




ResNet



Connection & Reference Guide

The wireless
ResNet is now
more secure
than ever!

Fire-up your
laptop, select **tu-guest**
for your *initial*
connection, then
click the secure
setup graphic. Our
wizard will help
you configure your
computer.



Student Computing Services
Office of Technology Services
Towson University

410-704-5151
scs@towson.edu
www.towson.edu/resnet

On behalf of the Office of Technology Services (OTS), welcome to Towson University. The information in this booklet pertains to University-managed residence halls and is important both for returning students and those experiencing campus housing for the first time.



In this guide, we describe your connection options, explain how to properly connect to the ResNet, how to safely access the Internet, and how to get technical assistance if necessary.

We encourage students connecting wirelessly to configure their computers for the secure wireless network, aptly named **tu-secure**. That process has been simplified by the implementation of an online tool (described on pages 3-4). When you first connect to **tu-guest**, look for the Secure Setup graphic shown here.



If after reading this booklet, you have questions or incur problems, help is available. Contact Student Computing Services (SCS) :

- ▶ Call 410-704-5151 (recommended during move-in)
- ▶ E-mail scs@towson.edu
- ▶ Visit the Service Desk in Cook Library, Room 35
- ▶ Consult www.towson.edu/resnet

SCS Staff will help you troubleshoot your connection issues and dispatch ResNet field staff to your room if required.

Be sure to read “The Beat Aboveboard” on Page 6 for an overview of the legal risks inherent in peer-to-peer (P2P) networks and file downloads.

On a final note, cable television service to your residence hall is provided by Comcast. Channel line-up and support information is available at www.towson.edu/cabletv.

Contents

Welcome	1
Introduction	2
Install Antivirus Software	2
Prepare Your Computer for TU's Wireless Guest Network	3
Prepare Your Computer for TU's Secure Wireless Network	3
Prepare Your Computer for TU's Wired Network	4
The Beat Aboveboard	6

Introduction

Towson University is committed to providing the best possible balance between network security and user convenience. As a member of the campus community, you have three connection options: wired, secure wireless (**tu-secure**) and guest wireless (**tu-guest**).

Wired	Secure Wireless	Guest Wireless
<ul style="list-style-type: none">• Fast, secure connection• Login required weekly• Wall port required• NAC Agent required	<ul style="list-style-type: none">• Best balance between convenience and security• Login required weekly• NAC Agent required	<ul style="list-style-type: none">• Convenient, less secure connection• Login required twice daily• NAC Agent not required

Access to all TU networks requires a NetID. If you host a visitor on campus, you can use **sponsor.towson.edu** to create a temporary (5-day) account with which your visitor may use the **tu-guest** network only.

Install Antivirus Software

For the most trouble-free ResNet experience, OTS recommends that you install **Microsoft Security Essentials** for Windows-based machines and **ClamXav** for Macs. (Note: antivirus software is required for PCs and recommended for Macs.) To download these antivirus products and view their installation instructions, open <http://www.towson.edu/adminfinance/ots/downloadsforms/softwaredownloads.asp> and click **For Faculty, Staff and Students**. Use your NetID and password to log in.

If you have already installed another antivirus application, you should uninstall it before installing one of these products.

Wireless Guest Network Setup

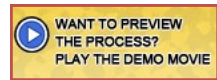
As long as you are a current student and have a NetID, you need only launch your browser and log in to access the Internet via the **tu-guest** network. You will be able to open most Web pages, work with your Web-based e-mail and calendar tools, and use WebDisk.towson.edu to move files in and out of your network storage space (or H Drive).

You will **not** be able map your storage space and student Web site as a network drive, install network printers (where allowed), or perform other tasks which require a more secure connection. Also, and perhaps most importantly, your computer will not benefit from the same level of protection on the guest network as it would on the secure network.

Secure Wireless Network Setup

Using the **tu-secure** wireless network requires that you take steps to insure that your computer is adequately protected against viruses, spyware and other threats. This in turn helps to prevent such threats from attacking the larger campus network and other students' computers.

While **tu-guest** might be more convenient, **tu-secure** is a safer option that allows full access to network resources. To configure your computer for **tu-secure**, follow the steps below. If you would like to preview the process, open www.towson.edu/resnet and click the button shown here.

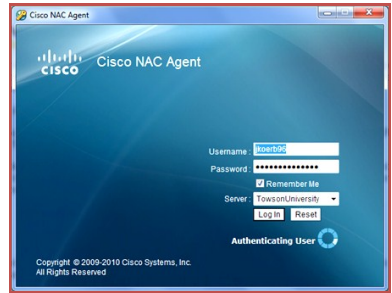


1. From on campus, start your laptop and view the list of available wireless networks. Among them, you should see **tu-guest**.
2. Connect to **tu-guest**.
3. Launch your Web browser. You will be redirected to the Guest Network Login page.
4. **DO NOT** log in. Instead, click the Secure Setup graphic shown here. The Secure Wireless Network Configuration wizard will display. (If you accidentally logged into



the guest network, just open www.towson.edu/resnet in your browser and click the Secure Setup graphic there.)

5. Follow the wizard's on-screen instructions, selecting **Student TU-Secure Wireless Network** and logging in with your NetID where prompted. The wizard will display a confirmation page once your computer has been configured and connected to **tu-secure**.
6. Click the **Set Up Cisco NAC Agent** link on the confirmation page, log in on the NAC Authentication page and follow the on-screen instructions to install the Cisco NAC Agent on your computer.
7. When prompted, log into the blue Cisco NAC dialog shown here. If there are mandatory requirements that your computer does not meet (e.g., out-of-date virus definitions or missing OS patches), Cisco NAC will grant you temporary access to the network and prompt you to correct the problems. Remember, SCS can help: 410-704-5151.



8. Once your computer meets all of the security requirements, the NAC Agent may again prompt you to log in. Once you do, you can enjoy the peace of knowing that your wireless activities will be as secure as possible.

Wired Network Setup

If you plan to plug your desktop or laptop computer into the wall port in your room, the following steps should speed you along. Be sure to enable your computer's AutoUpdate feature and make sure that all operating system (OS) security patches are up to date. Also, be sure to install antivirus software as described above.

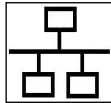
1. Start your computer and make sure that the built-in Windows or Macintosh firewall is enabled. If you don't know how, search your computer's help system. Windows users can select **Help and Support** from the **Start** menu and search for "turn Windows firewall on." Mac users can select **Help** from the **Menu bar** and search for "turn on firewall protection."

2. After verifying that the firewall is enabled, **turn your computer off.** *LinkSys Switch*

3. Locate your Ethernet cable.

4. Locate the blue and gray LinkSys **switch** (pictured right) mounted on your wall. If you have a *single* room, you will not need a switch; you can plug directly into the wall port. If your switch has more ports than are shown here, follow the instructions on the label affixed to the switch.

Ethernet Symbol



5. Connect one end of your network cable to your computer's Ethernet port, bearing the symbol shown here.

6. Connect the other end of the cable to one of the ports **numbered 1-4** on the LinkSys switch. **DO NOT** connect your computer to the ports labeled 5, 6, 7 or *Uplink*. The reference label on the metal bracket will help you identify the ports.

7. Start your computer, launch Internet Explorer or Firefox, and open the page www.google.com. At this point, the Network Access Control (NAC) system will intercept your page request and display the **Cisco NAC Authentication** page.

9. Log in to the NAC Authentication page with you NetID and password and click **Continue**. Then, follow the on-screen instructions to install the Cisco NAC Agent on your computer.

10. When prompted, log into the blue Cisco NAC dialog shown on Page 4. If there are mandatory requirements that your computer does not meet, Cisco NAC will prompt you to correct the problem. Don't forget, SCS can help: 410-704-5151.



You're an intelligent person. So when you weigh the risks and benefits, we think you'll find that it just doesn't make sense to download music and video illegally, not when there are so many great legal alternatives.

The beat aboveboard

Online stores such as Amazon, MP3.com and iTunes offer song

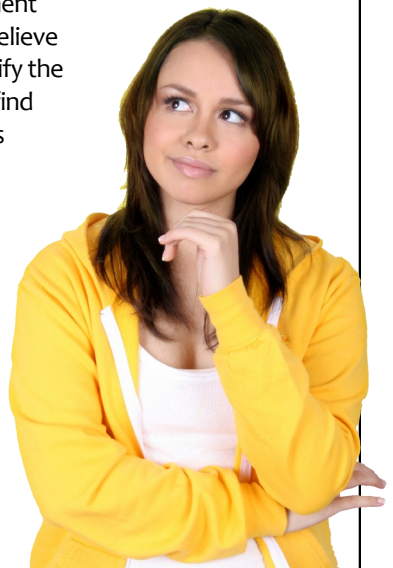
downloads for about a dollar each. Music streaming services such as Pandora and Live365 allow users to stream entire songs and create their own playlists to revisit at will. And there are dozens more legal music sites identified at RIAA.com.

Universities are not sanctuaries from prosecution. Like other campuses, TU is committed to supporting copyright laws, not to protecting those who violate them. For the relatively little money you could save by downloading music and video via unauthorized peer-to-peer networks, such as Kazaa and BitTorrent, you risk a lot more than you may realize. Did you know. . .

- ▶ Federal law states that unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject violators to civil and criminal penalties including loss of computing devices, responsibility for actual damages and legal costs, punitive damages up to \$1,000,000 and imprisonment up to 10 years.
- ▶ The Recording Industry Association of America (RIAA) and other representatives of the entertainment industry contact the University when they believe illegal downloads have occurred. They identify the offending IP addresses enabling officials to find the copyright violators. The University issues warnings to first-time offenders; repeat offenders can face sanctions ranging from loss of network privileges to suspension.

The risks are considerable, but completely avoidable. So, review the information at www.towson.edu/filessharing, explore the legal media services, and help TU. . .

Keep the beat aboveboard!





© 2011 Towson University. Produced by Student Computing Services.