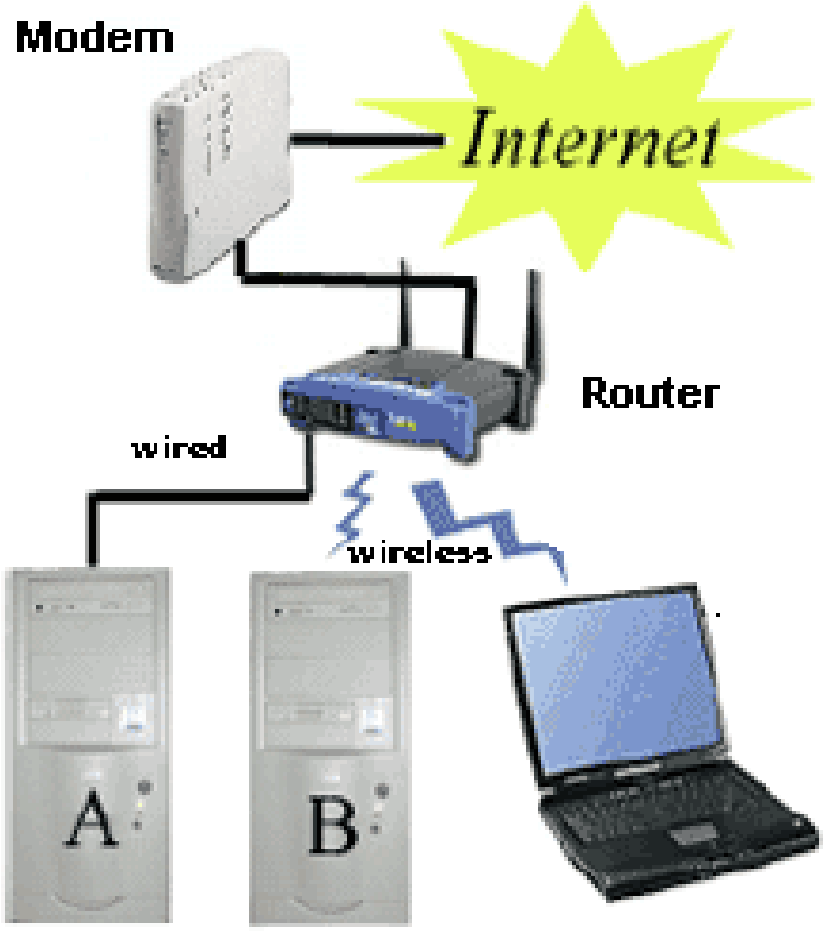
THE 123 OF WIRELESS SECURITY AT HOME/SOHO

家居WIFI 保安 123

CONFIGURING YOUR HOME WIRELESS NETWORK

Presented by: WTIA & PISA

Home Network



- Internet – ISP
  - **Wire to home**
- Modem
  - **Translates electronic data**
- Router
  - **Disperses electronic data**
- Network Adaptor
  - **Required for each Computer**
  - **Wired**
    - NIC (network interface card) or ethernet card
  - **Wireless**
    - Wireless Adaptor

Functions of a Home Wireless Router

- Router
- Access Point
- Firewall

What is a Router

- Connects one network to another … Sometimes called a “Gateway”
- Connects your computer to the internet (cable modem or DSL Line) – keeps LAN traffic local
- Routers keep track of IP addresses and physical (MAC) addresses of hosts
  - IP (Internet Protocol) address … your computers internet address
  - MAC (Media Access Control) … id for each physical communication device

What is an Access Point

- A point where computers access a network
  - Device which links wireless users to network
  - Transmits and receives data (Transceiver)
  - Bridge between wireless and wired networks
- Can be linked together to cover broad area
- No security or firewall implemented
- Wireless Networking Standards
  - 802.11 a, b, g, n and ac
    - configuration specifications to insure compatibility
    - Different speed/range capabilities
  - Equipment conforming to “n” and “ac” are most popular/available
    - Good for 100-400 feet … in a house

What is a Firewall

- A device that filters packets of data or traffic
- Its job is to be a traffic cop
- You configure the firewall:
  - What will allow to pass
  - What will it block
- Hides your home network from the outside world
- Can be either in hardware or software
- Most popular routers for home have built in firewall protection

What Does a Firewall do?

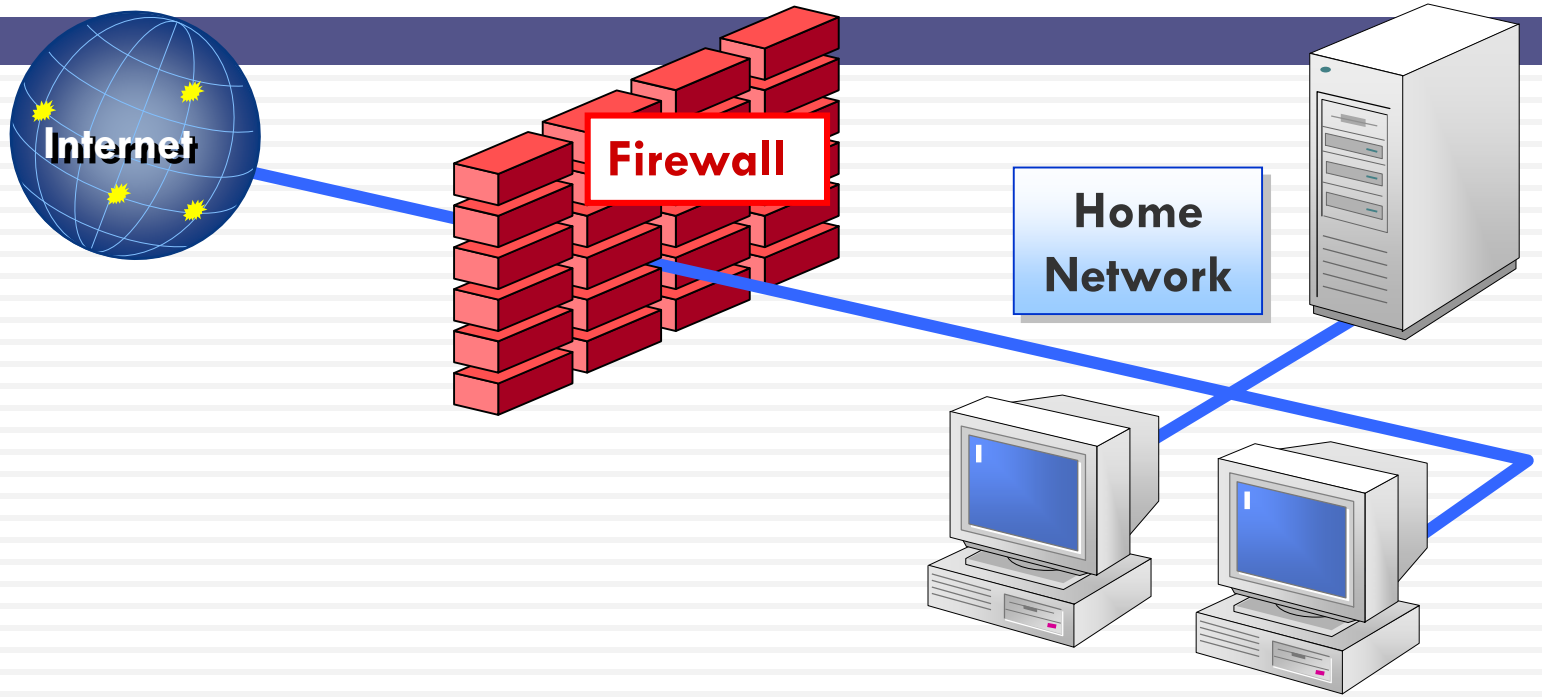
They:

- Protect your home computer from the bad guys
- Keep your information private
- Make you less of a target

By:

- Stopping viruses
- Hiding your computer from the world
- Making the bad guys work harder to get your info

Firewall Protection



1. Checks incoming traffic from the network before it gets to your home network ….
   default – Blocks all Incoming connections
2. Traffic leaving your home network …
   default - Allow all outbound connections
3. Hardware firewalls protect you home network by stop all traffic before it get to your computers
4. Personal software firewall on your computer blocks incoming and outgoing (lets you know what is leaving your computer)

Configure Wireless Firewall/router Overview

1. **Set Account name** and password
   - Change name and password … don't used default
2. **Basic Settings** … name, internet connection, ip address, etc
   - Check for firmware updates
3. **Wireless Settings**
   - SSID broadcast …
     - make sure that remote computers are set to automatically connect
   - Do **NOT** enable DMZ
   - Do enable ping blocking
4. **Security** - Blocking and Filtering
   - Wireless Security encryption
   - MAC filtering
5. **Backup settings**

Account Name

- Change name
  - Default name is set by manufacturer … eg, Belkin54
  - Bad guys know defaults and default administrative passwords
- Create Administrative Password
  - Use Strong Password
- Record your password where you can find it so you can make changes

Default Info

- Router default info is easily available on internet for consumers … and the bad guys
  - eg
    - http://www.otosoftware.com/wwhelp/Default_Router_Usernames_and_Passwords.htm
    - http://forum.pcmech.com/showthread.php?t=64258
    - http://www.defaultpassword.com
- So Change Name and Password

Mfg	*Default IP*	*User Name*	*Password*
Belkin	192.168.2.1	admin	blank
D-link	192.168.0.1	admin	blank
Linksys	192.168.1.1	blank	admin
Netgear	192.168.0.1	admin	password

Passwords

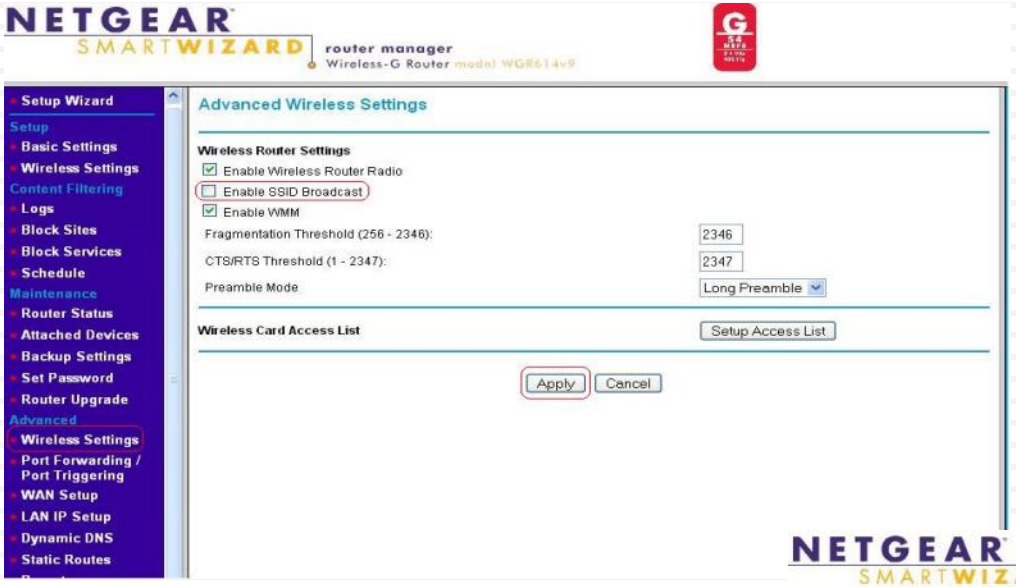
Your computer password is the foundation of your computer security

- No Password = No Security
- Old Passwords & Same Password = Reduced Security
- Set and change the "administrator" password on router (and your computer logon)
- STRONG PASSWORD … 8 characters
  - use upper, lower case, numbers and symbols

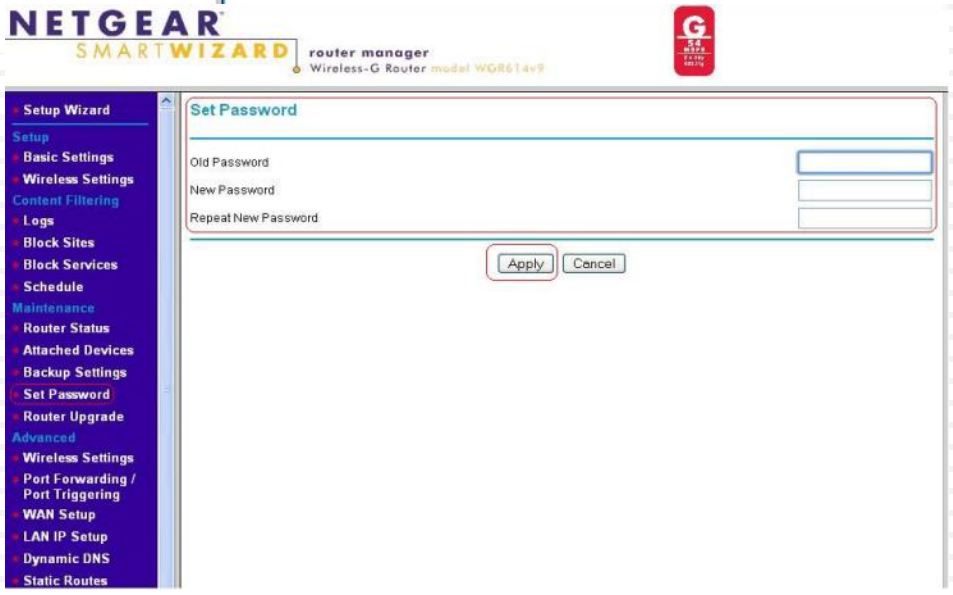
Wireless Settings

- SSID - service set identifier
  - name given to your wireless network, change it
  - Broadcasting this ID makes network visible to PCs in area
    - can be turned off so it will not be detected by other PCs in area
    - Be sure to set up your own pc to automatically detect and logon to your WLAN
- DMZ –
  - allows you to select a PC to access WLAN outside the firewall
  - do not enable unless firewall interferes with some activity
- Ping Blocking - troubleshooting tool
  - Signal sent and echo received indicates valid ip address
  - Used by hackers to find active computers
  - Enable ping blocking … won't send echo back
- WPS … Wi-Fi Protected Setup
  - Disable WPS after use

Example: SSID Setting



Go to Advanced-> Wireless Settings →Disable SSID Broadcast option



Change the Default Settings

Go to set password-> Change the default password

Security

Blocking and Filtering

- **Encryption** – coding transmissions
  - Multiple variations, WPA2, WPA & WEP in Wi-Fi
- WPA2-PSK … Wireless Protected Access (Pre-shared key)
  - Use same password for all computers
  - Use AES
  - Best Choice in Home/Soho
- ~~WPA-PSK~~
  - ~~2nd Choice (if WPA2 not supported)~~
- ~~WEP … Wired equivalent privacy~~
  - ~~64 or 128 bit encryption …~~
  - ~~Never never use this~~

Example: Authentication and Encryption

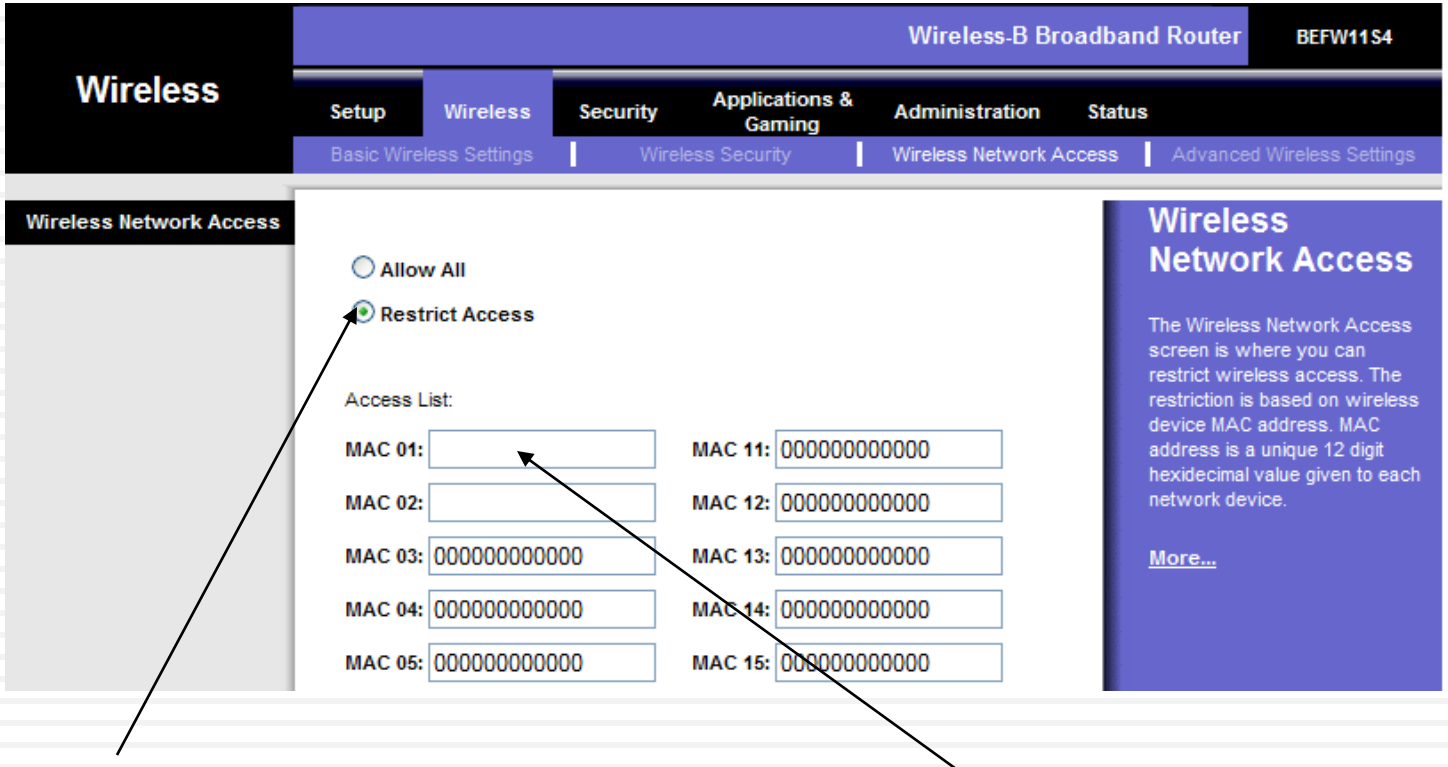
Go to Wireless Settings

- Authentication-WPA2-PSK
- Cipher type(Encryption)-TKIP or AES
- Pass phrase- Configure the pass phrase (Minimum 8 characters)
- SSID-Change the default SSID

MAC Filtering

- **MAC address …** Media Access Control address
  - Unique ID permanently attached to each communication device by manufacturer – hardware id
  - Can find MAC address (Windows Example):
    run → cmd → netsh wlan show interface
- Enter MAC addresses of acceptable network clients
  - If address is not on filter list, access to network will be denied
- Added Security

Example: MAC Filtering



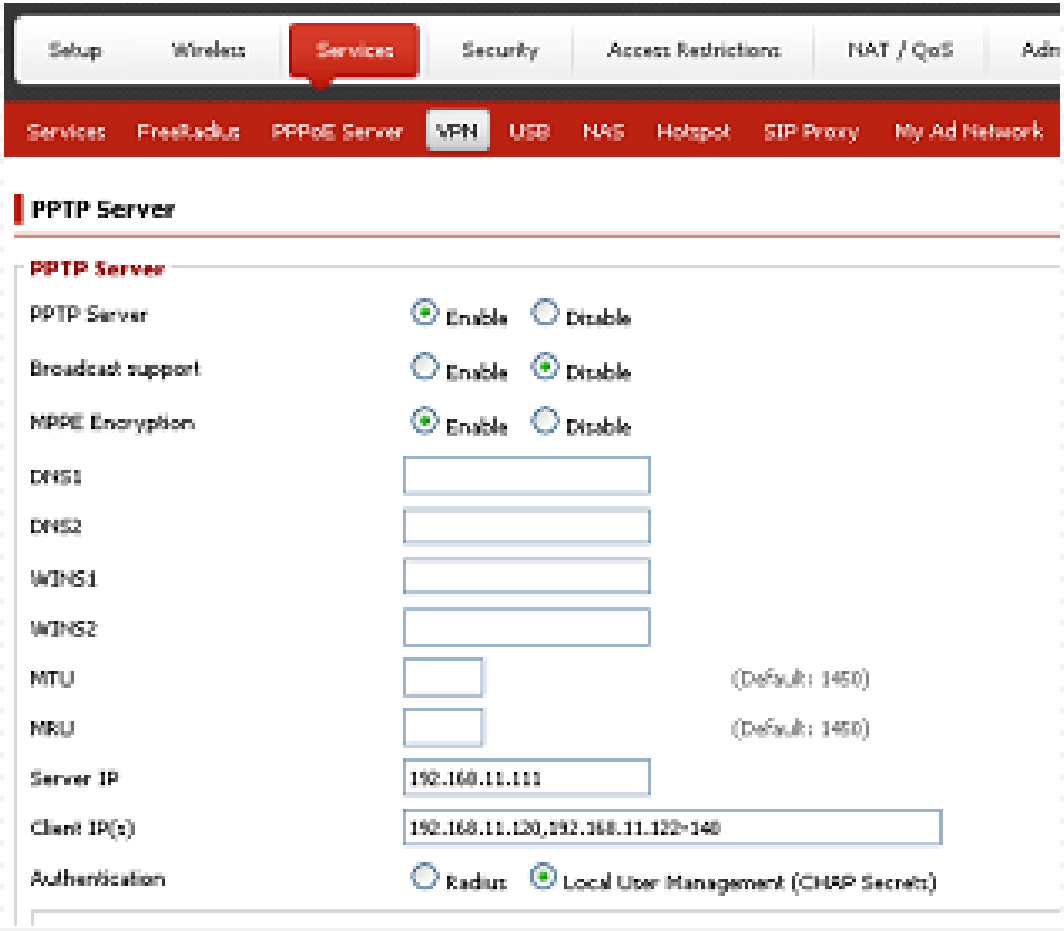
Check this to restrict access to prescribed MAC ids

Enter allowed MAC ids

To get the MAC address of your Wireless card, Go to "Command Prompt" and type "ipconfig /all" or "netsh wlan show interface"

Extra:

- Enable VPN Virtual Private Network
  - PPTP server
  - If available



RECAP- Steps to protect your wireless network

1. Change the default admin password on your router
2. Enable WPA2(AES) on router and wireless workstation
3. Use Strong WPA2-PSK key
4. Update Firmware
5. Disable WPS after use
6. [Added Security] Use MAC address filtering
7. SSID broadcast off
8. Prohibit Peer-to-peer (Ad Hoc) networking
9. [Advanced User] Turn on VPN, if available

Questions