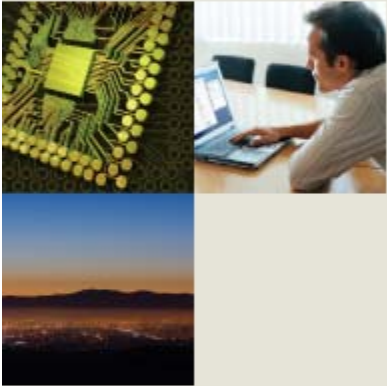




Converging Work and Home Networking



Session 3153

SHARE Summer 2009 Denver

Tom Hadley, Network Consultant, tom@lauraknapp.com

with Thanks to Victor Freyer

Work and Home Networks

- When you work from home, you still need access to the office network
- Today that connection is usually the public Internet, via a secure connection – a Virtual Private Network (VPN)
- The Internet is full of bad people doing bad things
- How do you protect your home network?
- How do you prevent bad things from infecting your work network via your Internet connection (VPN) from home?



Agenda

- Security
 - Hardware
 - Software
- Wireless networking
 - Bluetooth
 - 802.11a/b/g/n
- Useful Tools
 - Discovering wireless
 - Secure public networking (Windows VPN)
 - SPAM filters

Security

- Hardware firewall
 - Cable/DSL routers
 - Firewall appliances
- Personal firewalls
 - Zone Alarm
 - Comodo
 - Sunbelt Kerio
 - Windows XP/Vista/???
- Windows IP security policies
- Linux firewall
 - IPCop
 - Endian
 - Firestarter
 - Custom iptables



Hardware Firewall - Appliances

- Consumer products < \$100
 - Firewall + network address translation (NAT)
 - Small number of streams
 - Most support VPN
 - Limited configuration
- Commercial products - \$100's-\$10,000s
 - High throughput
 - Multiple interfaces
 - Intrusion detection
 - Multitudes of streams
 - Multitudes of VPNs
 - Additional setup and monitoring



Personal Firewalls - Software

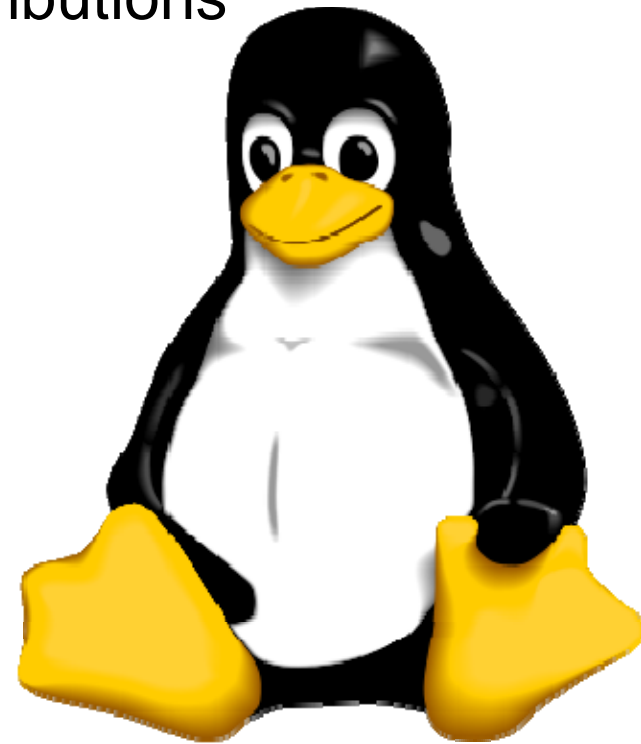
- PC-based firewall functions
 - Keep bad stuff out – “Don’t be a server”
 - Block inbound packets: ping, TCP SYN, UDP
...but allow inbound responses for established sessions
 - Disallow unknown programs from being servers
 - Keep good stuff in – “Don’t be an unintentional client”
 - Control outbound connections
 - Allow iexplore.exe to be a client, for example
 - Disallow unknown programs from being clients
- Free personal firewalls
 - ZoneAlarm – www.zonealarm.com
 - Comodo – www.comodo.com
 - Sunbelt Kerio – www.sunbeltsoftware.com (free mode)
 - Windows XP / Vista – default setting blocks inbound only

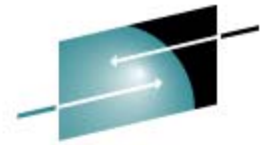
Windows 2K & XP – IP Security Policies

- Identify the ports you want to allow
 - For example, DNS (UDP 53), HTTP/HTTPS (TCP 80/443)
- Edit IP security policy
 - Control Panel->Administrative Tools->Local Security Policy->IP Security Policies on Local Machine
 - Action->Create IP Security Policy
- Create deny all rule
- Create permit rules
- Select your policy, Action->Assign
- Rules are evaluated from most specific to least specific

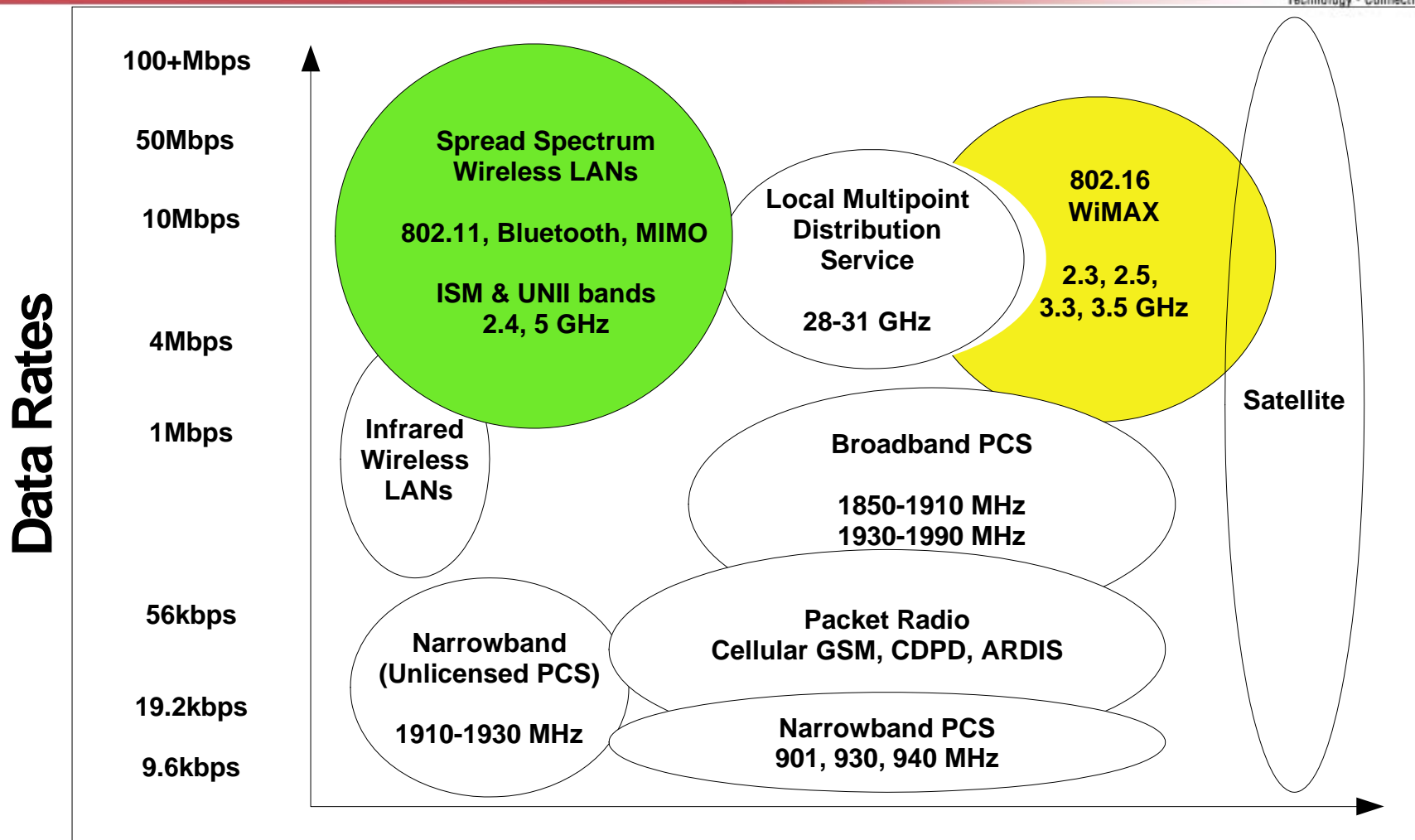
Linux Firewalls

- Turnkey Open Source firewall distributions
 - IPCop – www.ipcop.org
 - 4 interface types (Internet, DMZ, wireless, secure)
 - Endian – www.efw.it
 - 4 interface types (Internet, DMZ, wireless, secure)
 - Firestarter – www.fs-security.com
 - 2 interface types (Internet connected, local)
- Home grown - iptables
 - Greatest flexibility
 - Greatest complexity
 - Least manageability





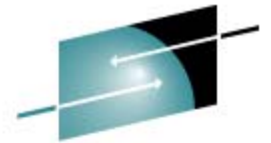
Wireless Technologies



Local

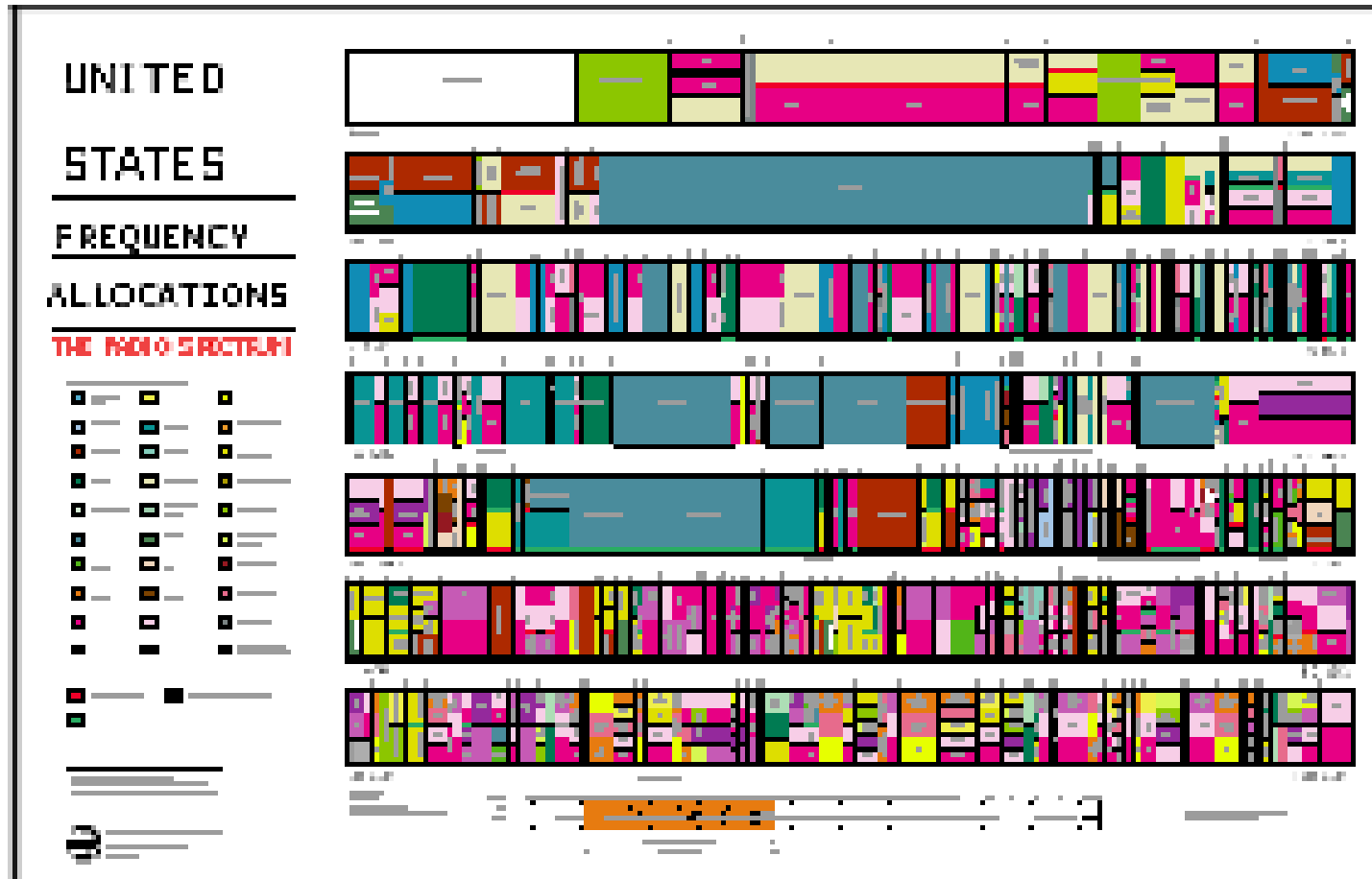
Coverage Area

Wide

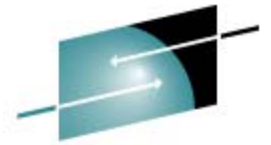


SHARE
Technology • Connections • Results

US Radio Spectrum

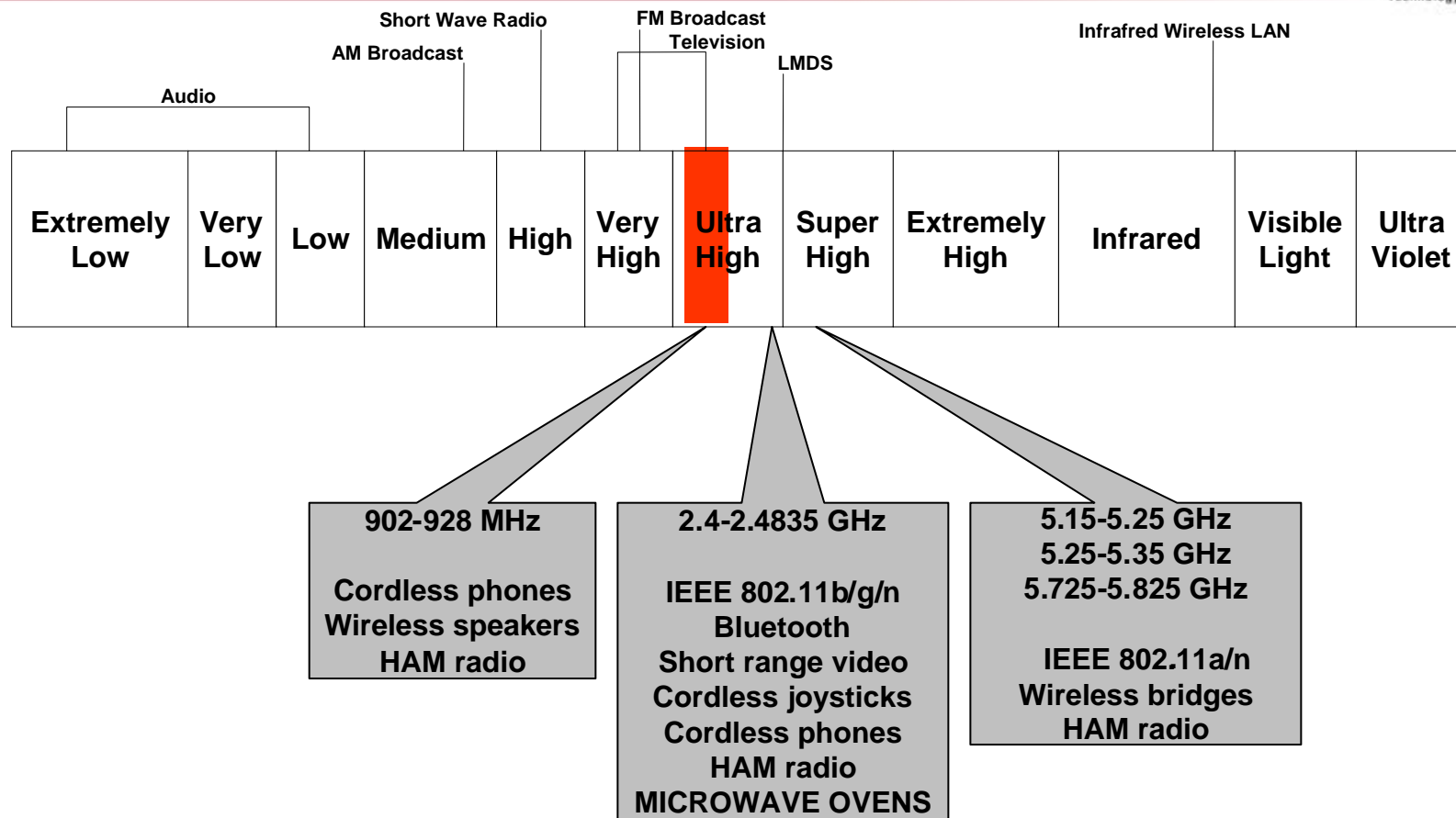


<http://www.ntia.doc.gov/osmhome/allochrt.html>



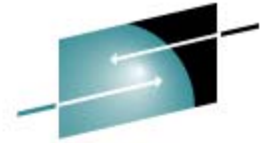
SHARE
Technology • Connections • Results

Unlicensed Frequencies



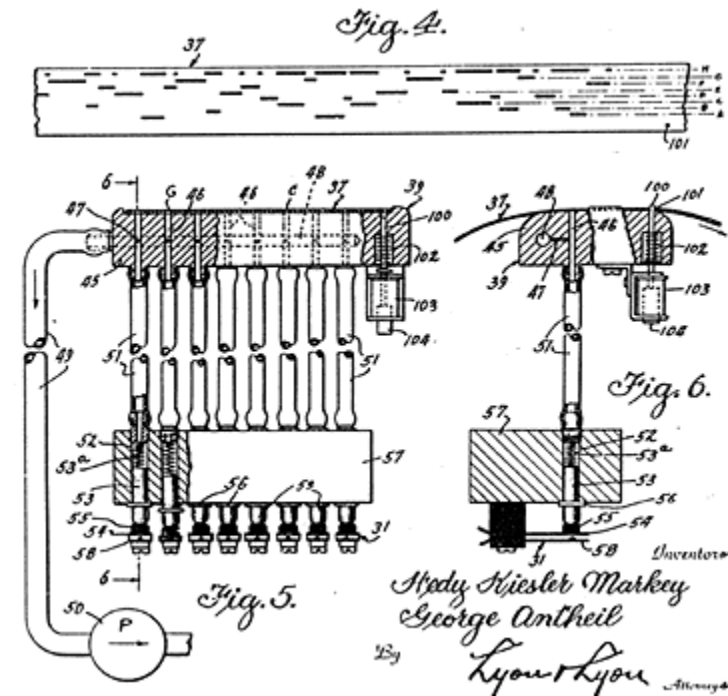
- No license required but usage **is** regulated

Spread Spectrum



SHARE
Technology • Connections • Results

- Conceived and patented (2,292,387) in 1942 by actress Hedy Lamarr and husband, composer George Antheil
- Patent based on mechanical process
- First electronic implementation in late '50s



Bluetooth Background

- IEEE 802.15 Wireless Personal Area Network
 - Voice and data via wireless
 - 10 to 100 meters
- Not originally intended to be an IP transport
- Most frequent uses
 - Wireless headsets for phones
 - Remote keyboards and peripherals
 - Ad-hoc conference room network
 - Automotive cellular phone and sound systems
- Emerging uses
 - Wireless power
 - Social networking
 - Remote medical biosensors



Bluetooth Vulnerabilities

- Vulnerabilities and security issues

- Bluejacking

- Cracker sends anonymous “business cards”

- Bluebugging

- Cracker takes control of your Bluetooth phone

- Bluesnarfing

- Cracker retrieves information from your device

- Bluetagging

- Covert surveillance of your whereabouts

- Car Whisperer

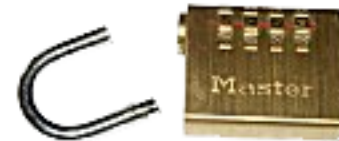
- Cracker monitors your cellular microphone and may send audio to your speakers

- Cabir/Mabir worm

- Malware that propagates from phone to phone

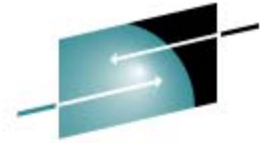
- PIN discovery

- PINs used to establish secure pairing can be compromised by brute-force analysis



IEEE 802.11 Terminology

- Access point – AP
 - Base station in an infrastructure network
- Infrastructure network
 - A hierarchal design in which wireless stations communicate directly with only a central access point
- Peer-to-Peer or Ad Hoc network
 - Wireless stations communicate directly without central control
- SSID – Service Set Identifier (Network Name)
 - Differentiates one wireless network from another
- WEP – Wired Equivalent Privacy
 - Static shared key encryption
 - Very weak but better than nothing
- WPA/PSK – WiFi Protected Access / Pre-shared Key
 - Dynamic encryption keys
 - Longer initialization vector
- MIMO – Multiple In Multiple Out
 - IEEE standard pronunciation (my-moe)
 - Multiple transmitters, multiple receivers
 - Improves non-line of sight (NLoS) networks



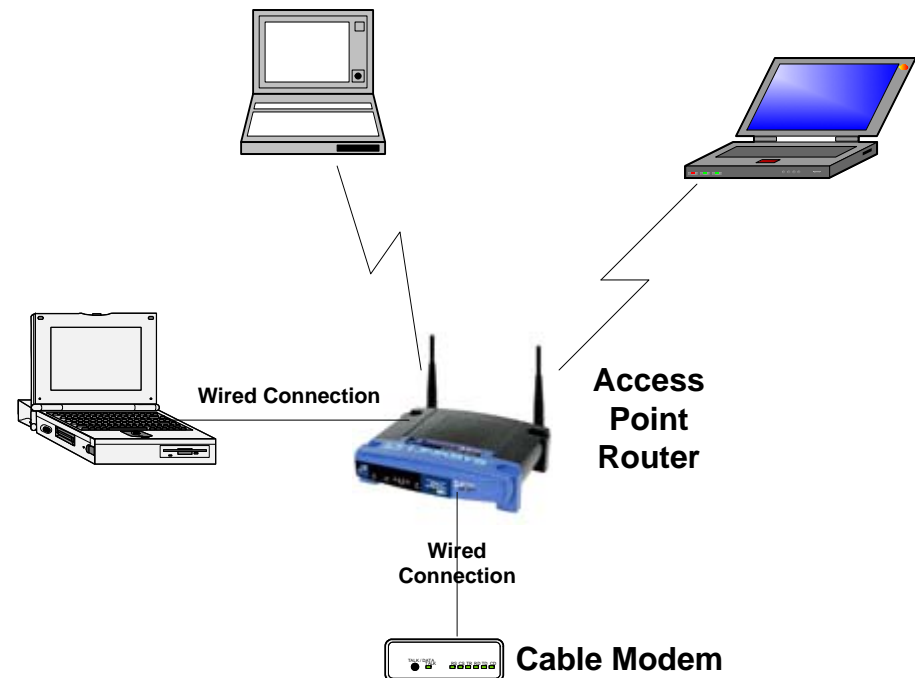
SHARE
Technology • Connections • Results

IEEE 802.11 Standards

| 802.11b | 802.11a | 802.11g | 802.11n |
|--|--|--|--|
| 2.4 GHz (3 not overlapping) | 5 GHz (8 not overlapping) | 2.4 GHz (3 not overlapping) | 2.4 GHz 5 GHz opt. (2 bonded 20Mhz) |
| Worldwide | US/Japan | Worldwide | Worldwide* (* 5GHz varies) |
| FHSS/DSSS PBCC (opt.) | OFDM | OFDM PBCC (opt.) | OFDM + MIMO |
| 1-11 Mbps (22 Mbps) | 20-54 Mbps | 20-54 Mbps (100 Mbps) | 40 Mbps - 2.4G 85^ Mbps – 5G |

Home Office Design

- Access point can provide network address translation and firewall capabilities
 - All wireless communication goes through AP
- Change your AP's SSID. Wireless stations will connect to an AP based on SSID
- Will associate with AP but "hang" if WEP/WPA keys don't match
 - Most support WPA2 today
- Set radio power to lowest level that covers your area
- 802.11n is faster and MIMO allows signal to go much further
 - Basement location reduces RF bleed around neighborhood



Windows VPN at Home

- Server side: Network Connections -> Create a new connection -> Set up an advanced connection -> Accept incoming connections
- You can create a PPTP endpoint ...or, allow dialup access
- Firewall setup – allow TCP port 1723 and IP protocol 47
- Limited to 10 simultaneous connections
- Client side: Create a new connection -> Connect to the network at my workplace
- Set MTU on PPTP interface in client's Registry to 1396
- *Secure access to home remote desktops, file servers and printers*
- *Somewhat secure Internet access from public/insecure networks*

SPAM Filters

- Email filters
 - Web email – Yahoo Mail, Google GMail, MSN Hotmail, etc.
 - Client side – Eudora, Mozilla, Thunderbird, MS Outlook
 - Server side – Spamassassin, SpamBayes
- Bayesian classification (Unix and Windows)
 - SpamBayes : <http://spambayes.sourceforge.net/>
 - POPFile : <http://popfile.sourceforge.net/>
- Filtering research
 - <http://www.paulgraham.com/paulgraham/bayeslinks.html>
- Top Windows SPAM filters
 - http://email.about.com/cs/winspamreviews/tp/free_spam.htm

In Conclusion

- If “always-on,” use a firewall/router
- If portable or dialup, use personal firewall software
- Configure Windows™ local IP security policy for extra protection
- Wireless devices may interfere with each other
- Bluetooth vulnerabilities are being discovered
- Minimize your 802.11 exposures
- Be wary when using public wireless – use a VPN
- SPAM filters will reduce your frustration