RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

CAMDEN | NEWARK | NEW BRUNSWICK | SEARCH RUTGERS

Computing Services:University | Camden | Newark | New Brunswick/Piscataway | Instr & Res Tech
Telecommunications | Admin Computing Svcs | Security | Report and Plans

Wireless LAN Policy

Wireless networking has great potential for improving access to services at Rutgers. For this reason, it has been spreading rapidly around the campus. Unfortunately, many implementations are being done informally, with little or no planning. There are two major risks:

1. **Security and access control:** Unless steps are taken to protect them, wireless LAN installations are open to anyone within range of the access point. If a wireless access point is connected to the Rutgers network without restrictions, anyone with the proper equipment will be able to access the Rutgers network, even from outside the building. Furthermore, anyone with the proper equipment can spy on traffic. They can see users' passwords as well as other data. As Rutgers moves more and more services online, the amount of damage that can be done by unauthorized people learning passwords of Rutgers users is increasing.
2. **Interference:** There is a finite amount of bandwidth available for wireless use. The most common wireless LAN technology (802.11b) defines 14 possible frequencies. However they are close enough together that they can interfere with each other. Thus it is common practice to use only 3 (or possibly 4) channels. If wireless LANs are installed without coordination with others in the area, interference is likely. This may result in significantly degraded performance for everyone.

These dangers are not just theoretical: Tools to tap nearby wireless networks are widely available, even for palmtop devices. A whole subculture has sprung up of people going around, scanning for open wireless nodes, and publicizing them to people who want free wireless access. Interference among installations is already visible in several buildings at Rutgers.

This document sets out policies to deal with these issues. The policies fall into three areas:

1. Registration of access points
2. Policies to deal with allocation of channels
3. Policies for security and access control

The Office of Information Technology (OIT) is available to support units in this in several ways:

1. Maintaining the wireless access point registration system
2. Creating model implementations, with documentation and assistance for units that want to do wireless LAN installations that follow the model
3. Providing recommendations for dealing with security and other key issues
4. Providing consulting
5. Doing implementations on a chargeable basis

However neither OIT nor any other unit is in a position to monitor and oversee wireless LAN activity in every building at Rutgers. Therefore the policies assume that wireless LAN installations are the responsibility of the units in whose space they reside.

Because this document is intended as a policy that will have a significant lifetime, it does not emphasize the specifics of technology. See Wireless Security Recommendations for a more technical discussion of security issues.

This document sets out policies to deal with these issues. The policies fall into four areas:

1. Responsibility of units
2. Required registration of access points
3. Policies dealing with the allocation of channels
4. Policies for requiring security and access controls

Definition(s)

Access Point: The term "access point" includes special-purpose hardware access points, as well as general-purpose computers that are configured to act as base stations for wireless LANs. For pure peer-to-peer applications (where it may not be clear which system is the base station), one unit should be registered, so that the channel, SSID and other information are in the database.

Policy Statements

- **Responsibility defined by Geography.** Wireless LAN implementations *are the responsibility of the units that control the space in which they operate.* Units are expected to know what is occurring in that space, and to take steps to make sure that all wireless implementations active in their space follow the policies defined here.
- **Required Access Point Registration.** All access points in Rutgers-controlled space, including the residence halls, *are required to be registered in this database.* To assist in carrying out this responsibility, OIT shall maintain an online database of wireless access points.
- **Unit/School/Department Authorization.** Every wireless LAN installation within Rutgers must be authorized by the leadership of the unit in which it is occurring. While they may choose to delegate details to technical staff, the department chair or other responsible person should know what activities are occurring and take responsibility for verifying that a security plan exists, and that proper coordination is occurring with other units close enough that interference might occur.
- **Channel conflict.** Conflicts over channel allocation are expected to be handled by the manager of the unit that controls the space, or a designee, with advice from technical staff. Where multiple units are involved, leaders of the units are expected to arrange an equitable allocation of channel space.
- **Due Diligence Prior to Installation.** Anyone installing wireless LAN equipment is expected to check the registration database, and not to install any new equipment that might reasonably be expected to interfere with existing equipment without first discussing their plans with contacts for the existing equipment.
- **Residence Halls.** In the residence halls, students may install wireless LAN systems without any special permission. They must be registered in the registration database. Students are expected to work with each other to deal with interference. While OIT staff will not in general manage channel allocation in the residence halls, they may intervene if a particular wireless installation is being operated in a manner that unreasonably interferes with other users, if an installation interferes with University-operated installations, or in support of student-led initiatives to coordinate allocation of channels. See below for security requirements.

In order to allow all units to have access to wireless LAN technology, it may be necessary for some units to adjust their behavior to make more efficient use of channels. For example, if one unit has a large number of access points in individual offices, these might exhaust the available channels. It would be reasonable to ask such a unit to replace these individual access points with a more coordinated approach. It may often be advantageous for all the units in a building to do a single building-wide wireless system.

Be aware that items other than wireless LAN hardware may use the same frequencies. For example, certain wireless phones use the same 2.4 GHz frequenices as the common 802.11b wireless systems. For this reason some universities have prohibited the use of 2.4 GHz wireless phones. While Rutgers does not have such a blanket prohibition, the importance of wireless LANs is sufficient that units would be expected to discontinue use of wireless phones or similar equipment if it interferes with the use of wireless LANs. This includes Bluetooth-enabled devices, to the extent that they interfere with wireless LANs, except possibly wireless LANs with just one or two users.

- **Required Security.** Every wireless LAN implementation within Rutgers *must be done in accordance with a security plan.* This plan must address at least the following issues:
  1. restricting access to the network so that only authorized people can use it
  2. preventing unauthorized users from being able to see confidential data appearing on the network, particularly Rutgers passwords

Wireless installations are often done informally by staff or users. If not done with proper planning, such installations can expose data on networks which most users believe are secure.

Unfortunately technology for wireless security is changing rapidly. The technology is not currently stable enough for us to standardize on a single technology for security and access control. However there are approaches currently being developed that may permit us to standardize this area in the future.

Installation Recommendations

At the moment we recommend that departmental or building projects either pick a commercial security/access control technology such as the joint Cisco/Microsoft technology, or use one of two existing Rutgers models, from OIT and the New Brunswick Computer Science Department.

For installations involving one or two offices, and installations done by students in the dorms, we recommend using standard commercial tools, but enabling all of the relevant security features. This means enabling 128-bit WEP, disabling SSID beacons (often referred to as a "closed network"), and limiting access to specific wireless cards by MAC address.

Because WEP has significant weaknesses, networks where that is the primary protection against snooping should use additional protection for confidential information, including passwords. Email, file access, and anything else involving passwords should be encrypted using SSL, SSH, or similar technology.

In residence hall installations, students are responsible for making sure that wireless devices use only IP addresses that have been assigned to them by the residential networking project. For projects involving more than one student, we recommend that the organizers consult Resnet staff before doing the implementation. The operator will be expected to cooperate with OIT staff in dealing with any abuse by others who use the wireless access.

As indicated above, OIT can provide assistance to departments in doing wireless implementations. OIT maintains a central database of usernames/NetID's and passwords. It can be accessed using standard network protocols such as RADIUS and LDAP. Many of the devices intended to help secure wireless networks can use one or both of these protocols. This can make it fairly easy to check whether someone is a Rutgers user.

OIT will work with departments in developing wireless palsn if desired by the individual units developing such implementations. Early engagement of OIT would help minimize redundant effort. The initial contact should be with the director of the unit's campus division (NBCS, NCS, CCS). In any event, whether OIT is used as a resource or not, all units with the University are expected to comply with the above referenced policy statements.

BACK TO TOP

For questions or comments about this site, contact webmaster@nbcs.rutgers.edu.

Last Updated: 5/10/2007