

UNC Wireless Standards

The widespread availability of low-cost wireless network equipment compatible with TCP/IP/Ethernet based wired networks has fueled UNC's individual users and departments interest in deployment of such technology to provide mobile access to network resources and to avoid costs of wiring infrastructure in cases where high bandwidth (speed) isn't required or where the connection location is transitory or temporary.

Purpose

This document only addresses the current generation of wireless ethernet products operating in the 2.4 to 5 GHz area of the unlicensed radio spectrum, which collectively conforms to the IEEE 802.11b and 802.11a specification for wireless ethernet connectivity. The 802.11a standard allows users to share up to a theoretical 54 MBps. In actual use, this rate will vary, but normally does not exceed 24 MBps, due to the considerable overhead in the wireless protocol. The same is true for the 11MBps 802.11b standard which typically does not exceed 5Mbps.

This document will be modified as necessary, to address the rapidly changing wireless technologies and applications.

This document's purpose is to describe the UNC wireless standard for constructing and supporting a ubiquitous campus wireless environment and a localized wireless network.

This document develops a wireless security and authentication standard for the University, addressing the privacy of academic and administrative data and the process for preventing unauthorized access to campus and departmental LANs.

This document specifies the minimum University requirements that are essential in order to prevent interference between different colleges/departments and other uses of the 2.4 to 5 GHz section of the spectrum.

This document defines the wireless service and support levels provided by UNC Information Technology.

The standards given here are in addition to other relevant UNC system policies, procedures and all applicable laws governing the use of the UNC network. Individuals desiring wireless campus computing should adhere to these standards.

Assumptions

Two wireless network environments will co-exist on the campus. The roaming wireless network and the localized wireless network. The roaming wireless network will be ubiquitous, meaning students, faculty and staff will be allowed to 'roam' the campus and remain connected to the network, without re-configuration. The localized wireless network will provide network access to a relatively small (less than 40) population, such as a classroom. In a localized wireless network clients will no longer attach to the network upon leaving the wireless boundary

Both the roaming and the localized wireless networks will allow only UNC faculty, staff and students access to the UNC network.

All wireless networks are an extension of the wired network and will be installed, supported and managed centrally. Wireless network connectivity is a service complementary to wired networks.

Wireless networks are not suited nor will be used as a replacement for existing or planned wired network infrastructures. The major benefits of wireless networking can be achieved through focusing development in classrooms, labs, library's and selected other indoor and outdoor public spaces.

Definitions

Wireless Ethernet technology, in this document, is broadly defined to include Multipoint Access as well as Point-to-Point implementations.

An Access Point is a wireless LAN transceiver that acts as a transmitter/receiver and bridges between wireless clients and wired networks.

A bridge is a device used to connect LANs by forwarding packets across connections at the Media Access Control (MAC) layer.

Client is the end user device used to communicate with an Access Point, such as a notebook computer or a Personal Digital Assistant (Palm Pilot, iPaq, etc.).

The campus network includes the campus backbone and local area networks and all electronic equipment connected to those networks

Wireless Minimum Standards

In order to provide a ubiquitous inter/intra-building and public service area, wireless must meet the 802.11a and 802.11b standard and be registered with Information Technology before installation.

Information Technology working in conjunction with the departments of Facilities & Operations and Planning & Construction will be the sole installer of the University wireless Ethernet service.

Information Technology will manage the wireless access points and associated network connections.

Departments will be responsible for operational and maintenance costs of the localized wireless equipment; the roaming wireless network operational and maintenance costs will be funded centrally.

Information Technology is responsible for the design, operation and management of the University wireless Ethernet service.

Wireless access points are considered part of the campus backbone network, not as in-room attachment devices. The wireless access points will be interconnected into a campus-wide access network.

Access points will be connected to the campus network only if the access point location has been designated and registered by Information Technology. Information Technology will conduct tests for coverage and interference. Where potential conflicts are noted the affected departments will be consulted.

The use of wireless networking services provided by the campus shall be subject to all applicable State and Federal laws. Similarly, general campus polices and procedures shall apply.

Security

Unencrypted wireless Ethernet service shall be considered to be completely unsecured.

Unencrypted wireless access to institutional financial and student systems will not be permitted. Unencrypted wireless will be regarded as un-trusted and non-secure. No one should be accessing institutional systems such as HRMS (Peoplesoft) or the mainframe (Tn3270) from the wireless Ethernet network. This applies to both encrypted and unencrypted transmission.

Physical security of the wireless devices will be maintained whenever possible to protect from theft or direct access (ie. connecting to the data port on an access point).

Network access will be limited to UNC faculty, staff and students only. Authentication is required for access to the wireless network.

Site Survey, Design and Installation

Information Technology will perform all site surveys prior to the installation of any 802.11 devices.

The site survey conducted by Information Technology will insure Radio Frequency integrity for the client using the Access Point and identify possible interference problems.

Information Technology working with Facilities & Operations and Planning & Construction will find access point locations that will facilitate the connection of power, category 5e network cable and antenna placement and type.

Information Technology will generate drawings of the roaming and localized wireless network.

Access points and bridging devices will not be mounted in any way that will conflict with health, building or fire codes.

Power must be supplied to the Access point in a manner that is safe, preventing accidental disconnection and is not in a position that will cause injury. Some vendors provide power over Ethernet, this is an acceptable alternative.

Only a Facilities & Operations and/or Planning & Construction approved Electrician will provide power to access points. Use of extension cords in a permanent installation is not permissible.

Access points may be installed in outdoor or common areas. Security boxes may be used for the purpose of access point mounting. Keys to these units will be maintained by IT.

Information Technology will determine the method of installing the wireless campus network equipment and determine network cable routes to the access points.

Interference from Other Devices

In the event that a wireless device interferes with the campus wireless Ethernet system, it may be necessary to disconnect or relocate that device.

Support

Installation and maintenance services performed by Information Technology for the roaming ubiquitous wireless network will be centrally funded.

Installation and maintenance services for the localized wireless network will be billed to the respective department/college on an hourly basis.

Information Technology will be responsible for the entire design, operation and management of the roaming and localized wireless Ethernet service provided. Including:

- Hardware selection

- Wireless standards definition (This document)

- Access Point management

- Management of all University IP addresses (DHCP and static) and the DNS for the wired and wireless network.

- Installation of the Access Points in coordination with Facilities & Operations and Planning & Construction