

Networking 401

(Advanced Wireless Networking)

Lab

Presentation to UCHUG - 1/02/08

Networking 401 lectures presented on 9/05/07 and 10/03/07

G. Skalka

A Quick Review of Wireless Networking Basics

What is a wireless network?

- A wireless network uses RF (radio frequency) data links to connect one or more computers together or to a wired network.

A Quick Review of Wireless Networking Basics

Wireless Network

- Wi-Fi - WLAN (wireless local area network) based on IEEE 802.11 specs
- Uses wireless access points (WAPs) to transmit to and receive from WiFi-enabled devices.
- Most implementations operate in the unlicensed spectrum near 2.4 GHz.

A Quick Review of Wireless Networking Basics

Wireless “Flavors”

- 802.11a (rare)
 - 54 Mbps max, 75 feet max, uses 5 GHz band
 - Lower interference, higher signal attenuation
- 802.11b (first and most popular standard)
 - 11 Mbps max, 150 ft max, 2.4 GHz, lowest cost, obsolete
 - Interference from cordless phones and microwave ovens
- 802.11g (current leader in new sales)
 - 54 Mbps max, 150 ft max, 2.4 GHz band
 - Backwards compatible with 802.11b
- 802.11n (standard not yet finalized - due March 2009)
 - 248 Mbps max, 160 ft max, 2.4 or 5 GHz
 - MIMO - multiple-input, multiple-output (uses multiple antennas)

Why Go Wireless?

- To connect to devices or networks where having a wired connection would be difficult or impractical
 - Isolated areas in home or building
 - Outdoors
 - Public and private “hot spots”
- To allow mobility in a network connection

Disadvantages of Wireless (as Compared to Wired Networking)

- Lower bandwidths
- Range limits to performance (performance limited by distance to access point)
- Interference problems
- Security
 - Data transmissions generally not as secure
 - Source of connection can be uncertain

Hardware / Software Required

- Wi-Fi capable laptop
 - Wireless adapter either built into the motherboard, or connected via Cardbus or USB
 - All that is needed to connect to “hot spots”
- Wireless access point (WAP) or wireless router
 - Needed to connect to your wired network
- Wireless adapters (built-in, PCI or USB)
 - For your desktop computers to connect

Connecting to a Wireless Network

A Review

- The settings of the computer's wireless network adapter must be set to match the settings of the wireless access point
- To connect to an existing wireless network, get the wireless configuration
- To initially set up a new wireless network
 - Use a configuration wizard
 - Use the most basic (default) settings

Wireless Network Settings

- Things to set in a typical wireless router or WAP
 - Configuration password
 - DHCP server
 - Band or 802.11 standard (a, b, g, n)
 - SSID (service set identifier)
 - The public name of a wireless network
 - Channel
 - Security (WEP, WPA, WPA2)

The Most Basic Wireless Settings

- For easy initial connection, set as follows:
 - DHCP server (assigns IP addresses)
 - Computer set to accept IP address
 - Band with most options (B+G, B+G+N)
 - Default SSID, SSID broadcast
 - Default or auto channel
 - Security or encryption disabled

For Increased Security

- Set as follows for greater security
 - Unique router configuration user name and password
 - Makes it harder to hack in and take control of your router
 - Set band to only the one you are using
 - G-only would not allow B or N connections
 - Set a unique SSID and don't broadcast it
 - No broadcast SSID may make your network a little more invisible
 - Enable security or encryption
 - Use the strongest security setting that is compatible with both sets of hardware
 - Connect using a VPN (virtual private network)

SSID (Service Set Identifier)

- A 32-character unique identifier
- Attached to the header of packets sent wirelessly
- Name that identifies a network
- Device must provide the unique SSID to connect and join the network
- SSID is not secure
 - Broadcast in the clear in plain text in a packet

SSID Security

- Set your SSID to reduce your chances of being a target
 - Don't use the default SSID
 - Don't use personal information as part of the SSID (don't give away your identity)
 - Don't use a tempting SSID (Sexy, TopSecret)
 - Use letters and numbers and use maximum length
 - Random characters could also make you a target

SSID Non-Broadcast

- Network may not show up, or displays as “Unnamed Network” to user
- Users need to manually enter the correct SSID to connect
- This may deter the casual interloper
- It also may make it more difficult for legitimate users
 - Can often set clients to automatically connect

SSID Non-Broadcast Issues

- SSID is still being broadcast periodically
 - Can still be “sniffed” by hackers
 - Hackers can then “spoof” the legitimate network’s SSID, luring in devices set to automatically connect
- SSID security can be argued either way
 - Not broadcasting SSID may increase or decrease security

Wireless Encryption

- Three types and levels of security, in increasing strength
 - WEP - Wired Equivalent Privacy or Wireless Encryption Protocol
 - Original IEEE 802.11 standard from 1999
 - WPA - Wi-Fi Protected Access
 - 2003, intermediate measure to replace WEP
 - WPA2
 - Full 802.11i standard, 2004

WEP Details

- Standard 64-bit WEP
 - 40-bit key and 24-bit initialization vector
 - Users typically enter 10 hex characters (4 bits per character)
- 128-bit WEP
 - 104-bit key and 24-bit initialization vector
 - Users typically enter 26 hex characters
- Either type has rather weak encryption

WPA Details

- Uses 128-bit key and 48-bit initialization vector
- Temporal Key Integrity Protocol (TKIP)
 - Dynamically changes keys as the system is used
- Mode with 802.1X authentication server
 - distributes user keys
- Pre-Shared Key (PSK) Mode
 - Less secure mode where users are given the same pass-phrase

WPA Details

- WPA2 adds AES (Advanced Encryption Standard) based algorithm
- WPA and especially WPA2 may not be supported (or fully supported) on older equipment
- Use WPA2 if possible, otherwise use WPA
- Use WEP only if WPA is not supported (consider upgrading)

How Safe Is Wireless?

- Wired networks are inherently more secure than wireless
 - Network communications between computer and router can't normally be monitored
- Private wireless can be secured so additional susceptibility is minimal
- Public wireless is not secure
 - Secure VPN or SSL needed for comm security
 - Physical security could still be a concern

The Spectrum of Safety

- Listed from most to least secure:
 - Private wired network with full security
 - Private wireless network with full security
 - Public wired network with full security
 - Public wireless network with full security
 - Private wired network with low security
 - Private wireless network with low security
 - Public wired network with low security
 - Public wireless network with low security

Security Measures

- Wired Private Networks
 - Secure router (NAT)
 - Firewall (hardware and/or software)
 - MAC address filtering in router
 - Other security software
 - Anti-virus, anti-spyware, OS security updates, SSL
 - Verify security settings for “invisibility”
 - Physical security
 - Shield visibility and hardware from public access
 - Safe computing practices

Security Measures

- Wireless Private Networks
 - All of the security measures mentioned for wired private networks (previous slide)
 - Especially MAC address filtering in router
 - Wireless security (encryption): WPA2, WPA
 - Avoid WEP
 - Set a unique SSID and don't broadcast it
 - Locate hardware to minimize public access
 - Disable transmission when not in use
 - Connect using a VPN (optional)

Security Measures

- Wired Public Networks
 - Software Firewall
 - Other security software
 - Anti-virus, anti-spyware, OS security updates
 - Physical security
 - Shield visibility from public access
 - Safe computing practices
 - Connect using a VPN, use SSL (required for sensitive data)

Security Measures

- Wireless Public Networks
 - All of the security measures mentioned for wired public networks (previous slide)
 - Especially: connect using a VPN, use SSL (required for sensitive data)

For Sensitive Data

- Online banking, personal info, passwords
- For these sensitive online sessions, I would only trust:
 - Private wired or wireless connection with full security
 - Public wired or wireless connection with full security (SSL, VPN and physical security mandatory)

Public Wireless Dangers

- Man in the middle attack
 - You get tricked into connecting to a fake public network
 - Info stolen
 - usernames and passwords
 - files
 - your identity
 - Your computer receives spyware
 - Hackers can control your PC and can use it to propagate more attacks

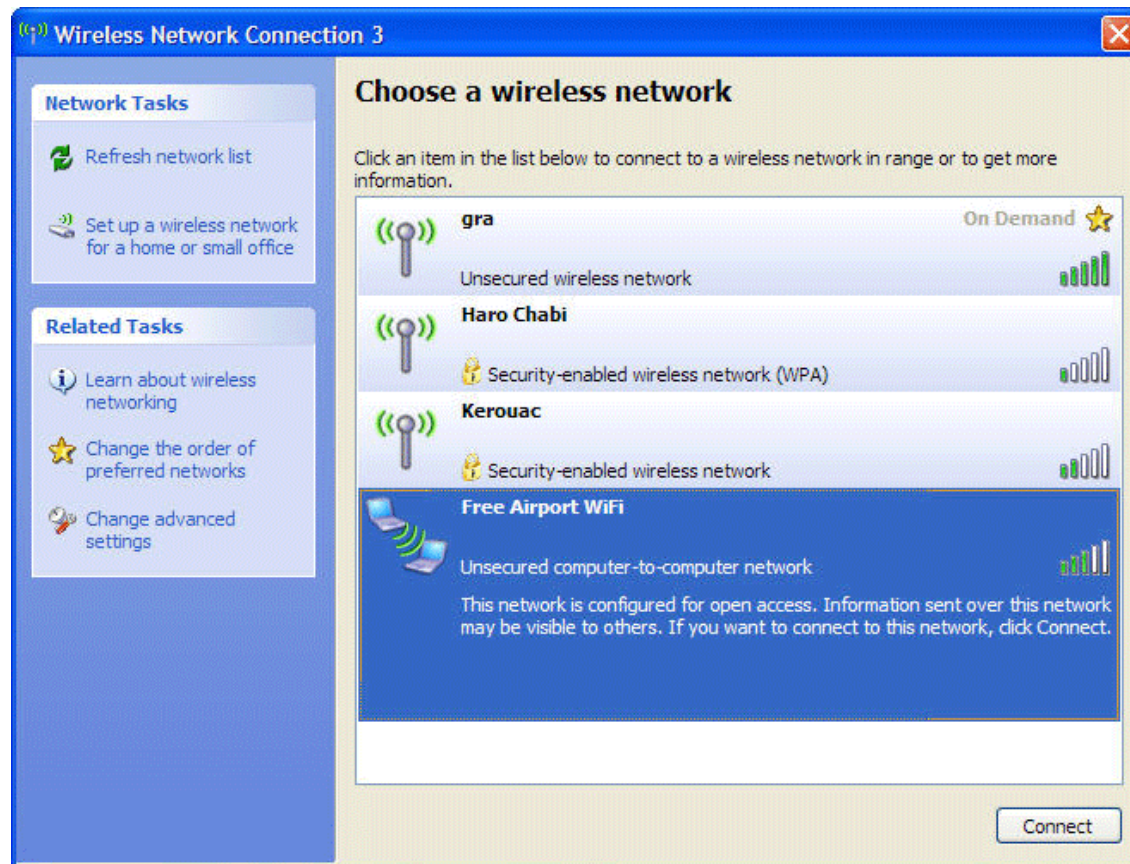
Man in the Middle Attack

- Victim is tricked into connecting to an ad hoc (peer to peer) network
- Set up by a hacker nearby
 - Uses SSID that is the same or similar to a legitimate network
 - Beware of auto connection
- Objective is to steal files and passwords and to plant malware

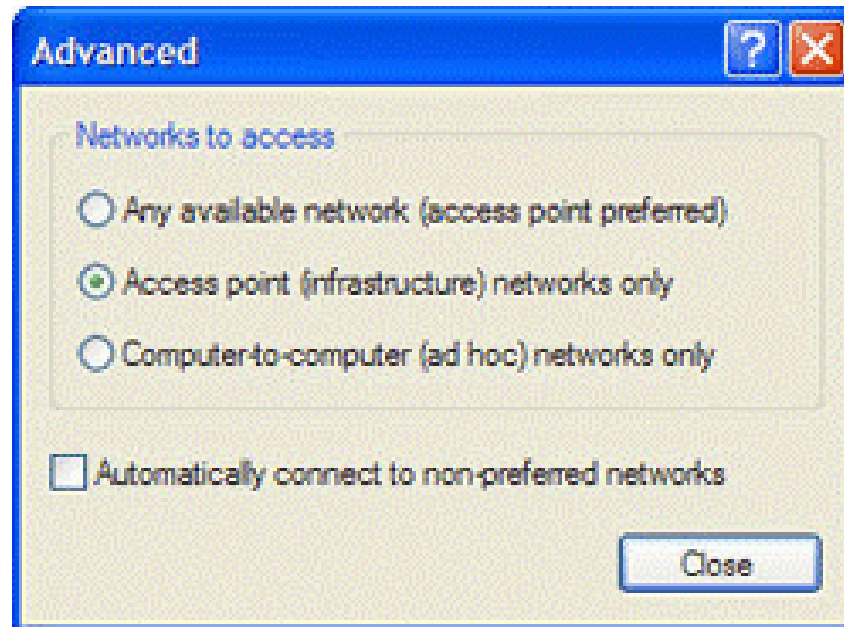
Protection from Attack

- Never connect to an ad hoc network, regardless of name
 - Set XP to never use ad hoc and never auto connect
 - Vista is more susceptible (icon is only indication of ad hoc)
- Turn off file sharing to minimize risks
- Use VPN
- Disable wireless when not using

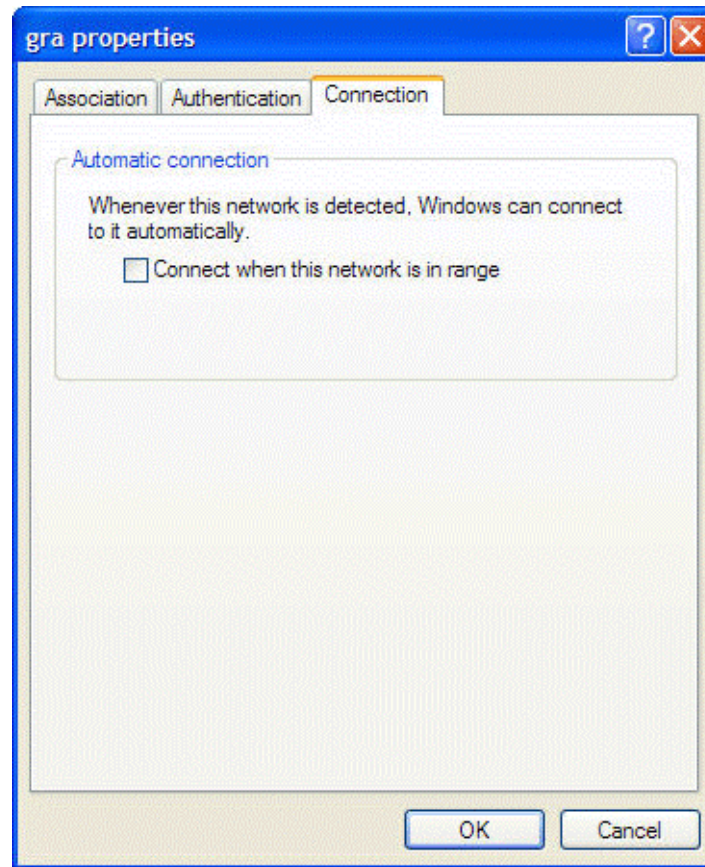
XP Provides Text Identification



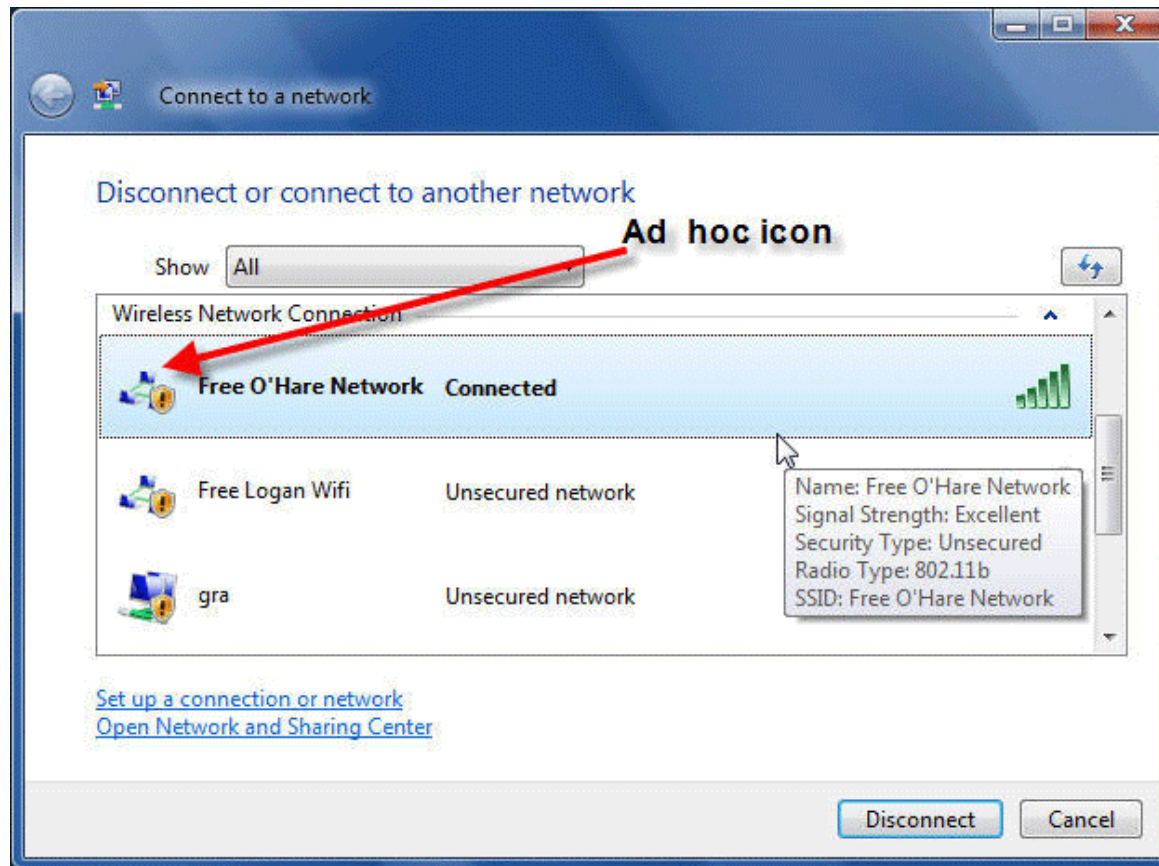
Set XP to only connect to infrastructure, not ad hoc



Be careful about setting to automatically connect



Vista Shows Only Icon



Acknowledgements

- Wikipedia (entries include 802.11, SSID, WEP, Wi-Fi Protected Access, VPN) Sept. 2007
- About.com: Improving network security, VPN
- Webopedia.com: SSID
- tech-faq.com: SSID
- networkworld.com: SSID
- Preston Gralla - Computerworld.com, Jan. 2007: Man in the middle attack / prevention