

Opening Remarks

- This is a technical topic that we will attempt to explain in terms that everyone can understand. There will be a lot of technical jargon, that you may have heard before. Hopefully you will build a basic understanding on what it means.
- It is important to all of us, as we have all become dependent on the access to the Internet, and eMail that our home networks provide.
- After all, you all drive cars, that are pretty darn technical. I'm sure that you have all built a basic understanding of how they work, if for no other reason than to be able to understand a mechanic when they tell you 'this repair will cost you \$\$\$' !
- *I'm sure that some of you with an engineering background may feel that I am over-simplifying, or skimping on detail. Please understand that I feel it necessary to allow the non-engineering members to build a reasonable picture in their minds.*

Home Network Security

by Mark R. Mach, CISSP

Mark R. Mach

- Mark has almost forty years of education and experience in the management and application of Information Security and Technology
- Chief Information Security Officer (CISO) at Certilytics, Inc.
- Certified Information Systems Security Professional (CISSP)
- Member of the International Information System Security Certification Consortium (ISC)2
- Member of and Director at Large for the board of the International Information System Security Certification Consortium (ISC)2 Phoenix Chapter
- Member of American Mensa
- Background includes: information security, management, information technology and security governance, systems integration, systems administration, network administration, independent verification and validation (IV&V), software development, process development and improvement, and technical documentation
- Studied Computer Science at Michigan Technological University
- Served in the United States Navy



What is a Computer (or Data) Network?

“A computer (or data) network is a digital telecommunications network which allows nodes to share resources.”

–*Wikipedia*

If you're connected to the Internet, using services from Cox or CenturyLink, or some other “ISP” (Internet Service Provider), you are a node connected to a computer network that spans the globe.

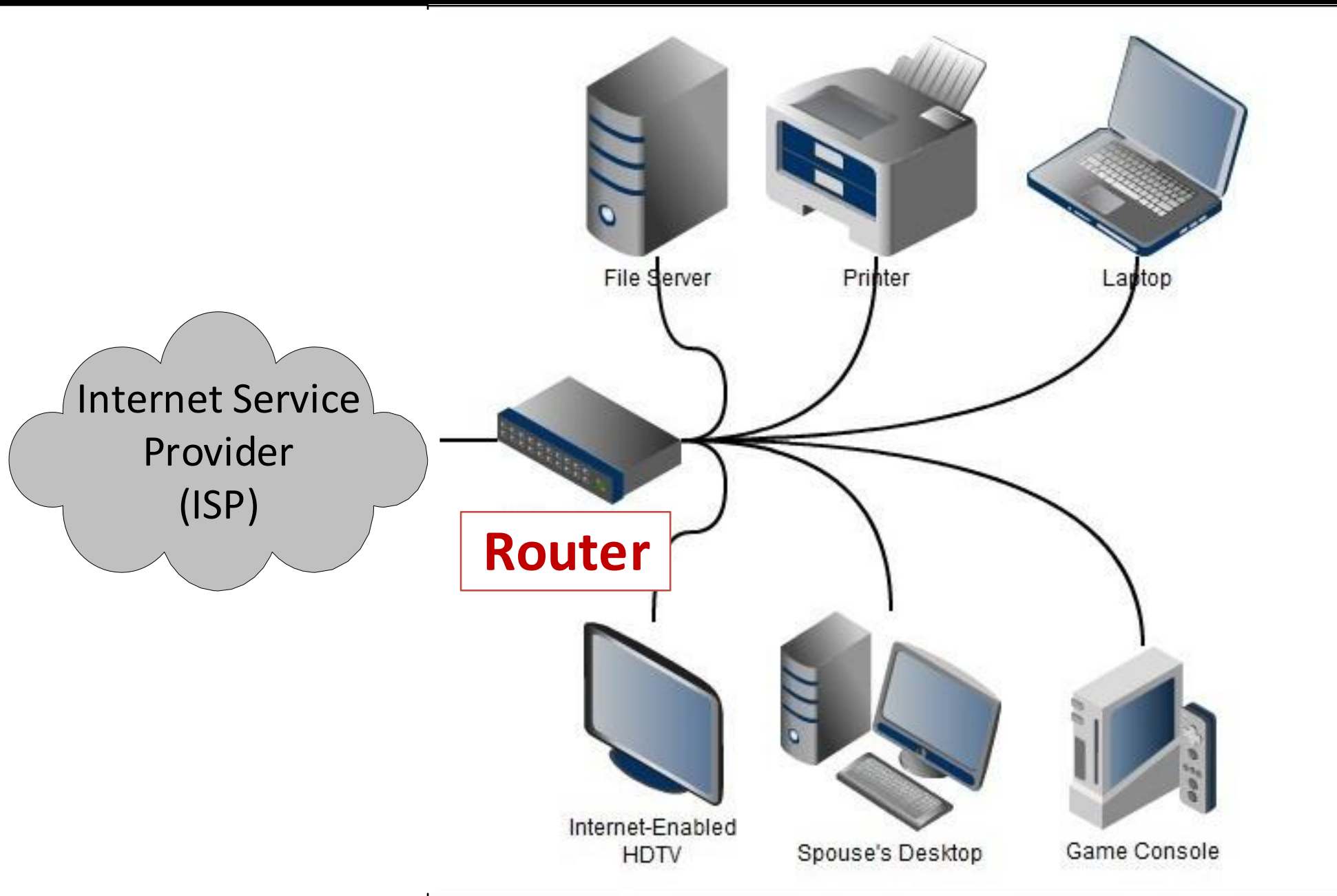
You will have a small piece of computer networking equipment, usually called, simply, a “router” or a “modem”, in your home. It manages all of this communication.

Your router is your front door to the world. It must be protected!

What's a 'network node'?

- Before I dive into more detail, let me explain that any device connected to a network is called a 'node' on the network.
- Your computer is a node on your home network. Your router is a node on your ISP's network.
- For this discussion, please keep in mind that when we talk about 'computers on the network', we also include any electronic device that you may use that communicates via your network with some other digital device. It's easy to picture them as PCs talking to the Internet, but we must include mobile phones, tablets, printers, TVs, security cameras, refrigerators, emergency pagers and all of the IoT (Internet of Things) that are now coming 'Internet enabled'.

Home Network



Identification of Network Nodes

When computers talk across a network:

- They send data from one node to another, up and down the chain. They're called 'data packets' (something like sentences).
- A single message (like a web page) may include thousands of packets.
- Each packet includes the ID of the sender and the ID of the recipient.
- These node IDs are called 'IP Addresses'
- Every node must have an assigned IP Address to send and receive data.

IP Addresses

- In order to hold a conversation with another node on a network your computer must have an IP Address.
- An Internet Protocol (IP) address has four segments (bytes), generally designated by four numbers ranging from 0 to 255, separated by periods (dots).

For example, the address of the computer I am working on now, on my home network is: 192.168.1.3
- IP addresses are unique, within the network where they reside. No two devices can use the same network address (an error will appear on both devices if this happens).
- We've found that with the growth of the Internet, they need to double the size of the IP Address to handle all of the nodes.

(IPv4 from 1984 could only support 4.3 billion nodes → IPv6)

IP Address Assignment

- IP addresses are either assigned permanently, by a management authority, or automatically, as needed by a Router ('DHCP facility').
- A block of IP Addresses have been reserved for use within a 'Private' network, like the one established in your Home.
- 'Public' IP addresses are used outside your home and across the Internet
- Your home router will assign private IP addresses for the devices within your home.
- Your home router has a Public IP address assigned by your ISP (Cox, Centurylink, etc.), that it uses to talk to the outside – to the Internet.
- You can see the public IP address that you are using by going to: <https://whatismyipaddress.com>

<https://whatismyipaddress.com>

My IP Address Is:

IPv4: **71.223.** [REDACTED]

IPv6: [REDACTED]

My IP Information:

ISP: CenturyLink

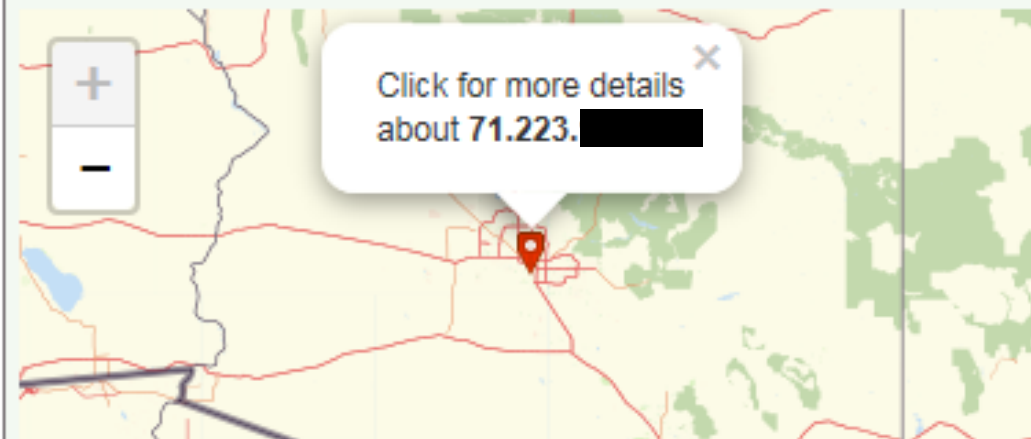
City: Phoenix

Region: Arizona

Country: United States

Make My IP Address Private

[Click Here](#)



Domain Name Services (DNS)

- One final technology...
- If all computers on the Internet have IP Addresses, and that's how we communicate with that computer node, how is it we get to Amazon using www.amazon.com.
- An important service, built into the Internet is a huge index of all web site (domain) names and their associated IP address.
- Your router, with the help of this index (the DNS service) finds the IP address based on the name you type into your web browser.

Home Routers



Your Home Router

The little black box that is connected to your telephone line (for CenturyLink) or your TV Cable (for Cox) handles all of your communication to the Internet.

- **Modem** – a device that converts signals from telephone, human-speak or TV cable speak, to digital computer-speak, and back.) I won't get into the difference between 'analog' and 'digital' communication. Just think of it like translating between English and Latin.

The modem may plug into your telephone line, your TV cable, or even connect to a satellite antenna.

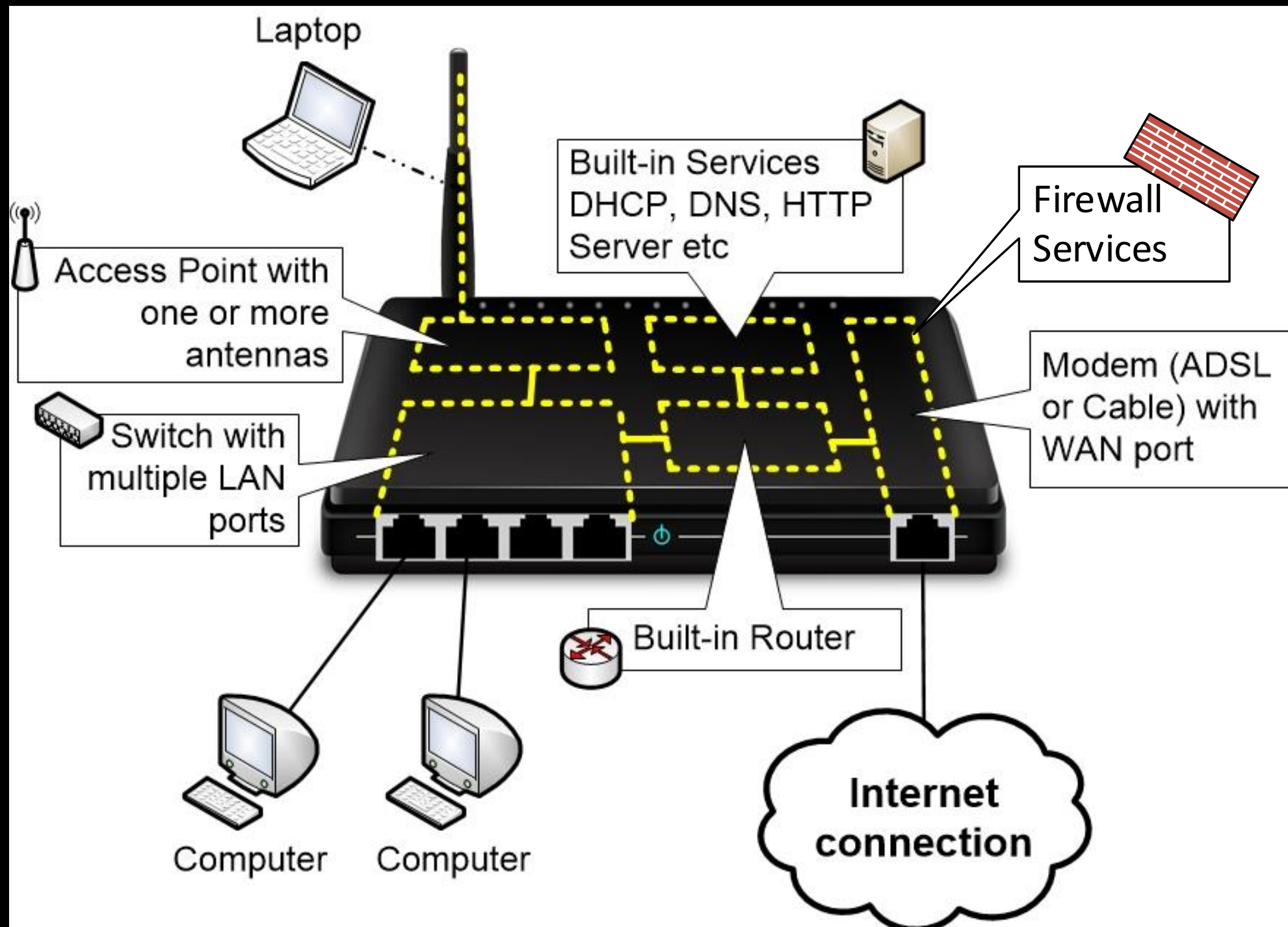
- **WiFi Router** a device that manages computer communication traffic (a traffic cop role) and allows computers to communicate over the airwaves. The Router and Switch work hand-in-hand, with the Router focusing on longer distance traffic (like to the Internet) and the switch focusing on local traffic (like within your home). These are called WANs (Wide Area Networks) and LANs (Local Area Networks)
- **Switch** a device that allows multiple computers to share a single line in/out, remember the old 'telephone 'party lines'?

You may not pass data back-and-forth between multiple computers in your home, but you may very well be utilizing this facility with a printer in your house.

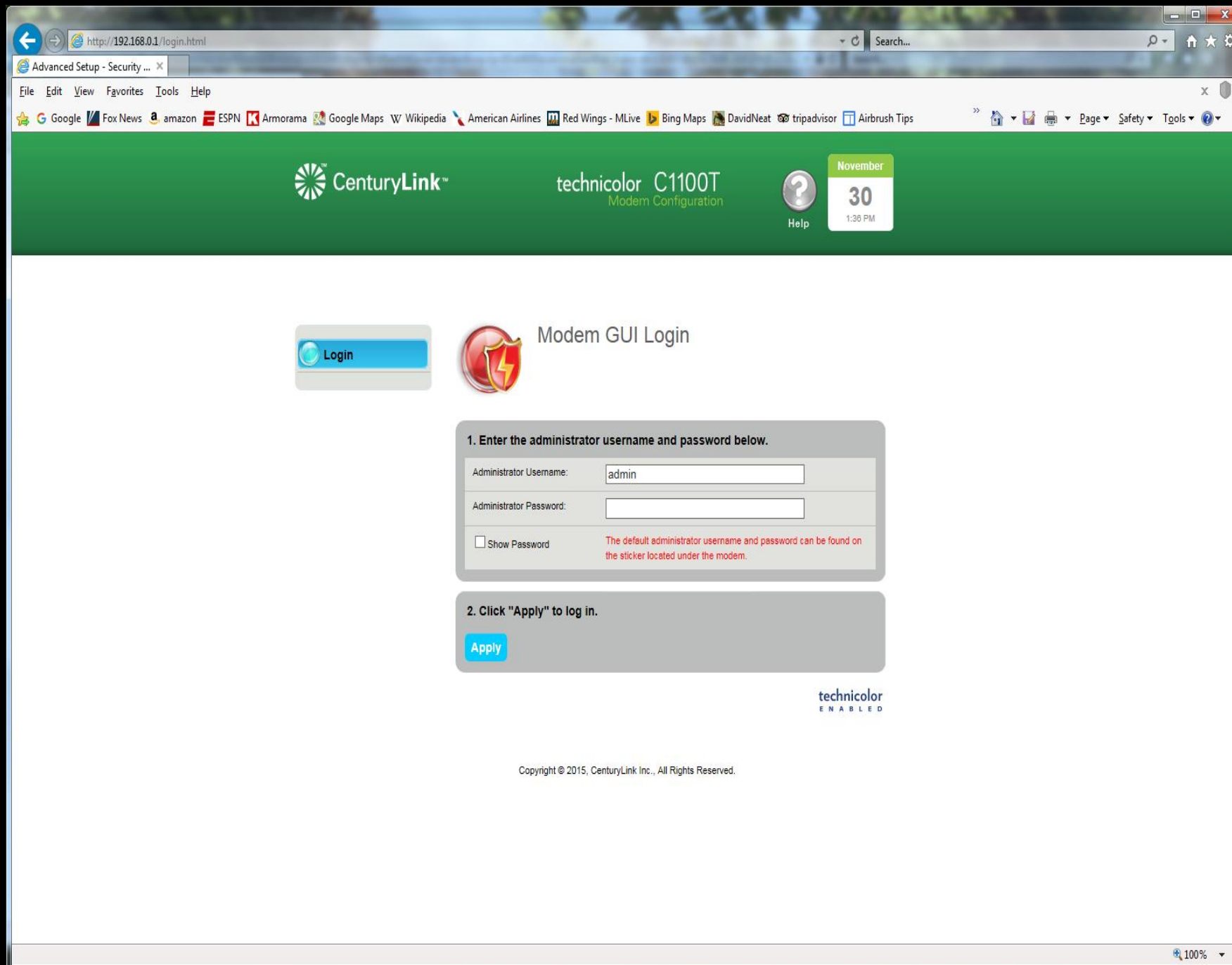
Your Home Router (cont.)

- **Services** to include assigning IP Addresses, looking up Domain Names and IP Addresses and a Control panel for configuring your router.
- **Firewall** a feature or device that enforces usage rules, for security purposes. The rules can define who and how computers can communicate with each other. This now-common facility is often overlooked (*except by Security geeks*)

Home Router Functions



My Router Control Panel



My Router Control Panel

CenturyLink™ technicolor C1100T Modem Configuration

Help November 30 1:18 PM Logout

Modem Status Quick Setup Wireless Setup Utilities Advanced Setup

Device Table

The list below displays all devices connected to your Local Area Network (LAN) with the connection type.

DEVICE NAME	IP ADDRESS	MAC ADDRESS	CONNECTION TYPE	SHARED FOLDERS
Ralphs-iPad	192.168.0.6	ec:ad:b8:8c:80:48	SSID 1	Unavailable
amazon-202 be0fad	192.168.0.7	34:d2:70:dc:c8:61	SSID 1	Unavailable
Main-2017	192.168.0.11	dc:4a:3e:6b:d4:3d	Ethernet 4	Unavailable
iPhone	192.168.0.28	80:b0:3d:cc:5a:74	SSID 1	Unavailable
EPSON42C 7E7	192.168.0.16	f8:d0:27:42:c7:e7	SSID 1	Unavailable

Show inactive devices






Connection Status

My Router Control Panel


IPv4 Addressing

IPv4 Parameter	Status
Modem IPv4 Address:	71.223. [REDACTED]
Modem IPv4 Subnet Mask:	255.255.255.255
DNS Address #1:	205.171.3.65
DNS Address #2:	205.171.2.65
Remote Gateway Address:	67.40.227.69
NTP Server:	206.196.149.2
IPv4 Packets Sent:	44357876
IPv4 Packets Received:	211637790
IPv4 Link Uptime:	73 Days, 10H:53M:54S

My Router Control Panel

Ethernet Port Status				
Ethernet	Port	Connection Speed	Packets Sent	Packets Received
	1	DISCONNECTED	N/A	N/A
	2	DISCONNECTED	N/A	N/A
	3	DISCONNECTED	N/A	N/A
	4	1G	85160099	48446555
	WAN/LAN	DISCONNECTED	N/A	N/A

My Router Control Panel



Access Scheduler

Access Scheduler sets Internet access rules for LAN devices.

1. Select Device, or manually enter an IP address.

Select Device:

Enter IP Address:

2. Set the days of the week on which access is allowed.

Sunday:	<input type="checkbox"/>	Wednesday:	<input type="checkbox"/>	Saturday:	<input type="checkbox"/>
Monday:	<input type="checkbox"/>	Thursday:	<input type="checkbox"/>	All Days:	<input type="checkbox"/>
Tuesday:	<input type="checkbox"/>	Friday:	<input type="checkbox"/>		

3. Select the time range access is allowed.

From:

To:

My Router Control Panel



Service Blocking

Service blocking provides the ability to block specific Internet services per device.

1. Select Device, or manually enter an IP address.

Select Device:

Main-2017 - 192.168.0.11



2. Select service to block.

Service:

FTP



Create New Rule

My Router Control Panel



SSID Setup

Follow the steps below to set up SSID's 1 thru 4. SSID's are also referred to by network name.

1. Select the SSID (Network Name).

SSID:

2. Set SSID broadcast.

SSID Broadcast:


Broadcast SSID

Hide SSID

3. Set the SSID network name.

Network Name:

My Router Control Panel



IPv4 Firewall

Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.

- 1. Set the stealth mode state.**

Stealth Mode: Enabled Disabled
- 2. Select the IP address or IP addressing type to which the firewall rules should apply.**

Addressing Type:
- 3. Select the Firewall Security Level.**

Security Level:

[Create Rule](#)
- 4. Set the firewall table below. Services checked are allowed. (optional)**

Service	Service Type	Service Port	Traffic In	Traffic Out
DirectX	Multimedia Control	2300-2400 TCP/UDP, 47624 TCP, 6073 UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DirecTV1	Multimedia Control	27161-27163 TCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DirecTV2	Multimedia Control	27161-27163 TCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DirecTV3	Multimedia Control	27161-27163 TCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Home Network Security Essentials

Network Firewall

- If your router that connects you to your ISP does not have a firewall, then buy a separate firewall device for home use.
- It should have stateful inspection (understands different types of transactions so it can intelligently accept incoming connections)
- Set it to block **EVERYTHING** incoming by default.
- If you need some incoming connections, you can add those as an exception to the ruleset.
- It is generally a bad practice to open connections to your internal network, so avoid doing so. Sometimes, an application will require certain ports open to function properly, and you may have to make those exceptions.
- When creating an exception, use rules that restrict the exception to the bare minimum needed. For example, if you connect to an audio conferencing server that requires UDP port 6000 to be open, then specify to the firewall that only the IP address from the conferencing server can connect to the specified host on UDP port 6000.
- Keep the firmware/software on your home router/firewall up to date. Bookmark the web pages if you can get and install the firmware yourself.
- For your home router that connects you to your ISP, you will generally need to get updates from your ISP, and they are notoriously slow at pushing out important updates. If you know there is a severe security vulnerability, call them, harass them, and tell them you will hold them liable if you are breached as a result of their negligence. (It has not worked yet for me, but good luck to you!)

Wireless Security

- Change the name of your wireless network (SSID) to something personal
- Password protect your wireless network.
- No, really—password protect your wireless network, and use a strong password that cannot easily be guessed.
- Use encryption on your wireless network, in this order of preference:
 - WPA2: the most secure of the protocols
 - WPA: not recommended, but it is better than nothing if WPA2 is not available
 - WEP: this is a weak encryption algorithm with known issues—do not use it if other encryption schemes are available. Upgrade your wireless access point if this is all it offers.
- Type your password for guests on their devices if you want to grant them internet access—a guest wireless network would be best for them (provides internet access but not access to the same network as your personal devices).
- Use discretion before giving out wireless access in your home. My wife (before we were married), provided her wireless password to her children's friends, and one of them was using BitStream to pirate software. She received a letter from her ISP threatening to suspend her ISP services as a result.
- Have actual trust before providing access to your home network.

Endpoint (Computer) Security

- Run a host-based firewall. Windows and Macintosh both have them built into the operating system.
- You can open services as required, but be selective like you are with your network-based firewall. You might need to open up some services for scanners, printers, or other devices on the local network.
- Restrict permissions appropriately. It might be convenient to have a file share on one device so you can access your financial records on all other computers in your house, but ensure that only you can access those files. Set your permissions accordingly.
- Use anti-malware (anti-virus) software. Don't consider running without it.
- Use strong passwords. My password is always fourteen characters or longer, with lots of complexity.

Beware Of Social Engineering

- Computer criminals find it harder and harder to break into computers, and are resorting to hacking the human instead of the machine. It's generally an easier target.
- Emails or web pages that announce that you won a free iPad are usually trying to get you to click on something that you shouldn't.
- Hover your mouse pointer over links in emails or on web pages before you click on them to see where they will take you. If the description says "[target.com](#)" and the URL that appears when you hover over it is not [target.com](#), then there is probably a huge risk in following it.
- Microsoft does not monitor your system remotely and help you when you have issues or they suddenly detect malware. Don't provide anybody remote access to your system, even if they claim that they are trying to help. Phone calls like these are a scam to break into your computer.
- Don't trust anybody that calls you—they can claim to be somebody they are not, and even use a phony caller ID. Call them back at published numbers for their organization (not numbers that they provide you).
- Don't use USB thumb drives that you find laying around. They may be infested with malware waiting for somebody to plug it in.
- Be skeptical!

Home Networking/Computing Physical Security

- Do not leave any important computing assets outside, in an open garage, or anywhere that people can easily access it without your knowledge.
- Cable runs are best done within walls or a secure space. A wired connection to a security camera on your network is easily disabled if it is stapled to the outside of your wall.
- Don't use untrusted equipment. That thumb drive sitting in the parking lot may be free, but it could be a trap that somebody left there, hoping that you would use it resulting into a malware infestation of your computer.
- Encrypt your computer hard drive. If your computer is stolen, it is what stands between keeping your data secure, and allowing somebody else to access it. There are third party tools to allow this, and it is a built-in feature of some versions of Windows, and all up to date versions of Mac OS.
- While you're at it, make sure that your mobile phone is encrypted and password protected. If somebody finds it and it is wide open, they have a key into your home wireless network, along with your name, address, and probably more personal information than you want to provide.

General Security Tips

- Update your software regularly—at least every month.
- Remove unnecessary services and software. If you don't need something, don't keep it installed on your PC.
- Adjust factory-default configurations on software and hardware. Do not leave the default admin account and password on your router or firewall—change them to use a well chosen password!
- Regularly back up your data.
- Improve your password security. You have had presentations on this topic before, so this is just a reminder to use long, complex passwords.
- If you have a techie friend receptive to answering questions and helping out, use them as a resource to answer questions if needed.

The Bottom Line

- Understand your home network. Knowledge is power, and the better you understand it, the better you can safeguard it.
- Use common sense. If something doesn't feel right, it probably isn't.
- Be skeptical about people wanting to access your computer, or wanting you to click on links on web pages or emails. Don't let them convince you to click by appealing to your motivators: greed, willingness to be helpful, not wanting to defy authority figures, etc. Social engineers are experts at manipulating people, and will use every trick in their book to do so.

Happy Networking!

Questions?