



This is a discussion draft please send your comments to rechew@cats.ucsc.edu by 03/21/01.

CATS/NTS Wireless Policy

1. Introduction

The widespread availability of low-cost wireless network equipment compatible with TCP/IP/Ethernet based wired networks has fueled UCSC individual user and department interest in deployment of such systems to provide mobile access to network resources, and to avoid costs of wiring infrastructure in cases where high bandwidth isn't needed, or where the connection location is transitory or temporary. While some departments may be considering use of wireless networks as a method of aggregating user traffic to avoid network connection charges, that use is an explicit violation of current campus cost recovery policy.

This document will only consider the current generation of Wireless Ethernet products operating in the 2.4 GHz area of the unlicensed radio spectrum. These products collectively conform to the IEEE 802.11b specification for wireless Ethernet connectivity.

2. Purpose

1. It is a given that Wireless Ethernet systems and interface cards will be deployed at UCSC in support of a variety of applications. This document's purpose is to guide that deployment and propose a set of CATS services in support of campus wireless connectivity, with associated suggested cost recovery.
2. Policies and guideline's for deployment of such systems are essential to prevent interference between different departmental implementations and other uses of the 2.4 GHz section of the spectrum. Polices are essential to safeguard security of campus network systems, and to ensure that a baseline level of connection service quality is provided to a diverse user community.
3. This document will be used to help define the levels of service that the campus community should assume to be part of the campus wireless infrastructure.

3. Definition

1. The term the UCSC Wireless Network or use of "wireless network" when used in this document is broadly defined to include Multipoint Access for clients as well as Point-to-Point systems.
2. An Access Point is a wireless LAN transceiver that acts as a center point and bridges between wireless clients and wired networks.

3. A bridge is a device used to connect LANs by forwarding packets across connections at the Media Access Control (MAC) layer.
4. Client is the end user device used to communicate with an Access Point.
5. Wired Equivalent Privacy (Optional security mechanism defined within the 802.11 standard designed to make the link integrity of the wireless medium equal to that of a cable).
6. The campus network includes the campus backbone and local area networks, all equipment connected to those networks that are managed by CATS personnel, and all computers in the UCSC.EDU and address domains contained and maintained by CATS.

4. Scope and initial Scope Limitations

1. The policies stated below deal with known concerns and in aggregate do not necessarily form a comprehensive policy statement. Network communications is changing rapidly both in terms of technology and application and additional policy questions will surely arise in this area. The policy statements given here, other relevant UCSC system policies, and all applicable laws govern use of the UCSC Network. Individuals using wireless campus computing and networking services should be particularly aware of the policies and limitations, which apply to security of the wireless network.
2. In common with other UC campuses, we view wireless network connectivity as a service complementary to wired networks. Wireless networks are not suited as a replacement for existing or planned wired network infrastructure.
3. At this point, UCSC does not anticipate a campus-wide deployment of 802.11b access points providing ubiquitous in-building and public area service. From information we have received from MIT and Microsoft we estimate that the wireless portion alone (Access Points and associated infrastructure) would cost \$1,500,000. However, CATS will continue to test technology to provide both public and administrative access.
4. We believe that the major benefits of wireless networking can be achieved through focusing development on classrooms, labs, library indoor and selected other indoor and outdoor public spaces. Nothing in this document precludes equipping a departmental workspace for ubiquitous wireless access. But that should not be the focus of start-up efforts.

5. Initial Wireless Implementation Policies

1. CATS will be the sole provider of "backbone" on-campus wireless Ethernet service. The wired access points and connection to the campus network will be CATS property; mobile clients will be purchased for the departments by CATS on a cost pass-through recharge basis. Departments will be responsible for operations/maintenance costs of the mobile radios and associated devices.
2. CATS/NTS is responsible for the design, operation and management of the Campus wireless communications service provided at the campus level.
3. Wireless access points are considered part of the campus backbone network, not as

in-room attachment devices. As installed, the wireless access points will be interconnected into a campus-wide access network (see 8.2).

4. Wired access points will be connected to the campus network only if the access point location has been designed or approved by NTS, and after NTS has conducted coverage and interference tests (see site survey 9.0) for the desired service area/building. Where potential conflicts are noted between a local deployment and building-wide coverage design considerations, potentially affected department building occupants will be consulted before installation.
5. Should conflicts arise between a general access (public) application of wireless and a departmental application, the general access application will be favored.
6. Until appropriate technologies have been tested and deployed, wireless service shall be considered to be a totally insecure network connection method. Use for access to institutional systems and applications will not be permitted.
7. UCSC Wireless Ethernet service will conform to the proposed Wired Equivalence Protocol (WEP) standard. Among the provisions of WEP is that only encrypted sessions between the wired access point and the mobile devices are allowed. WEP alone *does not* ensure security.
8. All client to Access Point sessions will be authenticated both for UCSC "citizenship" (CATS maintained) and (if appropriate) for permission to use that access point. To the extent that wireless network service delivery requires additional/separate authentication/authorization infrastructure, the annual wired access point charge will recover those costs.
9. The University of California at Santa Cruz is a class1 research institution, and 802.11b operating at 2.4GHz can have a disannulling affect on certain experiments. Academic research will take precedence over wireless.
10. The use of wireless networking services provided by the campus shall be subject to all applicable State and Federal laws. Similarly, general campus system polices shall apply.
11. CATS/NTS does not assume any responsibility for intrusion into the wireless network. Practical attempts will be made to locate an intruder. It may be necessary to shut down an access point for this purpose.

6. Security

1. CATS/NTS will maintain the highest security available for the device installed. Security of the wireless network has many facets. There is much concern about the encryption of data over the air. As a matter of general security, user education is needed.
2. Physical security of the wireless devices will be maintained whenever possible by CATS/NTS. In common areas, a device will be used to protect the Access Point from theft, or access to the data port.
3. All use of the wireless network should be considered "clear text". Even with the use of Wired Equivalent Privacy (WEP).

4. Education in the use of programs such as Secure Shell (SSH) and PGP for mail should be made available to the clients. Whenever possible, application level encryption programs should be used.
5. Access points will have the ability to provide 128 bit WEP encryption to the end user. WEP codes will be maintained by CATS/NTS. WEP will be offered in the Pilot project.
6. Recently Lucent and Cisco have announced support for RADIUS. CATS has begun the process of purchasing and testing both manufacture that have announced support for RADIUS.
 1. Once RADIUS has been tested with other security measures (such as WEP), CATS will generate a public document that will present our recommendations for the appropriate levels of security that will broken into three categories.
 1. Public: Access for common areas; for example, library, residential etc.
 2. Administrative: This will be for common administrative use such as email, file services and correspondence.
 3. Secure: For applications such as BANNER, SIS, AIS and other confidential correspondence.
7. Until security issues are resolved wireless networking should be treated as "untrusted". This applies to both encrypted and unencrypted transmission.
8. Hardware MAC addresses will be maintained in a DHCP server. Access to the wireless network will only be allowed from valid entries in the DHCP server.
9. As security develops in the industry (RADIUS, 802.1x, etc.), CATS/NTS will re-evaluate and determine new security methods, security principles and protocols.

7. Initial Funding Model

1. All one-time costs associated with establishing a new wired access point will be recharged to the requesting department, or to whatever initiative or other source of one-time funding is defined. Network Services working capital accumulated from wired network recharges will not be used to establish wireless service.
2. Wireless Ethernet service will be treated as a new service type within the overall Network Services rates and cost recovery model. The charge will be a fixed charge per wired access point per period.
3. The service demarcation point will be the Wired Access Point itself, although CATS will have a role in the registration of devices and/or users of the service. Departments will be responsible for the costs of the wireless network card.
4. Departments will be responsible for operations/maintenance costs of the mobile client adapters and associated devices.
5. Network Services working capital will be used for any parts and equipment required to install wired access points.
6. Network Services will continue to invest staff time in R&D to resolve open issues with product quality, with security/authentication and with a scaleable method for

user registration and documentation.

7. The following are proposed fees for wireless networking:
 1. Coverage survey: \$200.00 minimum, \$500.00 maximum per location. Larger locations may require an outside contractor, so the costs would equal the contractor's cost plus 15 percent.
 2. Power installation: We estimate the cost of installation \$1,000.00 on average.
 3. Access Point Installation: \$2,200.00 estimated.
 4. Operational Cost Recovery Charge: \$950.00 per access point per year.
 5. Client Activation: \$50.00 per client.
 6. Temporary Client Activation Fee: No cost for visiting UC faculty and staff (30-day limit).

8. Support

1. Services beyond the levels listed in this document will assume an attached fee.
2. CATS/NTS is responsible for the design, operation and management of the Campus wireless communications service provided at the campus level. Responsibilities include:
 1. The choice of hardware supported by the network.
 2. The definition of campus standards necessary for efficient operation of the wireless network or for the security of transmitted data.
 3. Application of network management policies adopted by the campus to ensure inter-operability of departmental wireless LANs.
3. CATS/NTS service ends at the Access Point.
4. CATS/NTS will maintain a separate DHCP and authentication server for the wireless network.
5. CATS/NTS will maintain a dedicated RADIUS server for wireless.
6. As security develops in the industry (RADIUS, 802.1x, etc.), CATS/NTS will re-evaluate and determine new security methods, security principles and protocols.
7. CATS/NTS will inventory client cards and register the MAC addresses of each card into a database.
8. CATS/NTS will maintain the operability of the DHCP server and DNS for the wireless network.
9. CATS/DCG will provide support for the wireless software. This may incorporate a fee to the client.
10. CATS will provide a web site for access of information, registration and software updates.
11. CATS/NTS will coordinate and install Access Points, and will be responsible for all service requests concerning the Access Points.

9. Site Survey and Design

1. The purpose of a site survey is to insure Radio Frequency integrity for the client using the Access Point. Identify possible interference problems. To find a location for the Access Point that will facilitate the connection of power, category 5 network cable and antenna placement. CATS/NTS will use the results of the site survey to determine placement and the type of antennas to be used on the access point.
2. CATS/NTS will provide the service of performing site surveys for all requested wireless services. This will include the design of the wireless network infrastructure.
3. Site Surveys constitutes a collaboration of information between CATS/NTS and the end user.
4. Site Surveys will be performed prior to ANY installation of an 802.11 device.
5. CATS/NTS will maintain archives of site survey information.

10. Installation of Access Points

1. Installation of antennas must comply with FCC Sec. 15.203 Antenna requirements.
2. Access points and bridging devices will not be mounted in any way that will conflict with health, building or fire codes.
3. 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.
4. Only a University approved Electrician will be used to provide power to access points. Use of extension cords in a permanent installation is not permissible.
5. 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 CATS/NTS.
6. Although CATS/NTS will make every attempt to eliminate possible interference, CATS/NTS cannot be held responsible for interference of the installed 802.11 equipment. This equipment operates in an unlicensed band in the 2.4 GHz spectrum.
7. It is the responsibility of CATS/NTS to determine and provide campus network connection and routing to the access points.

11. Interference From Other Devices

1. In the event that a wireless data device interferes with the CATS/NTS installed system, it may be necessary to disconnect that users device. CATS/NTS reserves the right to disconnect any device that interferes with the CATS/NTS wireless system.
2. In the event that a device other than data (i.e. wireless phone, video etc) interferes with the CATS/NTS wireless system, CATS/NTS will work with the owner of the equipment to eliminate the problem. In some cases it may be necessary to remove that equipment.

12. Pilot Project (Administrative)

1. Phase 1 CATS/NTS will work with department coordinators to determine a suitable pilot.
2. Phase 2 may include installation of small sites either on or off campus.
3. Phase 3 will include installation of Access Points in common areas of campus. If remote powering of access points not available.

Note: Thanks to UCSD, to MIT for their for cost detail assistance and to UC Riverside's Mark Wilson who is now UCSC's Mark Wilson. Text and experiences cited have contributed to the rapid crafting of this document.

Contact rechew@cats.ucsc.edu.

Last updated February 26, 2001.

