Western Kentucky University

Wireless Network Policy

Network Computing and Communications

Approved by the Administrative Council
April 18, 2005

Western Kentucky University Wireless Network Policy
Network Computing and Communications

1.0 Purpose

This document sets forth the guidelines for using wireless network technologies at Western Kentucky University. The information contained herein describes how wireless technologies are to be implemented, administered and supported at all University sites. The primary goals of this policy are to:

1) Describe the requirements of the centrally managed WKU wireless network infrastructure.

2) Encourage the safe and secure use of a shared wireless communications infrastructure that can meet the communications needs of the faculty, staff and students at the University.

Computer, network, and wireless technologies are continually evolving, and so are the security issues that threaten the privacy of information transported across the network. In order to adapt to these new conditions, Network Computing and Communications will periodically review and update these requirements, policies, and procedures as required to help protect information and ensure the ongoing operation and security of both the network and attached services.

2.0 Technical References

Due to the nature of wireless networks, it is inevitable that any discussion of this topic will contain references to terms and acronyms that may be unfamiliar to many readers. Because of this, please refer to section **8.0 Definitions** for descriptions of technical terms used in this document.

3.0 Technology

The WKU wireless network infrastructure is based on the 802.11g networking standard and uses strategically placed access points to provide connectivity to the campus network. 802.11b connections are also supported because of the backward compatibility of the 802.11g standard.

802.11b WLANs (Wireless LANs) provide a theoretical 11 Mbps[1] of bandwidth, operate in the unlicensed 2.4 GHz frequency range, and conform to the IEEE 802.11 DSSS (Direct Sequence Spread Spectrum) specification. Wireless devices that use the same 2.4 GHz frequency band, as well as certain other devices that may create harmonic disturbances in this frequency range, have the potential to interfere with and disrupt the operation of Western's wireless network services. Examples of these devices include cordless/wireless phones, wireless keyboards and mice, wireless headphones and audio speakers, microwave ovens, fluorescent lights, and other WLAN devices, including Bluetooth and earlier versions of 802.11. 802.11b is currently the most prevalent 802.11 wireless implementation.

802.11g WLANs provide a theoretical 54 Mbps[1] of bandwidth, also operate in the unlicensed 2.4 GHz frequency range, and can interoperate with 802.11b equipment at data rates of 11 Mbps and below. The range of 802.11g is somewhat less than that of 802.11b, and it is susceptible to the same types of interference as 802.11b.

The only protocol supported on the WKU wireless network connection is IP.

For University owned equipment, the recommended wireless PC cards include the Cisco Aironet 802.11b/g wireless LAN client adapter, as well as the built-in wireless adapters included in any of the University supported notebook systems. Other adapters that are fully 802.11g/b compliant may also work, but compatibility cannot be assured since there could be unanticipated configuration issues, and performance may not be optimal.

4.0 Security

An authentication process must be completed in order to gain access to the WKU wireless network. This process does not currently involve any special client software, but only requires the use of a browser supporting SSL (Secure Socket Layer) connections, and a valid WKU e-mail account and password for authentication.

Although 802.11g/b supports an encryption standard known as WEP (Wired Equivalent Privacy), this method of encryption has not been implemented due to known security

[1] Note the maximum practical throughput will typically be about half of the theoretical maximum.

weaknesses and potential issues when configuring the client wireless device. Because of this, the security of all sensitive transmitted data must be provided by the application, which is typically done through the use of SSL (Secure Socket Layer), SSH (Secure Shell) or a VPN (Virtual Private Network) connection.

Additionally, information transported across a wireless network of any kind is not constrained by the location of communications cabling, but can be accessed well beyond the physical limits of a traditionally wired network. Similarly, due to the unbounded coverage area of radio signals, access to an otherwise secure network can be unintentionally provided to unauthorized persons.

Because of the weak security of wireless LANs, applications that use encryption, such as SSL-based secure websites, should always be used when transferring sensitive or private information.

Western IT services such as e-mail, Webmail, Topnet, and select other systems provide the capability for encrypted connections.

It is imperative to understand that data transmitted and received over a wireless connection which is not encrypted using one of the above listed methods, will generally be in clear text, un-secure, and potentially available for viewing by others.

5.0 Requirements

Minimum requirements for support using the WKU wireless network are as follows:

Hardware: Supported computer or PDA with 802.11g/b wireless network card. This includes University systems purchased from the Network Computing web site, and student provided systems meeting the minimum ResNet requirements.

Operating System: Windows XP, Macintosh OS X, Windows Mobile 2003, or later versions with up-to-date security patches applied. Palm OS supporting 802.11g/b wireless network adapter.

Browser: Mozilla 1.6, Firefox 1.0, Internet Explorer 5.5, or later versions. Internet standards compliant browser for handheld devices.

Security: Windows XP firewall (or equivalent); Symantec Anti-Virus (or equivalent) with up-to-date virus definitions.

6.0 General Policy

The WKU wireless network provides access to many of the same resources and services as the campus wired network, and is therefore subject to the same policies of acceptable use and rules of operation as Western's wired network. However, due to the nature of wireless networks, additional security and control mechanisms are needed in order to maintain the security, operation and inter-operability of both traditional and wireless systems. The following policies have been developed to prevent interference between wireless devices, provide security for campus network systems, and to maintain an acceptable quality of service for all users.

1. The WKU wireless network is a centrally funded initiative of Information Technology and is being deployed campus wide beginning in the Spring of 2005. A deployment schedule and additional information about the project can be found at http://www.wku.edu/wireless.

2. Wireless Access Points or other wireless networking equipment may not be installed, operated, or used to extend access to any University wired network without the express written permission of Network Computing and Communications.

3. To accommodate departments that may be using non-IT provided wireless equipment, and as a proactive measure to eliminate potential interference and address possible security concerns, Network Computing and Communications will work with the department to replace existing wireless equipment with the University provided wireless network service prior to the scheduled deployment for the building. This accommodation will only be made for wireless equipment in operation prior to March 1, 2005.

4. Academic departments with an instructional requirement for wireless technology will be accommodated by working with Network Computing and Communications to develop a solution that will not interfere with the operation of the WKU wireless network.

5. In the event an on-campus unit or Western affiliate has an urgent requirement to provide or use wireless network technology in advance of the deployment schedule, Network Computing and Communications will work with the unit to see what can be accomplished.

6. Network Computing and Communications is the sole provider for all network-side equipment, specifications, design, installation, operation, maintenance and management of wireless networking services on property owned or serviced by the University. This includes, but is not limited to, all network switches, routers, access points, and gateway devices.

7. Acquisition and maintenance costs of client access devices, such as wireless network cards or wireless notebook computers, are the responsibility of the department or individual desiring to use WKU wireless network services.

8. Access to the network facilities at Western Kentucky University are made available to all faculty, staff and students of the University. By connecting to the network and using any of the available services, a user agrees to abide by all applicable rules and conditions.

9. To ensure radio frequency integrity and proper operation of equipment, a wireless site survey must be performed under the direction of Network Computing and Communications prior to the installation or use of any wireless networking equipment. Additional testing and analysis may also be requested for operational systems to resolve performance or interference related problems.

10. All installations of wireless equipment must comply with Federal, State and Local health, safety, building and fire codes, along with all applicable Western Kentucky University standards.

11. Current wireless network technologies only provide a limited amount of available bandwidth that must be shared between all concurrent users. Because of this, certain activities, such as large file transfers, will tend to reduce overall network performance and should be avoided. In general, applications placing a high demand on network resources will operate more slowly over a wireless network than when using a wired network connection. The WKU wireless network should not be considered as a substitute for a wired network connection, but rather it should be viewed as a supplement.

12. No device acting as a server may be used on the WKU wireless network without permission from Network Computing and Communications.

13. All Access Points and wireless client adapters will use an SSID maintained and provided by Network Computing and Communications.

14. All wireless equipment shall communicate through an Access Point and operate in Infrastructure mode. The operation of Ad-Hoc wireless networks is not permitted due to interference concerns with infrastructure mode access points.

15. IP addresses for networking devices, including wireless devices, will be assigned and maintained by Network Computing and Communications.

16. Wireless Access Points shall be fully manageable and will not be configured to provide specialized services such as DHCP, DNS, NAT, or other restricted services, unless deemed necessary by Network Computing and Communications.

17. Any wireless networking equipment not fully meeting the criteria listed in this document must be removed from service.

18. Only the IP protocol will be supported on the WKU wireless network.

19. Secure user authentication is required to access the WKU wireless network. The required authentication credentials consist of a valid WKU username and password.

20. Network applications, services, functions, and resources which are not required as part of the normal and approved operation of the University, may be bandwidth limited or blocked by network control devices.

21. Network Computing and Communications may suspend network access to any location or system that interferes with or disrupts normal network operations. If a determination is made that a specific piece of equipment may (or does) interfere with the operation of the WKU wireless network, Network Computing will work with the equipment owner to resolve the issue. In the event of a confirmed interference issue that cannot be resolved, the resolution will be to remove the equipment that is not part of the WKU wireless network, unless the equipment in question is life safety equipment.

22. "Hacking" activities such as those used to attempt to gain access to systems or information to which access permission has not been explicitly granted, is expressly prohibited. This includes, but is not limited to, unauthorized ping sweeps, port scans, network sniffing, and IP address spoofing.

23. The use of any packet capturing or network monitoring software or device by non Network Computing personnel is strictly prohibited.

7.0 Enforcement

Violations of this or other relevant Network Usage or Acceptable Use Policies may be reported by sending e-mail to abuse@wku.edu, or by contacting the Department of Network Computing and Communications at 270-745-7000. Network Computing and Communications performs routine network performance monitoring and will investigate all suspected policy infractions regardless of their source. In the event that evidence of a violation is found, Network Computing and Communications reserves the right to take actions necessary to protect the integrity of the network.

8.0 Definitions

For the purposes of this document, the following definitions shall apply.

802.11 -- Refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

802.11a -- An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an OFDM (Orthogonal Frequency Division Multiplexing) modulation scheme rather than DSSS (Direct Sequence Spread Spectrum).

802.11b -- An extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS (Direct Sequence Spread Spectrum).

802.11g -- Applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band using an OFDM modulation scheme.

Access Point -- A piece of wireless communications hardware, which creates a central point of wireless connectivity. Similar in function to standard wired “hubs”, access points are shared bandwidth devices that can be connected to the wired network, thus allowing wireless access to the campus network.

Ad-Hoc wireless network -- A wireless network between two or more wireless capable devices (normally PCs), where no wireless access point is involved.

Bandwidth -- The rate at which information travels through a network connection, usually measured in bits per second, kilobits (thousand bits) per second, or megabits (million bits) per second.

Bluetooth -- A short-range radio technology aimed at simplifying communications among mobile devices. It also aims to simplify data synchronization between Internet devices and other computers.

Coverage Area -- The geographical area where a usable level of wireless connection service quality is available.

DHCP – see Dynamic Host Configuration Protocol.

DNS – see Domain Name System.

Domain Name -- The unique name that identifies an Internet site. Domain names always have two or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A machine may have more than one domain name but a domain name points to only one machine.

Domain Name System -- An Internet service that translates domain names to or from IP addresses, which are the actual basis of addresses on the Internet.

DSSS -- Direct Sequence Spread Spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

Dynamic Host Configuration Protocol – A system by which IP addresses and other low-level network configuration information can be dynamically assigned to a computer each time the system boots.

Hacking -- Unauthorized use, or attempts to circumvent or bypass the security mechanisms of a computer system or network.

IEEE -- Abbreviation of Institute of Electrical and Electronics Engineers, an organization composed of engineers, scientists, and students. The IEEE is best known for developing standards for the computer and electronics industry, including the IEEE 802 standards for local-area networks.

Infrastructure Mode -- An 802.11 networking framework in which devices communicate with each other and a wired LAN by first going through an Access Point.

Interference -- Interference is the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless connection by introducing errors in the transmission, or completely eliminate it depending on the strength of the signal.

IP -- An abbreviation for Internet Protocol, the basic network transmission protocol of the Internet.

IP Address -- The numeric address of a computer on the Internet. An IP address is written as a set of four numbers separated by periods (each number can range from 0 to 255). An example of an IP address is 192.168.1.5.

IP Address Spoofing – A process by which a system attempts to impersonate another system by using its IP network address.

LAN – see Local Area Network.

Local Area Network -- A data communications network often consisting of host computers, personal computers and other equipment interconnected via twisted pair or fiber cables. LANs allow users to share information and computer resources. Typically a LAN is limited to a single organization, department or limited geographic area.

Mbps – An abbreviation for megabits per second. A measurement of the transmission speed of data measured in 1,048,576 bits per second.

NAT -- Network Address Translation. Used by a Firewall or Gateway to hide LAN IP addressing from devices on the other side of the firewall or gateway.

Network Sniffing -- A term used to describe the use of a "sniffer" program to monitor data traffic transported across a network.

OFDM -- Orthogonal Frequency Division Multiplexing. A modulation method used for certain types of wireless communications.

PDA – Personal Digital Assistant - A term used to describe computers small enough to fit in the palm of your hand.

Port Scan – A process often used by hackers to send a series of messages to a network attached device (i.e. a computer) in order to determine what services are running and to identify vulnerabilities that can be exploited to break into the system.

Protocol – A standardized set of rules used by the network and attached systems to control the flow of information between devices across a network.

Secure Shell – A packet-based binary protocol that provides encrypted connections to remote hosts or servers.

Secure Socket Layer -- A security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

SSH – see Secure Shell.

SSID -- Service Set IDentifier. A unique identifier that stations must use to be able to communicate with an access point.

SSL - see Secure Socket Layer.

Virtual Private Network -- A mechanism used to provide secure access to a private network over an otherwise insecure network connection, such as a wireless network or the Internet.

VPN – see Virtual Private Network.

WEP – see Wired Equivalent Privacy.

Wired Equivalent Privacy – A standard for encrypting data over an 802.11 wireless network using 40 or 128 bit encryption. This standard has been shown to be insecure and current recommendations are to use SSL or a VPN to protect sensitive data.

Wireless Network Infrastructure -- The wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Wireless Local Area Network -- A local area network that uses radio signals to transmit and receive data over distances of up to a few hundred feet.

WLAN – see Wireless Local Area Network.