Handheld
    - PocketPC vs. CE vs. PALM
  - Expandability
- Interoperability
  - Where can you use it?
  - What can you get to?
- Device management
  - Ease of configuration, upgrades

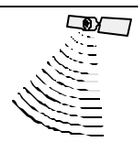
Notes:

Where are We?



- From 50,000’ to 5’
- Handheld Practicals
- **LAN Practicals**
- *NIX and Wireless
- Currents
- Antennas

Section Contents



- **802.11**
- Access Points 101
- Deployment Examples

Wireless LAN Technologies

- Made up of three primary semi-competing technologies
  - IEEE 802.11 {802.11b is our focus}
  - Bluetooth
  - HomeRF

Upcoming WLAN

- IEEE 802.11g (Next generation WLAN)
  - Data rates of 20+ Mbps
  - Selected Intersil's Orthogonal Frequency Division Multiplexing (OFDM)
  - TI's Packet Binary Convolution Coding (PBCC) technology was not selected
- 802.11a
  - …more later

802.11 Local Area Wireless

- IEEE 802.11 makes up the majority of Wireless LANs
- 802.11b (a.k.a. Wi-Fi™) is the current favorite
  - Encodes data using DSSS (direct-sequence spread-spectrum) technology
  - Runs in the 2.4-GHz range
    - different ranges in different regions US, Europe, Japan, France, Spain
  - Four “speed” ranges: 1-Mbps, 2-Mbps, 5.5-Mbps, and 11Mbps

802.11b Components

- Client
  - Wireless Stations
- “Servers”
  - Residential Gateways
  - Enterprise Access Points
  - Access Servers
  - Outside Routers

Current 802.11 Security

- Privacy
  - Wired Equivalent Privacy (WEP)
- Authentication
  - Shared key
  - Open system
- Authorization
  - MAC

Wired Equivalent Privacy (WEP)

- Purpose it to provide “privacy of a wire”
- Uses RC4 for encryption
  - WEP Key + initialization vector (IV) are fed into a pseudorandom number generator
- The IV, Encrypted Message, and checksum are sent in the 802.11 packet
  - Checksum is not WEP key dependent
- IV is changed periodically
  - Implementation dependant, but best if every packet (problem is running out)
- Packet-by-packet data encryption

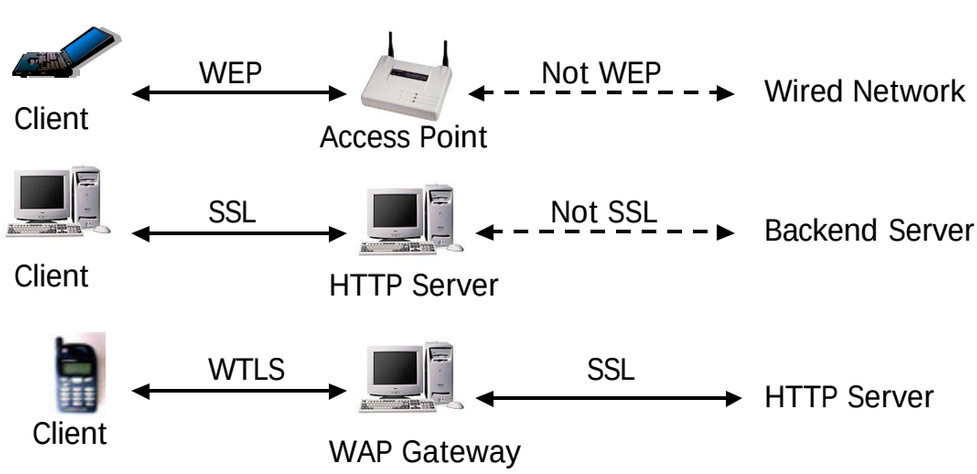
More on WEP Keys

- Standard says 40bit, but many vendors support or 128 bit
  - 40bit is actually 64bit: a 40bit key and 24-bit IV
  - 128bit is a 104-bit key with a 24-bit IV
- No key-management protocol
- Also no inter AP protocol (IAPP) to pass keys

SystemEXPERTS

Access Points and WEP

Q: What does WEP do for you?
A: Think of SSL and WTLS

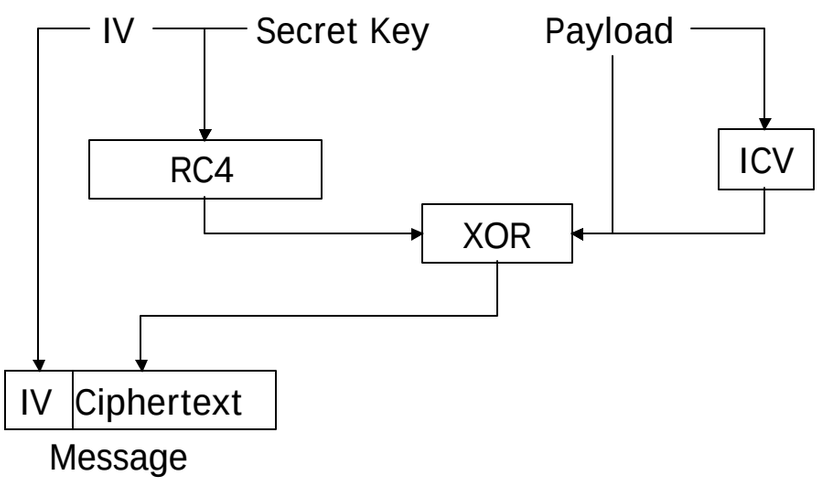


SystemEXPERTS

WEP Encryption Steps

- Integrity Check Value computed
  - Checksum of payload (i.e., plaintext) using CRC32
- Select encryption key
  - One of four keys selected
- Generate IV
- Use RC4 to generate a keystream RC4(IV,Key)
  - Note IV is prepended to key
- Concatenate ICV to payload, then XOR with the generated keystream to get ciphertext
- Send IV+keynumber+ciphertext over the air
  - Key number is the key selected in the second step

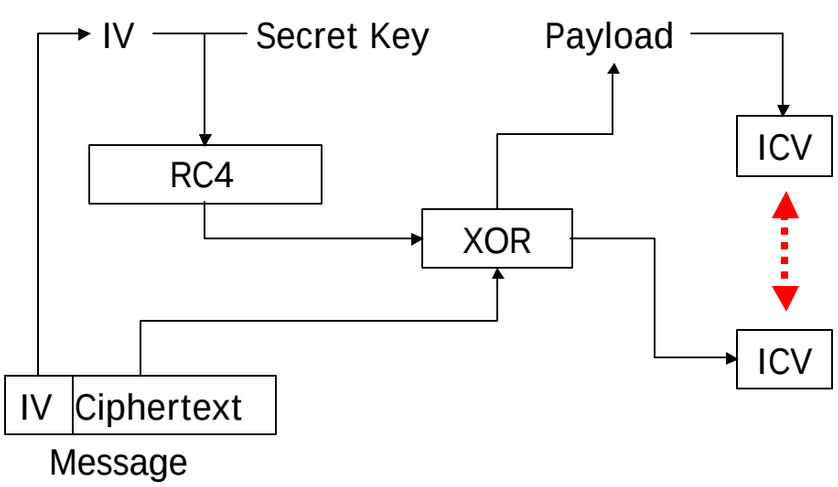
WEP Encryption



WEP Decryption Steps

- Use key number to get private key
- Use sent IV to generate keystream
  - RC4(IV,Key)
- XOR received ciphertext with keystream
  - Get ICV+Payload
- Compute ICV on Payload
- If new ICV == sent ICV, then packet good

WEP Decryption



128-bit Version (WEP2)

- Stronger Key
- Non-standard, but in wide use
- 104-bit key instead of 40-bit in standard WEP

WEP Key Management

- Static keys
- Manually distributed
- Up to four keys
  - Can be mixture of 40/128 bit keys
- Either set as hex data or ASCII
  - ASCII string is converted into key by key generator
    - this limits the key strength to 2^21 because of high ASCII bit and PRNG not being very random
    - to interoperate, they all use the same algorithm
  - Configuration tool usually determines

The Major WEP Problems

- Key Generators
- Keystream Reuse
- RC4 Key Scheduling Algorithm
- Message Authentication

Problem: 40-Bit ASCII Generator

- Folds the ASCII string into a 32-bit number (2^40 now 2^32)
- Use this in a PRNG to generate the 40-bit key, same key every 2^24
- Folding method guarantees only 2^21 unique sets of WEP keys
  - It takes about 35 seconds of time on a 500MHz PIII
- 128-bit Generator
  - Not the same problems
  - Relies on strength of ASCII test and MD5

Problem: Keystream Reuse

- The shared key is static and rarely changed
- Randomness of key stream depends on IV
  - When IV is reused, then you have two messages encrypted with same keystream (a collision)
  - 2^24 possible IV, so repeated after ~16 million packets
  - Most clients reset IV to 0 and increment by 1 for each packet
    - lots of collisions

Problem: Keystream Reuse Attack

- Attacker sends you a known packet (i.e., ping)
  - A bunch of them ☺
- Sees the response: Ciphertext and IV
- Now knows Plaintext and Ciphertext, can get keystream
  - K = P XOR C
    - note: the attacker does *not* know the key, but the keystream
- Makes a database indexed with IV
  - Now for any IV he/she sees in the future, then have the keystream needed to decrypt the packet
  - Major problem because of shared keys

Problem: Key Scheduling Algorithm of RC4

- Documented by Scott Fluhrer, Itsik Mantin and Adi Shamir
  - Paper indicated that an attacker could gain access to an entire WLAN in less than 15 minutes
  - Requires between 1 million and 8 million packets, and does not require significant CPU power
- Main problem is a weakness in the way the RC4 encryption algorithm is implemented in WEP
  - By having a “known” plaintext prepended on the key (I.e., the IV), it leads to weak keys that will generate known ciphertext output from the RC4 engine
  - It allows the attacker to go back and "reverse engineer" the secret key from encrypted packets

Problem: Key Scheduling Algorithm of RC4

- Longer keys won’t help because the attack recovers each key byte individually, rather than attempting to decrypt the key as a whole
- The attack scales linearly -- not exponentially -- as key length increases

Problem: Message Authentication

- The Cyclical Redundancy Check (CRC) chosen for the authentication is weak
  - It is designed for errors, not authentication
- It is possible to modify a message such that the CRC will be valid for the messages, but is not the messages that was sent
- Can also inject messages in much the same manner

Current Status of WEP

- IEEE 802.11 Task Group I (tgi)
- Message Integrity Check (MIC): Doc 594
  - Re-keying
  - Add MIC to data before encrypting
    - Algorithm not yet selected
  - No replay protection (done with IV)
- Temporal Key Hash: Doc 550
  - Temporal key to derive per-packet key
  - Countermeasure to key-scheduling algorithm
- Re-Keying
  - Re-key Proposal: Doc 540
    - Re-key faster than the attacker can attack
  - Authenticated Key Exchange at the MAC Layer: Doc 508
    - A different way ☺

Current Status of WEP (cont)

- Use AES vice RC4
- 802.1X rekey be accepted as normative text
- “WEP2” to be known as “Temporal Key Integrity Protocol (TKIP)”

Current 802.11b Authentication

- Two specified in the standard: Open and Shared
  - Open system authentication: This is the default
    - any client can associate with the access point
      - doesn’t mean the get an IP though
  - Shared key authentication: Uses a shared secret key (i.e., the WEP Key) to authenticate the client to the AP
    - client sends an Authentication frame to the AP
    - AP replies with an Authentication frame containing a 128bit challenge
    - client will send the “encrypted” challenge back
    - AP will decrypt and compare, if it matches, then replies with a “success” authentication

Other 802.11b Authentication Mechanisms

- Closed network (no broadcast SSID)
- Enhanced Security Network (ESN)
  - Many call it 802.1x inappropriately
- Captive Portals
  - NoCat

Current 802.11 Authorization

- MAC Layer
  - Can configure the AP to talk to specific MAC addresses
  - Controls access to wired network not wireless

ESN: The Wireless Security Future?

- Defined in the 802.11 Security Baseline
- Depends on 802.1X
  - Protocol definitions between client and bridge and bridge and authentication server
- Provides
  - Enhanced authentication
  - Key management algorithms
  - Dynamic, association-specific WEP keys
- Open authentication method
  - Looks like many vendors are using RADIUS
- Uses EAP encapsulated in 802.11b Frames
  - EAP is defined in RFC 2284

Wireless EAP: Cisco's Version

- Lightweight EAP (LEAP)
  - EAP Type 17: EAP-Cisco Wireless
  - Based on EAP and IEEE 802.1X
- Provides authentication service for clients whose host OSs do not support EAP
  - LEAP distinguishes between authentication provided by the client firmware from that provided by the host OS
- Backend RADIUS server (Access Control Server 2000 V2.6)
- Uses MS-CHAP as Authentication Protocol

Future 802.11 Security Enhancements

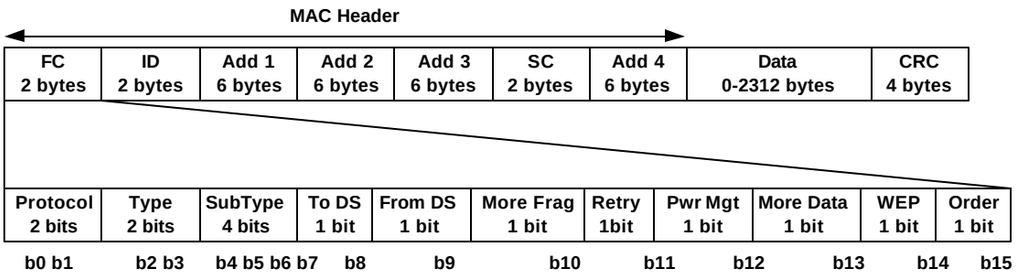
- Standard 128-bit WEP encryption (WEP2)
  - Already implemented by all of the major vendors but has not been standardized yet
- Advanced Encryption Standard (AES) for WEP
- Standard key exchange and distribution
  - EAP & LEAP seem to be the wave of the future
- Improved data integrity via keyed message authentication
  - Better message integrity checking

Observations

- This is relatively new territory, so watch for significant changes
- WEP can be a legitimate tool in the security arsenal
  - View 802.11 networks as an insecure MAC layer, over which you run secure IP protocols
  - Use WEP/EAP/802.1x to protect against casual snoopers, local DoS attacks, and bandwidth theft
  - WEP won't help with stolen equipment and ex-employees
- It appears that ESN/802.1X has more momentum than anything else
  (i.e., Cisco and Lucent support it)

Let's take a look…☺

- 802.11b packets
  - Beacon
  - Probe Request
  - Open Authentication
  - Shared Authentication
  - No WEP
  - WEP



SystemEXPERTS

Notes:

SystemEXPERTS

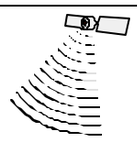
Notes:

SystemEXPERTS

Notes:

SystemEXPERTS

Section Contents

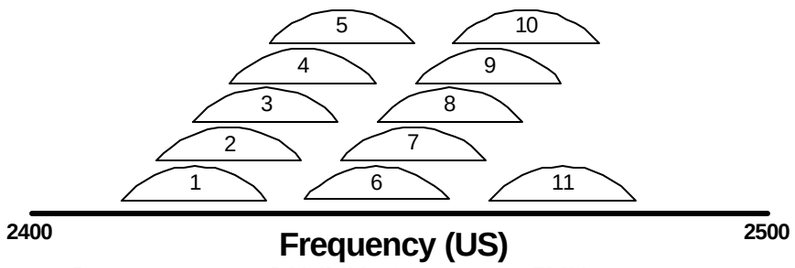


- 802.11
- **Access Points 101**
- Deployment Examples

Access Points 101

- Access Points (AP) broadcast their service (beacon)
  - FCC (US) allows 11 channels for Direct Sequence Spread Spectrum (DSSS)
    - in North America and Europe, they start at 2412 MHz (2.412 GHz)
  - The spread spectrum for DSSS crosses over several channels
    - i.e., channel bandwidth is 22MHz (25MHz is required to minimize interference) , yet they are spaced at 5MHz

Frequency Overlap

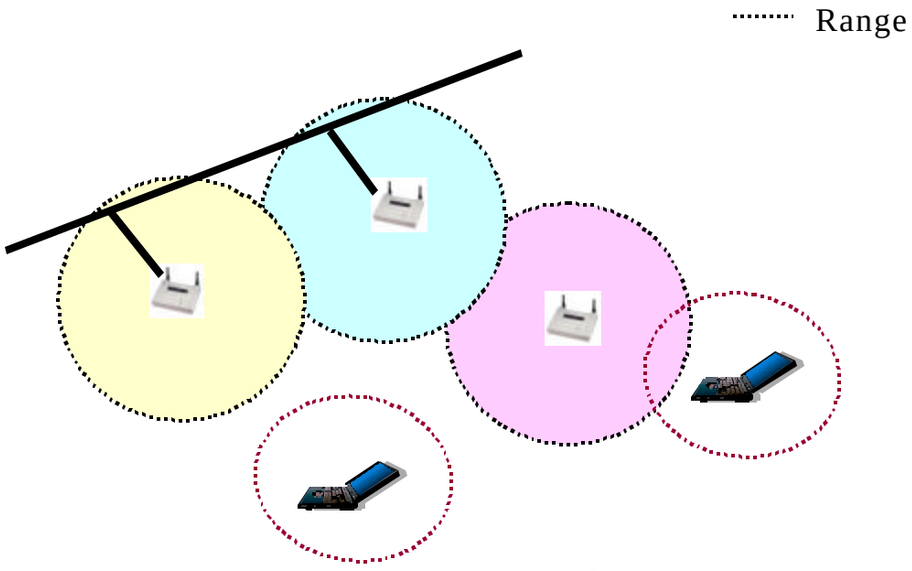


Channels start at 2414MHz, increase by 5MHz, and have about a 20MHz range up to 2483.5MHz

Access Point Usage

- Number of clients supported depends on device “memory” size, aggregation, congestion, noise, quality, etc., etc., etc.
  - As we’ll see later, the Apple Airport AP (e.g.) has enough slots to cover about a dozen clients and the Cisco Aironet 340 series, up to 2,048 slots
- Typically connects wireless and wired networks
  - If not wired, then it is an Extension Point (EP), i.e., a wireless bridge

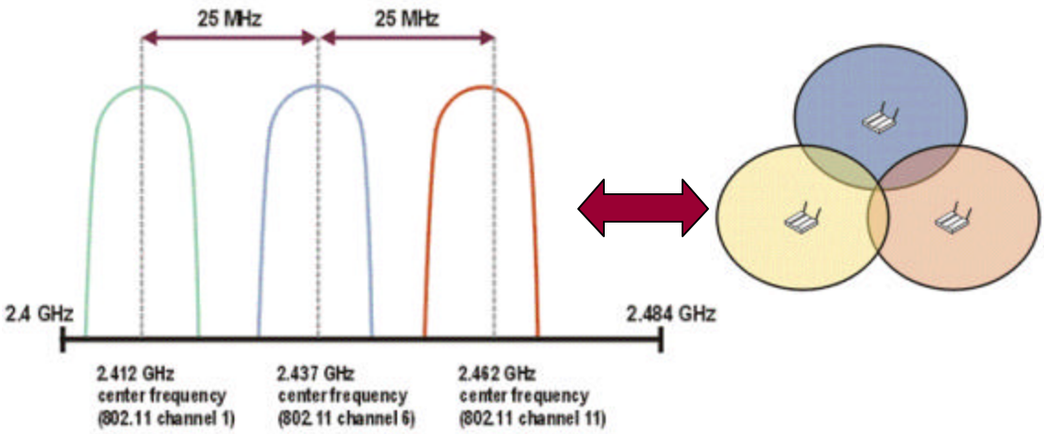
Extension Point



Access Point Placement

- Roaming can be achieved by having slightly overlapping APs on different channels
  - …more on roaming in just a bit
- 2.4Ghz contains 80MHz of spectrum
  - 25MHz to minimize interference
- Only 3 equivalent-width non-overlapping DSSS channels

Placement (cont.)

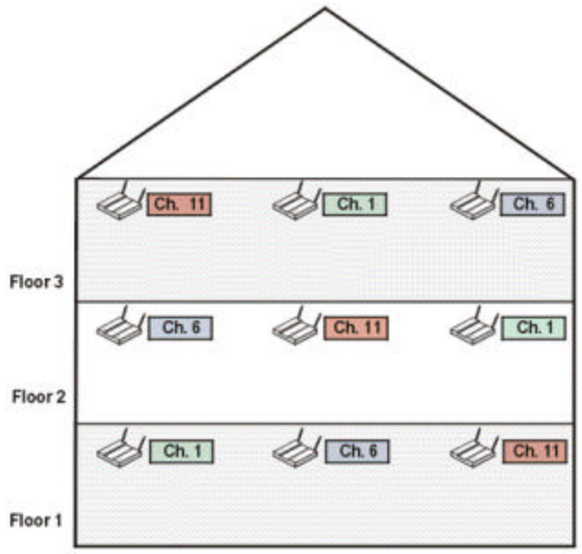


Source: *The IEEE 802.11 Handbook: A Designer's Companion*

Placement (cont.)

- Developing configurations to maximize roaming and minimize interference is hard
  - Remember it's 3 dimensional broadcasts
  - Remember it goes through walls!
    - out to the street, to your neighbor, to your competitor!

Placement, 3 Dimensional



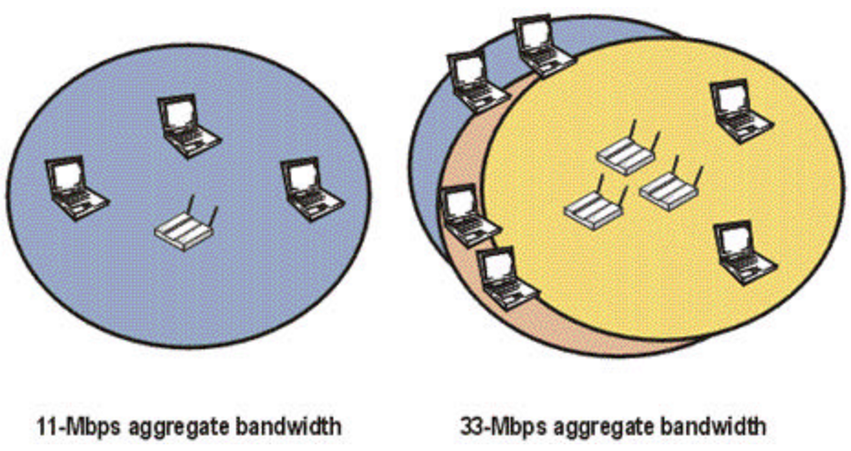
Capacity and Bandwidth

- Maximum of 11Mbps
  - Not really: since the Physical Layer Convergence Protocol (PLCP) layer is always transmitted at 1Mpbs, 802.11b is only 85% efficient as the physical layer
- Goes down because of
  - Distance, barriers, collisions, interference, congestion, capacity usage

Capacity and Bandwidth (cont.)

- Stays “higher” because of
  - Reducing size of coverage areas
  - Reducing client-to-AP ratio
  - Using aggregation
    - increasing AP-to-client ratio and using load balancing

Bandwidth Aggregation



Anatomy of 802.11b

- Looking at some of the guts of the protocol to help us understand:
  - Modulation determines speed/distance
  - What effects the transmission rate
    - other than distance or barriers
  - Congestion resolution
  - Hidden nodes
- The MAC layer is our friend!

Anatomy of 802.11b: the bits

- As we said before, data is encoded using DSSS
  - i.e., The data stream is modulated (XOR'd) with a sequence called the Barker code (11 bits: 10110111000 – it's just a really good pattern for generating radio waves) to generate a series of data objects called chips
  - These chips are then sent out by the wireless radio (i.e., the wireless card)

Anatomy of 802.11b: the wave

- …then the wireless radio generates a 2.4 GHz wave and modulates it…
  - 1Mbps is done using Binary Phase Shift Keying
  - 2Mbps uses Quadrature Phase Shift Keying (QPSK)
  - 5.5 & 11Mbps use Complementary Sequences (vs. Barker code) then uses QPSK
- …so all of these yield a 22 MHz frequency spectrum
  - Hence, the reason only 3 channels fit without overlap because there is this ~25MHz range
  - Hence, all management packets are sent via BPSK: to ensure they "get there" (they go the furthest!)

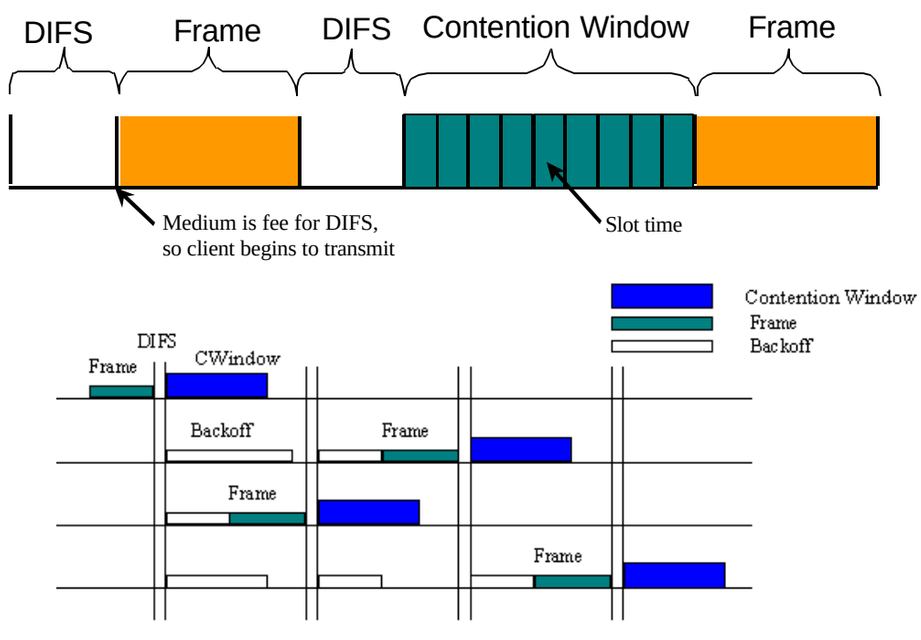
Anatomy of 802.11b: congestion

- Everybody is "broadcasting" this stuff out, where is the traffic cop?
  - MAC layer "waits" for a quiet time: it's been idle for the Inter-Frame Spacing period
    - if it's still busy, wait for this spacing period plus a random number of slot times, and try again
    - so each station is keeping track of it's allocated number of slot times (i.e., **they trust each other**)
      - think about TearDrop and Land DoS

Congestion (cont.)

- Each station listens to the network
- 1st station to finish it's allocated slot times sends data
- If another station "hears" another station talk, it stops counting down its back-off timer
- In addition to the MAC back-off, 802.11 adds another back-off to ensure fairness
- When in this "contention window" it uses these back-off timers

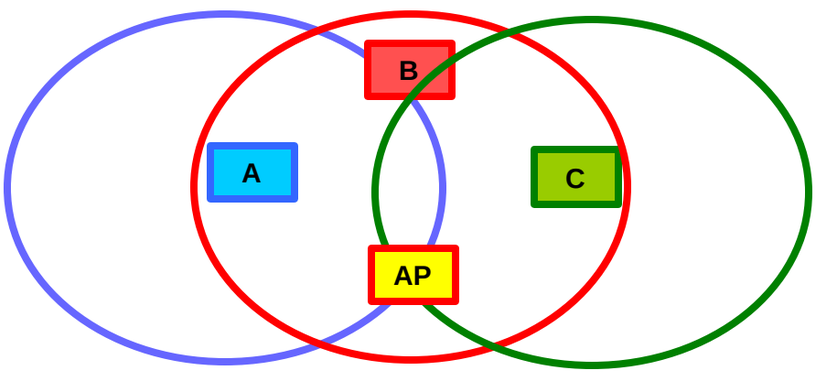
Congestion (cont.)



Anatomy of 802.11b: Hidden Node Problem

- AP P sees A, B, and C, but A and C can't see each other (see means, the packets don't reach)
  - Optional feature of RTS/CTS added to 802.11b
  - RTS packet includes target address
    - A sends: "This is for B" (C doesn't see this)
  - CTS includes sender address
    - B sends: "Please send A" (C DOES see this)
- This feature is significant overhead but a very common condition that needs to be accounted for

Hidden Node Problem



"Hidden node": STA 3 Out of range STA 1, in range STA 2

Hidden Node Problem: Let's try it again

- 802.11
  - basically designed for indoor, relatively short distances, active and long-lived connected clients, and low noise level
  - but 802.11 ("wi-fi") is "winning" in the wireless arena and being increasingly used as well in outdoor, long distant, occasionally connected, potentially high noise level environments
- So what does that mean to hidden nodes?
  - The key is the need to minimize the amount of overhead you introduce to manage them

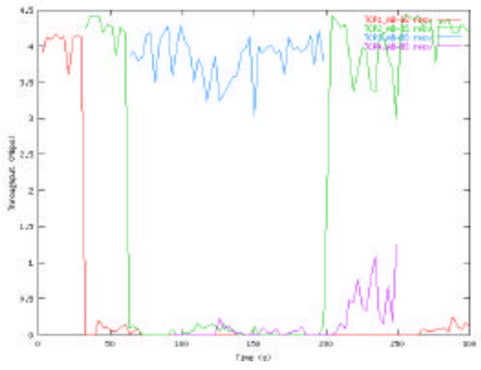
Finding those Hidden Nodes

- Carrier Sense Multiple Access (CSMA)/ Collision Avoidance (CA)
  - CSMA – the device listens to the media before transmitting
  - Request To Send (RTS)/ Clear To Send (CTS) – media reservation mechanism
- Polling – adaptive mechanism
  - Device can not start transmission before receiving a special acknowledgement packet (a marker) from the AP
  - Defend against "sudden" chaos

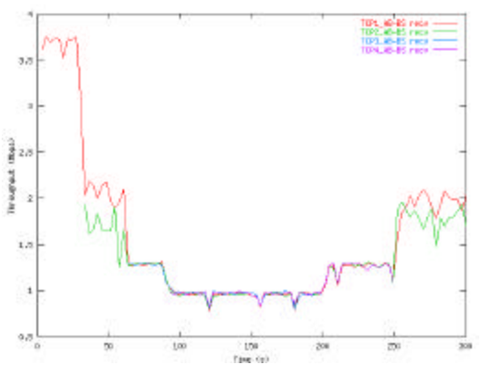
Surprising Results

What does this mean?
In certain circumstances, the method used makes a HUGE difference!

with RTS/CTS



Polling



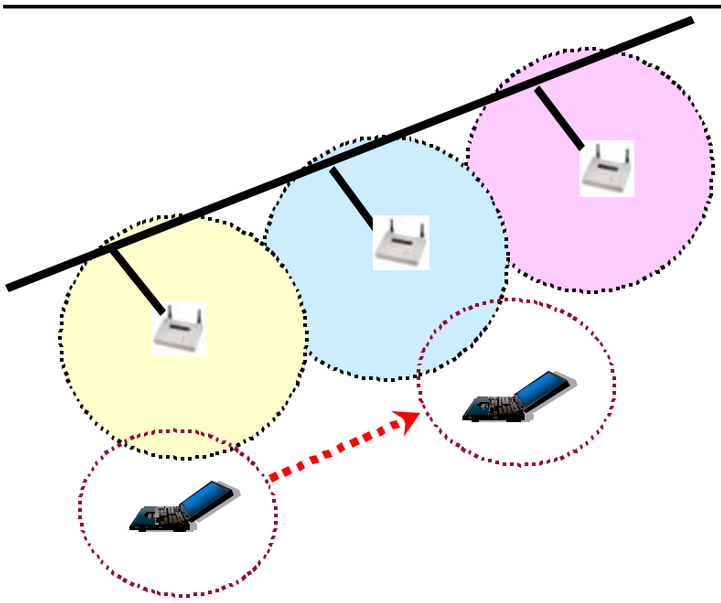
What Does This Mean?

- Media reservation systems (e.g., RTS/CTS) work “better” in stable environments with expectations of full/long-lived connectivity
  - e.g., in your office building, point-to-point connections, small number of nodes
- Adaptive systems (e.g., polling) work “better” in other environments
  - e.g., city (or larger) wide environments
  - Remember you’ll tend to have lower speed but much more predictable and controllable

Anatomy of 802.11b: Roaming

- More than 1 AP providing signals to a single client
  - The client is responsible for choosing the best AP
    - signal strength (#1) and network utilization (#2)
  - When existing signal degrades (to poor), it tries to find another AP
    - either passively listening or actively probing the other channels and getting a response
    - once it finds one, it tries to authenticate and associate

Roaming (cont.)



Wireless Extension Point

Important Concepts: Strength vs. Quality

- Received Signal Strength
  - Signal energy at the location of the station
    - (i.e., the power level)
- Received Signal Quality
  - Ability to coherently interpret the signal
    - (i.e., the usability level)

Roaming Activities

- IAPP or Inter Access Point Protocol is intended to standardize roaming features and protocol
  - Started by Aironet (Cisco), Digital Ocean, and Lucent
  - 802.11f is the proposed extension to 802.11
- Wireless Ethernet Compatibility Alliance (WECA) as part of the Wireless ISP Roaming Initiative has published a roadmap
  - Cisco, IBM, Intel, 3Com, and Microsoft
  - “Technical Outline for Wi-Fi Inter-Network Roaming Framework”

IEEE IAPP

- Accomplishes roaming within a subnet
  - Basically, within a corporate wireless LAN
- 2 transfer protocols
  - 1 for single logical LANs
  - 1 for crossing router boundaries
- Crossing subnets is a vendor specific solution
  - It requires mobile IP software on every client
  - Cisco, e.g., is expected to release Mobile IP

Wi-Fi Inter-Network Roaming Framework

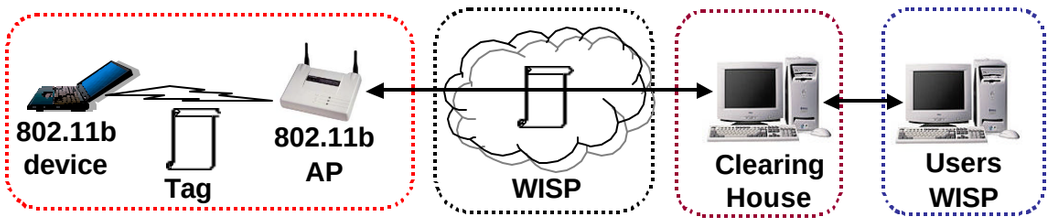
- Assumptions
  - Inter-service roaming
  - All components are Wi-Fi certified
  - No client footprint other than browser
  - RADIUS is the protocol for authentication, authorization, and accounting data
  - Pagers, cell-phones, WAP-phones, and PDAs will be addressed “later”

Wi-FI Roaming (cont.)

- 802.11b
  - Boot up with correct SSID for Wi-Fi network
  - Local WISP login screen
    - which details charges
    - separate window tracks session information
- 802.1x
  - Boot up
  - Prompted with username/password for local WISP
- Windows XP is only 1x implementation available today

WISPr

WECA is looking to form a set of relationships and network standards between wireless ISP's that will eventually enable Wireless 802.11b roaming between them.



Wireless user connects. A unique tag identifies users home WISP account

Roam WISP passes this "Tag" & request for service to a clearing house

Clearing house passes info to users WISP

WISP authenticates user and authorizes access. Then bills user and pays roaming WISP

Configuring an Access Point

- How to manage it
  - HTTP, Telnet, SNMP or Serial Interface
- Security Settings
  - SSID, WEP, & EAP
  - RADIUS servers and shared key
  - MAC layer Filters
- Making it work easily with clients
  - DHCP

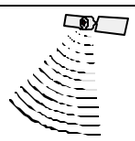
Access Point Medicine

- Enable WEP
- Change SSID
  - And not just a little
- Disable broadcast
  - Otherwise, your SSID is there to see
- Change the password on your AP
- Periodically survey your own site
- Use MAC address filtering
- Reconsider using DHCP
- Consider using fixed IP addresses for your wireless NICs
- Look into other mechanisms (SSL, VPN) for privacy & confidentiality

Notes:

Notes:

Section Contents



- 802.11
- Access Points 101
- **Deployment Examples**

SystemEXPERTS

Wireless at Home

- Goals
  - Extend network capabilities without physical alterations and costs – other than wireless
  - Share existing resources without specialized or unique (weird) configuration setup
  - Allow visitors easy access to the home network resources (e.g., ISDN, printers)
  - Feel comfortable about the security of the additional wireless services

SystemEXPERTS

Wireless at a Conference

- Goals
  - Reduce time to setup fully functional temporary network resources
  - Scale down terminal room requirements
  - Reduce effort and cost to provide Internet access to tutorial instructors and their students
  - Allow attendees ubiquitous access to the Internet within a reasonable distance to the conference center

Industry Setup: Ariba

- Goals
  - Increase efficiency of people in meetings
  - Readily available communications: Instant Messenger
  - 802.11b support
    - wanted the speed that this standard brings to the table
  - Standard design
  - Speed and Range
    - designers had experience with other wireless networks
  - Cost
- Only deployed at headquarters
  - It has met expectations

CyberCafe

- Typically an Open AP
- Use a captive portal to allow access
- Costly
- Starbucks is one of the first
  - Use MobileStar as their ISP
  - Seem to use a combo of special SSID and captive portal
- Watch for Neighborhood Area Networks

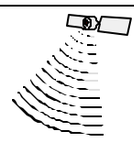
Architectural Considerations

- Need to have a defined goal
- Segregate the wireless infrastructure
  - Isolated sub-network/DMZ
- Use appropriate data protection mechanisms
  - VPNs
  - SSL
  - SSH
  - etc.
- WEP is good for
  - Protecting against casual snoopers and bandwidth theft

Notes:

Notes:

Where are We?



- From 50,000' to 5'
- Handheld Practicals
- LAN Practicals
- ***NIX and Wireless**
- Currents
- Antennas

Linux Wireless RF Sniffer

- Most of the existing sniffer renditions use cards based on the prism II chipset from Intersil
  - With either prismdump or patched Libpcap
  - …and Ethereal
- AirSnort and WEPCrack both use these
- Some more popular Prism II cards include the following:
  - D-Link DWL-650
  - Linksys WPC11
  - SMC 2632W
  - Zoom Telephonics ZoomAir 4100

Linux Sniffer: How-To

Directions at Tim Newsham's site
http://www.lava.net/~newsham/wlan

- Get an SMC2632W wireless card
- Get a wlan-ng driver with RF monitoring code
  - Get linux-wlan-ng-0.1.8-pre13 and apply wlan-monitor.patch
  - Or linux-wlan-ng-0.1.6.tar.gz
- Get ethereal-0.8.17
  - Apply patches from wlan-mods.tgz
- Get Libpcap-0.6.2 or Prismdump
  - Apply LibPcap patches from wlan-mods.tgz

How-To (cont.)

- Compile them up and install them
- Start the monitor
  - wlanctl-ng wlan0 lnxreq_wlansniff channel=<pickone> enable=true

Sniffer Observations

- It works! Its Linux! Its free!
- Only one channel at a time ☹
  - You can write a script to change that ☺
- You have to type “prism” as the interface for ethereal if you use LibPcap

AirSnort

- Need wlan-ng and Newsham’s patches
- You run prismdump to capture packets to a file …
- Run AirSnort on that file (real-time) to attempt cracking
- So after starting the monitor mode …
  - prismdump > WEPCapture
  - capture –c WEPCapture
    - "Interesting Packets”: ~1500 for 104-bit and 575 for 40-bit
  - crack (at intervals)
- airsnort.sourceforge.net
  (also wepcrack.sourceforge.net)

Home Spun Access Point

- What is it
  - A system that gateways between the wireless and wired networks
    - a.k.a. Wireless Gateway
  - Implements IBSS (Ad-hoc) or BSS modes
  - Typically provides DHCP and firewall/NAT services
  - May provide authentication and authorization
  - Usually some flavor of Unix (Linux or FreeBSD)
- What does it entail
  - Get the equipment
  - Install the software
  - Tweak a bit

Building your own AP

Condensed from http://www.oreillynet.com/pub/a/wireless/2001/03/06/recipe.html

- Equipment
  - PC, wireless card, ISA-to-PCMCIA adapter, and a NIC
- Operating System: Unix-like
  - Clients can be anything that can do Ad-Hoc
- Install the PCMCIA adapter in the gateway and insert the wireless card
- Build and install the new kernel
  - Don't forget to edit /etc/lilo.conf and then run /sbin/lilo
- Install the pcmcia-cs package
- Configure wireless and NIC IP options
- Install and configure DHCP (if desired)

Directions (cont.)

- Harden the rest of the system (read: TURN OFF ALL UNUSED SERVICES)
  - Keep the PCMCIA, firewall, and DHCP services running
- Reboot and see what you broke ☺
  - Probably should reboot before the firewall and DHCP install/configure
- Setup clients

My Problems

- Trouble getting DHCP working correctly on the wireless net
- Setting up firewall rules
  - Getting ipchains to actually pass traffic through double NAT
    - wireless gateway and my firewall
    - could do HTTP but not SMB
- Links would drop every so often
- It worked, but not painlessly using 2.2.x
  - Once I went to 2.4.x and iptables it worked for me
    - no DHCP though ☹

My Observations

- Functionality is limited in some instances
  - IBSS only
    - WLAN-NG supposedly supports BSS, I never got it to work
- Functionality is enhanced in others
  - Firewall and potential authentication/authorization hub
- If education and experience is what you want, then this is the way to go
- If a up and running or many-client is what you want, then buy an AP
  - Especially for people with limited time and/or experience

Wireless Firewall Gateway (WFG) by NASA

- Design Objectives
  - A method to authenticate/identify a user
  - Simplicity
- What it does
  - Acts as a router between a wireless and external network with the ability to dynamically change firewall filters as users authenticate
  - Acts as a DHCP server,hosts the user authentication site, and maintains accounting records
- Purpose
  - To keep the wireless network as user-friendly as possible while maintaining some level of security for everyone

OpenAP

- OpenAP
  http://opensource.instant802.com/
  - Open-source software
  - Fully 802.11b compliant wireless access point
- Has the ability to:
  - Do multipoint to multipoint wireless bridging, while simultaneously serving 802.11b stations (i.e. and AP)
- Runs on Eumitcom WL11000SA-N board based AP's
  - US Robotics (USR 2450) (tested)
  - SMC 2652W EZconnect Wireless AP (tested)
- Why use it?
  - You have the source
  - It is customizable
  - It can do anything that Linux can do

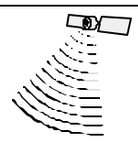
How Does it Work?

- The basic recipe is this:
  - Get the hardware
  - Create a programming image
  - Write the image to a PCMCIA SRAM card
  - Open the access point and insert the SRAM card in place of the 802.11 PCMCIA card
  - Power on the AP
  - Short a jumper to boot from the SRAM card and reprogram the onboard flash
    - Watch what happens on the serial port
  - Replace the 802.11 card
  - You are done
- Now it can be upgraded over the network

Notes:

Notes:

Where are We?



- From 50,000' to 5'
- Handheld Practicals
- LAN Practicals
- *NIX and Wireless
- **Currents**
- Antennas

IEEE 802.11a

- Next generation High speed WLAN
  - Speeds 6, 9,12,18, 24, 36, 48, & 54 Mbps
- Uses 5 GHz Unlicensed National Information Infrastructure (U-NII) band
  - U-NII devices will provide short-range, fixed, point-to-point, high-speed wireless digital communications on an unlicensed basis
- Uses Orthogonal Frequency Division Multiplexing (OFDM)
- Different chip set than 802.11b, so no upgrades
  - Can co-exist, as they are on different spectrums

802.11a Spectrum

Band	USA/ Canada	Europe	France	Spain	Japan
5.150-5.250	50mW	200mW	200mW	200mW	200mW
5.250-5.350	250mW	200mW	200mW	200mW	
5.725-5.825	1W				

- 3 primary non-contiguous bands
  - 100MHz each band with power restrictions
    - split into 20MHz channels
  - 5.15-5.25 GHz: Indoor, short-range
  - 5.25-5.35 GHz: Indoor or outdoor, medium range(campus-type networks)
  - 5.725-5.825 GHz: Outdoor, long-range (several km)

802.11a Spectrum (cont.)

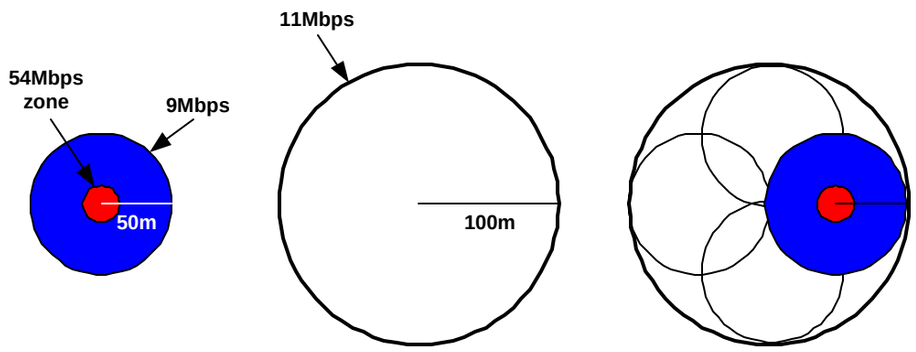
- 12 non-overlapping simultaneously operating networks
- 4 channels in each band
- OFDM the splits each channel into 52 sub-channels

802.11a Coverage

Tech	Data Rate	Throughput	Range and Data	Shared
802.11b	11Mbps	5-7Mbps	100m @ 11Mbps	Yes
802.11g	24Mbps	10-11Mbps	100m @ 12Mbps	Yes
802.11a	54Mbps	31Mbps	50m @ 9Mbps	Yes
			30-40m @ 9-12Mbps	Yes
			10-15m @ 36-54Mbps	Yes

- 802.11a signals lose strength more quickly
  - Higher frequencies lose power more quickly
- Limited coverage areas
  - About ¼ of WiFi for similar data rates and environments
  - Need to increase (4x) AP density or power to compensate

802.11a Coverage Graphic



802.11a **802.11b**

This is using similar throughput and transmit powers

802.11a Problems

- Use of 5 GHz band will cause contention in different parts of the world
  - Remember the problems with spectrums in handhelds
- Coverage will cost
  - Number of APs
  - Power (i.e., battery life)

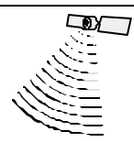
802.11 Thoughts

- Usage
  - Use 802.11a for dense populations and high speeds
  - Use 802.11b/g for greater coverage
- Coexistence
  - Likely to be working together for many years to come
- Price
  - 802.11b/g will have the price advantage for a while

Notes:

Notes:

Where are We?



- From 50,000' to 5'
- Handheld Practicals
- LAN Practicals
- *NIX and Wireless
- Currents
- **Antennas**

Antennas: The Skinny

- 2.4 GHz ISM Band
  - You don't need a license to operate a transmitter…
  - …But you MUST be prepared to accept interference from other other users/devices
- Good antenna deployment…
  - May be one of the best security measures you can implement
    - reduce stray RF signals
    - less susceptible to interference
    - better control who can have access to the AP RF

Antennas: Basics

- A radiation pattern is a diagram that allows us to visualize in what directions the energy will radiate from an antenna
  - If an antenna radiates in all directions equally we say it is an “isotropic radiator”
  - The radiation pattern is split into two perpendicular planes called Azimuth and Elevation
  - When RF energy is concentrated, it means the antenna has “gain” over a portion of the radiator
    - gain is measured in decibels and written dBi

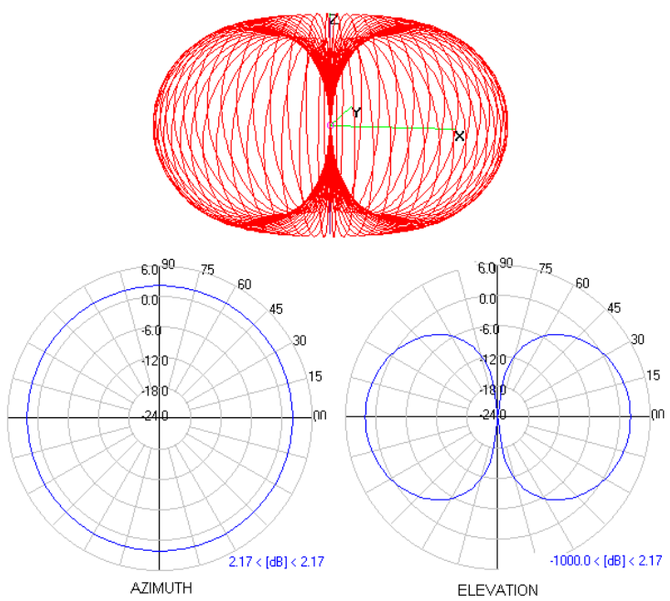
Antennas: Basics (cont.)

- Gaining coverage is achieved thru gain, which again, is measured in decibels dB
- Calculation range
  - Indoors, each 1 dB increase in gain results in a range increase of 2.5%: outdoors it’s 5%
- Positioning
  - Normally should be mounted as high and as clear as obstructions as possible
  - Best performance is when the transmitting and receiving antenna are at the same height and in direct line of site

Antennas: Dipole

- Most common antenna and the default type on most APs
  - Usually a 1-inch radiating element
  - Note: the higher the frequency, the smaller the antenna and the wavelength become
- Radiation pattern
  - “Donut” like
  - Radiates in equally in all directions around its axis but NOT along the length of the wire
    - also called omnidirectional

Dipole Radiation

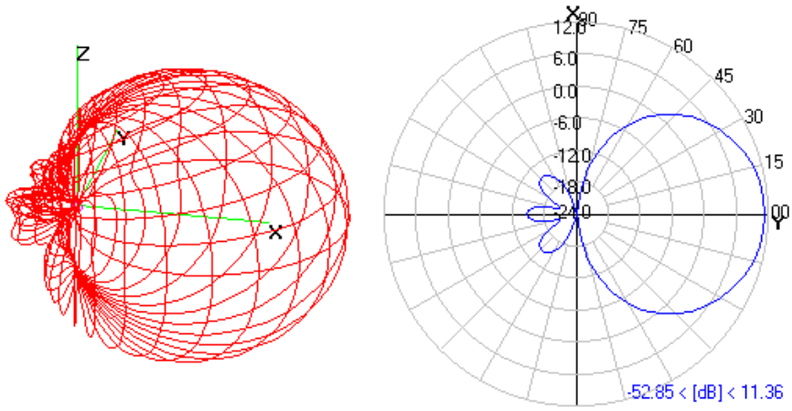


Antennas: Directional

- Directional antenna concentrate their energy into a cone
  - Known as a beam
- Radiation pattern
  - It depends on what kind of directional antenna you have

SystemEXPERTS

Directional Radiation: Biquad



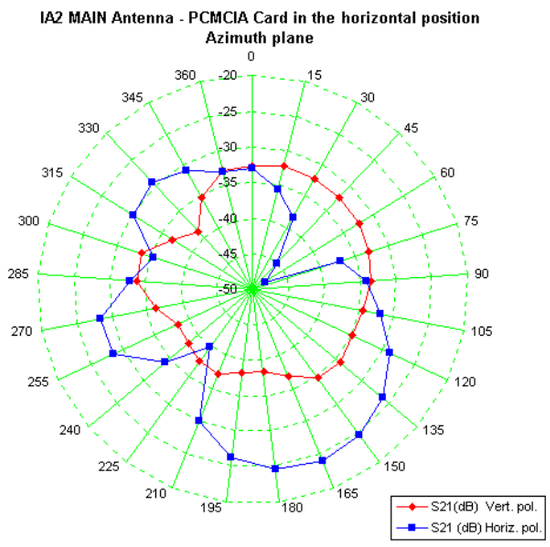
SystemEXPERTS

Antennas: PCMCIA Cards

- Their terrible, awful, did I mention yuck?
  - It's hard to form antennas onto the card
  - The effective gain is low
  - They tend to be VERY directional
- These are some of the reasons that your signal strength can change dramatically with small changes

SystemEXPERTS

Typical PCMCIA Radiation



SystemEXPERTS

Antennas: More Facts

- Constant trade-off of range and throughput
  - Remember that the “low” speed of 1 Mbps is slightly slower than a T1 connection (1.544 Mbps)
  - Remember that the top speed of 11 Mbps is only over the air: the Ethernet it’s connected to is 10 Mbps and then you have contention, etc.
  - Current client cards have only 1 radio in them
    - that means half-duplex (they can’t listen and talk at the same time)

Antennas: More Facts (cont.)

- The design of most external cards (PCMICIA) puts the antenna in the worst possible orientation: sideways
  - Tip your laptop sideways and you’ll see
  - The Apple built-in AirPort is an exception
    - the antenna connector runs up the LCD panel
- Attaching external antennas (and orienting it) makes a really big difference
  - Therefore, buy cards that take an external antenna

Notes:

Notes:

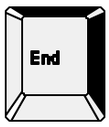
Review

- Why is it basically impossible to get full 2, 5.5, or 11 Mbps?
- What's the common management interface to ALL APs?
- What's the difference between AP aggregation and AP DoS?
- What are the security implications of broadcast SSID?
- What is the problem with MAC based ACL security?

Review

- What are the security implications of shared keys?
- How easy/difficult it is to exploit WEP vulnerabilities?
  - Name one!
- What is the Gap in WAP?
- What are the roaming limitations with using a home spun AP?
- What is the ratio of 802.11a to 802.11b APs for constant power and throughput?

The End



- Thank you for attending!
- Thank you for your comments!
- **Please fill out the Instructor Evaluation Form!!**
- www.SystemExperts.com/tutors/wirelessip.pdf

Thanks to …

- David Lounsbury
  - Vice President of Research for The Open Group
- Lynda McGinley
  - University of Colorado
  - Coordinator or USENIX wireless services
- Richard Rothschild
  - Director Ariba Network Operations for Ariba

References

- Access Points
  - www.cisco.com/warp/public/cc/pd/witc/ao340ap/
  - www.apple.com/airport/specs.html
  - www.wavelan.com/template.html?section=m58&page=103&envelope=94
  - www.3com.com/products/proddatasheet/datasheet/3CRWE74796B.pdf
- Cell Phone Internet Services
  - www.sprintpcs.com/wireless
  - www.verizonwireless.com
  - www.attws.com/personal/explore/pocketnet
  - www.nextel.com/phone_services/wirelessweb

References (cont.)

- Security
  - www.datafellows.com/products/white-papers/sec_wap_env.pdf
  - www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html
- Sniffing
  - www.sniffer.com/products/wireless/
  - www.robertgraham.com/pubs/sniffing-faq.html
  - www.wildpackets.com/products/airopeek

References (cont.)

- Reference material
  - www.cmu.edu/computing/wireless/index.html
  - www.teleport.com/~samc/psuwireless/
  - www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.drivers.html
  - www.proxim.com/wireless/glossary/index.shtml
  - www.motorola.com/SPS/WIRELESS/information/glossary.html
  - www.wireless-online.com/glossary.htm
  - www.zdnet.com/pcmag/stories/reviews/0,6755,2603595,00.html
  - http://allnetdevices.com/faq/
  - www.wapforum.org/
  - www.ntia.doc.gov/osmhome/allochrt.html (Frequency Map)

References (cont.)

- Seminal 802.11 Security Press
  - The Isaac project at UC Berkeley
    - Integrity checking mechanism, and Use of Initialization Vector (IV) in RC4 algorithm
    - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
  - Wireless Ethernet Compatibility Alliance (WECA) response to the UC Berkeley paper
    - http://www.wi-fi.net/pdf/Wi-FiWEPSecurity.pdf
  - University of Maryland paper “Your 802.11 Wireless Network has No Clothes”
    - Shared Key to derive WEP key, MAC authentication
    - http://www.cs.umd.edu/~waa/wireless.pdf
    - RC4 Key Scheduling
      - http://www.crypto.com/papers/others/rc4_ksaproc.ps
      - Using the Fluhrer, Mantin, and Shamir Attack to Break WEP

Wireless Stuff

- Wireless performance article
  - www.networkcomputing.com/1113/1113f2full.html
- IEEE 802.11 page
  - www.ieee802.org/11/
- 802.11b Primer
  - www.personaltelco.net/download/802.11b-primer.pdf

Mailing Lists

- Bay Area Wireless Users Group
  - http://lists.bawug.org/mailman/listinfo/wireless/

  NOTE: This is THE list to watch!
- Aironet
  - http://csl.cse.ucsc.edu/mailman/listinfo/aironet
- O'Reilly
  - http://oreilly.wirelessdevnet.com/

Glossary

3G (third generation) An industry term used to describe the next, still-to-come generation of wireless applications. It represents a move from circuit-switched communications (where a device user has to dial in to a network) to broadband, high-speed, packet-based wireless networks (which are always "on"). The first generation of wireless communications relied on analog technology, followed by digital wireless communications. The third generation expands the digital premise by bringing high-speed connections and increasing reliability.

802.11 A family of wireless specifications developed by a working group of The Institute of Electrical and Electronics Engineers. These specifications are used to manage packet traffic over a network and ensure that packets do not collide—which could result in loss of data—while traveling from their point of origin to their destination (that is, from device to device).

AMPS (advanced mobile phone service) A term used for analog technologies, the first generation of wireless technologies.

Analog Radio signals that are converted into a format that allows them to carry data. While cellular phones and other wireless devices still use analog in geographic areas where there is little or no coverage by digital networks, analog will eventually give way to faster digital networks, analysts say.

AP (Access Point) A base station in a wireless LAN. Access points are typically standalone devices that plug into an Ethernet hub or server. Like a cellular phone system, users can roam around with their mobile devices and be handed off from one access point to the other.

BlackBerry Two-way wireless device, made by Waterloo, Ontario-based Research in Motion, that allows users to check e-mail and voice mail (translated into text), as well as page other users via a wireless network service. Also known as a RIM device, it has a miniature qwerty keyboard for users to type their messages. It uses the SMS protocol. BlackBerry users must subscribe to a wireless service that allows for data transmission.

Bluetooth A short-range wireless specification that allows for radio connections between devices within a 30-foot range of each other.

CDMA (code division multiple access) U.S. wireless carriers, such as Sprint PCS and Verizon, use CDMA to allocate bandwidth for users of digital wireless devices. CDMA distinguishes between multiple transmissions carried simultaneously on a single wireless signal. It carries the transmissions on that signal, freeing network room for the wireless carrier and providing interference-free calls for the user. Several versions of the standard are still under development. CDMA promises to open up network capacity for wireless carriers and improve the quality of wireless messages and users' access to the wireless airwaves. It's an alternative to GSM, which is popular in Europe and Asia.

Glossary (cont.)

CDPD (cellular digital packet data) Telecommunications companies can use CDPD to transfer data on unused cellular networks to users. If one section, or "cell," of the network is overtaxed, CDPD automatically allows for the reallocation of resources.

COFDM (Coded Orthogonal Frequency Division Multiplexing) The same as OFDM except that forward error correction is applied to the signal before transmission. This is to overcome errors in the transmission due to lost carriers from frequency selective fading, channel noise and other propagation effects. For the discussion of terms OFDM and COFDM are used interchangeably

Cellular Technology that sends analog or digital transmissions from transmitters that have areas of coverage called cells. As a user of a cellular phone moves between transmitters from one cell to another, the user's call travels from transmitter to transmitter uninterrupted.

Circuit switched Used by wireless carriers, this method lets a user connect to a network or the Internet by dialing in, such as with a traditional phone line. It's a dial-in Internet service provider for wireless device users. Circuit-switched connections can be slow and unreliable compared with packet-switched networks, but for now circuit-switched networks are the primary method of Internet and network access for wireless users in the United States.

Dual-band mobile phone Phones that support both analog and digital technologies by picking up analog signals when digital signals fade. Most mobile phones are not dual-band.

Extensible Authentication Protocol (EAP) An extension to PPP, that provides a standard support mechanism for authentication schemes such as token cards, Kerberos, Public Key, and S/Key.

EDGE (enhanced data GSM environment) A faster version of the GSM standard. It is faster than GSM because it can carry messages using broadband networks that employ more bandwidth than standard GSM networks.

FDMA (frequency division multiple access) An analog standard that lets multiple users access a group of radio frequency bands and eliminates interference of message traffic.

Frequency hopping spread spectrum A method by which a carrier spreads out packets of information (voice or data) over different frequencies. For example, a phone call is carried on several different frequencies so that when one frequency is lost another picks up the call without breaking the connection.

GPS (Global Positioning System) A series of 24 geo-synchronous satellites that continually transmit their position. GPS is used in personal tracking, navigation, and automatic vehicle location technologies.

Glossary (cont.)

GPRS (general packet radio service) A technology that sends packets of data across a wireless network at speeds of up to 114Kbps. It is a step up from the circuit-switched method; wireless users do not have to dial in to networks to download information. With GPRS, wireless devices are always on—they can receive and send information without dial-ins. GPRS is designed to work with GSM.

GSM (global system for mobile communications) A standard for how data is coded and transferred through the wireless spectrum. The European wireless standard also used in Asia, GSM is an alternative to CDMA. GSM digitizes and compresses data and sends it down a channel with two other streams of user data. The standard is based on time division multiple access.

HDML (handheld device markup language) It uses hypertext transfer protocol (HTTP, the underlying protocol for the Web) to allow for the display of text versions of webpages on wireless devices. Unlike wireless markup language, HDML is not based on XML. HDML also does not allow developers to use scripts, while WML employs its own version of JavaScript. Phone.com, now part of Openwave Systems, developed HDML and offers it free of charge. Website developers using HDML must recode their webpages in this language to tailor them for the smaller screens of handhelds.

iDEN (Integrated Digital Enhanced Network) A Motorola-enhanced mobile radio network technology that integrates two-way radio, telephone, text messaging, and data transmission into a single network.

I-Mode A wildly popular service in Japan for transferring packet-based data to handheld devices. I-Mode is based on a compact version of HTML and does not use WAP, setting it apart from other widely used transmission method.

Industrial, Scientific, and Medical (ISM) An unlicensed Radio Frequency spectrum used primarily for industrial, scientific, medical, domestic or similar purposes, excluding applications in the field of telecommunications These bands support spread spectrum operation on a non-interference unlicensed basis. Operation in this band is authorized under FCC Rule Part 15.247. Spread spectrum systems share these bands on a non-interference basis with systems supporting critical government requirements, secondary only to ISM equipment operated under the provisions of Part 18. Many of these government systems are airborne radiolocation systems that emit a high ERP, which can cause interference to other users.

Multipath Effect The effect that occurs when a transmitted signal is reflected from objects resulting in multiple copies of a given transmission arriving at the receiver at different moments in time. Thus the receiver receives multiple copies of the same signal with many different signal strengths or powers.

OFDM (Orthogonal Frequency Division Multiplexing) A multi-carrier transmission technique, which divides the available spectrum into many carriers, each one being modulated by a low rate data stream. This is the basis for ADSL as well

PCS (personal communications services) An alternative to cellular, PCS works like cellular technology because it sends calls from transmitter to transmitter as a caller moves. But PCS uses its own network, not a cellular network, and offers fewer "blind spots"—areas in which access to calls is not available—than cellular. PCS transmitters are generally closer together than their cellular counterparts.

Glossary (cont.)

PDA (personal digital assistant) Mobile, handheld devices—such as the Palm series and Handspring Visors—that give users access to text-based information. Users can synchronize their PDAs with a PC or network; some models support wireless communication to retrieve and send e-mail and get information from the Web.

Physical Layer Convergence Protocol (PLCP) A protocol specified within the Transmission Convergence layer that specifies exactly how cells are formatted within a data stream for a particular type of transmission facility.

Physical Medium Dependent (PMD) Performs wireless encoding

Satellite phone Phones that connect callers via satellite. The idea behind a satellite phone is to give users a worldwide alternative to sometimes unreliable digital and analog connections.

Service Set Identifier (SSID) An identifier attached to packets sent over the WLAN that functions as a "password" for joining a particular radio network (BSS). All radios and access points within the same BSS must use the same SSID, or their packets will be ignored

SMS (short messaging service) A service through which users can send text-based messages from one device to another. The message—up to 160 characters—appears on the screen of the receiving device. SMS works with GSM networks.

Symbol A term for the information contained in a message. I can be though of as a discrete block of digital information.

TDMA (time division multiple access) This protocol allows large numbers of users to access one radio frequency by allocating time slots for use to multiple voice or data calls. TDMA breaks down data transmission, such as a phone conversation, into fragments and transmits each fragment in a short burst, assigning each fragment a time slot. With a cell phone, the caller would not detect this fragmentation. Whereas CDMA (which is used more frequently in the United States) breaks down calls on a signal by codes, TDMA breaks them down by time. The result in both cases: increased network capacity for the wireless carrier and a lack of interference for the caller. TDMA works with GSM and digital cellular services.

WAP (wireless application protocol) WAP is a set of protocols that lets users of mobile phones and other digital wireless devices access Internet content, check voice mail and e-mail, receive text of faxes and conduct transactions. WAP works with multiple standards, including CDMA and GSM. Not all mobile devices support WAP.

WASP (wireless application service provider) These vendors provide hosted wireless applications so that companies will not have to build their own sophisticated wireless infrastructures.

Glossary (cont.)

WCDMA (wideband CDMA) A third-generation wireless technology under development that allows for high-speed, high-quality data transmission. Derived from CDMA, WCDMA digitizes and transmits wireless data over a broad range of frequencies. It requires more bandwidth than CDMA but offers faster transmission because it optimizes the use of multiple wireless signals—not just one, as with CDMA.

Wireless LAN (WLAN) It uses radio frequency technology to transmit network messages through the air for relatively short distances, like across an office building or college campus. A wireless LAN can serve as a replacement for or extension to a wired LAN.

Wireless spectrum A band of frequencies where wireless signals travel carrying voice and data information. Wireless carriers are bidding at Federal Communications Commission auctions on slivers of airwaves through which they will ultimately be able to send third-generation communications. The auctions, which began in December 2000 in the United States and already occurred in several European nations, will give providers access to new pieces of the spectrum that will allow them to move to third-generation services. More auctions relevant to 3G communications are on tap.

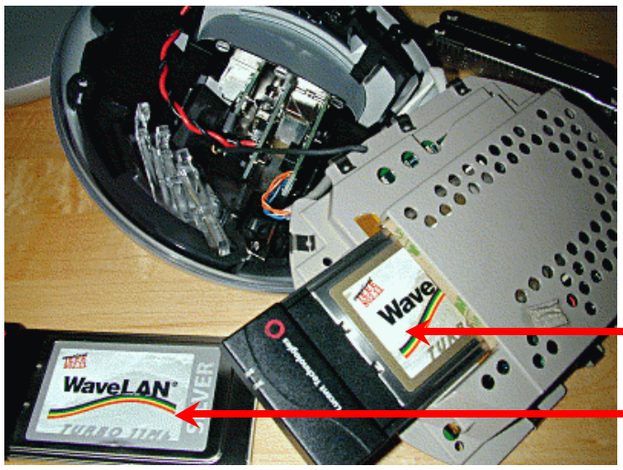
WISP (wireless Internet service provider) A vendor that specializes in providing wireless Internet access.

WML (wireless markup language) A version of HDML, WML is based on XML and will run with its own version of JavaScript. Wireless application developers use WML to repurpose content for wireless devices.

End Matter

- Pulling apart an Apple Airport
- Building your own AP on *NIX
  - Linux or FreeBSD
- Floppy based Wireless Gateway
- WFG Internals

Apple Airport



Building your own AP

Condensed from http://www.oreillynet.com/pub/a/wireless/2001/03/06/recipe.html

- Equipment
  - 1 desktop PC, 386 or better
  - At least one 802.11b wireless Ethernet PCMCIA card
    - Lucent WaveLAN/ORiNOCO, Cisco, and Prism II cards are popular
  - One ISA-to-PCMCIA or PCI-to-PCMCIA adapter
    - ISA is preferred
  - At least one NIC card connected to the network
    - can be any type of connectivity (cable modem, DSL, ordinary Ethernet, another wireless link, a satellite downlink, modem and a PPP dialup, etc.)

Building your own AP (cont.)

- Operating System
  - A Unix-like operating system
    - Linux and FreeBSD seem to be the OS of choice
  - Clients can be anything that can do Ad-Hoc
- Hints
  - Use an ISA-PCMCIA adapter
  - Lucent cards work great and have ability to have external antenna
  - Be prepared to spend time debugging
    - depending on the OS level

Building your own AP (cont.)

- Install the PCMCIA adapter in the gateway and insert the wireless card
- Install the OS and software
  - You will need NAT (IP Masquerade)
    - firewall software (ipchains or iptables)
  - You will want a DHCP and SSH server
- Get kernel source
  - At least 2.2.18, 2.4.x is best
- Get the latest pcmcia-cs and wireless_tools source code
  - Pcmcia-cs.sourceforge.net
  - http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html

Directions (cont.)

- Update the kernel
  - Enable loadable module support
  - Enable support for your other NIC cards
  - Enable kernel firewall support
  - Enable IP masquerading (i.e., NAT)
  - Enable Wireless Networking (also known as "non-ham")
    - do not select any modules
  - When compiling a 2.4.x kernel Disable PCMCIA support
    - we'll use the external pcmcia-cs package

Directions (cont.)

- Build and install the new kernel
  - Don't forget to edit /etc/lilo.conf and then run /sbin/lilo
- Install the pcmcia-cs package
- Install the wireless_tools package
  - Your OS may have it (i.e., RedHat 7.1)
- Edit wireless options
  - /etc/pcmcia/wireless.opts
  - ESSID to "yourfavoritename"
  - Rate is "auto"
  - Mode is "Ad-hoc"

Directions (cont.)

- Configure wireless IP options
  - /etc/pcmcia/network.opts
  - Use private IP range
  - Set IP, netmask, and broadcast
- Configure NIC IP options
  - /etc/sysconfig/network-scripts/eth0
  - Set it to DHCP or static IP values
- Install or configure the firewall/NAT package
  - Configure it to masquerade packets from your wireless network to the outside
  - Ensure that you do proper “security” filtering (i.e., drop spoofed IP packets)

Directions (cont.)

- Install and configure DHCP (if desired)
  - This will only be running on the wireless interface
- Harden the rest of the system (read: TURN OFF ALL UNUSED SERVICES)
  - Keep the PCMCIA, firewall, and DHCP services running
- Reboot and see what you broke ☺
  - Probably should reboot before the firewall and DHCP install/configure
- Setup clients

Floppy based Wireless Gateway

- Same basic hardware requirements
  - System, ISA-PCMCIA, NIC, Wireless card
  - NIC cards are much more sensitive
    - Trinux experience helps when adding modules
- http://nocat.net/ezwrp.html
- My Problems
  - Got it up quickly
  - Problems with DHCP
  - Never got it passing traffic
  - Unclear how to manage firewall rules

WFG Internals

- OpenBSD Unix
  - Three interfaces on different networks
    - Wireless
    - external (gateway)
    - internal (management)
- DHCP
  - ISC's DHCPv3
    - modified to dynamically remove hosts from the firewall access list when DHCP releases a lease for any reason
      - the DHCP server will not issue the same IP address until it frees the lease of the last client
  - Listens only on the wireless interface
    - also packet filters prevent any DHCP requests coming in on any other interfaces

WFG Internals (cont.)

- IP Filtering
  - OpenBSD's IPF software
  - IP routing is enabled
  - Packet filtering between the wireless and external network interfaces
    - static filters are configured on boot up
      - limit initial wireless network access
      - NTP, DNS, DHCP, and ICMP
      - for all users: selected email servers, VPN, and web
  - When a user authenticates, they are allowed unrestricted access

WFG Internals (cont.)

- Web Authentication
  - Used for cross-platform
  - Apache with SSL
  - User enters username and password
    - Perl/CGI script then communicates with a Radius server
    - if accepted, then commands to allow their IP address are added to the IPF access rules
- Security
  - System access with SSH
  - Logs: Syslog, DHCP, and Web authentication logs

Notes:

Notes:

Philip Cox
Consultant

Phil.Cox@SystemExperts.com
530-887-9251 direct
530-887-9253 fax
978-440-9388 main
http://www.SystemExperts.com/

Brad C. Johnson
Vice President

Brad.Johnson@SystemExperts.com
401-348-3099 direct
401-348-3078 fax
978-440-9388 main
http://www.SystemExperts.com/