

# Securing a Home Wireless Router

## Sunland Springs Computer Club

### January 19, 2011

## How can you protect your wireless network?

### **1. Allow Network Address Translation and DHCP to handle IP addressing.**

NAT & DHCP (Network Address Translation and Dynamic Host Configuration protocol): Two services offered by the router to hide internal network addressing from the outside and automatically assign IP addresses and networking information to hosts. Advanced users can consider changing the range of addresses assigned to the internal network.

### **2. Change the default SSID (network name) and disable SSID broadcast.**

Change the default SSID (The name used to identify your wireless network). Wireless devices have a preset SSID that also by default advertises your network through a broadcast. Hackers know these defaults and can try them to join your network. Change the network's SSID to something unique and disable SSID broadcast.

### **3. Change the default password needed to access a wireless device.**

Wireless products such as access points and routers will be ask you for a password when you want to change their settings. They have default passwords set by the factory. Once again, the hackers know these defaults and will try them to gain access. Change the password to make it more difficult for unauthorized users to get in to your devices.

### **4. Enable MAC address filtering.**

Enable MAC address filtering if your wireless products offer it. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. This makes it harder for a hacker to access your network using a random MAC address.

### **5. Encrypt your data using WEP or WPA technology.**

Encrypt your data by using WEP or WPA to make intercepted data packets unreadable by the hacker. WPA is a much superior technology and should be used instead of WEP if available.

### **6. Use up-to-date anti-virus and anti-spyware utilities on your workstations.**

Keep your PC up to date by patching Windows with the latest security updates, use anti-virus and anti-spyware software and, for extra protection, use a software firewall. Some possible software to consider: Norton Antivirus, McAfee Antivirus, Ad-Aware, Spybot Search & Destroy and Microsoft Windows anti-spyware and Internet Firewall.

### **7. Turn off your wireless if you are not using it.**

Most laptops and routers allow you to disable the wireless interface, limiting the ability of someone nearby being able to access your computer or network.

[Robert.Samson@mcmail.maricopa.edu](mailto:Robert.Samson@mcmail.maricopa.edu)

Mesa Community College Networking Academy

## Glossary (Inquiring minds want to know!)

**802.11:** The designation for the standard that defines how wireless networking will be implemented. The 802.11-N standard defines a 50-600 megabits/second connection, which is the most widely used today. The 802.11-A and 802.11-G standards are also popular because they offer 54 megabits/second. 802.11-G is backwards compatible with 802.11-B, the previously most popular standard.

**DHCP** (Dynamic Host Configuration Protocol): A method of automatically assigning network addresses and other configuration information to a host (PC, laptop, etc) to allow it to communicate on a network. Addresses may be configured manually, but it is much easier to allow the network devices to figure it out for you, therefore it is the default setting for Windows 2000 and XP.

**IP Address** (Internet Protocol Address): This is a 32 bit number, usually represented in the form X.X.X.X, which gives a unique identifier to a network device. PC's, laptops, printers, routers, refrigerators, PDA's, security systems, cameras, etcetera can all have IP addresses. This is the address that allows communications outside of your Local Area Network.

**MAC Address** (Media Access Control Address): A unique serial number that is embedded in each networked devices interface to allow it to communicate within the Local Area Network.

**Modem:** A device that converts signals from your Local Area Network format into a format suitable for transmission across the Internet. Both cable and DSL (Digital Subscriber Line) modems are used in residential installations.

**NAT** (Network Address Translation): A method of using different IP addresses on your inside network from the ones used outside on the public network (Internet).

**Password:** a word used to restrict unchallenged access to a network or device.

**Passphrase:** Used by some wireless routers to generate the WEP key. This is the "seed" value that is used to produce a unique key that can be shared with users to allow them to use the encrypted network.

**Router:** A device used to connect your Local Area Network to other networks. The most common use is to access the Internet.

**SSID** (Service Set Identifier): A unique name shared among all points on the wireless network. This name, which is required for connectivity, may be broadcast to anyone with wireless access to identify the network.

**WEP** (Wired Equivalent Privacy): A data privacy algorithm based on encryption using 64, 128 or 256 bit shared keys. This is currently a primary defense against eavesdroppers obtaining data from your home wireless network.

**WPA** (Wi-Fi Protected Access™): A security method that encrypts the data transmitted on a wireless network so that only users who know the passphrase or shared key can access the network or understand the transmitted data. This newer form of security is replacing WEP until even stronger WPA-2 is implemented in 802.16 wireless protocol.