George Mason University

Wireless Network User Guidelines

Wireless Data Networking at Mason

With laptop and handheld PC's becoming increasingly popular, the demand for mobile computing is skyrocketing. There is no disputing the convenience of cracking open your laptop and instantly getting a network connection without having to hunt down an active DHCP-enabled jack. Although the current economic climate has slowed development of a campus-wide wireless network, Mason is conducting a wireless pilot project at the Innovation Hall and Johnson Center.

Currently, the only "public" wireless access points are on the Fairfax campus, in the Innovation Hall and the Johnson Center. Some of the University's academic departments also have their own wireless LANs that are available to their faculty and, in some cases, to students enrolled in their courses. Check with your department for more information.

Wireless LANs are convenient, but their performance and security does not match that of a modern wired network. Mason is fortunate to have relatively new buildings, with high-quality cabling in place that supports high performance connections. A large-scale wireless LAN would be expensive to build, expensive to manage, and provide minimal benefit beyond convenience. For the time being the deployment will be limited to areas having the highest demand.

What is Mason Wireless?

The Mason wireless access allows students, faculty and staff members to check their e-mail, surf the Web and access the Mason network without connecting to a conventional Ethernet port. The wireless service is in pilot stage that provides authenticated wireless access at selected areas at Innovation Hall and Johnson Center.

The system is built on IEEE 802.11b (Wi-Fi) industry standards. Users with compatible wireless network cards and valid Mason MEMO user accounts can connect to the service through a simple Web based user authentication method.

Security

The wireless access service is protected by a secure authentication system with which users need to log in to enable network access.
Since wireless networks use radio frequencies as transport medium, information transmitted over the network can be intercepted by others. To protect your personal information, we recommend the use of encryption. Sensitive data such as passwords, Social Security numbers, credit card information, etc. should never be sent over a wireless connection (or a wired connection, for that matter!) unless the connection is encrypted.

NOTE: Websites having a URL that starts with “https://” are generally safe to use, since the data stream is encrypted with SSL. However, you should check the name and expiration date of the site’s certificate to make sure it is valid (click on the padlock icon at the bottom of your browser.)

Other tools for encrypting your connection are Secure Shell (SSH), and Virtual Private Network (VPN) tunnels.

The IT Security Office (http://itu.gmu.edu/security/) provides general security information. Links below provide specific information on protecting your wireless connection:

- How to Get/Install/Use the Secure Shell: http://itusupport.gmu.edu/help/keywordcontent.cfm?contentid=214
- IT Security Factsheet: Includes Suggestions for Desktop Users: http://itu.gmu.edu/security/practices/ITsecurity.pdf

Reliability

The wireless access service is designed to complement the existing Ethernet wired ports. While the service is convenient, its performance and reliability do not match that of a modern wired network.

The IEEE 802.11b wireless LAN standard is most commonly used as of late 2002, which operates at a frequency range of 2.4 to 2.4385GHz. The Federal Communications Commission (FCC) assigned this part of the radio spectrum to unlicensed “Industrial-Scientific-Medical” equipment uses; this means that 802.11b devices must share the airwaves with unrelated devices such as microwave ovens, some cordless phones, “Bluetooth” personal area networks, and various types of medical equipment.

Safety

No conclusive evidence exists that low-power radio frequency (RF) devices such as cellular phones and wireless LANs cause health risks to humans. However, this remains a controversial issue and research is ongoing. Wireless devices must comply with FCC regulations regarding output power, and users should follow the manufacturer's guidelines when operating any such equipment. (For example, wireless LAN antennas on laptop PC's should be kept at least eight inches from the body.)

The public wireless network at Mason is based on Cisco Aironet products. These devices transmit at a maximum power of 100 milliwatts – a level that is significantly less than cellular phones. All antennas and access points are placed at ceiling height away from public access.

The following Safety Information for the Cisco Aironet Access Point is quoted from Cisco's website:

> The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. Cisco Aironet wireless LAN products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio according to the instructions found in this manual and the hardware installation guide on the Cisco Aironet Access Point and Bridge CD will result in user exposure that is substantially below the FCC recommended limits.
>
> - Do not touch or move antenna(s) while the unit is transmitting or receiving.
> - Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
> - Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use.
> - Do not operate the radio or attempt to transmit data unless the antenna is connected; otherwise, the radio may be damaged.
> - Antenna use:
>   - Always orient the antenna so that it is at least 8 in. (20 cm) away from your body.
>
> This equipment has been tested and found to comply with the European Telecommunications Standard ETS 300.328. This standard covers Wideband Data Transmission Systems referred to in CEPT recommendation T/R 10.01.
>
> This type-accepted equipment is designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

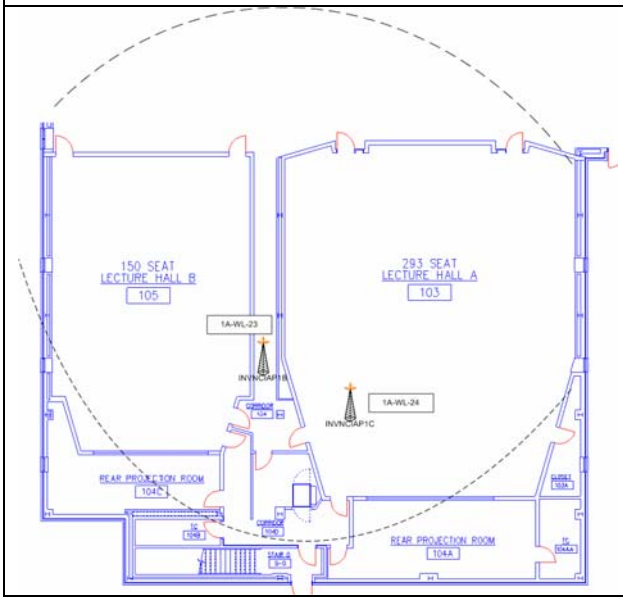
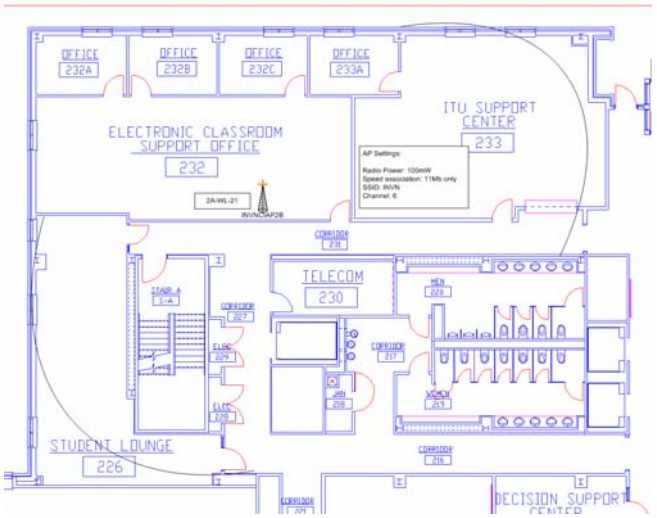
Visit Cisco website (http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350qs.htm#xtocid17) for more safety information.

Access Fees

Students, faculty, and staff may use the Mason wireless access service for free. If you need to purchase a wireless network card, Patriot Computers carries compatible hardware.

Wireless Access Coverage

Wireless access service currently consists of three wireless points. Detail coverage map is shown below.

Area around Rooms 103 & 105	Area around Rooms 232, 233, 226
	

Guest Access

Temporary account for the wireless network can be obtained by Mason faculty and staff members through the registration webpage at: http://itusupport.gmu.edu/forms.asp

Getting Started

Hardware Requirements

- An IEEE 802.11b (Wi-Fi)compatible wireless network card (laptop or PDA)
- Almost all Wi-Fi certified wireless network card should work with the service. However, it is impossible for us to be familiar with all cards considering the number of wireless cards on the market.
- Patriot Computers carries compatible network cards.

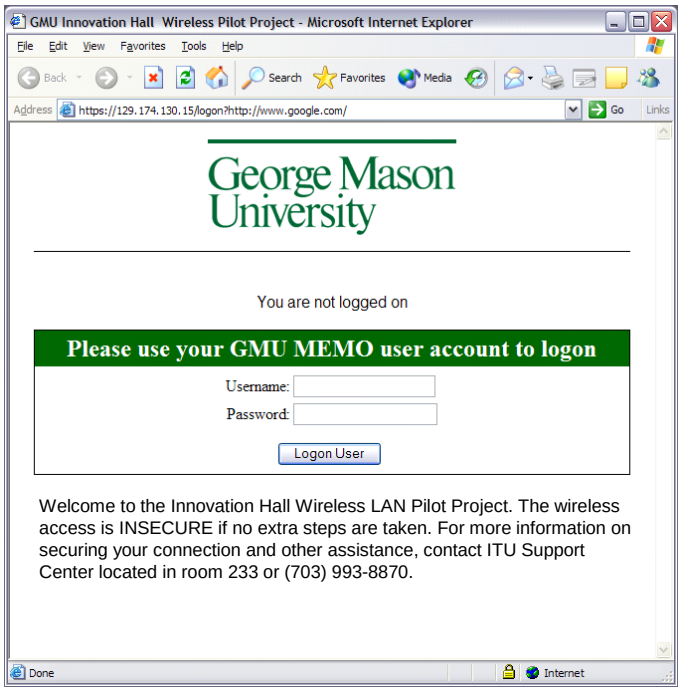
Operating System Supported

- PC: Windows 9x, 2000, XP
- Mac: OS 8.6 and above
- Linux (should be compatible but not supported)

Get Connected

- A MEMO user account. MEMO (email) user account is free to all Mason students, faculty and staff. If you don't have one, go to http://itusupport.gmu.edu/ for more information on account activation.
- Install your wireless network card by following the manufacturer's instructions.
- Set your wireless network profile with network name (SSID): gmu (lower case).
- Open a webpage with any SSL enabled browser (e.g. Internet Explorer, Netscape Navigator)
- Your will be redirected to a secure logon page similar to the one shown below.
- Use your MEMO user name and password to logon.

- Once authenticated, you will be redirected to the default web page of the browser.



Contact Mason wireless at: **wireless@gmu.edu**