Router Fundamentals

I recently reviewed a couple of flagship routers - the Linksys EA4500 and the Netgear WNDR4500. To help with the comparison, I monitoring the radio signal from my router. Imagine my surprise when I found that almost 50% of the 24 networks in range were running with little or no encryption!

My neighbors were either very trusting or very naïve.

Of course, another possiblity was that they were just overwhelmed by the challenges of setting up their home router - a device that is beguiling in terms of the wireless freedoms that it promises; a device that is powerful enough to be a little computer in its own right; a device that is so complex that its configuration runs into 30 pages of settings, replete with technical networking jargon!

Now, if you have chosen to unleash the power of this awesome device in your home, it is up to you to ensure that you use it wisely. As uncle Ben would say, “With great power comes great responsibility”.

That's where this article comes in.

My goal is to make you comfortable enough with the most critical aspects of your home wireless router, so that you can effect the necessary changes easily and painlessly.

3 things you need to know about wireless networks

Bandwidth and Throughput

Bandwidth is defined as the amount of data that can be pushed through a network.

A good analogy is the maximum number of vehicles that can simultaneously use a stretch of freeway – assuming perfect driving conditions, that the vehicles are being driven by the best drivers in the country, are traveling at the top speed limit, are maintaining the minimum proper distance from each other, and are not changing lanes. Highway bandwidth might be measured as the number of cars that pass per second.

Throughput is what happens in the real world. I.e., when construction areas, inclement weather, and inattentive drivers happen - causing ripples in the fabric of smooth traffic flow.

Network bandwidth is measured as the number of bits or bytes that pass through every second - e.g., as Mbps (million bits per second) or MBps (million bytes per second). While bandwidth with a N900 device is estimated at 900 Mbps, I average a throughput of mere 24 Mbps on my network.

So what happened to the rest of the promised bandwidth?

That remainder is lost due to interference, due to overhead bits needing to be transmitted for error correction and other control tasks, etc.

Range

Another key measure for routers is the distance to which it is able to project a workable signal. This is a function of the power of router’s transmitter, the sensitivity of the receiver, and the material that the signal must pass through to get from one to the other.

As you can see, only one of these relates to the router.

To ensure maximum coverage:

1. purchase the router with the most powerful transmitter (29 dbm for the WNDR4500).

2. use a wireless adapter that matches the full bandwidth of the transmitter. I.e., if you are using a N900 router, then your adapter should be N900 compliant as well.
3. move your router to the most central location in your home. The more central the location, the better the strength of your signal as it radiates outward.

Standards

Wireless standards have evolved by giant strides since 1999, when the 802.11b standard was rated at 11Mbps. Since then 802.11g (2003) raised this to 54Mbps, and 802.11n (2009) has upped the ante even farther – from 600 Mbps (N600), to 750 Mbps (N750), all the way up to 900 Mbps (N900).

The latest 802.11n standard has a few tricks up its sleeve to make these high speeds possible.

1. Multiple Input Multiple Output – it supports the use of multiple antennas that can transmit/receive simultaneously.
2. Channel Bonding – the width of the Radio Frequency channel used is increased from 20MHz to 40MHz. Since the width of a RF channel determines the throughput, this has a beneficial effect on network bandwidth.
3. Dual Bands – the radios in 802.11b/g routers transmitted on the 2.4GHz radio frequency - a rather noisy band – even your microwave transmits at this frequency. 802.11n devices can also use the cleaner and less populated 5GHz band.
4. Frame aggregation – Grouping multiple frames together amortizes the cost of acknowledgements and allows for smaller interframe spaces, improving bandwidth.

The number of MIMO antennas coupled with the dual bands give us the familiar Nxxx numbers that we see associated with 802.11n routers.

Total bandwidth = Bandwidth per Antenna x Number of Antennas x Frequency Bands

For the WNDR4500 and AE4500, which are N900 capable, this is:

150 Mbps/antenna x 3 antennas x 2 bands = 900.

A consequence of multiple antennas is increased power consumption. This is a problem with mobile devices such as tablets and phones. To conserve power, many wireless adapters limit the number of bands they support or the number of transmit/receive antennas they have. For instance, the Intel 5100 adapter has only 1 transmit radio, and 2 receive radios. As a result, it can only transmit at 150Mbps, and receive at 300Mbps. In other words, the bandwidth you can achieve will be limited by your weakest component. In most cases, this will be your wireless client.

That said, having more radio transmitters on the router than receivers on the adapter, means that the router can use additional techniques to ensure clear communications. For e.g., a router could choose the best transmitter/antenna to use to communicate with an adapter based on measures such as packet error rate or received signal strength. In addition, the router could transmit the same information using two antennas - increasing the chance that at least one copy of a packet will get through to the receiver.

3 things you need to know about the Internet

Addressing in Networks

Every device that connects to a network is associated with a unique 48-bit network address called its Media Access Control (MAC) address. This is a physical address encoded on to the network interface card, which encodes the manufacturer and a unique card identifier. Once a packet arrives at a given network on which the destination host lives, it is this physical address that ensures that a packet actually reaches its destination.

However, the MAC address does not provide any information about the location of a network. For that, we have an Internet Protocol (IP) address, that combines a network identifier and a host identifier, into 32 bits. This takes the form a.b.c.d, where each of the parts is a number from 0 to 255.

Network appliances on the Internet are able to use IP addresses to route packets over the Internet to the appropriate network on which the destination host resides. Hence, these are termed *routable addresses*. Once the packet reaches its network, the IP address is converted to a physical address for actual delivery to a destination host.

A special set of private IP addresses, in the range 192.168.0.0 to 192.168.255.255, are meaningful only within a given network, and are not routable on the wider Internetwork.

TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) is the language of the Internet. It is a layered system that defines everything from the physical interfaces (such as connectors, cabling, voltage levels, etc), to the logical addressing of networked hosts, to the error correction and the sequencing of individual packets in a given transmission, to the delivery of these packets to a given application.

Just as a given host on a network is identified by an IP address, an application is represented in this model using a port. For instance, a HTTP server program would listen on port 80 on its host, while a SMTP mail server would listen on port 25. Together, the IP address and port represent a connection end point.

Port numbers 1 to 1023 are termed well known ports, and are reserved by the Internet Corporation for Assigned Names and Numbers (ICANN), while ports 1024-49151 are registered with the ICANN by vendors. Ports 49152 to 65535 are private ports that you are free to use any way you see fit.

The idea of a “well known” port 80 for HTTP web servers is why you can reach my web site using http://www.swengsol.com, and not http://www.swengsol.com:80. The implicit “:80” suffix is appended by the browser software.

There is nothing magical about that port. As long as you are willing to always type in the port number, you could have your private web server running on port 65535 instead.

DHCP and NAT

As we saw, an Internet Protocol (IP) address uniquely identifies a computer on the Internetwork. Unfortunately, addresses on that network are a limited resource, and expensive to boot. As a result, rather than get an individual Internet address for each of my home computers, I lease them from my Internet Service Provider (ISP), Comcast, Inc.

Let us rewind to a simpler time, with a single home computer. Your computer would contact Comcast and request an IP address. Comcast would hand off an IP address from the thousands that it owns, say 11.22.33.44. From then on, this computer had a presence on the Internet - and could be found by any of the millions of computers out there.

Now this computer could reach out to a server computer out in the wild yonder, and make a request for some resource (such as an image file). That server services the request by locating the bits and bytes that make up that resource, and sent it to the IP address from which the connection originated - 11.22.33.44. My computer rendered the returned information as appropriate.

However, here is the problem. I get one IP address. Yes, ONE.

Fast forward to today. Unfortunately, the average home today has about a dozen devices that all need to connect to the Internet. These include computers, smart phones, security cameras, tablet computers, media servers, streaming devices, TVs, Network Attached Storage (NAS) appliance, and even normal appliances like refrigerators. (This diversity of networked devices is also why we talk of network hosts rather than network computers).

The challenge is that we have only one IP address, that must be shared across all these devices.

Fortunately, our router can manage the sharing of this resource.

We begin by assigning our unique IP address to the router itself. I.e., the router is now identified using the IP address 11.22.33.44.

Next we use a **Dynamic Host Configuration Protocol (DHCP)** server to assign a private IP address (in the special range 192.168.x.x) to every computer on the local network. If you have 10 hosts on your network, then each will be assigned an IP address in this range - e.g., 192.168.1.2 … 192.168.1.11. This solves one problem - all the computers on your LAN are now uniquely identified.

Note that our router is also a host on this network, and reserves the address 192.168.1.1 for itself. In other words, our router has two IP addresses - a private non routable IP address (192.168.1.1) and a public routable address (11.22.33.44) that can be used to locate it on the Internet.

(Enter **Network Address Translation (NAT)** stage left.)

The private IP addresses used for internal communication within our network, must be translated to this single public IP address when packets of data leave our network. This has the effect of making all request packets look like they originate at our router.

On the way back, all responses will be returned to our router. At the router, NAT maps the public IP address (11.22.33.44) on the response packets to the appropriate private IP address of the host making the request.

In other words, through the magic of DHCP and NAT, our single IP address is now shared across all the devices on our network!

3 things you need to know about your router

A Router is a versatile device

Today's wireless routers combine multiple devices into a single convenient package.

1. **Switch**
   A router provides at least 4 Ethernet ports which you can use to hard wire network devices using standard Ethernet Cat 5e cables. The connected devices are then part of this private network. A computer transmitting data, causes packets to arrive at a switch port, which then establishes a dedicated circuit connection to the destination host. Multiple simultaneous connections can exist.
2. **DHCP Server and Network Address Translation**
   As we saw in the previous section, DHCP and NAT make it possible for a computer to interact with another over our local network as well as over the Internet.
3. **Firewall**
   It functions as a hardware firewall by hiding the hosts on your network from hostile port scanning tools. In addition, a Stateful Packet Inspection firewall inspects incoming data packets to make sure they correspond to an outgoing request, and automatically rejects packets that were not requested.
4. **Access Point**
   It supports connectivity with wireless hosts using RF transmitters and receivers, provides a connection to the wired LAN, and handles the conversion between the data formats used for wireless and wired networks.
5. **Router**
   It straddles two networks – the Internet as well your private LAN, and is the first link in the chain for communicating across hosts that live within these two networks.

Router and Wireless Security

Think about how you use your computer to access your bank statements or about how you store private documents and photos on your computer's hard disk or on a network attached disk. Now think about someone being able to eavesdrop on your communication, or to access your network, without your ever knowing about it.

Scary enough?

Fortunately, you can keep yourself relatively safe if you follow these basic guidelines.

1. Establish a router administration password.
   This way no one can sneak in and, for example, point your DNS server name at a malicious server. A DNS server converts domain names you type in to a browser's URL bar into their equivalent IP addresses. An evil DNS server is probably the scariest of all possible threats.
2. Enable WPA2 Personal (AES) security for all your wireless networks
   The older WEP is useless, and WPA2 (TKIP) is obsolete. Instead, use WPA2 with a strong passphrase (8-20 characters long, with upper and lower case characters, special characters, and numbers). Disabling SSID broadcast and enabling MAC filtering are pointless. They add nothing to security and are an avoidable inconvenience.
3. Harden your router by turning off all unnecessary options
   Many router features are provided for convenience. Unfortunately, they are also security penetrations waiting to happen.

Disable **Wi-Fi Protected Setup**, **UPnP** support, as well as **remote administration** of your router.

Disable your **guest network**. If you need to use it, limit guest devices to only accessing the Internet. Use WPA2 (AES) even for your guest network.

4. Upgrade your router to the latest firmware on a reasonable schedule. I usually wait for 4-8 weeks to let the bugs be worked out before upgrading.
5. Make sure that you are not using the DMZ option (that places one of your computers outside the router's firewall) unless you really know what you're doing.

Router Firewall configuration

By default, your router's firewall will block external computers from connecting to any computer on your private network. However, in some cases such access may be desirable.

For instance, you may have a security camera whose video feed you would like to access from a computer outside of your network (say, while on holiday).

To connect with the camera, which has a private IP address of the form 192.168.1.x, you must configure the router's firewall to allow access to it from external hosts.

You do this using a port forwarding rule and specifying an external port on the router (say, 9009), the private IP address of the security camera (192.168.1.3), and the port on which the camera listens for video requests (say, 80).

You can then access the router's by specifying its routable IP address (11.22.33.44) and the configured external port (9009). The router will automatically forward this request to port 80 of the camera at private IP address 192.168.1.3.

The IP address of your router is displayed on the Router status page. On the WNDR4500, this is the Administration > Router Status page.

ALL the rest is Noise

Everything else is fluff.

No you don't need a USB print server - a wireless printer can be got for about $50.

No you don't need a USB hard drive or a built in DLNA media server – it is rarely as performant or as convenient as it might seem.

And, no you don't need thick clients to configure your router – these simply serve to give you a false sense of security.

To summarize -

As long as you spend the time to get to know this critical piece of hardware, you will gain an incredibly resourceful companion. However, take it for granted at your peril.

Watch for my next installment – I'll spell out the screens that you will use to configure the critical aspects of your brand new WNDR4500 or EA4500 routers.