

# Connecting to the Campus Wireless Network

A guide to using wireless Ethernet networking at Texas Wesleyan University

The Information & Communications Technology department welcomes you to campus! Steps outlined in this document will walk you through the process of establishing a wireless network connection at Texas Wesleyan.

## How will I connect?

First determine which type of network connection is available in your residence hall or building. The EJW Library, Dora Roberts dining hall, Brown-Lupton campus center, GPNA building, and Wesleyan Village apartments all have wireless access available.

## Your Account and Password

In order to register your machine for the campus network, you will need to know your university userID and network password. If you don't already know it, you can determine your university userID through the RamLink web page at <http://ramlink.txwes.edu>.

In most cases, your network password is set to the last 6-digits of your Social Security number. Passwords for students who do not have a Social Security number area set to the student or university ID number.

## Before you Begin... Know the RULES!

### About the Wireless Network

The wireless network is a shared resource and a complimentary service that is not intended to be a replacement for the campus wired infrastructure. To use your system with a wireless connection, you must configure your system for wireless usage.

### Your Personal Legal Exposure to RIAA or MPAA Lawsuits

For anyone accessing the Internet through Texas Wesleyan's network, using either an institutionally-owned or personally-owned computer, the university serves as their Internet Service Provider (ISP). The university is therefore bound by laws and policies that apply to ISPs.

As an ISP, the university is required to and has responded to complaints from copyright holders and organizations representing copyright holders, such as the Recording Industry Association of American (RIAA) and the Motion Picture Association of America (MPAA), regarding computers on campus illegally distributing copyrighted materials. Most complaints received by the university are associated with peer-to-peer music and video distribution.

The university requires that all users of the Texas Wesleyan network learn and abide by relevant university policies such as the Texas Wesleyan University Computing Policy.

For more information, review the policy and guidelines available at <http://ict.txwes.edu>

### Wireless Network Bandwidth Usage Guidelines

The Information & Communication Technology department developed guidelines to ensure fair use of network access to the Internet. Since the university's connection to the Internet is a limited resource that is available to anyone who has a system connected to the network, exceptionally high use of this resource has an impact on all other users.

The main objective of the wireless network is to provide a network connection that can be used virtually anywhere; it is not intended to be a replacement for the wired infrastructure. Because the activity of one wireless network user dramatically affects the wireless performance for other users, ICT has established wireless usage limitations and prohibits network services such as web servers, peer-to-peer file sharing, or FTP servers on the wireless network.

### **Purpose of the Guideline**

The Texas Wesleyan Acceptable Network Use Policy establishes a general policy for the use of computing, telephone and information resources. The purpose of this guideline is to establish acceptable practices that support the policy as it applies to wireless network bandwidth usage.

This guideline was established to ensure that the Texas Wesleyan community has a clear understanding of proper procedure and usage, and that each system on the wireless network has access to a fair share of the available bandwidth. It takes only a few high-traffic users to degrade the performance of the wireless network for others.

ICT reserves the right to modify this guideline as necessary. Any changes to this guideline will be posted on this web page.

Services which can have a negative impact on the wireless network include but are not limited to:

- Web servers
- Peer-to-Peer file sharing
- FTP servers
- Multiplayer Gaming and Game Servers

Many of these services are provided within the overall research and educational goals of the university. Even so, those providing services must do so in a way that does not cause degradation of the entire wireless network.

Additionally, there are other issues which can cause your system have a negative impact on network bandwidth. The following list contains some examples and should not be considered to be exhaustive:

- Worm or viral infections
- Compromised systems running ftp, IRC, or other services
- Malicious spyware programs

Some activities may also cause a system to use excessive wireless bandwidth. The following list contains examples and should not be considered to be exhaustive:

- Reinstalling an operating system
- Performing Windows Update or Apple Software Updates
- Downloading and installing applications
- Performing system backups

- Transferring large files (images, video, music, databases) to other systems

If you need to perform any of these types of high-bandwidth usage tasks, consider using a wired network connection.

### **Wireless Network Bandwidth Usage Guideline**

The Wireless Network Bandwidth Usage Guideline: ICT states that no individual service or system running on the wireless network should use more than a total of 750 megabytes (750MB) of bandwidth per day, regardless of whether it is inbound or outbound.

Examples of overuse:

- A system can trigger an overuse notification if a five day average inbound or outbound total exceeds the usage limit. This allows machines infrequent bursts of activity above the daily limit, but only by a factor of 5 in any 5 day period. Once an overuse notification for a five day average is sent, checks are performed daily. Continued violations will result in further warnings that may eventually lead to loss of network access.
- A system with 300 megabytes inbound and 500 megabytes outbound traffic on the same day would exceed the usage guideline.
- A system with over 750 megabytes inbound or 750 megabytes of outbound traffic on the same day would exceed the usage guideline.
- A system with 800 megabytes inbound traffic on one day and 900 megabytes of outbound traffic on a second day would incur two overuse incidents.

In cases where a user has been asked to disable a service, and does not do so, ICT may revoke access to the network and initiate appropriate disciplinary procedures against the user. Disciplinary actions may include loss of network access for 45 days.

### **User Responsibilities**

The wireless network is a shared resource and a complimentary service that is NOT intended to be a replacement for the campus wired infrastructure. Because RamNet coverage is limited, we recommend a wired connection when you need to use a higher limit of bandwidth for your own purposes or when providing a service to others. (For limits on wired bandwidth usage, see "Network Bandwidth Usage Guidelines").

Users should be aware that some applications such as peer-to-peer file sharing applications, web servers, SQL applications and others, may turn on servers by default. In most cases, the server portions of these applications can be disabled. Users must also be aware that if a computer is running these services while connected to the wired network, the services should be stopped before connecting the computer to the wireless network.

## **How to establish a WIRELESS CONNECTION**

### **Step 1: Hardware Requirements**

#### **Wireless**

You'll need a wireless Ethernet card. We recommend the Proxim ORiNOCO Wireless card (PC) or the Apple Airport or Airport Extreme card (Macintosh).

#### **How do I know if I have a Wired Ethernet or Wireless Card?**

To determine if you have a Wired Ethernet or Wireless card, follow these steps:

## **Windows XP OS**

Do one of the following:

On Windows XP: Select **Start > Control Panel**.

On Windows 2000: Select **Start > Settings > Control Panel**.

Double-click on **System**. (If you don't see System, click Switch to Classic View under Control Panel.)

Select the **Hardware** tab, then click **Device Manager**. The Device Manager list appears.

Click the (+) sign next to Network Adapters.

If you have a WIRED Ethernet card you will see an entry that includes "Ethernet" in the name.

If you have a WIRELESS card you should see a "Wireless" or "WLAN" or "ORiNOCO" entry.

## **Macintosh OS X**

Select **Apple** menu > **System preferences**, then click the **Network** icon.

Click the **Show:** pull down menu and select Network Port Configurations.

If you have a wired card you'll see an entry for "Ethernet" or "Built in Ethernet".

If you have a wireless card you'll see an entry for "Airport".

## **Step 2: Install Hardware**

### **Wired**

- Install the Ethernet card in your computer (For help, refer to manufacturers instructions.)
- Once the Ethernet card is installed in your computer, connect your Ethernet card to the data outlet using your Ethernet cable.

### **Wireless**

- **All operating systems EXCEPT Windows 2000:** Follow the manufacturers instructions to install your wireless card and driver.

## **Step 3: Configure Your Software for Wireless Networking**

### **Determining your Service Pack Level**

In order to complete the appropriate configuration instructions on Windows XP, you'll need to determine your Service Pack level. Follow these steps:

1. On your desktop, right-click the **My Computer** icon and select **Properties** from the pull-down menu. The System Properties dialog box appears.

2. **Note:** If the My Computer icon does not appear on your desktop, select **Start > My Computer > View System Information**.



3. The Service Pack level appears on the **General** tab as either Service Pack 1 or Service Pack 2.
4. Depending on your Service Pack level, follow the appropriate configuration steps, SP1 (Service Pack 1) or SP2 (Service Pack 2) steps for Wireless networking.

### **TROUBLESHOOTING on Windows XP**

Follow these steps:

- Select **Start > All Programs > Accessories > Communications > Network Connections**.

#### **For WIRELESS connections:**

- Right-click **Wireless Network Connection** and select **Properties**.
- The Local OR Wireless Network Connection Properties window appears.
- Select **Internet Protocol (TCP/IP)**, then click **Properties**.

**Note:** If Internet Protocol (TCP/IP) is **NOT listed** you will need to install it before you can configure. Follow these steps to install:

- From the Local OR Wireless Network Connection Properties window, click Install. The Select Network Component Type dialog box is displayed.
- Select Protocol then click Add. The Select Network Protocol dialog box appears.
- Select Internet Protocol (TCP/IP) and click OK.
- Restart your computer and return to step 1 of Troubleshooting on Windows XP on this page.
- The Internet Protocol (TCP/IP) Properties window appears. Verify that both the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons are selected.
- Click **OK** to close the open windows.

## Wireless Ethernet Connections

### ***Wireless Networking: Windows XP Service Pack 1***

Windows XP users: These instructions assume that you are using the Windows XP menu structure, not the Classic menu structure. To edit your menu structure, right-click on the **Start** button, select **Properties**, make sure that the Start menu radio button is selected, then click **OK**.

Log on to your Windows XP system with the Administrator account or an account with Administrator privileges.

**IBM Users ONLY:** Perform this step first!

- Select **Start > Control Panel > Add or Remove Programs**.
- Select **Access IBM Tools** and click **Remove Program**. A list of IBM Access tools appears.
- Select the **IBM Access Connections** item and click **Remove**. (If prompted, select the option to remove the program and profiles.) Close the dialog box.
- Select **Start > All Programs > Accessories > Communications > Network Connections**.
- From the **Advanced** menu select **Network Identification**. The System Properties dialog box is displayed.
- Select the **Computer Name** tab and click **Change**. The Computer Name Changes dialog box is displayed.
- In the Computer name field type a unique name to identify your machine. Then, select the **Workgroup** radio button, and type **CAMPUS** (all caps) in the text field.
- **Note:** If you do not have explicit permission to join an approved Windows domain, you **MUST** join the CAMPUS Workgroup. Faculty and staff members who are unsure of their Workgroup should contact their department administrator.

- Click **OK** to close the dialog boxes. You'll be prompted to restart your computer for the changes to take effect.
- Select **Start > Connect to >** then right-click on Wireless Network Connection.
- Select **View Available Wireless Networks** from the menu. The Wireless Network Connection window appears.
- Select **the 1st Access Point listed** and click in the checkbox to select **Allow me to connect to the selected wireless network, even though it is not secure**. Click **Connect**.
- The wireless card lights will begin flashing and network connectivity should start within a few seconds.

**Note:** If you are not connected, you may need to **RESTART your computer**.

### Turn on Firewall

- Click **Start > Control Panel**.
- Double-click **Networking and Internet Connections**, and then click **Network Connections**.
- **Right-click** the connection on which you would like to enable ICF, then click **Properties**.
- On the **Advanced** tab, click the box to select the option to **Protect my computer or network**.

**Note:** If you want to enable the use of some applications and services through the firewall, click the **Settings** button then select the programs, protocols, and services to be enabled for the ICF configuration.

- Restart your computer for the changes to take effect.

**Advanced Usage Note:** Once you've established a network connection, you can enable the use of SOME applications and services through the firewall.

### **Wireless Networking: Windows XP Service Pack 2**

- Log on to your Windows XP system with the Administrator account or an account with Administrator privileges.

**IBM Users ONLY: Perform this step first!**

- Select **Start > Control Panel > Add or Remove Programs**.
- Select **Access IBM Tools** and click **Remove Program**. A list of IBM Access tools appears.
- Select the **IBM Access Connections** item and click **Remove**. (If prompted, select the option to remove the program and profiles.) Close the dialog box.
- Select **Start > All Programs > Accessories > Communications > Network Connections**.
- From the Advanced menu, select **Network Identification**. The System Properties dialog box is displayed.

- Select the **Computer Name** tab and click **Change**. The Computer Name Changes dialog box is displayed.
- In the Computer name field type a unique name to identify your machine. Then, select the **Workgroup** radio button, and type **CAMPUS** (all caps) in the text field.

**Note:** If you do not have explicit permission to join an approved Windows domain, you **MUST** join the CAMPUS Workgroup. Faculty and staff members who are unsure of their Workgroup should contact their department administrator.

- Click **OK** to close the dialog boxes. You'll be prompted to restart your computer for the changes to take effect.
- Select **Start > Connect to >** then **right-click** on **Wireless Network Connection**.
- Select **View Available Wireless Networks** from the menu. The Wireless Network Connection window appears.
- Select the **1st Access Point listed** and click in the checkbox to select **Allow me to connect to the selected wireless network, even though it is not secure**. Click **Connect**.
- A Wireless Network Connection dialog box appears. Click **Connect Anyway**. The wireless card lights will begin flashing and network connectivity should start within a few seconds.

**Note:** If your wireless card does not establish a connection, you may need to **RESTART** your computer.

## Configure Firewall

Follow these steps to configure **the Windows XP SP 2 Firewall**:

- Click **Start > Control Panel**.
- Double-click **Networking and Internet Connections**, and then click **Network Connections**.
- **Right-click** the connection on which you would like to enable Windows Firewall, then click **Properties**.
- A Network Connection dialog box appears. Select the **Advanced** tab, then click the **Settings** button. The Windows Firewall dialog box appears.
- To enable Windows Firewall, select the **On** radio button. Restart your computer for the changes to take effect.

**Advanced Usage Note:** Once you've established a network connection, you can enable the use of **SOME** applications and services through Windows Firewall. To do this, follow steps 1-4 above, then click the **Windows Firewall Exceptions** tab. Select the services you wish to **exclude** from using Windows Firewall, then click **OK**.

## Wireless Networking: Windows 2000

**Important!** As you follow these steps, do not insert the wireless card or driver CD until instructed.

- Select **Start > Programs > Accessories > Communications > Network and Dialup Connections**.

- Select **Advanced > Network Identification**. The System Properties dialog box is displayed.
- Select the **Network Identification** tab, and click **Properties**. The Identification Changes dialog box is displayed.
- In the Computer name field type a unique computer name to identify your machine.
- Select the **Workgroup** radio button and type **CAMPUS** (all caps) in the field.
- **Note:** If you do not have explicit permission to join an approved Windows Domain, you must join the CAMPUS workgroup.
- Click **OK** and restart your computer so the changes take effect.
- Close the System Properties dialog box.

Follow these steps to install the Proxim Wireless Driver. If you aren't using a Proxim card, use steps 4 and 5 as a guide to configure your wireless card settings. You may need to contact your card vendor for specific configuration instructions.

Insert the CD that came with your Proxim wireless card. **DO NOT insert the wireless card at this time.** The ORINOCO Wireless LAN Wizard appears.

- Click **Install a new product**. The Setup Overview for Windows 2000 screen displays.
- Click **Identity Settings**. The Select Type of Network page displays.
- Select **Base Station Network** and click **Next**. The Network Name page displays.
- In the Network Name field, type **Wesleyan** and click **Next**.
- The Set Data Security page displays. Select **Off** and click **Next**.
- The Setup Overview page redisplay. Click **Install Driver and Client Manager**. The InstallShield Wizard displays and installs the software needed to use your wireless card. When this step is complete, click **Finish**. The Wireless LAN Wizard page redisplay.
- Click **Install Hardware**. The Install Hardware page displays.
- Insert your Proxim Wireless card. Select **Insert PC Card** and click **Next**.
- The Client Manager icon appears in the system tray and should be green and solid.

### **Wireless Networking: Mac OS 10.3**

- From the **Apple** menu, select **System Preferences** (appears in the upper left of the screen display) and click the **Network** icon.
- Double-click **Airport**. On the Airport tab, set these options as follows:  
By default, join: A specific network  
Network: **Wesleyan**
- Allow this computer to create networks: Deselect this option
- Show AirPort Status in menu bar: Select this option.

- On the TCP/IP tab:  
Select **Configure IPv4: Using DHCP**
- Search Domains (optional): should be left blank or set to any or all of the following:  
**txwes.edu**
- Click **Apply now** to register these configuration changes.

### **Wireless Networking: Mac OS 10.1 or 10.2**

- From the **Apple** menu, select **System Preferences** (appears in the upper left of the screen display) and click the **Network** icon.
- Verify that **Show** is set to **AirPort**.
- Select the **TCP/IP** tab. The settings should appear as follows:  
Configure: **Using DHCP**
- Search Domains (optional): should be left blank or set to any or all of the following:  
**txwes.edu**  
DHCP Client ID: should be left blank.
- Select the **Airport** tab. Depending on whether you are running OS 10.1 or 10.2, do one of the following:  
**Mac OS 10.1**
- Preferred Network: should be set to the first access point on the list.  
**Mac OS 10.2**
- Click on the **Join a specific network** option.  
Network: set to **Wesleyan**  
Password: leave this blank
- Verify that "Allow this computer to create networks is" **NOT** checked.
- Click on the **Show AirPort status in menu bar** option.
- Select the **AppleTalk** tab. Verify that the **Make Apple Talk Active** checkbox is **NOT selected**.
- Click **Save** or **Apply Now**.
- Select **System Pref > Quit System Prefs**.

### **Step 4: Log on Your Machine**

Launch a web browser (Netscape or Internet Explorer) and visit any web page OUTSIDE of "www.txwes.edu" (e.g., www.cnn.com). You'll be diverted to the **Wireless Gateway System**.

### **Step 5: Protect Your Machine**

Viruses, worms and break-ins have become increasingly harmful. Break-ins are attacks that specifically target your computer. They occur through a file that you download and run or via a security hole exposed through a network connection. Break-ins are NOT always detectable through up to date anti-virus software. To combat break-ins, it's important that you load Microsoft's and Apple's latest updates against

operating system vulnerabilities. Worried that you'll forget? Configure your computer to run these updates automatically.

### **Windows & Macintosh: Running Automatic Updates**

In view of the recent rash of security vulnerabilities, you should already be aware of how to run Windows and Macintosh operating system updates. But did you know that you can configure your computer to run these updates automatically? If your computer has an ongoing Internet connection, the latest updates can be delivered directly to your machine.

**Note:** Computing Services recommends that you configure your machine for DAILY updates at a time when you know your computer will be ON and connected to the Internet.

*To configure a Windows XP machine for automatic updates, follow these steps:*

- Log on to your machine using the Administrator password.
- Select **Start > Control Panel**.
- Select **Performance and Maintenance**, scroll to the bottom of the screen and select **System** OR if in classic view, double-click **System**.
- Select the **Automatic Updates** tab.
- Select the radio button for **Automatically download the updates, and install them on the schedule that I specify**. Select the day and time preference that you desire.

*To configure Mac OS X for automatic updates, follow these steps:*

- Select **Apple** menu > **System Preferences**.
- Double-click the **Software Update** folder.
- From the Update Software tab, select the checkbox for **Automatically check the updates when you have a network connection**.
- Select **Daily** from the drop-down menu.
- Click **Check Now**.

### **Protect Your Machine: Run Live Update**

The ICT Help Desk witnesses attacks of new viruses and worms once or twice per week. Make sure you install and update your anti-virus program. (i.e.: Norton Anti-Virus, McAfee, etc.)

**Note:** Running an outdated version of anti-virus software won't protect your machine. Without continuous updates, the software's virus definition files quickly become obsolete and ineffective against the latest attacks. If you purchased a new computer, the anti-virus software that was bundled with it is probably only a trial package with anti-virus file definitions that expire in three months.

**Note:** When configuring your machine for automatic updates, be sure to select a time of day when your computer will be ON and connected to the Internet.

### **Protect Your Machine: Run a Spyware Removal Program**

### ***Windows XP Users***

Spyware cleaners can detect and remove a multitude of adware files and modules from your computer as well as annoying popup windows. You can download any spyware removal program of your choice, but we recommend Spybot.

To download and install Spybot, please go to <http://www.download.com/3000-2144-10122137.html>.