EITS

Last Modified: 10/20/15

Wireless Network Standard

Purpose

The standard and guidelines described in this document will ensure the uniformity of wireless network access points at the University of Georgia. These apply to all wireless networks at the University.

Development of the Wireless Network Standard

Wireless networking equipment is available that supports varying levels of industry communication standards. At present, the IEEE 802.11b/g/n/ac standard is widely accepted throughout the industry and provides the necessary balance of range, network throughput, and support for device mobility to effectively serve most needs of the University community. As newer standards emerge, such as IEEE 802.11enhancements, they will be evaluated and deployed should they offer security and throughput improvements over 802.11b/g/n/ac.

It is the University's goal to offer and maintain stable and reliable services for the benefit of the University community in the most cost effective manner for the institution. EITS will continue to evaluate available wireless network industry standards and equipment to ensure the University meets this goal.

Definitions

Wireless Access Point

A wireless communications hardware device that creates a central point of wireless connectivity. A wireless access point behaves much like a "hub" in that the total bandwidth is shared among all users for which the device is maintaining an active network connection.

Wireless Port

A network port that has been installed for the purpose of connecting a wireless access point to the University's wired network. Wireless ports provide both data and power service to the wireless access point.

Wireless client software or built in 802.1x supplicant

EITS provides client software client that allows for a computer to utilize 802.1x authentication to the University’s wireless networks. Some operating systems have built-in support for 802.1x and can be used for accessing the University's networks. The University provided client software will be preconfigured to support the specific setup for paws-secure.

Coverage Area

The geographical area in which an acceptable level of wireless connection service quality is attainable. Coverage areas for similar devices can vary significantly due to the presence of building materials, interference, obstructions, and access point placement.

Interference

Degradation of a wireless communication radio signal caused by electromagnetic radiation from another source, including other wireless access points, cellular telephones, microwave ovens, medical and research equipment, and other devices that generate radio signals. Interference can either degrade a wireless transmission or completely eliminate it entirely depending on the strength of the signal generated by the offending device.

Privacy

The condition that is achieved by successfully maintaining the confidentiality of personal, student, employee, and or patient information transmitted over a wireless network.

Security

Security is particularly important in wireless networks because data is transmitted using radio signals that, without implementation of specific data encryption mechanisms, can easily be intercepted.

Wireless Network Infrastructure

The collection of all wireless access points, antennas, network cabling, power, ports, hardware, and software associated with the deployment of a wireless communication network.

Wired Equivalent Privacy (WEP)

A security protocol for wireless networks defined within the 802.11b standard. WEP is designed to provide the same level of security as that of a wired network. Recent reports indicate that the use of WEP alone is insufficient to ensure privacy unless used in conjunction with other mechanisms for data encryption.

WPA

Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. This technology features improved data encryption through the temporal key integrity protocol (TKIP) and user authentication through the extensible authentication protocol (EAP), PEAP – MSChapV2.

802.1x

This standard enhances the security of local area networks by providing an authentication framework allowing users to authenticate to a central authority, such as LDAP or Active Directory. In conjunction with 802.11 access technologies, it provides an effective mechanism for controlling access to the wireless local area network.

Infrastructure Mode

The operating mode for wireless networks in which each end user device is configured to associate with a wireless network access point through which network services are accessed.

Ad hoc Mode

The operating mode for wireless service in which end user devices interact with each other in a "peer- to-peer" configuration. Ad hoc mode does not require the use of a wireless network access point.

Utilization

Prior to the installation of any wireless devices, EITS will review the usage requirements for the area in question to determine the optimum number of wireless access points needed to efficiently support all users in the area simultaneously. Space configuration, construction materials, anticipated number of end users devices to be served, and potential sources of RF interference will be taken into consideration when conducting a site survey.

EITS will provide support for infrastructure mode installations only. These installations require at least one wireless access point. Ad hoc wireless mode will not be supported.

In order to prevent problems caused by radio interference, to ensure the integrity of University resources, and to ensure the widest availability of reliable wireless networking services, the University shall remain the sole owner of all unlicensed spectrums of radio frequencies available for use on any of its campuses and related properties.

Wireless Networking Guidelines

Equipment

Integration of wireless network access points or other wireless communications equipment to University of Georgia network will only be performed by EITS.

University students, faculty, staff, and units may purchase the Wi-Fi certified wireless network interface adapters of their choice to connect end user devices to the University's wireless networks.

University units will be required to remove any wireless network infrastructure equipment (Wi-Fi routers, and bridges) not originally installed by EITS, and/or which were installed as a non-standard solution without written permission by the Chief Technology Officer.

Wireless network access points will be connected to the University's wired network by means of a specially designated wireless port that will be installed specifically for this purpose. University units and individuals may not disconnect a wireless access point from its associated wireless port or interfere with any components of the wireless AP assembly including antennas, antenna cables, or management cables. Wireless ports are specially configured to supply electrical power to the wireless access point and may cause permanent damage to an improperly connected end user device.

Wireless network installations at University locations consist of the necessary Wi-Fi certified wireless access point devices. The minimum number of access points required will be determined by initial estimates of demand for users and the size of the area to be covered. If the number of users to be served exceeds the practical number of users that can connect to single access point with sufficient bandwidth available to each user, additional access points may be installed contingent on budgetary approval. In areas with a high density of users, such as classrooms and lecture halls, additional access points will be installed to satisfy the usage requirements.

All wireless access point devices will be installed, and maintained by EITS. The primary funding source for initial and replacement purchases of wireless access point devices and services will be Student Technology Fee funds for academic areas and college/departmental budget funds for administrative/employee areas.

Network Reliability

In order to ensure the reliable performance of the University's network, EITS will investigate reports of specific wireless devices that are suspected of causing interference and performance problems in the same manner in which EITS investigates reports of specific devices connected to wired ports that are suspected of causing disruption. Although EITS will not actively monitor content carried on the University's wireless network radio frequencies when investigating reports of potentially interfering devices, wireless network detection equipment will be used to detect unauthorized wireless network equipment. Units will be required to remove any such equipment found in unit- controlled University space.

Wireless access service is provided on the basis of anticipated utilization data gathered during initial site surveys conducted by EITS. As the number of users increases, effective wireless network performance may be diminished.

Current industry standards for wireless network service do not provide sufficient throughput to effectively support bandwidth-intensive applications and network services. EITS prohibits the use of server-based applications (file, web, media servers) on the University’s wireless networks.

EITS will address problems encountered in the use of wireless network services according to the following priority list: academic, research, administrative, and staff use.

Security

Access to the University's wireless networks will require all authorized users in all areas to authenticate to the network using their assigned MyID username and password combinations or other approved authentication methods through the use of University provided wireless client software or 802.1x supplicant. Network access logs will be maintained containing the username, time of access, and duration of use for all users who access the network using wireless connections and this information and will be provided to authorized governmental authorities if the University is required to release such information, such as in the cases of criminal investigations.

Wireless technology deployed at the University of Georgia includes the use of WPA (Wi-Fi Protected Access), which provides improved data encryption through the temporal key integrity protocol (TKIP) and user authentication through the extensible authentication protocol (EAP). To provide additional security, all University wireless networks will require authentication of end users to the network upon connection of any wireless end user device using an 802.1x supplicant or provided wireless client software. Each user will be required to authenticate to the network using a valid MyID and password. The University's Central Directory Service will be used as the basis for authentication to services, including wireless network access.

University students, faculty, staff, and units must follow the terms of all applicable University acceptable use policies, network usage guidelines, and all applicable local, state, and federal regulations when using equipment connected to the University's network whether or not the individual is using wireless or wired network connections. Violations of such guidelines will be reported to the University's Office of Information Security and may be forwarded to the appropriate University or governmental authorities.

University students, faculty, staff, and units are reminded that the use of wireless network connections may increase the risk that confidential information can be intercepted by unauthorized or unintended parties and that this risk in inherent in wireless network technology irrespective of security measures that can be implemented by the University. Users should avoid sending or receiving confidential or other sensitive data via wireless connections whenever possible.

Wireless Usage

Some services can have a negative impact on a wireless network because they generate a high level of activity on the network. Such services can negatively affect your wireless network performance and the network performance of other wireless users. The wireless network is a shared resource, which means the bandwidth available to each user of an access point will decline as high-bandwidth services are used. If a student, faculty member, or staff member has a need for a service that requires high bandwidth, a wired network connection is recommended.

The following list provides examples of high bandwidth usage. Please note that this list is not all inclusive.

You cannot use the computer you have connected to the wireless network as a server of any kind, such as:

- Web servers
- Peer-to-peer file sharing servers
- FTP servers
- Multiplayer game servers

An unsecured computer may have problems that will also result in high bandwidth usage. Following are examples of possible problems:

- Infections by worms or viruses
- Compromised systems running ftp, IRC, or other services or malicious spyware programs

Some activities may also use excessive wireless bandwidth. Following are some examples of user activities that consume high amounts of bandwidth:

- Reinstalling an operating system
- Downloading and installing applications
- Performing system backups
- Transferring large files (images, video, music, databases) to other system

Airspace

Problems can occur if other devices use the same radio frequency range (2.4 GHz and 5 GHz) as the wireless network. Because of the potential for conflicts, it is important for all users to understand which technologies are permitted in our environment and which are not permitted.

In order to provide wireless network service at the highest level of quality, all non-client devices that use the 2.4 GHz and 5 GHz ranges should be removed from service in any University building. Only devices that are part of the University’s wireless networks will be permitted to use the 2.4 and/or 5 GHz ranges.

This includes any device that is used as a wireless base station or router, such as the Apple Airport Base Station, or any other wireless router. Cordless phones, cameras, and audio speakers that use the frequency band of 2.4 GHz or 5 GHz should also not be used in areas with wireless coverage.

If you think you have an existing system that may use 2.4 and/or 5 GHz radios for transmission, please contact the EITS Help Desk at (706) 542-3106 to determine if such devices will interfere with wireless network service in your area.

EITS Responsibilities

1. Development and maintenance of the wireless standard and wireless guidelines.
2. Installation and maintenance of all equipment supporting wireless network service at the University of Georgia.
3. Investigation and resolution of wireless communication interference problems.
4. Deployment, management, and configuration of wireless network access in academic areas, classrooms, and office areas.
5. Development and implementation of wireless network security protocols and practices.
6. Provision of user training on wireless network security issues and acceptable use of wireless network services.
7. Performance and security monitoring for all installed wireless access points and provision of performance statistics to University units upon request.
8. Monitoring of the development of wireless network technologies and evaluation of their potential use within the University's wireless infrastructure.
9. Responding to problems reported to the EITS Help Desk in accordance with standard procedures and levels of service.

Wireless User Responsibilities

1. Adherence to the wireless network standard and related guidelines and policies established by the University of Georgia.
2. Implementation of recommended security software, hardware settings, patches, and protocols on end user equipment used to access the University's wireless networks.
3. Following all relevant University policies and procedures along with federal, state, and local laws pertaining to the security of sensitive and confidential data when working with such data on the University's wireless networks.
4. Installation of wireless network interface adapters according to published instructions.
5. Assumption of responsibility for support and troubleshooting of problems when using wireless network interface adapters not supported by EITS.
6. Immediately reporting known misuse or abuse of the wireless network or associated equipment to the EITS Help Desk.