

**What is Wireless Service and DHCP?**

- Wireless service provides students, faculty and staff with wireless access to the campus network. This is done by using Radio Frequency (RF) technology to transmit data through the air without wired cabling. This provides the same access to network resources without being tethered to a cable. However, wireless technology has some bandwidth limitations. It is not recommended for FTPing large files or for video streaming. In addition, it is not recommended for highly secure transactions.

**What is Mobile Computing/DHCP?**

- DHCP stands for Dynamic Host Configuration Protocol. It allows individuals with laptop computers to take advantage of using internet connections located in classrooms and labs all over campus using either a network jack or a wireless connection. This service provides for ease of network connectivity for Faculty, Staff and Students who need to teach in the classrooms or labs, or who use laptops in their office and home.

**Where is Mobile Computing service available?**

- The Wireless service is located in the Robert E. Kennedy Library (building 35) and in the University Union (building 65) during the regular business hours.
  - The business hours of the Library are found on their web page <http://www.lib.calpoly.edu/>.
  - The university Union hours of operation are found by calling the information desk at 6-1154.
- Other buildings (Business, Architecture, Engineering West, and Computer Science) are wireless capable, but are currently supported by their respective colleges, not by ITS.
- Detailed coverage maps are available at <http://mobilecomputing.calpoly.edu>.

**Where is DHCP available?**

- The DHCP service is located in any wired classroom or lab on the Cal Poly campus. It is potentially active 24 hours/day. It is up to the Faculty or Staff individual to be able to obtain access into the classroom and also be authorized to be teaching in that classroom or lab by his/her department. Certain classroom and lab ports are kept hot 24 hours a day, but others must be turned on by the appropriate ITS group. Smart rooms allow for DHCP and network connectivity via network jacks. Refer to <http://netadmin.calpoly.edu> for a complete listing of available multimedia classrooms and labs and who is responsible for maintaining each lab.

- Students may make presentations or assist faculty with the teaching aspects of the course material and utilize this DHCP service on their own laptops while doing so. Classrooms and labs are not meant to be used by students wanting a quick place to "jump on the network" for their own personal reasons.

### **How can I get access to wireless service or DHCP?**

- Register your network card address with the Service Desk located in Bldg 14, Rm 114. Stop by the Service Desk *with your laptop* and fill out the Network Card Registration Form. This form will be used to register your wireless network card address to enable access to the wireless network. It will take about 48 hours to process your request before you can connect.

### **What equipment is required for wireless service?**

- Laptops must have a wireless network card which uses IEEE 802.11b standard technology with Direct Sequence Spread Spectrum (DSSS or DS). To ensure compatibility with the Cal Poly Mustang Mobile Computing system, look for the Wi-Fi\* symbol (Wireless Fidelity) on newly purchased equipment. WECA (Wireless Ethernet Compatibility Alliance) is the organization behind Wi-Fi that certifies products meeting the IEEE 802.11b specification through compatibility testing.

### **Is the wireless service secure?**

- Currently, the wireless service is not secure because an intruder does not need physical access to the traditional wired network in order to gain access to data communications. Accordingly, any user must be aware that there are serious risks or limitations if a secure connection is required. When using the system, your data is being sent over radio waves and can be picked up by anyone. However, IEEE 802.11b wireless communications cannot be received - much less decoded - by simple scanners, short wave receivers etc. This does not mean that eavesdropping cannot occur. Eavesdropping is possible using specialized equipment.