University Airwaves:

Standard for Campus IP Based Wireless Network

Effective Date: August, 2010

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

Campus Protocol and Equipment Standards

Wireless data connectivity on campus uses the IEEE 802.11a/b/g/n protocol standard. ITS has deployed ITRP2 (Information Technology Resource Planning, phase 2) standard equipment. Contact ITS/Network Administration for more information about the installed product.

Campus Usage of Wireless Networks

Security Considerations

The current campus implementation of wireless 802.11a/b/g/n networks does not include security of the data being transmitted over the airwaves. Implementation of a wireless environment that can encrypt data traversing the airwaves is scheduled for Fall, 2010.

Therefore, data 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 802.11a/b/g/n networks share the bandwidth between all users accessing that airspace. Until technology exists which 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, the use of applications that implement multicasting are prohibited as they can utilize a disproportionate amount of bandwidth, and as a consequence 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, wireless access is controlled through Cisco Clean Access (CCA). CCA provides user-based authentication for all campus constituents. Once logged in via ITS-standard Cal Poly Portal credentials, users have access to all wireless areas of the campus. Furthermore, all wireless access on the campus falls under the same data “cloud”, to ensure consistent coverage for users.

Non-Standard Equipment and Networks

ITS’s directive to manage and standardize all networks campus-wide includes wireless networks. For security and policy reasons the general use of non-standard wireless equipment on the ITS network is prohibited. Exceptions can be made but must be reviewed and approved by the OCIO/ITS. Non-standard equipment includes wireless routers/switches, wireless bridges, ad-hoc wireless networks and femtocell networks. (See ITS Network Procedure: Connecting Non-Standard Systems/Equipment to Campus Computing and Network Resources.)

Implementation and Support of Wireless Coverage Areas

Funding and Buildout

The university has implemented a comprehensive wireless footprint for the entire campus. This means that all buildings have wireless coverage; exceptions are Cal Poly Corporation buildings, Residence Halls and ASI buildings (i.e., non-state buildings). If a department has a specific programmatic need for additional coverage, 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 802.11a/b/g/n network. (See ITS Network 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 802.11n. ITS will implement this upgrade as funds become available.

User Support

Departments deploying wireless coverage areas must understand that full ITS Service Desk wireless support is not available for users. The ITS Service Desk can assist users in basic connection of the user’s computer to the wireless network. 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 802.11a/b/g/n 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 with 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.