Updated: August 2011

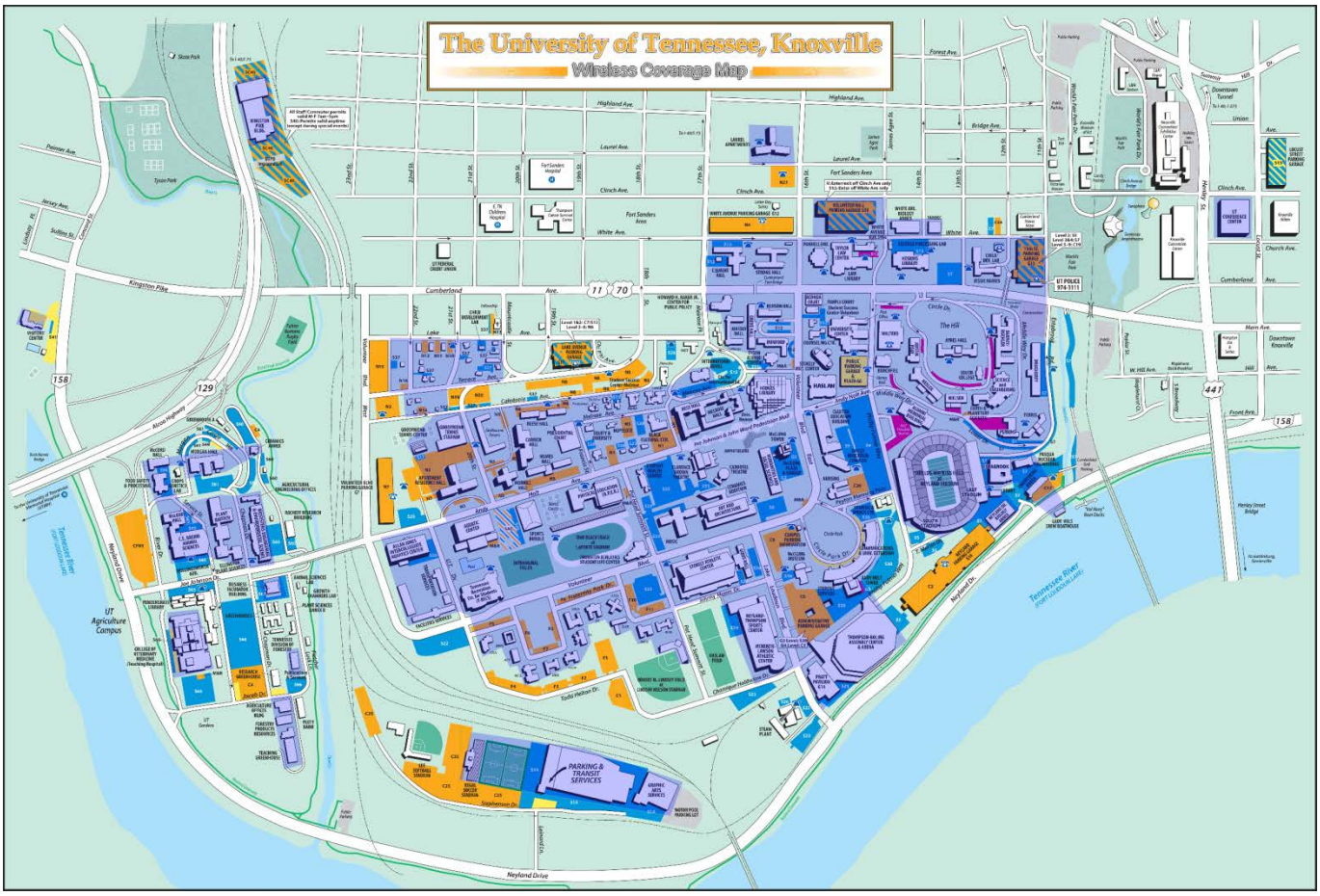
Wireless Access Appendix

UT Department of Theatre • 206 McClung Tower • Knoxville, TN 37996

Where is Wireless Available on Campus

Excerpted from the OIT Knowledgebase

Wireless coverage is provided in and immediately around most of the Knoxville Campus's academic, administrative, and residential buildings. The map below shows the coverage as of 8-15-11.



What is IEEE 802.11 b/g/n?

Excerpted from the OIT Knowledgebase

The Institute of Electrical and Electronics Engineers (IEEE) certified a new standard, 802.11g, by merging two incompatible wireless networking standards 802.11b (goes far but not fast) and 802.11a (goes fast but not far). The new "g" standard has a 150-foot range, and the top speed is 54 Mbps (as opposed to 11 Mbps that we had with the "b" standard).

Among its key innovations, 802.11n adds technology called multiple-input multiple-output (MIMO), a signal processing and smart antenna technique for transmitting multiple data streams through multiple antennas. This results in up to five times the performance and up to twice the range compared to the earlier 802.11g standard.

All of the wireless access points on our campus and in our guest artist housing are now compliant with the "n" standard so that you can take advantage of the faster connections. The good news is that 802.11n is backward-compatible with 802.11b/g. This means that if you have a "b" or "g" card you do not have to purchase a new wireless card if you are satisfied with your connection speed.

Keith Kirkland, LAN Manager • o.865.974.5659 • f.865.974.4867 • theatreadmins@utk.edu

WHAT IS A SECURE CONNECTION?

PORTIONS EXCERPTED FROM THE OIT KNOWLEDGEBASE

So, why are wireless connections not secure? Because the 802.11 wireless specification uses the 2.4Ghz frequency range (the same range as many portable home phones and other consumer wireless products), anyone with basic networking knowledge and a cheap wireless receiver can eavesdrop as information travels from your computer to an access point.

This means that someone can potentially see your user name(s), password(s), and whatever else you may be working on via the wireless network. While the 802.11 wireless specification did originally feature built in security, it was found to be too weak (about as secure as putting a check in an envelope). Since the 802.11 wireless network is not secure, it is crucial that you take the proper precautions and secure your communications over the network.

WHY ISN'T MY CONNECTION SECURE? – UT-VISITOR & UT-OPEN NETWORKS

Securing a connection requires that both the network and the computer/device share some piece of information that can be used as a "password" to establish the connection. In the case of visitors, there simply is no information both you and the network know, thus the ut-visitor network cannot be secured. ut-open for its part exists to provide faculty, staff, and students of UT what is known as legacy support—or support for devices—usually older PDA's or smartphones—that simply lack the ability to make a secure connection.

HOW IS MY CONNECTION SECURED? – GUEST ARTIST HOUSING WIRELESS & UT-WPA2

Wireless in the guest artist housing uses the WPA security system. The password/phrase you enter to initially join the network is used each time you connect to "prove" to the access point that you are an authorized user, and to generate a "key" which is shared between your computer and the access point. From there on, data between your computer and the wireless access point is encrypted using this "key" which is automatically changed at random intervals to help further protect you in case the "key" is ever guessed.

UT's ut-wpa2 network provides the exact same security for faculty, staff, and students by using your NetID and password to "prove" your authorization on the network and generate the initial "key".

SECURITY OPTIONS FOR UN-SECURE CONNECTIONS

For many activities (e.g. checking movie times, reading the news, etc.) a secure connection is simply not important. For some activities (e.g. checking your bank accounts, making a purchase with a credit card, etc.), using an un-secure connection puts you at risk.

Wireless security is what is known as hardware-based security because it is handled by the physical hardware that makes the wireless connection. When this type of security is not available, you can reduce (or nearly eliminate) your risk by using software-based security. Below is a short explanation of the two most common types of software security in use today. This security works much the same as hardware-based security; however, the encryption is performed by the software before data is even passed to the wireless card.

SSL (Secure-Socket Layer) is a type of security provided built into many software applications. Most browsers (Safari, Internet Explorer, Chrome, Firefox, etc.) offer SSL encryption, but **pages are only encrypted IF the server that you are connected to supports SSL**. Most university related sites that require password verification use SSL, but it is important that you check and make sure that the site does offer encryption. You can tell if a site is encrypted by checking to see if there is a padlock present in the bottom right corner of the browser or beside the address bar—the address should also begin with https://.

SSH (Secure Shell) is a secure protocol for use with remote terminal services. Developed to replace telnet, this protocol can be used to connect to all OIT resources, but requires an SSH compliant client to make the connection. If you use remote terminal services or telnet, contact your Administrator to see if SSH is available and, if so, how to obtain a SSH compliant client.