802.11b Wireless LANs

Got Wireless?
What’s a “Wireless LAN”?
“Wireless”

- Webster’s New World Dictionary, 2nd College Edition, defines “wireless” as:
  “without wire or wires; specifically operating with electromagnetic waves and not with conducting wire.”
“LAN”

- Newton’s Telecom Dictionary, 11th Edition, defines “LAN” as:
  “A short distance data communications network (typically within a building or campus) used to link computers and peripheral devices under some form of standard control.”
Wireless LAN Configurations

• Peer-to-peer Workgroup
  – Also known as Ad Hoc Network
• Small Office/Home Office (SOHO)
• Infrastructure or Client/Server Network
Wireless LAN Hardware

- Wireless Network Interface Card (NIC)
- Wireless Access Point (AP)
  - Small Office/Home Office (SOHO)
  - Enterprise
Wireless NIC

- Contains the radio transceiver, antenna, and circuitry to convert Radio Frequency (RF) to digital
- Form factors
  - PC Card
  - ISA or PCI NIC or PC Card adapter
  - USB
Peer-to-Peer Workgroup

- Simplest and cheapest to build
- Client computers communicate directly with each other
- All client computers must be within range of each other
- File & printer sharing using a peer-to-peer operating system
Wireless Access Point

- Bridges between wireless and wired segments to minimize traffic
- Frequency selection
- Authentication & Encryption
- Built-in radio & antenna(s) or slots for PC Cards
- Hardware vs. software APs
SOHO Access Point

- Allows multiple wireless clients to share a single IP address via broadband and/or dial-up modem
- Starting to see all-in-one devices with integrated wired and wireless
- Basic management features
- Limited number of users
Enterprise Access Point

- Standalone LAN or integrated into an existing enterprise network
- No IP address sharing capability
- Advanced Management
- Greater number of users
- Better performance, typically, than peer-to-peer networks
The Institute of Electrical and Electronics Engineers (IEEE) publishes the 802.11 standards.

- 802.11 (1997) was the 1st wireless standard from an internationally recognized, independent organization.
IEEE 802.11

• Infared (IR)
  – Never commercially implemented

• Radio Frequency (RF)
  – Frequency Hopping Spread Spectrum (FHSS)
  – Direct Sequence Spread Spectrum (DSSS)
Operating Frequency

- IEEE 802.11 (and a lot of other things) operate in the unlicensed 2.4GHz Industrial, Scientific, & Medical (ISM) frequency band.

ISM Frequency Band

- FCC regulations allow 1W of output power using spread spectrum
- Devices may not cause harmful interference and must accept any interference received, including interference that may cause undesired operation
What is Spread Spectrum?

- Spreads the transmission across multiple frequencies, making it difficult to detect or jam without knowing the code or sequence
- Used primarily for military applications until the mid-80’s
Who Invented It?

• Patent received by actress Hedy Lamarr and composer George Antheil in 1942

• Neither benefited from the 17-year patent, which expired before the idea was used by the U.S military
FHSS vs. DSSS

- Frequency Hopping SS
  - Carrier frequency hops among multiple narrow channels according to a unique sequence

- Direct Sequence SS
  - Data is encoded and decoded using a Pseudo Random Noise Code
Channel Assignments

- 11 channels are used in the U.S., 13 in Europe, 4 in France, and 1 in Japan
- The 11 channels used in the U.S. have center frequencies of 2.412GHz-2.462GHz in 5MHz increments
Center Frequencies (GHz)

- CH  1  2.412
- CH  2  2.417
- CH  3  2.422
- CH  4  2.427
- CH  5  2.432
- CH  6  2.437
- CH  7  2.442
- CH  8  2.447
- CH  9  2.452
- CH 10  2.457
- CH 11  2.462
Channel Selection

• Each DSSS channel is 22MHz wide
• Channels 1, 6, & 11 provide non-overlapping coverage
• A minimum of 3 channels of separation (e.g. 1,4,7 & 10) can be used in certain situations.
802.11 Drawbacks

- Low speed - 1 or 2 Mbps
- High cost of hardware
- Limited interoperability
- DSSS & FHSS not compatible
- Appropriate for vertical applications
IEEE 802.11b High Rate

- Published in 1999
- Higher speeds (11Mbps and 5.5Mbps) while maintaining backward compatibility with 802.11 DSSS 1 & 2 Mbps rates
- Throughput roughly equivalent to 10Mbps shared Ethernet
IEEE 802.11b Benefits

• Interoperability
  – Wireless Fidelity (Wi-Fi) certification by the Wireless Ethernet Compatibility Alliance (WECA)

• Affordability
  – PC Card NICs under $200
  – Starting to see built-in wireless NICs
Is It Wireless Ethernet?

• IEEE 802.3 Ethernet uses CSMA/CD-Carrier Sense Multiple Access with Collision Detection
• IEEE 802.11b uses CSMA/CA-Carrier Sense Multiple Access with Collision Avoidance
• Difference is transparent
Reasons Why You Would Want A Wireless LAN

• It’s cool
• It will facilitate increased user productivity by providing them with the mobility and flexibility to work in a more efficient environment
• Your boss wants it (yesterday)
When Should I Use Wireless?

• Wireless makes the most sense in situations requiring:
  – Quick setup and take down (conferences, trade shows)
  – Temporary facilities (leased or rented space)
  – Historical buildings
When Shouldn’t I Use Wireless?

- Wireless is not a substitute for a good wired infrastructure.
  - Speed
  - Cost
  - Reliability
Security

There are two main components involved in securing Wireless LANs:

- Authentication
- Encryption
Authentication

• Service Set ID (SSID)
  – Also known as Network Name
• MAC Address Access List
• Username and Password
Service Set ID (SSID)/Network Name

– Default client setting is “ANY”; all open networks within range will respond and the radio will usually associate with the strongest signal

– Closed networks require the exact SSID to be entered in the client configuration settings and only APs with the same SSID will be visible
SSID (continued)

- Allows assigning clients into specific groups by forcing them to associate with a specific AP or group of APs
- Updates would need to be performed on APs and clients simultaneously
- Shared Secret (doesn’t scale well)
- Hardware is being authenticated
MAC Address Access List

- Wireless NIC MAC address must be included in the list for the AP to allow data to pass.
- Creates a “black hole” for clients whose MAC addresses are not included in the list, since their NIC can associate with the AP but their data goes nowhere.
Access List (continued)

– Difficult to implement on a large scale or with transient users
– Lists need to be maintained in each access point, although querying a centralized list may be possible
– Maximum access list size varies
– Hardware is being authenticated
User Authentication

– ITS is currently evaluating the use of UHUNIX IDs to allow access to the wired campus network
– A key design goal is to perform this authentication without having to install software on each client
– User is being authenticated
Encryption

• WEP (Wired Equivalent Privacy)
  – Intended to provide privacy equivalent to that of a non-encrypted wired network
  – 40-bit encryption based on the RC4 algorithm.
  – 128-bit version may be vendor-specific
WEP (continued)

- Flaws were recently published by UC Berkeley computer scientists
  http://www.isaac.cs.berkeley.edu

- Wireless Ethernet Compatibility Alliance (WECA) Response
  http://www.wi-fi.com/pdf/Wi-FiWEPSecurity.PDF
WEP (continued)

- Encryption key updates would need to be performed on APs and clients simultaneously
- Keys can be entered in ASCII or Hex, depending on the manufacturer
- May impact AP throughput
- Shared Secret (doesn’t scale well)
Security

• Large-scale networks cannot rely on 802.11b alone to provide authentication and encryption.
• Authentication and encryption could be accomplished by using a Virtual Private Network (VPN), but that would not meet our key design goal
Security

• Encryption needs to be implemented at the two endpoints so that data does not traverse the wireless network in cleartext.
  – mail.hawaii.edu uses SSL
  – Secure Shell (SSH) vs. Telnet
  – Pretty Good Privacy (PGP)
Safety

• Most wireless NICs only output ~30mW to conserve battery power
• Radio transmits only when there is data to be sent; a cell phone which transmits throughout the entire call
• Read the manufacturer’s safety information
Design Considerations

- Maximum Coverage
- Maximum Throughput
- Channel Selection
- Roaming
- Allowed Protocols/Applications
Maximum Coverage

- Access points are spaced so that coverage barely overlaps
- Users will fallback to slower speeds as they move farther from the AP and signal strength weakens
- Lower cost since fewer APs are required
Maximum Throughput

- Access Points are spaced so there is significant coverage overlap
- Users connect at the highest speed
- Can provide redundancy or user segregation
- Higher cost since more APs are required
Channel Selection

- Using Channels 1, 6, and 11:

- Gets a little more difficult in 3-D
Access Point Range

- Open office: ~500’
- Semi-open: ~160’
- Closed Office: ~80’
- These are ballpark figures and can vary greatly depending on AP and client placement, wall construction, furniture, etc.
IP Addressing

- Transparent Bridge
- Network Address Translation (NAT)
  - Non-routable IP addresses behind one valid IP address
- Dynamic Host Configuration Protocol (DHCP)
  - Can serve valid or NAT IP addresses
Roaming

• Access Points need to be on the same subnet or VLAN
• Transparent bridging (no NAT)
• Seamless campus-wide roaming… would be nice but there are several technical issues to resolve first
Allowed Protocols/Apps

- ITS is planning to allow only TCP/IP on the campus wireless network.
- ITS would like to provide all applications over the wireless network, but applications like Multicast will need to be evaluated.
Access Point Placement

- Glass is good for transmitting through, unless the tint blocks RF
- “Higher is better, Higher is better”
- Datajack and electrical outlet
- Power over Ethernet (PoE)
Interference

• The unlicensed ISM band is subject to possible interference from:
  – Cordless phones, video monitoring devices, etc. that operate at 2.4GHz
  – Microwave Ovens
  – Other Wireless LANs
Troubleshooting

• Diagnostic tools are not part of the standard and will most likely be vendor-specific
• Sometimes difficult since problems tend to be more sporadic in nature than for wired networks
• Signal vs. Noise better than SNR
Other Wireless LAN Technologies

• HomeRF
  – www.homerrf.org
  – 2Mbps (10Mbps shortly)
  – Frequency Hopping Spread Spectrum

• Bluetooth
  – www.bluetooth.com
  – Low power Personal Area Networks
What’s Coming?

• 802.11b Extensions-22Mbps
• 802.11a (1999)
  – Products should appear later this year
  – 5GHz band
  – Up to 54Mbps
  – Shorter range
  – Not backward-compatible w/802.11b
References

• The Wireless LAN Association
  – http://www.wlana.com

• Wireless Ethernet Compatibility Alliance
  – http://www.wi-fi.com
Questions?

Steven Goto
sgoto@hawaii.edu