



An International
Association of Technology
& Computer User Groups

Home Networking

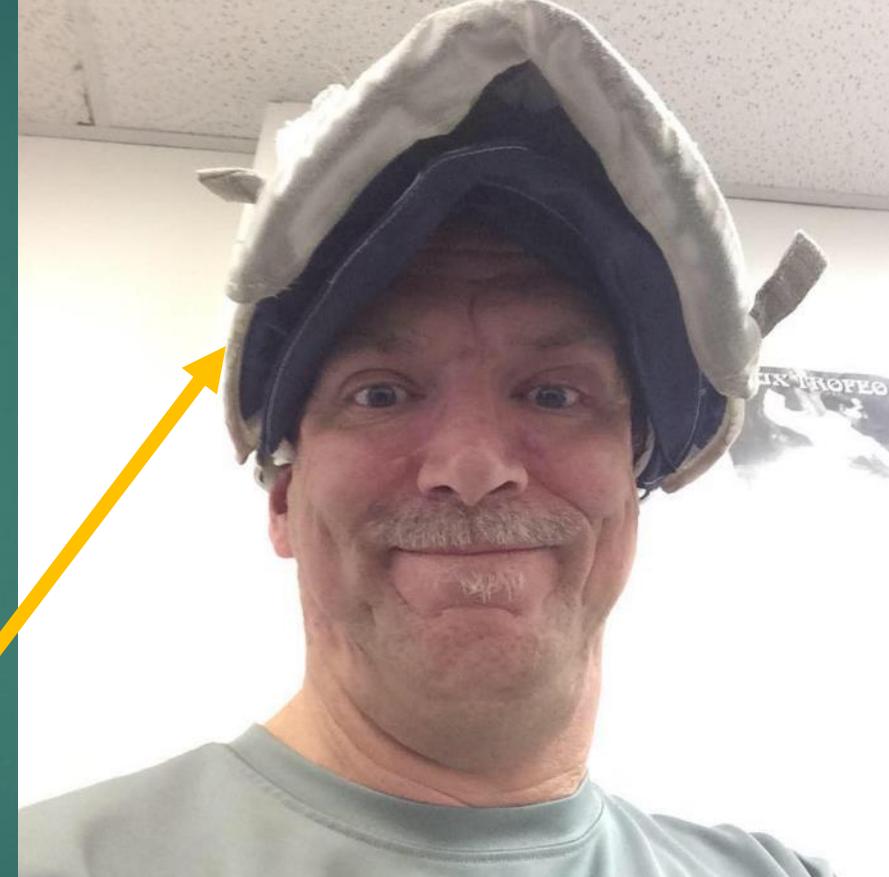
KEN ROGERS

APCUG VIRTUAL TECHNOLOGY CONFERENCE

MAY 7, 2016

Who Is This Guy?

- *Ken Rogers – a computer hobbyist all grown up (mostly), who has a fascination with PC networking*
- *Works as an IT Business Analyst at PNC Bank*
- *Lives in Ohio with his wife, kids, and 2.4 lawnmowers*
- *That's a fencing helmet on his head – yes, he plays with pointy weapons!*



What We'll Talk About Today

Wireless Networking in the Home

- Wireless Security – Two Commandments and Three Myths
- Improving Wireless Performance

Wired Ethernet Networking in the Home –
Not as impossible as you might think!

Computer Networking over Power Lines –
the future of home networking?

Home Networking – it all starts with the Router

- ▶ In a home network, the router is directly connected to the broadband modem
- ▶ All Internet devices (computers, printers, tables, smartphones etc.) access the modem through the router
- ▶ Most home networking routers also include a wireless access point, which sends and receives data over a radio signal that **cannot be hidden**



The router is the most important device in the home network, and has become as indispensable in the modern home as the microwave oven

Home Networking Terminology

I'm going to be saying these words a lot today . . .

LAN – Local Area Network; a home network is a LAN

WAN – Wide Area Network (e.g., the Internet)

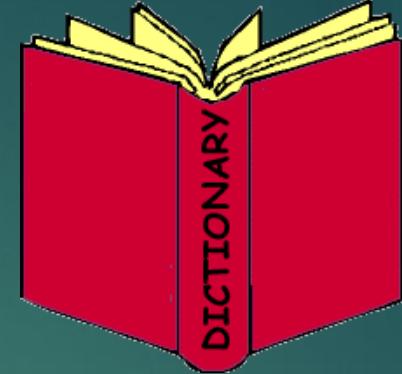
WLAN or Wi-Fi – Wireless LAN

Ethernet – the dominant technology standard for transmitting data over LAN cables

802.11 – these numbers (followed by one or two letters) appear frequently on wireless network devices, and represent standards maintained by the Institute of Electrical and Electronics Engineers (IEEE). Since these standards were designed to work with Ethernet, 802.11 is sometimes called “wireless Ethernet.”



More Terminology



Router – the most important device in a home network; among its many other functions, the router allows multiple devices on your home network to connect to the Internet

Access Point – a device that transmits and receives data for a wireless LAN; most home networking routers include an access point

Hub – a device that connects devices to a LAN

Switch – similar to a hub, but has more intelligence and transmits data much faster

Bridge – a device that connects and translates between two dissimilar LANs (e.g., Ethernet and Powerline)

Wardriver – a person who searches for unprotected wireless LANs

Piggybacker – a person who access an unprotected wireless LAN without permission

Wireless Network Setup

- ▶ Most wireless routers designed for home networks are ready to set up minutes after being unpackaged
- ▶ Immediately after you log in to your new router, heed the First Commandment of Wireless Security. . .

**THOU SHALT CHANGE THINE ADMINISTRATOR
PASSWORD!**

ADMINISTRATOR SETTINGS

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password : Verify Password :



- ▶ This is *critical*, as most routers allow remote administrative access over the Internet!

Wireless Encryption – It's Not Optional

- ▶ The Second Commandment of Wireless Network Security . . .

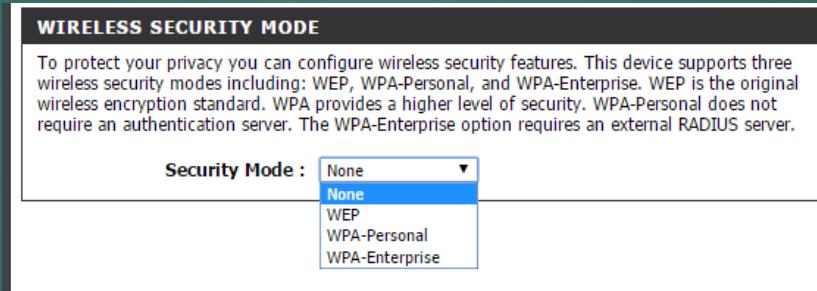
THOU SHALT ENABLE ENCRYPTION
ON THINE WIRELESS ROUTER!

- ▶ Your wireless router works by broadcasting a radio signal –
there is no way to hide your router's signal
- ▶ The only reliable option for protecting your wireless LAN is to enable encryption on this signal
- ▶ *In Germany, failure to encrypt your wireless LAN is punishable with a fine of over \$100!*



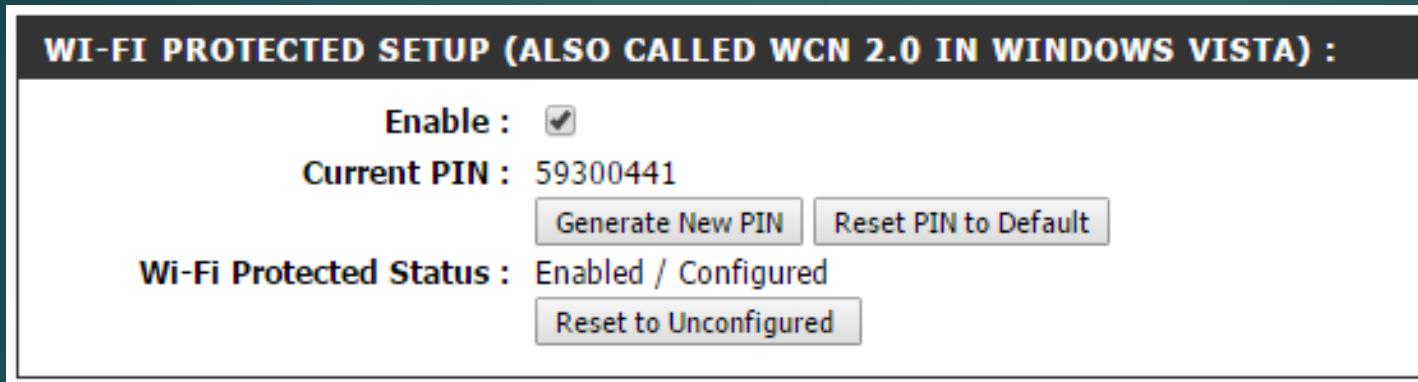
Enabling Encryption

- ▶ To encrypt your router's wireless signal, select an encryption type and enter an encryption code in your router's administration page
 - ▶ Where possible, choose WPA-2 or WPA, rather than WEP
- ▶ To add devices to your wireless network, you will have to enter the encryption code (only once – the device will remember the code)



- ▶ If you have a *Dual-Band* or *Tri-Band* router that communicates over both 2.4 and 5 GHz frequency bands, make sure you enable encryption on all bands!
- ▶ If you choose to enable the Guest network (Internet only), enable encryption on this as well

WPS



Most wireless routers provide a feature called Wi-Fi Protected Setup (WPS)

- ▶ WPS provides a simplified yet secure method for adding devices to your wireless network
- ▶ WPS works by pushing a button either on the router or in the router's administrative page, and then pressing a button or entering a PIN code on the device to be added
- ▶ Early implementations of WPS were vulnerable to hacks – the feature has become more secure, but some still consider it too risky to enable
- ▶ If you do use WPS, change the default PIN code

Wireless Security Myths

- ▶ In addition to changing your router's administrative password and enabling encryption . . .



WHICH YOU DID,
RIGHT?



. . . there are other security features available on your router you may choose to enable

- ▶ While these features will easily thwart wardrivers and piggybackers, they will do little to stop a resourceful hacker with malicious intent
- ▶ Since they don't offer significant security benefits over encryption, they are best considered myths

Myth 1: Turn Off SSID Broadcast

- ▶ Your wireless network name is actually called the Service Set Identifier (SSID)
- ▶ By default, your router broadcasts its SSID, so that wireless devices can more easily access the wireless LAN
- ▶ SSID broadcast can be turned off on most routers – some router manuals even refer to this as “hiding the network name”

Visibility Status

The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

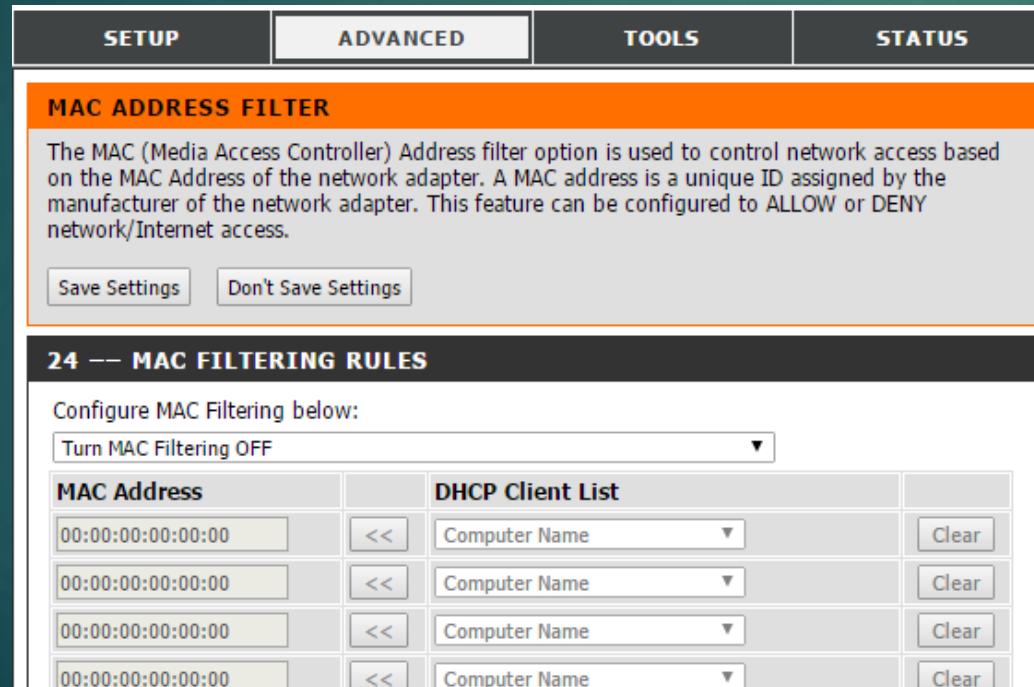
Does Disabling SSID Broadcast Make Your Wireless Signal Invisible?



- ▶ Sorry – the answer is no
- ▶ A Wi-Fi signal that's not broadcasting its SSID can still be detected by devices that search for Wi-Fi signals
- ▶ Disabling SSID broadcast might frustrate wardrivers and piggybackers – but will do nothing to stop a determined, resourceful hacker with malicious intent

Myth 2: Enable MAC Filtering

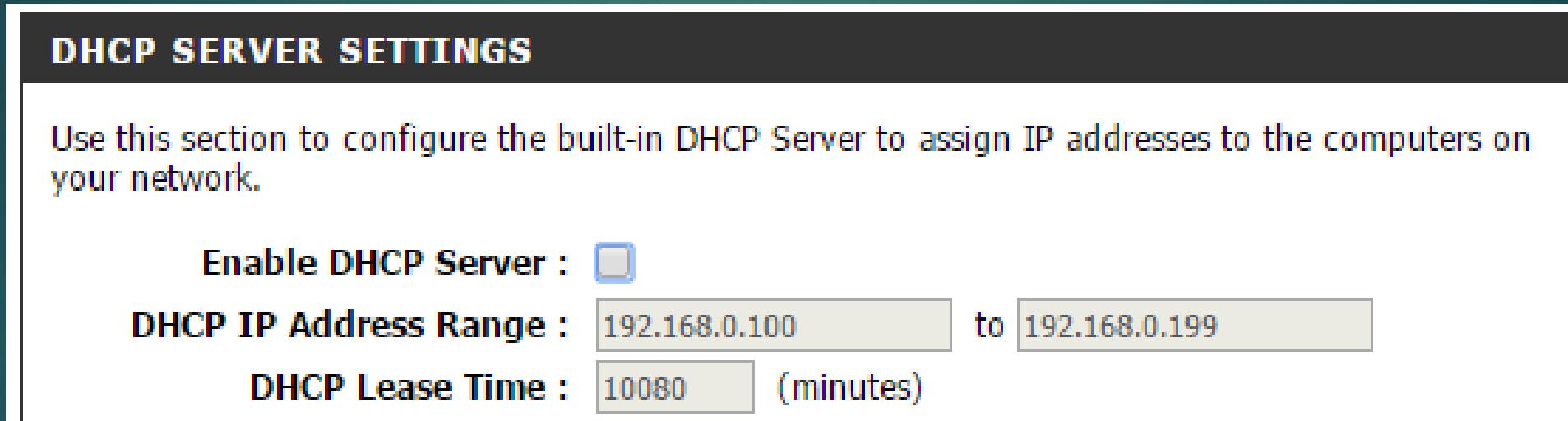
- ▶ Every network device (wired or wireless) has a Media Access Control (MAC) address
- ▶ If you execute an `ipconfig -all` command in a Windows command prompt, this will be the Physical Address



Most routers will allow you to restrict access to your network to a defined list of MAC addresses

Myth 3: Disable DHCP

- ▶ You can also use MAC addresses to manually assign IP addresses to network devices, instead of using DHCP



- ▶ By enabling MAC filtering and/or disabling DHCP, can access to a wireless LAN be effectively locked down – without having to use encryption?

Sorry folks . . .

NO.

You're wrong
so just sit there
in your wrongness
and be wrong.

- ▶ Remember, your wireless signal can never be hidden
- ▶ A determined, resourceful hacker with malicious intent can intercept that signal and, if it's not encrypted, fairly easily extract IP and MAC address information from that signal
- ▶ The hacker can then “spoof” this information, and gain access to your wireless LAN

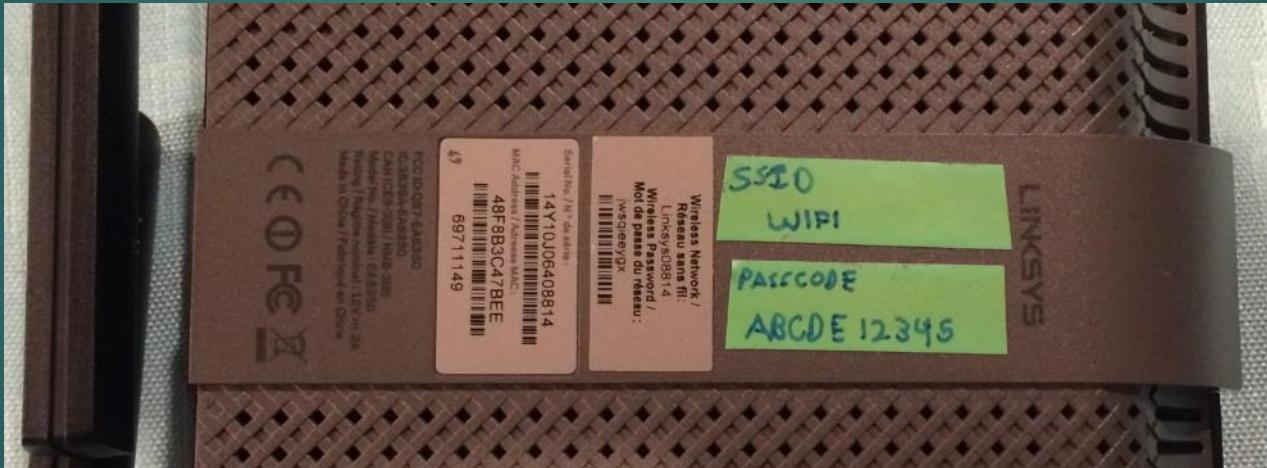
Keeping your Wireless Network Secure



- ▶ Disabling SSID broadcast, MAC filtering, and manual IP assignment all provide additional security – but not enough to justify the additional administrative work required
- ▶ None of these techniques will allow you to ignore the Two Commandments of Wireless Security – change your router's Administrator password, and enable encryption!

Wireless Security Made Easier

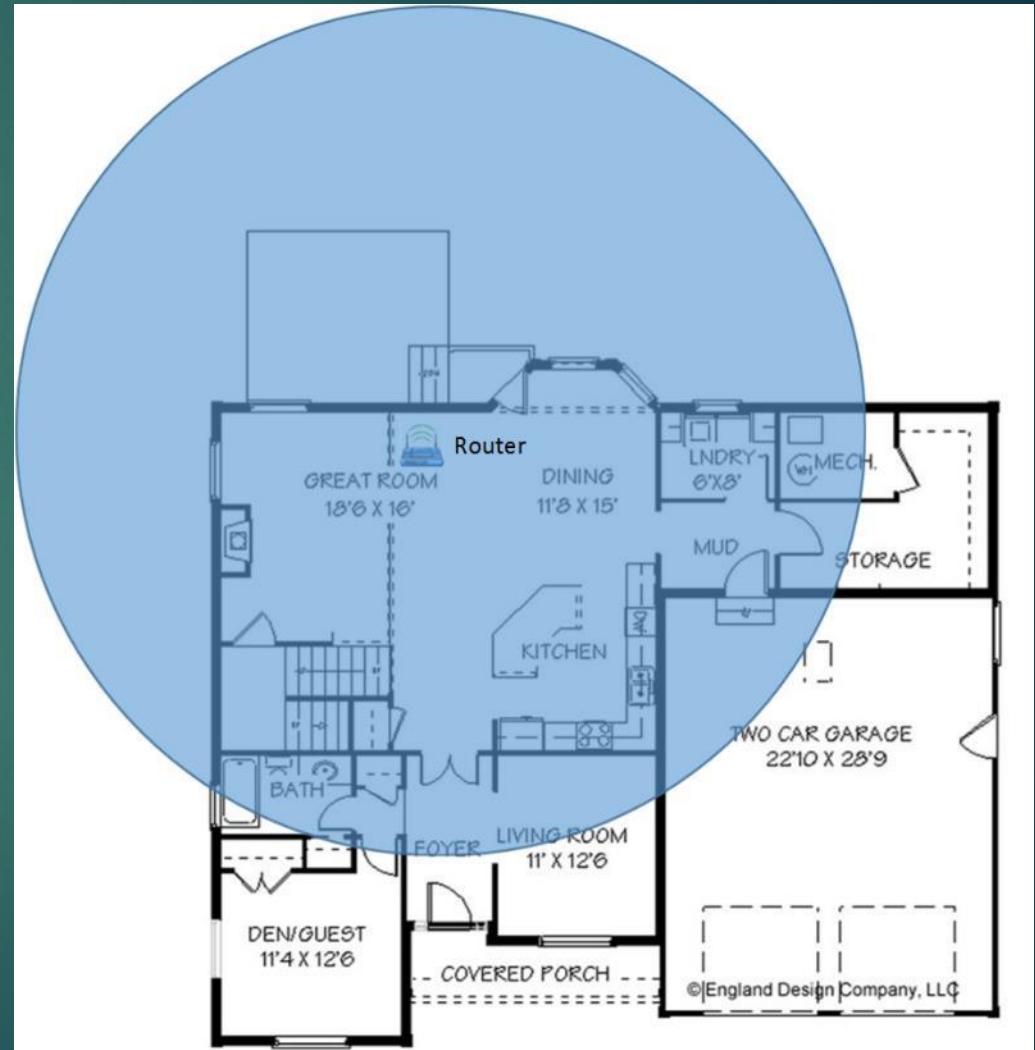
- ▶ The difficulty in adding new devices to a wireless network can be reduced by attaching some electrical tape to the bottom of the router
- ▶ On this tape, write the wireless network name (SSID) and encryption passcode



- ▶ This information is immediately accessible when needed, while remaining completely invisible to external threats

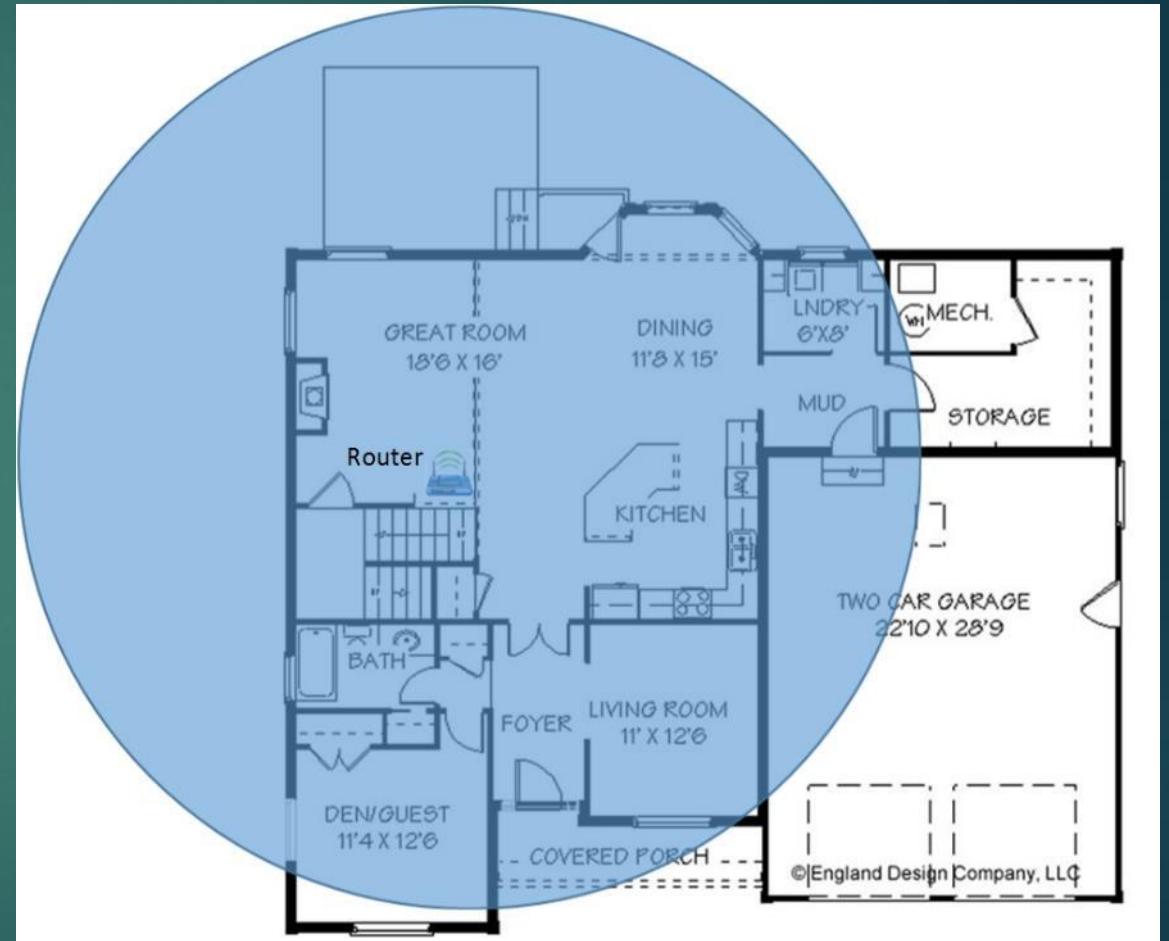
Improving Wireless Performance

- ▶ If you have a wireless LAN in your home, you've likely experienced outages and discovered "dead zones" where you get little or no signal (such as the Living and Den/Guest rooms on the right)
- ▶ Here are some suggestions for dealing with inadequate wireless performance



Location, Location, Location

- ▶ Your router's location has a direct impact on its performance
- ▶ Place your router in the most central location of your dwelling
- ▶ In the revised diagram, the router is moved to the Great Room, providing coverage for all living areas



Use the 5GHz Band



- ▶ 802.11g and older wireless technology standards communicated over the 2.4GHz frequency band, which is used by many other household devices
 - ▶ These devices can interfere and disrupt your wireless signal
- ▶ The 802.11n standard offered the option of communicating over the 5GHz band
- ▶ If your router and your mobile devices both support 802.11n, using the 5GHz band may improve performance by reducing interference



Upgrade Your Router

- ▶ As Wi-Fi technology continues to improve, routers are becoming more efficient and reliable each year
- ▶ Newer routers also come with additional features, such as USB ports that allow them to function as print and file servers



- ▶ If your router is more than 2 years old, you will likely see a noticeable if not dramatic performance increase if you replace it with a newer model
- ▶ A good replacement will cost between \$80 - \$120 – beware the bargain basement!

Router Tech Specs

- ▶ Several generations of 802.11 devices are available on the market:
 - ▶ 802.11ac (the latest generation commercially available) is expensive, but enhances performance for devices that can communicate in the 5GHz frequency band
 - ▶ 802.11n is affordable and performs well, and can also broadcast over the 5GHz band
 - ▶ 802.11g is yesterday's technology – it only communicates over the 2.4GHz band
- ▶ Look for Dual-Band or Tri-Band routers, which broadcast in both the 2.4 and (perhaps multiple) 5 GHz frequency bands
- ▶ Get as many antennas possible – they perform better, and look cool

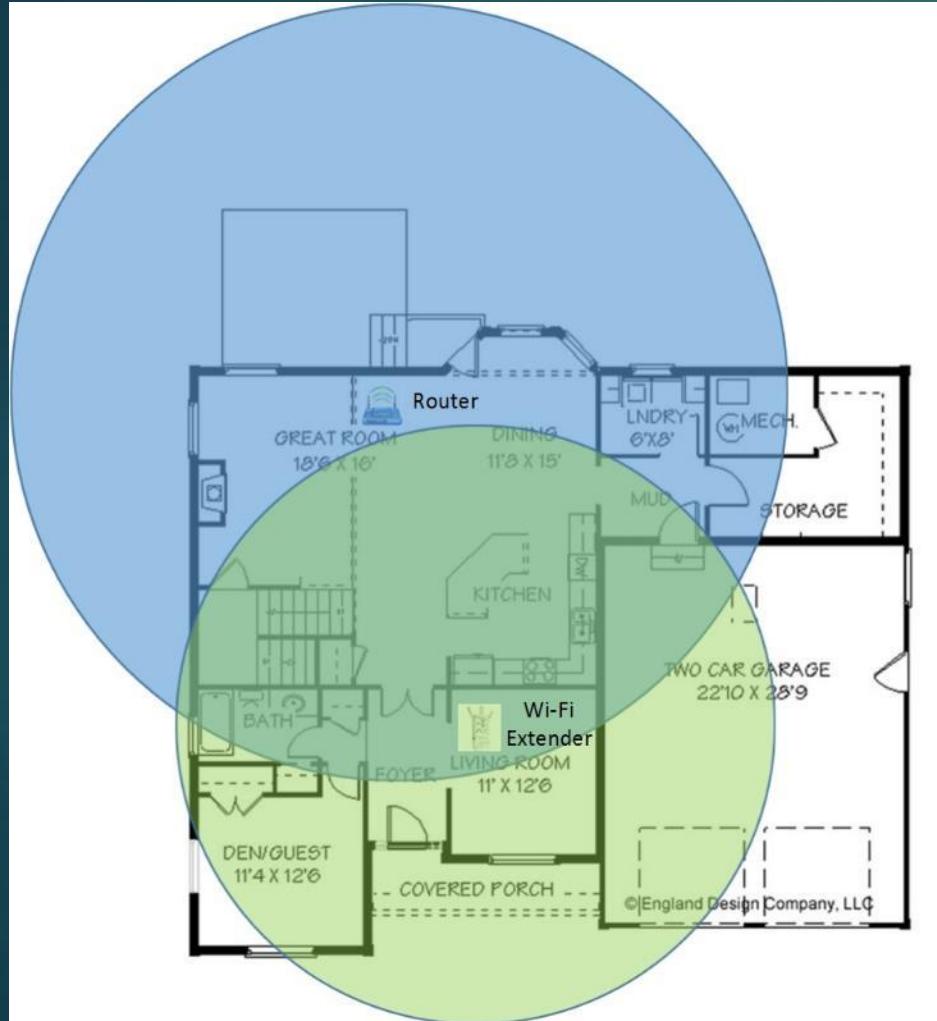


Wireless Range Extenders



- ▶ A wireless range extender, or signal booster, acts as a relay for your router's wireless signal
- ▶ Place the extender at the edge of your router's signal, and it should provide coverage across your dwellings "dead zones"

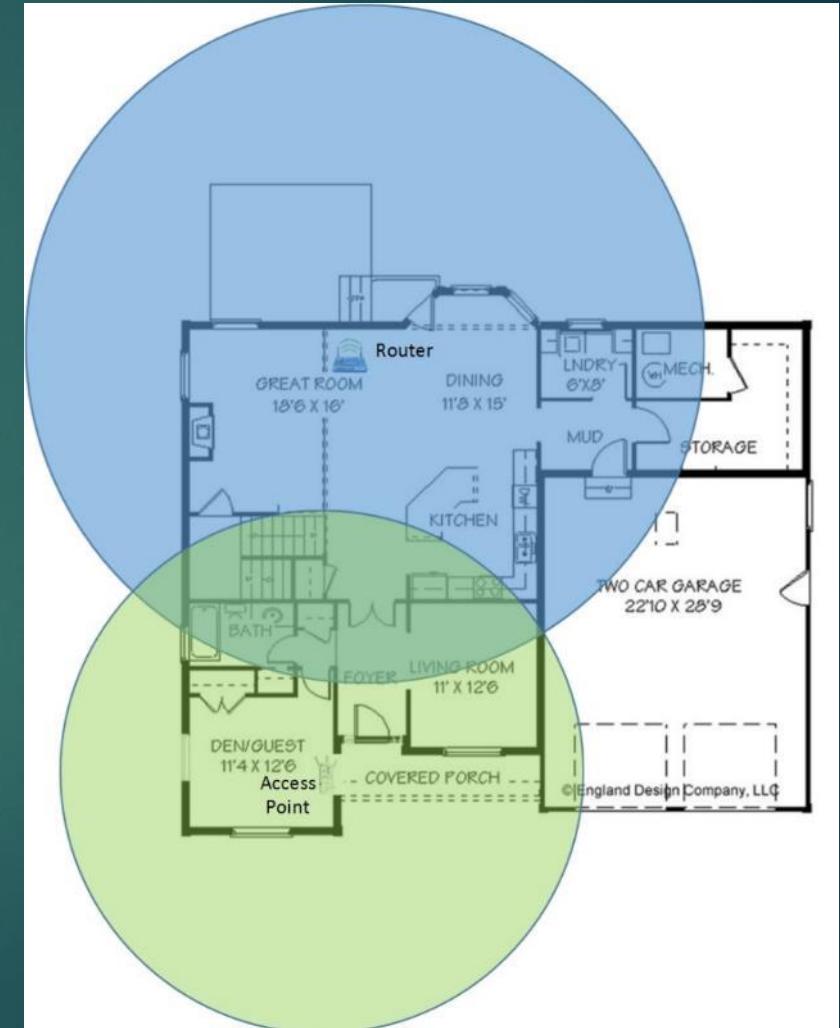
Issues with Range Extenders



- ▶ While wireless range extenders certainly work, using them may present additional issues
- ▶ In order to work, the extender must be in the router's signal range – and the extender's signal will overlap with the router's
- ▶ Mobile devices that connect to one signal will continue holding that connection even when it moves in range of the stronger signal

Alternatives to Range Extenders

- ▶ If your router has detachable antennae, you may be able to replace them with high-gain antennae that improve the router's range
- ▶ Another option is to add a wireless access point outside the range of the router's signal, as shown on the right
 - ▶ The area of signal overlap is greatly reduced
 - ▶ A mobile device that moves between areas of the floor is more likely to drop the fading connection as it approaches the stronger
- ▶ The access point would need a wired connection to the router – there's a couple options for making this connection

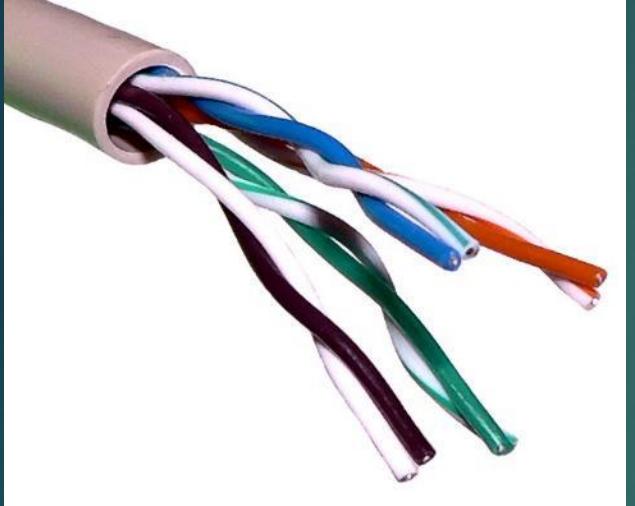


Wired Networking in the Home

- ▶ Wired networks will always be more reliable and secure than wireless, as well as faster (at least for the foreseeable future)
- ▶ Installing Ethernet cabling is not that difficult a task – especially if you have a drop ceiling above or beneath
- ▶ Several YouTube and online how-to guides are available for DIY cable installation

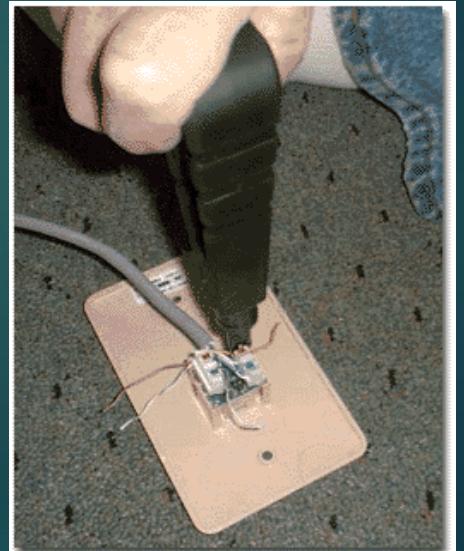


Making the outlets



- ▶ Cutting the outlet holes and running cable through the walls and ceilings is the hard part
- ▶ Making the outlets is the fun part!
- ▶ After cutting the cable and stripping its outer casing, you'll see four pairs of thin copper wires encased in colored sheaths

- ▶ You then use the punchdown tool to insert each wire into marked slots on the outlet – fasten the outlet into the wall, and you're done
- ▶ A pair of outlets can be installed in two rooms within a weekend



Non-Ethernet Wired Networks

If knocking holes in walls isn't an option or doesn't appeal to you, you can still install a wired network using cables that already exist in your home



Phoneline Networking (HomePNA) – my first home network; good luck finding these products today

Coaxial cable(MoCA)

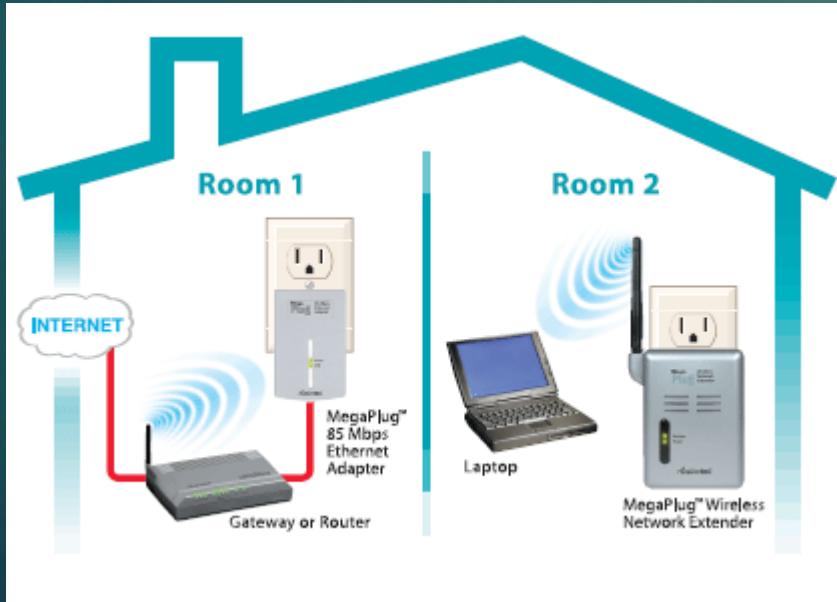


Powerline (HomePlug) – this technology is quickly gaining traction

None of these technologies are Ethernet – you will need a bridge to integrate any of these networks with a Wi-Fi LAN

Powerline Networking

- ▶ The advent of the “Internet of Things” has made Powerline networking an attractive option
- ▶ In the near future, you’ll be able to plug in your new appliance and have it immediately connect to the Internet



A Powerline connection can also be used to connect an access point to a router outside of range

Powerline Security



But Powerline comes with its own security concerns

- ▶ Powerline devices come with a default network name and password – if these are not changed, a hacker is one outlet away from home network access

- ▶ If you live in an apartment or condominium complex with shared electrical wiring, do not install Powerline devices without changing the default security settings
- ▶ The same advice applies for home owners with at least one outside electrical outlet

Questions?

