Wireless Networks

Geof Goodrum, *ggoodrum@bigfoot.com*
Washington Area Computer User Group, *http://www.wacug.org/*
18 September 2004

Glossary

802.11a - Wireless Network standard using unlicensed 5 GHz frequency spectrum with a maximum data rate of 54 Mbps.

802.11b - Wireless Network standard using unlicensed 2.4 GHz frequency spectrum with a maximum data rate of 11 Mbps.

802.11g - Wireless Network standard using unlicensed 2.4 GHz frequency spectrum with a maximum data rate of 54 Mbps; backwards compatible with 802.11b devices.

access point (AP) - a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network (LAN).

ad-hoc mode - An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point.

authentication - The verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter.

BlueTooth® - a wireless technology using the 2.4 GHz frequency spectrum with a data rate of 1 Mbps, designed to replace cables in a Wireless Personal Area Network (WPAN). Registered trademark of the BlueTooth Special Interest Group. Also known as IEEE Std 802.15.1.

community network - a not-for-profit Wireless LAN (WLAN) for public Internet access.

DMZ - Demilitarized Zone, an untrusted network outside a firewall.

hot spot - a public (not necessarily free) access point.

infrastructure mode - An 802.11 networking framework in which devices communicate with each other by first going through an Access Point (AP).

MAC address - Media Access Control identification number unique to a network device. The first three bytes contain a manufacturer code administrated by the IEEE, the last three bytes contain a unique station ID assigned by the manufacturer.

NIC - Network Interface Card

SSID - Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to an access point.

VPN - Virtual Private Network. A VPN allows data to be transported securely across a public network (e.g. the Internet).

wardriving - the act of searching for open access points while mobile.

warspamming - the act of using an open access point to send Unsolicited Commercial E-mail.

warchalking - the act of marking a building to indicate an open access point.

WEP - Wired Equivalent Privacy, a flawed security protocol for WLANs defined in the 802.11b standard. "Unsafe at any key size." Deprecated in favor of WPA.

Wi-Fi® - meaning "Wireless Fidelity", Wi-Fi is a registered trademark of the Wi-Fi Alliance and is used to refer to wireless devices and services. Any products tested and approved as 'Wi-Fi CERTIFIED' by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers.

Wi-Fi Alliance - a nonprofit international association formed in 1999 to certify interoperability of WLAN products based on IEEE 802.11 specification.

WiMAX - The name commonly given to the IEEE 802.16 specification for fixed broadband wireless Metropolitan Access Networks (MANs) that use a point-to-multipoint architecture. The standard defines the use of bandwidth between the licensed 10GHz and 66GHz and between the 2GHZ and 11GHz (licensed and unlicensed) frequency ranges with a range up to 30 miles.

WPA - Wi-Fi Protected Access implements the IEEE 802.1X standard and the Extensible Authentication Protocol (EAP). The combined framework uses a centralized authentication server which allows WPA to provide a secure authentication to the wireless network by authenticating each user prior to joining. Subject to Denial of Service attack.

WPA2 - Second generation of WPA with support for the Advanced Encryption Standard (AES).

Is Wireless for You?

Yes, if you need freedom of movement with networked devices (e.g. notebook PCs, PDAs) or to access a community wireless network.

Maybe, if you need to network devices in an existing structure where running cable is costly. Alternatives include phone line and powerline networking (HomePlug).

No, if you require secure network communications, or want to network devices in a single room (Ethernet is faster and cheaper).

Equipment

For a typical home installation sharing a DSL or Cable Internet connection, a wireless router ($70-110). Desktop PCs need a wireless NIC ($60, if supported by OS). Notebooks/laptops need a wireless PC Card ($50-70). Handhelds need a Compact Flash wireless card ($70). Game consoles or OS without drivers for wireless NIC need a wireless Ethernet bridge ($75).

802.11b is sufficient for home Internet access (11 Mbps exceeds DSL and Cable bandwidth); 802.11g is recommended for large bandwidth applications (e.g. video streaming) on-site or when Internet gateway is faster than 10 Mbps.

Homes or businesses that already have a wired router may use an access point ($75). To extend range, space access point devices across a wired network, or use a directional antenna ($210).

Range vs Rate

Data rate diminishes with distance. Range is ~300' indoors and ~800' outdoors. Each wall or ceiling reduces range 1 to 30m, depending upon angle and material. Directional antennas can extend outdoor range to 3+ miles.

Public Wireless Networks

Community wireless networks offer free or low-cost Internet access. Creating your own freenet may violate DSL/Cable Terms of Service/Acceptable Use Policy; a leased line (T1, 1.54 Mbps) is often required (~$650/month).

Public hot spots at coffee shops, airport lounges, etc. may be free or fee based. T-Mobile HotSpot service (e.g., at Starbucks, Borders Books) Unlimited National Annual plan is $29.99/month.

Do

* Change default AP/router password.
* Enable MAC address filtering.
* Use VPN for wireless connections, if possible.
* Change WEP key periodically, if applicable.
* Watch for vendor firmware upgrades.
* Monitor network for unusual activity.
* Place AP in DMZ, if possible.
* Minimize wireless network exposure beyond property.
* Check router configuration with ShieldsUp! (*http: //www.grc.com/*).

Don't

* Attach AP to a network hub.
* Enable SSID broadcast.

Web Sites

http: //standards.ieee.org/wireless/ - Technical information on IEEE wireless standards.

http: //www.bluetooth.com/ - The official BlueTooth wireless information site.

http: //www.wifialliance.org/ - The official WiFi Alliance web site, list of Wi-Fi CERTIFIED products.

http: //wi-fiplanet.com/ - General interest site with articles, tutorials, glossary, "hot spot" search engine.

http: //www.freenetworks.org/ - a voluntary cooperative association dedicated to education, collaboration, and advocacy of the creation of free digital network infrastructures.

http: //www.wififreespot.com/ - List of free wireless hot spots.

http: //airdefense.net/ - Commercial wireless security solutions vendor, white papers, training.