



802.11 Wireless Local Area Network Standards for the University of Georgia

Network Infrastructure and Services
Enterprise Information Technology Services
The University of Georgia

Updated March 11, 2011

1. INTRODUCTION

- 1.1. This document specifies the wireless local area network (WLAN) standards for the University of Georgia for IEEE 802.11 PAWS wireless systems. These standards apply to installation and use of all WLAN systems connected to the PAWS network which are installed on the campuses of the University of Georgia or any remote locations directly connected to the campus network.
- 1.2. Only hardware and software consistent with these standards shall be used in conjunction with the PAWS wireless network.
- 1.3. New plans for buildings and gathering areas shall consider the need for and use of wireless networking, similar to the planning done currently for wired networking.

2. PURPOSE

- 2.1. A coordinated, centralized delivery of wireless networking services is essential to provide a successful wireless service. Our goal is to provide a common user experience across campus, efficiently support users, protect network resources, and provide a quality service. This coordinated effort is best handled by the University of Georgia's Enterprise Information Technology Services (EITS). To this end, EITS shall be solely responsible for the deployment and management of IEEE 802.11 and related access points at UGA. No other departments shall deploy IEEE 802.11 or related access points without coordination and approval by EITS.
- 2.2. The purpose of these standards is to assure students, faculty, and staff access to a reliable, robust, and integrated wireless network and to increase security of the campus wireless network to the extent possible.
- 2.3. EITS establishes and maintains wireless data standards to prevent interference and to ensure vendor interoperability. EITS will respond to reports of interference and reserves the right to restrict the use of wireless devices in University-owned and leased buildings and all outdoor spaces as necessary to ensure reliability of the campus wireless network.
- 2.4. EITS reserves the right to deploy wireless networking equipment as a part of a campus-wide wireless service in UGA owned and leased spaces. This may require the removal of non-EITS equipment.

3. SUITABILITY

- 3.1. Wireless networks are not a replacement for a wired network. All new and renovated buildings shall have wired data and voice networks as required by the University of Georgia cabling standards. Wireless systems offer a different type of service from wired service with respect to reliability, available bandwidth, security, and portability. Wireless service is an extension of the wired network for general-purpose network needs. It enables applications that require the mobility offered by wireless, but which do not require the bandwidth, reliability, or security of wired connections.
- 3.2. Wireless bandwidth availability is more limited than wired bandwidth and is shared among users in an area. As the number of users in an area increase, the available bandwidth to the end user decreases. So wireless is less appropriate in areas of high user density, especially if high bandwidth applications are a requirement.

4. FREQUENCY USE

- 4.1. The 2.4 GHz radio frequency used by 802.11b and 802.11g is an unlicensed shared spectrum band. The 5 GHz radio frequency is another unlicensed shared spectrum which is used by 802.11a access points. 802.11n radios may use either one of these frequency ranges. In addition, there are only three non-overlapping channels within the 802.11b and 802.11g specifications.
- 4.2. Consequently, access points can interfere with each other and other communications devices or appliances if not administered or deployed properly. Microwave ovens and cordless phones are prominent examples.
- 4.3. EITS will manage the shared use of unlicensed radio frequencies for the campus community and has campus authority to resolve interference issues.

5. RESPONSIBILITY AND ENFORCEMENT

- 5.1. EITS is responsible for implementation of wireless technology, enforcing campus network standards, and has the authority to resolve frequency interference issues.
- 5.2. All users connecting to the campus network will gain access through their UGA MyID which determines the identity of and authenticates the user.

6. PERSONAL WIRELESS ACCESS POINTS

- 6.1. Setting up personal wireless access points attached to the campus network (including the residence halls) is prohibited.
- 6.2. Personal wireless access points do not provide the ability to require UGA MyID authentication which is required by UGA standards.
- 6.3. Wireless technology is highly sensitive to overlapping frequencies; therefore, its deployment must be carefully planned.
- 6.4. In addition, access points can act as routers or DHCP servers if configured improperly, which can disrupt service to other network users.

7. DEPARTMENTAL WIRELESS SERVICE

- 7.1. Departments can provide wireless service within buildings in locally controlled areas. Any access point departmentally purchased and/or connected to the campus network shall meet the campus wireless standards outlined in this document.
- 7.2. Departmentally owned access points shall be part of the centralized PAWS network and be managed and maintained by EITS.
- 7.3. Prior to purchase or deployment, EITS shall be consulted and will be responsible for approving and overseeing the design, planning, installation, and configuration.

8. AUTHENTICATION

- 8.1. Access to wireless network connectivity is limited to authenticated users (users whose identity has been verified).
- 8.2. Wireless access requires secure UGA MyID authentication or some other secure method approved by EITS that uniquely identifies the individual connecting.

8.3. MAC authentication is prohibited.

9. GUIDELINES FOR BEST PRACTICE

- 9.1. Wireless access points installed in public spaces, classrooms, etc. shall be securely mounted (and locked) or in places not easily accessible by the public.
- 9.2. Access points installed in private places shall be secured like other computing equipment.
- 9.3. Only connect access points to an Ethernet switch. Hubs shall not be used in wireless networking.
- 9.4. Use of 100 Mbps Ethernet is sufficient when connecting 802.11g and 802.11a access points to the campus network. Use of 1000 Mbps Ethernet when connecting 802.11n access points to the campus network is recommended.

10. ALLOWED ACCESS POINTS

- 10.1. Any Cisco LWAPP access points are compatible with the centralized PAWS system and shall be the only access points deployed on campus.

11. REQUIREMENTS

- 11.1. All end-user devices or systems connecting to the campus network must comply with the same policies, procedures, and practices governing the use and operation of any end user device or system connecting to the campus wired network.
- 11.2. No WLAN may be placed into operation without advance consultation and approval with EITS.
- 11.3. All WLAN access point purchases shall be coordinated through EITS.
- 11.4. All WLANs will be operated in such a manner that they do not interfere with other WLANs or the UGA enterprise wired data network.
- 11.5. All wireless network access shall utilize the enterprise authentication and authorization mechanisms prescribed by EITS.
- 11.6. Wireless networking equipment not installed by EITS can be removed if it interferes with EITS wireless equipment, is insecure, or causes other network services to be impaired.

12. DEPARTMENTAL RESPONSIBILITIES

- 12.1. Departments shall request installation, repair, replacement, or the move of an existing access point from EITS.
- 12.2. Departments will be responsible for all costs associated with installation, repair, or replacement of its access points (exclusive of access points provided by Student Technology Fees).

13. EITS REPONSIBILITIES

- 13.1. EITS is responsible for establishing and maintaining standards for IEEE 802.11 wireless access points (equipment and installation) for use for the University of Georgia.
- 13.2. All WLAN systems shall be installed, configured, and managed by EITS.
- 13.3. EITS will maintain a database of access points, their locations, the frequencies in use, and the name(s) of the department's designated Departmental Network Liaison.

- 13.4. EITS will attempt to resolve frequency coordination problems between WLAN owners. However, EITS cannot guarantee interference-free operation of any WLAN from other unknown or non-university owned WLAN systems or from other devices operating in the same spectrum as the WLAN.