Wireless Networking at Western Carolina University: A Planning Document

- Background and History -

Scott Swartzentruber

Introduction

Wireless LANs are continuing to grow in popularity, particularly in enterprise environments that require or desire a high level of mobility. In the education environment a number of colleges and universities have implemented wireless projects to provide enhanced mobility to their clientele and to extend their network into those areas that are not served well by traditional wired connections.

The first implementations of wireless at WCU have been in the area of research. This research has been primarily the study of the practical application of wireless LAN technology in an educational setting. A project designed to study the utility of handheld wireless devices in the classroom has seen the implementation of 15 wireless access points around campus in several academic and common spaces. A more recent implementation has been the installation of 24 access points in Belk building by the Engineering Technology department to study the utility of wireless devices including ruggedized handheld devices and cordless IP telephones.

Technology

Wireless networking is a rapidly changing technology. All users of wireless technology must be aware of the risks inherent in deploying cutting-edge technology. Complete functionality, adherence to standards, and interoperability are all areas in which wireless (or any other new technology) must be closely evaluated to insure a good return on the resources invested in their purchase and use

As is the case with many information technologies today, several wireless technologies exist that do not work together. The most common wireless technology standard in use today is IEEE 802.11b. This standard defines a wireless network using direct sequence-spread spectrum allocation of the 2.4 Ghz ISM band and provides an 11 Mb/s shared connection to the users. WCU's current wireless network is build to this standard and provides that greatest possible amount of interoperability available given today's technology.

Security

On the wired network WCU has been able to control access by limiting physical access to the wired network. Only those individuals associated with the university have access to a port on the network. The broadcast nature of wireless precludes using physical controls as a means of limiting network access with means other than distance.

Privacy on the wired network has been protected by the nature of how traffic flows in the network. Traffic that leaves one system is only seen by the intended recipient and can not easily be captured by a third party on the network. The broadcast nature of the wireless network means that any traffic sent on the wireless network can be easily captured by a third party.

Limited security features built-in to the wireless standard are not sufficient to control access or ensure an equivalent level of security. At this point WCU has implemented rudimentary access control by requiring all

wireless network users to register their devices. There is currently no privacy capability on the WCU wireless network. Some capabilities do exist in the market but none of them are applicable to all of the devices that we are currently using on the wireless network.

Spectrum

The frequency that is used for the 802.11b wireless LAN is the FCC defined 2.4 Ghz Industrial/Scientific/Medical (ISM) band. Other wireless technologies use a similar FCC defined band in the 5 Ghz range. It's important to note that this is a shared bandwidth with many other wireless devices (cordless phones and keyboards for example) using these same frequencies.

Wireless Networking at Western Carolina University: A Planning Document

– Positions and Policies -

Controlled deployment

- Understand that wireless LAN technology is an enhancement to, not a replacement of, the wired network.
- All wireless devices are considered to be network attached devices and their use is governed by WCU's policy #52 – *Acceptable use of Computers and Data Communications*.
- Focus future deployment efforts on those areas that would enhance desired mobility or those areas not easily connected via a wired network.
- The Computer Center will provide consulting for those campus organizations contemplating wireless LAN implementations.
- All infrastructure wireless devices will be managed and serviced by the Computer Center.
- No deployment or purchase of wireless LAN devices without approval of the CIO or designee.

Academic use

- It is understood that certain departments will need to use wireless devices in an academic setting to educate students on the technology used.
- Academic use of wireless devices (i.e. the use of wireless devices to enhance the education of wireless technology) will take place in a controlled environment in coordination with the Computer Center.
- Channels, frequencies, access controls, and other settings will be agreed upon by both the academic department and the Computer Center prior to deploying wireless units for academic use.
- Ongoing management and maintenance of wireless equipment being used for academic purposes is the responsibility of the department using it.

Protect bandwidth

- The ISM bands in the 2.4Ghz and 5Ghz range are reserved exclusively for wireless network use. Other devices operating in these ranges (e.g. cordless phones, cordless keyboards) can cause significant interference and are not to be used on the WCU campus.
- If another device causes interference with the wireless LAN, Computer Center staff will work with the device owners to help eliminate or mitigate interference. If the interference can not be mitigated or eliminated, priority will be given to wireless LAN access vs. other intended or accidental uses of the frequencies.

Insure interoperability

- Standardize on a single vendor for access points.
- Standardize on a limited number of wireless cards for Computer Center staff to provide support on.
- Once a list of current approved products is created it will be available by contacting the help-desk.

Secure Network

- No sensitive traffic on the wireless network until security safeguards are put in place. In this case sensitive traffic is defined as any traffic carrying data subject to FERPA, HIPPA, or any other federal, state, or local regulations limiting access to such data.
- Access controls will be put in place to block non-secure access to local systems that contain sensitive data.
- Access controls will be put in place to limit utilization of the wireless network to only authorized individuals.
- Embrace goal of user centric authentication with all sensitive traffic protected with a single strong encryption method (e.g. 802.1x, VPN, WPA, etc…).
- Implemented security methods will, at a minimum, protect sensitive data to the extent required by the regulation that calls for their protection (e.g. FERPA for student data, HIPPA for medical data, etc…)
- Devices that can not participate fully in the established security scheme will not have access to sensitive data.
- All access and security controls will be approved by the CIO or designee.

Future Scalability

- Ensure selected vendors have plans to support future wireless standards and technologies.
- Deploy wireless access points in such a way as to make best long-term use of wireless capabilities.

Exceptions

- Exceptions to these policies will be addressed on a case-by-case basis by the CIO or designee.