

## Guest Access

Wireless security standards are still in their infancy. Until they mature, there will be many different methods for connecting and providing security.

During the early stages of wireless implementation at the University of Manitoba we had to provide and support a method for connecting to the wireless network that would allow us to securely authenticate wireless users. We accomplished this with our “Guest Access” model. During the authentication process, data that is transmitted to the authentication server is secure and protected. Once authentication is complete, any data, including passwords, are sent in clear text and are susceptible to being captured by anybody able to receive these wireless transmissions. Examples of this include using programs such as telnet, ftp, and pop mail.

## Secure Access

In order to secure your wireless connection and your data we have provided secure methods of authentication and data encryption using 802.1X and EAP- TTLS. We *recommend and strongly encourage* all wireless users at the UofM to use these standards for securely connecting to our wireless network. You can get the information you require to secure your connection at <http://www.umanitoba.ca/acn/networking>.

You can use “guest access” to get online and get the information you need to set up a secure wireless connection.

## Client Process for Guest Mode Wireless Authentication

Authentication permits wireless end users to identify themselves to the network and gain access to the campus network while they remain connected. There are several steps required to successfully connect.

1. Currently we support the 802.11b (11 Mbps) and 802.11g (54 Mbps) wireless standards. You will need to activate a wireless NIC card that at least supports 802.11b.
2. Your computer’s network settings must be configured to use DHCP.
3. You may have to release and then renew your old IP address settings. This is done differently depending on what version of Windows you have running. Other operating systems will likely be supported and documented in a later phase of this project. If this becomes necessary, follow the procedure below.
  - In Windows 9X, run **winipcfg** from the Start/Run menu. Select your wireless Ethernet adapter and use the Release and Renew buttons to get an address. Windows 98 also supports the **ipconfig** commands described below from a Command shell prompt.

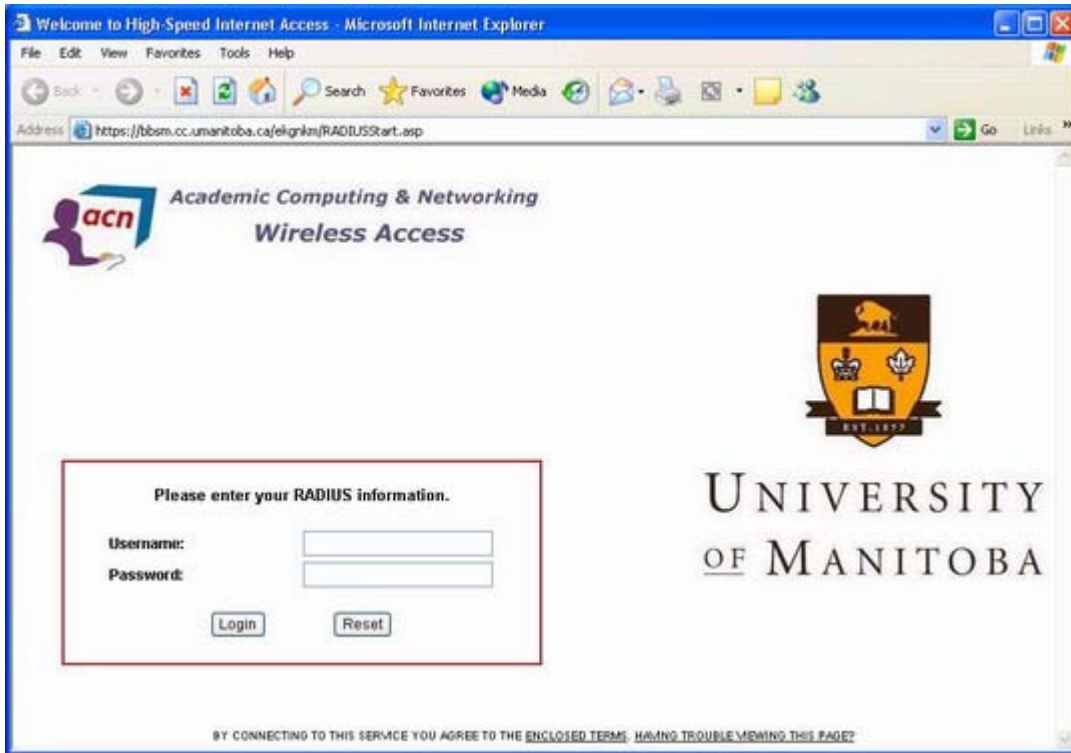
- In Windows NT, 2000 and XP, open a DOS command shell window. Use the commands **ipconfig /release** and **ipconfig /renew** to release and then get a temporary address from the network. You can check your IP configuration using the command **ipconfig /all**
4. To verify and view your IP address, you can use **winipcfg** or **ipconfig** where supported for Windows 9X systems. For Windows 2000 or Windows XP use the command **ipconfig /all** from a command shell prompt. On the Fort Garry campus you will get an address in the range of 130.179.252.1 to 130.179.252.254. On the Bannatyne campus the address range will be 140.193.230.11 to 140.193.231.244.
  5. All testing and verification has been done with Internet Explorer 6.X. You may see some differences with other browsers.

Open a web browser. After a few seconds, a **Security Alert** window may open indicating that there may be a problem with the site security certificate. It is asking you whether you want to proceed. The reason for this message is that the certificate is unsigned by a certificate authority. This process is safe and will provide encryption while you authenticate.

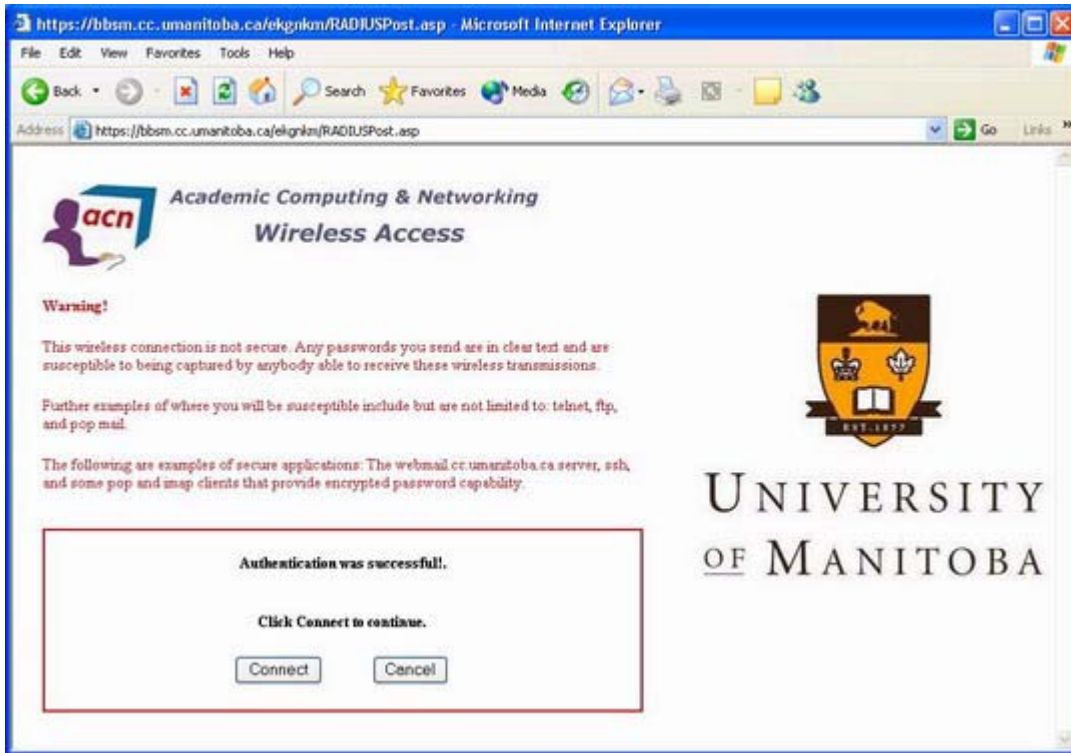
Click **yes** to process.



6. Your browser will be re-directed to web page allowing you to provide authentication credential to access our network. Enter your Unix username and password in the appropriate fields and click the **login** button.



7. If you have entered a valid username and password, you will see a new page indicating that the authentication was successful; otherwise, you will see an indication that your authentication has failed.



8. Once you have authenticated successfully, be sure you read and understand the warning message on this page. You can now click **Connect** to be connected to the campus network. You will be directed to the University of Manitoba Home Page and from then on our campus network. A BBSM Toolbar window will open. This window allows you to **disconnect** (un-authenticate) from the network. This window will not close until you click the **disconnect** button.



9. If you try to close the window, it will re-open unless you are running a pop-up blocker. If you just shut your PC off, you will automatically get disconnected after a timeout period.
10. When you disconnect gracefully, you should see the screen below.



## Troubleshooting

For information about setting up and using wireless on campus see: <http://www.umanitoba.ca/campus/acn/networking/>. If you require assistance connecting your wireless connection to the UofM's wireless network, you can contact the support desk at 474-8600 or email [support@cc.umanitoba.ca](mailto:support@cc.umanitoba.ca).

Our wireless network on campus is maintained on a best effort basis. If the wireless access service is not working, please report the problem via email to [trouble-desk@lists.umanitoba.ca](mailto:trouble-desk@lists.umanitoba.ca) or by phoning the Trouble desk at 474-8484. Please note that this procedure is for reporting a problem with the wireless network, not a client adaptor problem.

If wireless authentication is unavailable, you may see a web page with information describing the problem.

From time to time, the service may be unavailable for a few minutes while servicing is occurring. In these instances you may see a web page similar to the one below if you are trying to authenticate. If you have already authenticated, you shouldn't be affected. If you do see the page, close the window, wait a few minutes and try again.



Wireless networking at the University of Manitoba is subject to IST's "**Wireless Networking Procedures and Guidelines**" which can be found at: <http://www.umanitoba.ca/acn/networking/wireless-guidelines.pdf>