The University Senate of Michigan Technological University

PROPOSAL 6-04

(Voting Units: Full Senate)

WIRELESS LAN STRATEGY AND POLICIES

Purpose
The goal of this document is to outline a plan for deploying secured, wireless access with reasonable network performance to MTU's network infrastructure. It is critical that university personnel, who are accessing private, sensitive, or personal data, have a means to do so securely when they are using mobile computing devices. The document is divided into three sections; (i) A description of the rationale for and desired capabilities of a wireless network, (ii) A policy for usage of the FCC approved radio frequency spectrum for wireless devices and (iii) A policy for use of wireless devices on campus.

Justification for Centralized Strategy

University environments thrive when they are flexible and can support a wide range of activities tailored to the needs of specific groups. Wireless networking technology is very suited to students and faculty that are mobile, moving from classrooms to labs to offices. Wireless network devices developed for the home market are inexpensive and easy to configure, and there is a great desire to use these devices in research labs and office areas on campus. There are some compelling reasons to develop a centralized, rather than ad hoc, strategy for deploying a wireless network infrastructure on campus.

Wireless network devices have three main characteristics that must be managed to get adequate performance and utilization from a wireless network:

Devices share a transmission medium,
Devices that are too close to each other will interfere with each other, significantly lowering the bandwidth available to users.
Limited frequencies: 802.11b has only 3 usable channels to divide traffic into, 802.11a has 4. If device placement isn't engineered and devices aren't shared, the number of areas allowed to install independent systems is very small.

Even when transmission channels are shared, the number of VLANs (network groups) that can be supported by an access point is also relatively small. This isn't enough to pre-assign VLANs to support individual groups on campus, so some type of grouping is necessary.

The ultimate goal of developing a wireless infrastructure is to provide access to the MTU network by students, faculty and staff, who have wireless capable devices anywhere on campus.

To obtain the most coverage for the least cost, it is important to engineer the placement of all the access points and antennae to get the best coverage with the least interference. It is desirable that all access points allow users to access their "home folders" located on departmental/administrative servers regardless of the wireless platform in use as well as have ftp/http access to the Internet.

Since wireless networks are inhabited by personal machines that roam home with staff and students, it is critical to have a system that can track security vulnerabilities and infections before they get a chance to infect other machines on campus. It is also important that this system has a strong, encrypted, authentication and transport system to insure that network access is limited to members of the MTU community, and that data that needs to be protected remains so. It is much easier to do this once for the entire wireless network, than it is for every academic department on campus to provide these services.

Proposal

It is requested that the University endorse the deployment of a wireless infrastructure across campus. By this, it is understood that various types of wireless network services tailored to the needs of different groups may be available anywhere on campus, in labs, classrooms, or office areas.

It is recommended that funding for the installation and operation of the wireless network be provided from the general fund to ensure that service is uniformly available across campus to those who need or wish to use it, and that the required security/authentication is in place and functional. It is implicit in this proposal that access to the MTU network via wireless connections provides at least the same level of connectivity as the current wired network.

Telecommunications Engineering will work with users to determine what types of devices and services are desired, a priority for these services, and a schedule for deployment. Telecommunications services will provide a minimum specification for the deployment of "private" departmental wireless networks within the wireless environment at MTU. Wireless access devices should provide at least IEEE 802.11g functionality.

Wireless Spectrum Usage Policy

Purpose

The Federal Communication Commission (FCC) has jurisdiction over all radio frequency (RF) devices. Since this transmission medium is shared, there are many state and federal laws that govern its use. The goal of this policy is to preserve the quality of all university communication services that utilize wireless media, as well as to insure that Michigan Tech remains compliant with laws governing wireless spectrum.

Policy

All use of unlicensed spectrum for university-wide services will be documented and reserved through this policy. A Wireless Spectrum Review Committee will be commissioned to manage the allocation of unlicensed spectrum for use by particular departments or individuals.

The Wireless Spectrum Review Committee (WSRC) will have representation from each college and school, a representative selected by the Vice President of Research, a representative from both the graduate and undergraduate students, and an ex officio representative from Telecommunications Engineering. The WSRC will be responsible for establishing criteria for granting or revoking access to spectrum, as well as documenting these decisions for the public record.

Wireless communication devices used on campus, both licensed and unlicensed, must be registered with Telecommunication Services. Information required includes contact information, device location, operating frequencies, transmit power, approximate transmission range, and the FCC license information (license number, type, expiration date) for licensed bands. Devices that are exempt from being registered are: cellular phones, PCS devices, cordless phones, CBs, FRS, and marine radio devices. Any device not specifically excluded in the list above must be registered. Existing services will need to be registered within three months after the adoption of this policy. All new services must be registered prior to installation.

All unlicensed wireless transmission devices deployed on campus must conform to current standards for the frequency range in which they operate. To maintain maximum flexibility on campus, all devices deployed must be able to adjust transmission channels. Any exception to this policy must be approved in advance of deployment by the WSRC. All wireless services are required to transmit at the minimum power levels necessary to cover the desired service areas.

All new wireless services must insure that they will not interfere with existing, registered services prior to installation. Any new wireless service that desires to operate at a frequency currently in use by another may submit requests to the WSRC for consideration.

In addition to the above requirements that apply to all wireless devices used on campus, the following specific ISM and UNII Band requirements must be followed:

900MHz: no additional requirements

2.4GHz:

802.11b WiFi AP Devices:

Channel 1(2.412GHz): reserved for university-wide services
Channel 6 (2.437GHz): shared spectrum, available for local use
Channel 11 (2.462GHz): reserved for university-wide services
Channels 2, 3, 4, 5, 7, 8, 9, 10 shall not be used unless necessary to avoid interference with other devices on Channel 6 or approved by WSRC
Channels 12, 13, 14 are not authorized by the FCC for use in the US and shall not be used.

Bluetooth: no additional requirements

Wireless video products:

Channel 1 (2.41 GHz): Do not use (interferes with 802.11b channel 1)
Channel 2 (2.43 GHz): Do not use (interferes with 802.11b channel 6)
Channel 3 (2.45 GHz): Do not use (interferes with 802.11b channel 11)
Channel 4 (2.47 GHz): Shared spectrum, available for local use

Cordless phones:

2.4GHz phones are known to cause interference with 802.11b network devices and may not be used on campus.

Other 2.4GHz devices: no additional requirements

5.3GHz:

802.11a Network devices:

Channel 36 (5.180GHz): reserved for university-wide services
Channel 40 (5.200GHz): shared spectrum, available for local use
Channel 44 (5.220GHz): shared spectrum, available for local use
Channel 48 (5.240GHz): reserved for university-wide services
Channel 52 (5.260GHz): outdoor use only, reserved for university-wide services
Channel 56 (5.280GHz): outdoor use only, shared spectrum, available for local use
Channel 60 (5.300GHz): outdoor use only, shared spectrum, available for local use
Channel 64 (5.320GHz): outdoor use only, reserved for university-wide services

Other 5.3GHz devices: no additional requirements

5.8GHz

5.725GHz -5.825GHz reserved for University services.

MTU faculty, staff, and students deploying wireless services are responsible for understanding and adhering to any law or university policy governing their service. MTU Telecommunications Services is responsible for monitoring the university's compliance with federal, state, and local laws, and university policy that addresses wireless transmission and has the authority to power off any device found on campus that is disrupting university-wide or registered services or is transmitting illegally.

Wireless LAN Usage Policy

Use of any wireless network devices must comply with the Wireless spectrum usage policy set out above. All wireless network access devices must be registered with MTU telecommunications services to ensure that the device does not interfere with other wireless devices nor will additional devices installed at a later date interfere with the device to be installed.

Wireless network access devices may be attached to the MTU campus network provided that the device is attached outside the MTU firewall (e.g., to Resnet or Rovernet or other non-trusted subnet) and does not interfere with existing wireless access devices. No minimum network performance is guaranteed but it is recommended that devices comply with the IEEE standards for wireless networking. Access to departmental networks should be restricted to the rules used for off-campus (Internet) access.

Wireless or wired network access devices must restrict access to designated devices using their MAC or Ethernet device addresses and that all wireless communication transmitting private or sensitive data must be encrypted. Devices must be registered with MTU telecommunications services prior to installation and must not interfere with existing devices.

MTU telecommunications services is responsible for monitoring compliance with this policy and providing a register of all wireless network access devices on campus. Equipment that is not in compliance with the above policy will be removed from the network.

Draft of 5 February 2004