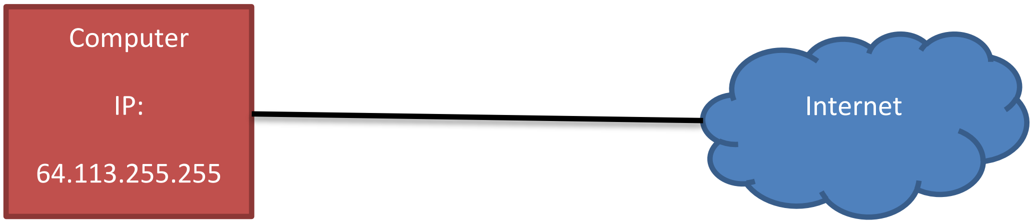
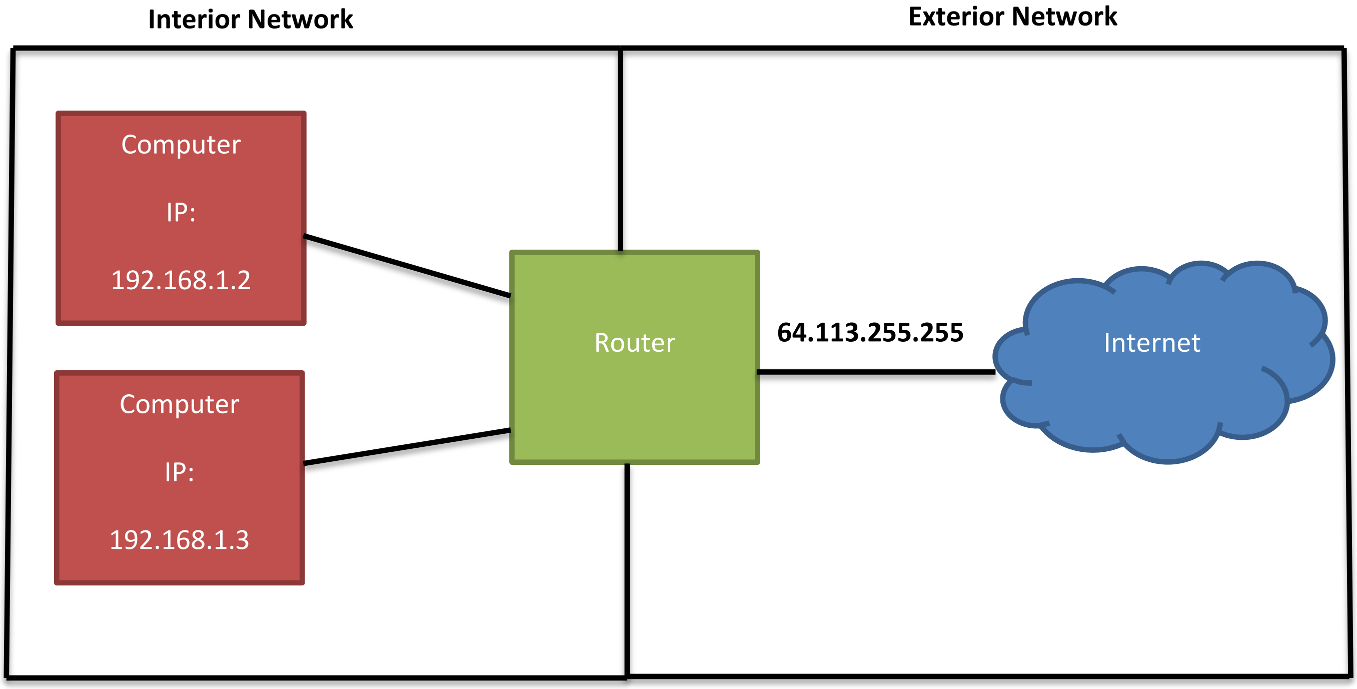
Wireless Encryption Protection

We're going to jump around a little here and go to something that I really find interesting, how do you secure yourself when you connect to a router.

Now first and foremost we should clarify what a router is and how it differs from a modem and switch, because if there is one term in networking that gets used WAY too much it's the term router for anything that people get Internet from.

Router – for our purposes we will assume we are talking about home routers, a device that forwards Internet packets of information by looking at the packet, deciding where it needs to go, and delivering that packet either by wired or wireless mode. This device is known as an active network element in that it can hand out DHCP leases to components behind it providing a hardware layer between the Internet and the internal network.





So the previous diagram shows the difference that adding a router can make to a network. In the first diagram the computer connected directly to the Internet getting a DHCP lease from his ISP. In the second diagram the router acts as an intermediary between the Internet and the devices. It hands out DHCP leases to the devices behind it and any device looking from the Internet cannot get the final IP address of the device it can only see the IP of the router, which is getting it's IP from your ISP.

This is a big distinction to make when doing your internal networking, making sure that services that are web based get your outward facing IP and internal services get your internal facing IP.

What the router is doing is effectively hiding your actual IP by putting a layer of networking in between, which is sometimes called network address translation or NAT. This hiding of IP addresses allows a device from inside the network to access the web but does not allow the web to access this device effectively making a barrier (there are circumstances that this can be overridden but for the purposes of this class we will assume this is not the case). While NAT protection provides a layer of security from the Internet, it also can cause problems with protocols that transport data over TCP connections like FTP, since no tunneling abilities are described in the NAT protocol (again there are ways to make this work, but the easiest solution is to have a public IP). Most users could have a form of NAT turned on and never know about it, but the power user will probably run into some situation that requires either port forwarding (will explain this more later) or a public IP.

Encryption

When data is passed over a physical line (like with Ethernet) if a person wanted to intercept the transmission, they would need a way to listen to that line. Now if that same person is connected via a wireless network the signal is broadcasted to the surrounding area, which makes it much easier for someone to listen in on the signal. The way to stop this is to encrypt traffic between the router and the end device. There are two prevalent forms of encryption in use today for wireless networks: Wired Equivalent Privacy or WEP and Wi-Fi Protected Access or WPA.

WEP –

1) Access point and device share a secret key to encrypt packets
    a. Key used to encrypt traffic is the password used for authentication as well
        i. Keys can be up to 128 bits
    b. Authentication is only done by the router and requires knowledge of the shared key

How connection is made to router:

1) Client sends an authentication request
2) Receives a challenge message from router in clear text
3) Client encrypts the challenge message with the shared key, and sends it back to the router
4) Router decrypts return message and compares it to the challenge message sent, if they match it send back a reply to the client that they are connected.

Since the number of keys used was very limited it was very easy for an attacker to eavesdrop on a network and watch packets being sent. After enough packets were sent, the key could be captured with relative ease. For those interested there is a WEP cracking tool implemented into Backtrack called aircrack-ng.

Do not use WEP encryption on any network, it provides a false sense of security to the people who use it with little protection.

WPA & WPA2 -

WPA encryption follows the same outline of WEP but has some key differences that make it a much better alternative.

1) Authentication is completely separate from encryption, meaning that the device will authenticate the user and then use a session key for the encryption process.
    a. Session keys are 128 bits
2) Each device is given its own session key, meaning that it is much harder to crack
    a. Session keys are only valid for the duration that the device is connected to the router

Weakness from WPA is the same as WEP, in that if someone has enough traffic they can still crack the session key used to encrypt data (albeit much more data must be passed).

How the connection is made to the router:

1) Client makes a request to the router
2) Router sends back password prompt
3) Client puts in password and send it back to the router
4) Router checks the authentication and if it does send ACK to client
5) Client then starts the key negotiation sequence
6) Router agrees on key and sends it back to the client
7) Connection is now established

WPA2 encryption uses a tougher encryption schema to deliver a more robust and harder to crack algorithm for protection but the method it uses is almost identical to WPA.

WPA2, the newest of the encryption schemes, came out in 2004 so it would be a safe bet to assume that a newer encryption method will probably take over the market sometime soon. There have been many different methods to crack wireless encryption from going after the packet encryption to going after the underlying data encryption scheme DES. All rely on packets being transferred to intercept.

As of right the best encryption to be using for your wireless router is WPA2, if your router has it available please select this. There are a few things to keep in mind though:

1) If you have a larger area you would like your router to cover, adding encryption will limit the range you can transmit to. I always suggest that people use wireless encryption when using home networks, just be prepared for a slight range loss when turning encryption on. You might also see some performance decrease as with encryption you are adding more overhead to the packets of data you really want.
2) Wireless encryption is a good start for home security, but it is far from the only protection you should be taking. In future lessons we will go over other things you can use to keep yourself safe.

Future lessons:

- Computer Passwords
- Router settings
- Suggestions for you all