

University Airwaves Policy: Guidelines for Standard Protocols, Procedures and Practices

Effective Date: March, 2004

As a companion document to the [University Airwaves Policy](#), this document describes the standard protocols, procedures and practices involved in implementing and using wireless devices on campus.

Information Technology Services (ITS) recognizes the increased use and availability of various wireless technologies at Cal Poly. At this time, the key wireless technology standards for the campus are for:

- The IP based data network protocol 802.11b

It is recognized that other wireless technologies that may require campus airwaves coordination will be incorporated into these Guidelines in the future.

Guidelines for 802.11b

Campus Usage of Wireless Networks

SECURITY CONSIDERATIONS

While it is a goal to implement a wireless environment that can secure all data traversing the airwaves, it is not something that is economically feasible for the campus to implement at this time. Therefore, the campus implementation of wireless 802.11b networks does not include security of the data being transmitted over the airwaves.

This implies that the data being transmitted over the airwaves is only as secure as the application (client/server combination) pushing/pulling the data across the network. Application managers and data stewards (as defined by the University's [Information Security Program](#)) should work together to determine if an application uses encryption mechanisms that match information security requirements and recommend appropriate use of wireless networks in that context.

Departments are encouraged to post notices in classrooms, labs, hallways or other affected areas spaces to inform users that wireless networks are not secure and the potential risk of using the airwaves to transmit confidential and other data. ITS will provide a sample notice upon request.

BANDWIDTH CONSIDERATIONS

At this time, wireless 802.11b networks share the bandwidth between all users accessing that airspace. Until technology exists that enables the dedication of bandwidth to wireless users based on usage policies, wireless users must understand that not all applications may be appropriate for wireless use. For example, use of applications that implement multicasting are prohibited as they can utilize a disproportionate amount of bandwidth and limit use by others.

NETWORK ACCESS

Cal Poly must ensure appropriate use of State resources and therefore must limit access to the network to authorized Cal Poly constituents. At this time, access is controlled through device management by registering a user's computer. ITS requires all qualified campus constituents to register the Media Access Control (MAC)

University Airwaves Policy: Guidelines for Standard Protocols, Procedures and Practices

Effective Date: March, 2004

address of their wireless card with the ITS Service Desk. Once registered, users will have access to all wireless areas of the campus.

It is the goal of ITS to institute a user based, policy based access mechanism. Limiting access for specific users to specific campus areas 1) creates confusion to users as to why they have access in some areas and not others and 2) would require human resources to manage the adds/moves/changes transactions or implementation of equipment at high costs requiring funding that is not currently available. Like bandwidth and security management, the state of maturity of wireless access and high implementation costs prohibit this approach at this time. Therefore, users and departments deploying wireless coverage must understand that all registered campus constituents will have access to all campus coverage areas.

Campus Protocol, Feature and Equipment Standards

Wireless data connectivity on campus uses the IEEE 802.11b protocol standard. ITS has considered the following features and standards support to determine the best product choice for the enterprise solution for the campus. Based on this feature set, ITS/Network Administration has selected a standard base station for deployment. Contact ITS/Network Administration for more information about the selected standard base station.

This feature set was established to allow for:

- Greatest flexibility for network design to ensure enterprise compatibility and consistency of service across campus,
 - In-Line power
Provides flexibility in placement of the access points to provide best coverage with the least amount of devices and AC wall receptacles
 - Plenum Rated
Allows for placement of access points in overhead ceiling air plenum space to reduce theft and damage
 - External Antennas
Allows for optimal configuration options as part of the enterprise design coverage
 - Adjustable gain of signal (range control)
Used to establish the best coverage design for an overall building/campus build out
- Lowest overhead in day to day management,
 - SNMP controls
Allows for management by network management software and downloads of MAC addresses via SNMP scripts
 - Compatible with campus DHCP services
Ensures proper identification of IP to MAC address tracking can take place and prevents pockets of private address networks on campus
- Longevity of product
 - Supports 802.11b and future upgrades to 802.11g
Current standard in use on campus is 802.11b; the next generation standard upgrade will be to 802.11g as client demand for this standard becomes more cost effective and prevalent

University Airwaves Policy: Guidelines for Standard Protocols, Procedures and Practices

Effective Date: March, 2004

- Security options that include
 - Large MAC address store space
 - Access to the best encryption protocols over time and
 - Implementation of network authentication and authorization using 802.1x
 - MAC address capacity (until network based logins can be implemented)
 - Used for access security until Cal Poly transitions to the planned 802.1x standard for network authentication and authorization
 - Must be large enough to handle all campus registered users
 - Support for future implementation of 802.1x, WPA and TKIP security standards, the planned campus standard for network access for wireless and public access points

Implementation and Support of Wireless Coverage Areas

FUNDING AND BUILDOUT

The university has determined that a blanket deployment for wireless coverage is cost prohibitive at this time. However, if a department has a specific programmatic need for deployment, they can fund the purchase of the initial equipment needed to provide the coverage they require. As the airwaves and network stewards for the campus, ITS will consult with the department to determine the network solution that meets their requirements, provide them with the costs to install the equipment, coordinate the purchase, install the equipment, and assume on-going maintenance and support. This follows a traditional campus network build-out model for services considered "above baseline".

If a department has a programmatic requirement that requires an exception to the standard deployment model, either on protocol, actual equipment standards, or implementation procedures, ITS will work with them to ensure the solution can meet their requirements and still maintain the integrity (security and reliable access) of the campus-wide 802.11b network. See "ITS Procedure: Connecting Non-Standard Systems/Equipment to Campus Computing and Network Resources".

WIRELESS NETWORK SUPPORT

ITS will provide troubleshooting support and replacement/repair in the event of wireless network equipment failure following standard campus network support practices. ITS does not troubleshoot end user problems (computer side) once access has been confirmed at the time of initial registration. (See User Support below.)

UPGRADES AND REFRESH OF EQUIPMENT

The identified equipment for deployment has the capability to be upgraded to the next generation wireless protocol 802.11g. As appropriate, if a department wished to upgrade to this protocol, ITS can work with them to identify and deploy the additional equipment needed. At this time, it is the funding department's responsibility to refresh equipment as it becomes obsolete over time. Standard refresh rates for network technology are approximately three to four years.

University Airwaves Policy: Guidelines for Standard Protocols, Procedures and Practices

Effective Date: March, 2004

USER SUPPORT

Departments deploying wireless coverage areas need to understand that full ITS Service Desk support is not available for end users. The ITS Service Desk will ensure that a users' computer can access the wireless network upon registration. If an employee encounters problems after that point, they should contact their LAN Coordinator for assistance. Students will be helped by the ITS Service Desk on a best effort basis.

It is the end user's responsibility to purchase and install an 802.11b compatible network card for their access device (computer, handheld device, etc.).

ITS requires IP address distribution for wireless device connectivity to be provided by the campus Dynamic Host Control Protocol (DHCP) services. ITS will configure wireless base stations to enable distribution of DHCP addresses.

Compliance to Campus Policy, Guidelines and Standards

ITS reserves the right to intervene as needed to enforce campus policy and/or protect network performance. Therefore, ITS may act to shutdown any campus-based wireless network due to irresponsible, inappropriate or illegal activity in accordance with Cal Poly's Information Technology Resources Responsible Use Policy. Please see <http://www.calpoly.edu/computing/policy.html>.