Wireless in the residence halls

Wireless in the residence halls

On this page:

All of the MIT residence halls have complete wireless coverage in addition to the wired ethernet network. There are now two ways to connect to MITnet. While the traditional wired network is useful for some desktop computers and server setups, Residential Computing asks that dorm residents with laptops try connecting to the wireless network for everyday computer use.

Personal access points

All residence halls have wireless coverage and IS&T strongly recommends not running personal or private access points. As discussed in the "interference" section below, 802.11b/g wireless traffic is sent on a relatively small range of radio frequencies. Adding additional APs that are not connected, configured, and optimized to integrate with the MIT wireless installation in the residence halls will interfere with the current setup. This causes signal degradation, loss of throughput and connectivity issues for those residents nearby.

It is true that the MIT wireless networks are unsecured, meaning that your traffic is visible to **anyone** within radio range of your computer? MIT and MIT Guest are unsecured, but MIT Secure provides a secure, fully encrypted connection. You should take extra care by using a secure VPN when using credit cards, social security numbers, passwords and other sensitive data over the wireless network. Computer security, whether it be over a wired or wireless network, shouldn't be taken lightly and is best when used in layers. Some tips to remember:

- Always connect to secure websites (https) when doing online banking, purchasing, or logins.
- If you are buying things online, try to always use a credit card with a low spending limit.
- Connect through the MIT Prisma Access VPN whenever you're in an unknown or untrusted environment, MIT open wireless included.
- Do not assume that WEP or WPA security is enough. Once your network traffic is on the wired network it can still be seen by determined parties.
- WEP is very easy to crack and should be considered just as insecure as open wireless networks

See IS&T's Secure Computing for more information.

As stated above, the MIT and MIT Guest wireless network is open and insecure. Not anyone can connect to the network and get online, but that doesn't stop them from reading all of the data being sent through the air. There is no way to enable a WEP or WPA connection to the MIT wireless network. While adding a non-MIT or private AP will allow your connection to be secured by WEP or WPA (if set up correctly,) this does not add much additional security at all. In fact, the amount of security WEP provides is near zero. There are programs that can crack a WEP key in a matter of minutes. While WPA is slightly more secure, it also can be hacked quite easily.

Additionally, once the network traffic passes the AP it is no longer encrypted. There are many dorms on campus that still use hubbed networks where traffic is sent to all computers connected, even if it's just meant for one computer. Every WEP/WPA encrypted packet sent between your computer and the wireless AP is then broadcast unencrypted to all other computers on your floor and the surrounding floors. The switched networks do not suffer as badly from this type of behavior, but all traffic is still sent through the network and internet unencrypted after it leaves the AP.

Installing a private AP does not offer a significant rise in security and Residential Networking will not accept this as a valid reason for installing an access point in your room. See the IS&T Security pages for tips on keeping your connection secure.

IS&T cannot do a site survey and determine a solution if there are private access points. These APs interfere with the current network and make it impossible to get a real picture of coverage and usage that is necessary in identifying problems and determining resolutions.

Troubleshooting a wireless connection

Below are some basic steps to troubleshooting your connection on the wireless network. If these steps do not prove useful, contact the Service Desk.

Each wireless card and computer manufacturer has a different way of disabling the radio or wireless card antenna. If you are receiving very low or no signal strength from the MIT wireless networks, be sure that your radio is on.

On **Mac OS X**, you can click the **airport icon** in your system tray and select **Turn Airport On**.

With **Windows**, each computer and card is different. Some options:

- Right click the wireless icon in the system tray and select **Enable**.
- Look for a hardware switch on your laptop. These are sometimes around the outer edge or near the LCD screen.
- Look for a keyboard switch. **Function + F1** through **F12** are often software switches. Fn-F1 may increase brightness or volume and one of them may turn your radio on/off. Read your laptop manual for more information.

Many computers are configured to only connect to "preferred" wireless networks. If your computer is not finding the "MIT SECURE" network you may have to manually type in the network name.

There are a large number of wireless cards and drivers available today. As with any technology, it is recommended to keep up to date with patches and firmware updates. These updates can decrease the risk of security exposure, fix bugs, add additional features, or make the product interact with other software or hardware better. If you are having connectivity problems between your wireless card and the MIT wireless network, try downloading and installing the latest updates from the card manufacturer.

It is also possible that the drivers have not been installed, have been installed incorrectly, or have become corrupted. Reinstalling the manufacturer's driver can often resolve non-connectivity issues. Check your network connections (Control Panel in Windows; System Preferences in Mac OS X) to be sure that a wireless card and drivers have been installed. Computer wireless networks communicate through radio waves in the 2.4Ghz range. Many home electronics also use this frequency range for wireless communications including cordless phones, wireless access points, microphones, headphones, and laptop computers. The large number of household devices that operate in this range makes these radio frequency bands very crowded, and can result in interference.

Wireless network signals can also be disrupted by physical obstacle, e.g., windows, building materials, furniture, and appliances. Refrigerators placed near a wireless device can cause degradation of signal.

If you are noticing problems connecting to the wireless network, keep these questions in mind:

- Do you have a cordless phone or microwave?
- Can you see or connect to networks not called "MIT SECURE"?
- How far away is the nearest access point?

Another type of interference happens when there are a large number of people using the same access point and are sharing the same limited medium to communicate. As with any other shared resource on campus, it is important to use the wireless network responsibly. It is a shared medium and the amount of network traffic that passes through it can greatly affect its performance. Some steps to take to help keep a healthy and useful wireless network:

- If you have multiple computers or wireless devices, try to connect as few of them at a time as possible.
- Keep high bandwidth traffic on the wired network when possible.
- Do not use filesharing programs unless necessary and legitimate.
- Do not connect personal wireless routers or access points to MITnet. They are biggest interferer to the MIT wireless network in a dorm setting and can degrade or impede performance for all users of the network in the areas where they are connected.

Often, wireless access points can be affected by the environment around them. Heat and overuse can cause them to operate incorrectly. This type of outage is different from an interference or signal coverage issue and has a different procedure for resolution. It is important to indicate how long you've been noticing problems and how the current behavior differs from the expected behavior.

Contact information

- FSILGS: ilg-net-help@mit.edu