Wireless

Effective: March 31, 2004
Updated: January 6, 2006
Contact: Information Technology Services (ITS)

Contents

Introduction
Policy Statement
1. Responsibility and Enforcement
2. Standards
3. Frequency Use
4. User Provided Equipment
5. Security
6. Experimentation
7. Service Spaces
7.1. Public Spaces
7.2. Department Spaces
7.3. Inter-building and Off-campus Spaces
8. Guidelines for Best Practice
8.1. Wireless Service Providers
8.2. Wireless Network Users
Resources

Introduction

Iowa State University's wireless network enables mobile computing and provides network services in situations where wiring is extremely difficult to install, such as historical buildings and large open areas.

The purpose of the wireless policy and related standards and guidelines 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.

This document provides policies, standards, and guidelines for best practice as they relate to providing and using Iowa State University's wireless network. Specifically, the policy identifies user and service provider responsibilities, lists the industry wireless standards supported on campus, addresses frequency issues, stresses the importance of security, and provides guidelines and best practices to improve security.
Policy Statement

1. Responsibility and Enforcement

Information Technology Services (ITS) is solely responsible for implementation of wireless technology, enforcing campus network standards, and has the authority to resolve frequency interference issues. All users connecting to the campus network will gain access through their Net-ID which determines the identity of and authenticates the user.

2. Standards

Iowa State University has adopted the following approved IEEE (Institute of Electrical and Electronics Engineers, Inc.) standard protocols for wireless networking:

- **IEEE 802.11b** provides 11 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11b is supported in all public spaces.
- **IEEE 802.11g** provides 54 Mbps of shared bandwidth per access point using the 2.4 GHz radio frequency. 802.11g is supported in many public spaces and is always compatible with 802.11b.
- **IEEE 802.11a** provides 54 Mbps of shared bandwidth per access point using the 5 GHz radio frequency. 802.11a is not compatible with 802.11b or 802.11g and is not recommended for public spaces where connection to the public IASTATE network is desired. 802.11a may be an appropriate choice for certain private network applications.

3. Frequency Use

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. In addition, there are only three non-overlapping channels within the 802.11b and 802.11g specifications. Consequently, access points can interfere with each other and other communications devices or appliances if not administered or deployed properly. Microwave ovens and cordless telephones are prominent examples. ITS Networks and Communications will manage the shared use of unlicensed radio frequencies for the campus community and has campus authority to resolve interference issues.

4. User Provided Equipment

Users are responsible for purchasing wireless clients or wireless Ethernet cards for devices connected to the campus wireless network. Specifications for wireless Ethernet cards are included as part of the Desktop Computers Standards. Tech Cyte is the recommended resource for obtaining 802.11b, 802.11g, and 802.11a Ethernet cards.
5. Security

Wireless networks are not as secure as wired networks. Security for wireless networks is evolving. ITS is responsible for establishing security policies for wireless communications based on current best practices. All wireless network installations must comply with established security policies including campus-wide IP (Internet Protocol) addressing and DHCP (Dynamic Host Configuration Protocol) services.

6. Experimentation

ITS continually tests new and emerging wireless technologies. Departments and colleges may test new technologies, but may not implement technologies that compete or interfere with the campus wireless network. Departments must notify ITS of any new technology trials.

7. Service Spaces

7.1. Public Spaces

ITS Networks and Communications is responsible for providing and upgrading wireless service in public spaces for a robust, seamless, and integrated wireless network.

- Public areas include but are not limited to areas such as atriums, general-purpose classrooms, and outdoor areas.
- Only 802.11b and 802.11g are supported in public spaces.
- ITS maintains a list prioritizing public areas for central funding. Departments may request ITS wireless services in public areas not yet covered by central funding. When additional funding becomes available to expand the public wireless network, priority will be given to departmentally funded ITS access points.

7.2. Department Spaces

Departments have two options for extending wireless service to locally controlled areas.

- ITS Wireless Service

Wireless service (including access points, technical support, software and hardware upgrades) is available from ITS for extending wireless networking beyond the public areas into departmental spaces. The ITS Networks and Communications division will provide engineering for optimal placement of access points and identify other devices operating in the same frequency range. They will also make a determination of the appropriate source of power, i.e. AC power at the device or power over communication lines from the Communications closet. ITS wireless service includes software and hardware maintenance and technology upgrades.
• **Self-supported Wireless Services**

Departments can provide access points within buildings in locally controlled areas. Any access point departmentally purchased and/or connected to the campus network must meet the campus wireless standards outlined in this policy. (ITS works with the University Book Store and Computer Sales to identify hardware and software that is compatible with the campus network.) Departmentally owned access points must be maintained and upgraded concurrent with university wireless policies and standards at departmental cost.

### 7.3. Inter-building and Off-campus Spaces

ITS is solely responsible for providing wireless networking between campus buildings and to off-campus locations. Departments are not permitted to provide inter-building or wide-area wireless services.

### 8. Guidelines for Best Practice

Wireless networks inherently have greater risks than wired networks because wireless transmissions occur on unlicensed radio frequencies. Consequently, it is difficult to know who or what devices are connected and listening. Security of wireless networking in the open culture of a university network requires the best efforts of both the wireless service provider(s) and wireless users. Following these best practices will not guarantee security but may reduce the risks.

#### 8.1 Wireless Service Providers

- Access points installed in public spaces, classrooms, etc. should be securely mounted or in places not easily accessible by the public.
- Access points installed in private spaces should be secured like other computing equipment (e.g. computers). For example, lock doors when the space is not in use.
- Only connect access points to an Ethernet jack or Ethernet switch. Hubs should not be used in wireless networking.
- Use 100 Mbps Ethernet where available when connecting 802.11g and 802.11a access points to the campus network.
- When installing an access point, change the default password immediately and change every access point password at least annually.
- Use static IP addresses for access points. Disable any DHCP functions built into an access point.
- Configure access points in bridging mode to the wired network. NAT (Network Address Translation) is not allowed.
- Configure all public access point SSIDs as IASTATE. Private access points may be configured with different SSIDs.
- Outdoor access points must only be installed by ITS.
- ITS employs directional antennas and other methods to reduce propagation of radio waves outside the perimeter of the campus.
The best practices for firewalls are the same regardless of whether they are connected with a wired or wireless connection. Mac address access lists can be used to control access through wireless access points. ITS does not use access lists in public areas, however, ITS will set up security in private areas using appropriately configured ITS access points. Colleges, departments, and units may set up Mac address lists to control access to private access points in private spaces. Access points used in public spaces must be WI-FI certified.

8.2. Wireless Network Users

Wireless should only be used for mobile computing. Anytime wired access is available, it should be used for increased security and performance. All campus network users must register with NetReg to obtain an IP address. The purpose of NetReg is for authentication of users and tracking users and devices, not to limit access. Guests must be registered by an employee or college/department/unit. Guest IP addresses should be issued for a limited period of time. Wireless users on campus must use DHCP and NetReg. Static IP addresses are not recommended for wireless clients. To ensure that communications are secure, wireless users should use VPN (Virtual Private Network) services.

Resources

Links

- Data Network Connections
- Tech CYte
- Access to the ISU Network
- Virtual Private Network (VPN)