WESTERN
WASHINGTON UNIVERSITY

TELECOMMUNICATIONS SERVICES

Date: February 12, 2003

Latest Issue: April 23, 2007

WIRELESS ETHERNET IMPLEMENTATION AND USE GUIDELINES

Wireless Ethernet technology has evolved quickly into a useful and widely embraced network option. The Telecommunications Services Department (Telecom) actively supports the use of wireless Ethernet. To ensure integrity and security of the network in the shared wireless environment, Telecom has developed guidelines to manage wireless Ethernet use on campus.

In order to establish a university-wide wireless environment, a variety of factors need to be considered. For instance, radio frequency (RF) channel allocations, device placement, access point configuration, and non-related sources of RF, all have the potential to disrupt critical campus wireless networking services. Compliance with the guidelines below will reduce network problems and provide for a robust and reliable service.

1. **IEEE Standards:** – Although at this time IEEE 802.11b/g has become the *de facto* wireless Standard on the Western Washington University campus, any 802.11 Standards that exist or are under development will be considered for future use on campus and are included under the scope of the managed campus wireless service. The 802.11b/g Standard uses Direct Sequence frequency patterns in the 2.4 GHz bandwidth. It can provide up to 11 MB (b) or 54MB (g) of shared bandwidth per access point. At this time the University has installed products utilizing the 802.11b and 802.11g Standards in areas as indicated on the wireless coverage map available at the Telecommunications Web Page: http://www.acadweb.wwu.edu/telecom/

2. **Guidelines for Frequency Use:** – The 2.4 GHz radio frequency used by the 802.11b/g wireless standard is an unlicensed shared spectrum band. Products using the same frequency, such as microwave ovens and cordless telephones, have the potential of causing network interference. In addition, there are limited non-overlapping channels in the 802.11b/g specifications. Access points can interfere with each other if not administered properly.

3. **Campus Wireless Service:** – Telecom is responsible for wireless service on campus and will manage the shared use of current and future radio frequencies under IEEE Standards for the campus community. Telecom will resolve interference issues as they arise.

4. **Infrastructure Requirements:** – An active line-powered data port and Ethernet service are required for each access point. Access point locations will be designed and installed by Telecom for strategic placement to achieve efficient and effective coverage and avoid conflicts with other devices (e.g., cordless telephones, microwave ovens, scientific equipment operating in the same frequency ranges).

5. **Public Intrabuilding or Interbuilding spaces:** As funding becomes available, Telecom will provide and expand wireless access coverage in suitable public areas around campus including lounges, lobbies, corridors, general-purpose classrooms, and outside spaces.

6. **Departmental Spaces:** Because wireless signals typically extend beyond individual spaces, departments that wish to implement wireless services for their assigned spaces must coordinate

with Telecom for design and installation. As a general rule, departments will be able to use the university wireless system for their needs. Telecom will work with the department to develop a physical design that will be responsive to departmental requirements and consistent with the university network. The services provided by Telecom include:

a. RF engineering for optimal placement of access points and to identify other devices operating in the same frequency range.

b. Installation, activation and testing of access point in compliance with campus standards.

c. Technical support, ongoing maintenance and software upgrades.

Services, including estimates, may be requested by completing the Data Service Request Form available on the Telecommunications Web Page, or by calling Telecommunications at ext. 3600.

If the needs of the department require a wireless system that is separate from the university system, Telecom will work with the department to design and install an appropriate system. Funding and on-going support for department-specific systems will typically be provided by the department.

7. **Wireless Ethernet Cards, Faculty and Staff:** – Users or departments will be responsible for purchasing wireless Ethernet cards that meet the University's Standards for 802.11b/g wireless Ethernet cards. ("PC Cards" or "PCMCIA Cards" in accordance with the standards created by the Personal Computer Memory Card International Association.) PC Cards may be purchased from the Campus Bookstore or private vendors. Ethernet cards that do not meet the University Standards may limit user access features.

8. **Wireless Ethernet Cards, Students:** – Students will be responsible for purchasing wireless Ethernet cards. Unless special access to University servers is required (and authorized), these cards need not meet the University's Standards. Ethernet cards may be purchased from the Campus Bookstore or private vendors. Ethernet cards that do not meet the University Standards may not provide the best possible security* and may limit the user on access and/or features of the wireless network.

9. **Security*:** –Telecom will be responsible for establishing security policy for wireless communications based on current best practice. All wireless network use must comply with established security policies including campus-wide IP addressing and DHCP services.

10. **Experimentation with new wireless technologies –** In order to prevent signal interference, departments wishing to test and/or implement new technologies must coordinate with Telecom as described in paragraph 6, above. Telecom will work with the department to develop a testing plan that will avoid problems in this regard.

11. **Wired Equivalent Privacy (WEP) –** 802.11b/g standard supports encryption security protocols such as WEP (Wired Equivalent Privacy), and others. WEP is currently not activated on the University's AP's.

***Note:** Wireless service networks are not inherently secure. It is the user's responsibility to adopt appropriate security measures while using WWU's wireless network.