

Policy Governing Wireless Networking and Other Uses of the Radio Frequency Spectrum at UC Merced

(Version 1.0, Approved 1/27/2004)

Introduction

Many individuals and groups at UC Merced sites have interest in leveraging wireless networking and other technologies employing radio frequency (RF) transmission to improve productivity and/or enhance the teaching, learning, research, and administrative environments. It is a goal of UC Merced to encourage and support the use of these technologies for these purposes. As the RF spectrum is inherently a shared resource, it is important to coordinate the use of the various technologies and frequency ranges to ensure that services do not interfere with each other, with external services that may be licensed to run at UC Merced locations (such as cellular relays), or with planned future services. Representative existing and planned services include 802.11 a/b/g wireless networking, Bluetooth wireless networking, 800 MHz emergency communication system, and mobile phone pico cells. Additionally, certain devices, such as cordless telephones, microwave ovens, and others, use or emit RF radiation, and must be taken into account when planning for and operating wireless services.

In addition to physical issues, we must also ensure that appropriate security functionality is implemented when wireless networks or other RF technologies are used for communications purposes. Security needs will vary according to the different services and specific uses they are put to.

Coordination

The UC Merced Information Technology department (IT) will assume the role of campus coordinator, and develop and publish a set of guidelines, similar to those in use at other universities, for the use of wireless networking and other RF technologies so that the entire campus community can benefit from the use of these technologies. In the role of coordinator, IT will keep track of all uses of wireless services and associated RF spectra, and act as gatekeeper for the deployment of wireless services and the utilization of the different frequency ranges.

In order to provide consistent services and functionality across campus locations, a specific department may, when appropriate, be assigned responsibility for deploying, supporting, and/or coordinating a given service. For example, Information Technology will deploy and manage campus-wide wireless networking, while Facilities Management will be responsible for the 800 MHz radio system.

Wireless Network Infrastructure

UC Merced will deploy a campus-wide wireless network utilizing products that conform to the IEEE 802.11 wireless LAN specifications. The deployment of any wireless infrastructure needs to be carefully planned and engineered. For a given location, the design and deployment of a wireless network is influenced primarily by interference and capacity planning factors. Each design must include careful and exhaustive signal strength measurements, which take into account the three-dimensional nature of wireless network devices, interference caused by other devices utilizing the same unlicensed spectrum and obstacles such as concrete walls and metal supports.

The design must also take into account the potential load on the wireless network. A large number of wireless users in one area such as a large classroom or lecture hall, for example, may require the use of two or more wireless access points configured to load balance. A less dense but more spread out coverage area, such as a lawn between two buildings may require a "coverage-oriented" as opposed to a "capacity-oriented" design with a different set of configuration options. Different technologies within the IEEE 802.11 specifications may be more or less appropriate for different coverage/capacity design points.

In addition, it is important to note that the data transmission capacity provided by the wired network far exceeds that which can be provided by wireless LANs. Design of any wireless network should take into account that the most appropriate and achievable uses of wireless technology are for mobile, low-bandwidth applications. Although wireless data rates are increasing, in practice, the actual rates achieved are much lower than the theoretical ones, and that the bandwidth is shared by all users of a given wireless access point. This is in contrast to the wired campus network, in which every port is capable of at least 100 Mbps dedicated capacity.

Security Concerns

The potential for unauthorized access to the UC Merced network will increase as the use of wireless networking becomes more prevalent. Security features defined by the IEEE 802.11 standard are vulnerable and are unable to completely prevent unauthorized access or to protect data traversing the wireless medium from determined attackers.

The inherently insecure nature of the wireless network medium makes it essential that users adhere to effective security practices. These may include, but are not limited to, the use of application level authentication and encryption technologies such as Secure Socket Layer (SSL) and Secure Shell (SSH).

IT will deploy and operate access control services that will restrict access to our wireless network requiring the use of 802.11 standard security features, and under the control of the campus-wide electronic directory. Provision will also be made to support guest access, with appropriate restrictions.

Nevertheless, even with when using access controls and exploiting the 802.11 security features, wireless networks cannot be made totally secure. To support departments or users working with extremely sensitive applications and communications, IT will deploy a Virtual Private Network (VPN) service. This may require additional end user configuration and/or the use of VPN client software.

Support for Special Case Wireless Network Needs

As the wireless network infrastructure is deployed, IT may not be able to initially provision all spaces and locations on campus where wireless access would be an asset. In cases where access is desired and non-IT funding is available to provision the access, IT will oversee or provide the design engineering, procure needed equipment in accordance with campus standards, configure the equipment, and incorporate it into the wireless infrastructure. This is in the aim of providing consistent access and services across the campus.

In cases where experimental, emerging, or private wireless access is required, IT will work with the requestor to ensure that interference is minimized with campus wireless network access and other RF applications, and that security issues are addressed.