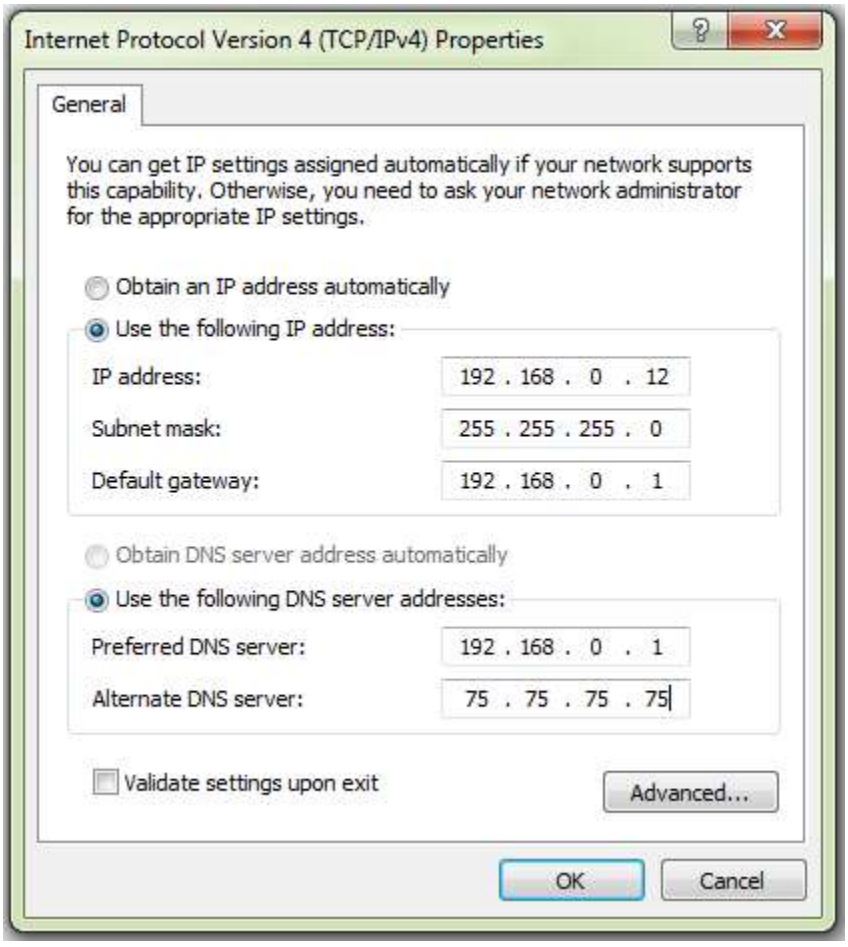
TCP/IP & Network Address Translation
Milt Hull

TCP/IP

Transmission Control Protocol and Internet Protocol (TCP/IP) are protocols that glue the Internet together. Every machine out there is connected to the Internet has a TCP/IP number assigned to it. The configuration has an IP number, a defined subnet mask, a route out to the internet which is called a gateway address and a set of DNS numbers to resolved hosts names to other TCP/IP numbers. A typical setup would look something like this:



Notice that these numbers are setup with four Octets separated by a period. This is because these separated numbers are sub sections of a total solution called subnets. Each subnet can handle a certain amount of machines within a defined set of logical, visible subdivision of IP addresses. That subnet is defined in the Subnet Mask. Then it needs a route out to the internet which is called a Gateway Address.

Gateway

The Gateway Address is simply a route through a common connection to the rest of the world. Most people call this the Router. Its job is to route packets out to the Internet and to receive packets coming in from the Internet. It usually uses Network Address Translation which we will also talk about later.

Subnet Mask

So let talk about why so many connections can connect to a range! This is defined in the Subnet Mask. A Subnet Mask defines how many IP address can fit within that Range.

Mask	Devices
255.255.255.252	2
255.255.255.248	6
255.255.255.240	14
255.255.255.224	30
255.255.255.192	62
255.255.255.128	126
255.255.255.0	254
255.255.254.0	510
255.255.252.0	1022
255.255.248.0	2046
255.255.240.0	4094
255.255.224.0	8190
255.255.192.0	16382
255.255.128.0	32766
255.255.0.0	65534
255.254.0.0	131070
255.252.0.0	262142
255.248.0.0	524286
255.240.0.0	1048574
255.224.0.0	2097150
255.192.0.0	4194302
255.128.0.0	8388606
255.0.0.0	16777214

Keep in mind that one device of each of those subnets is used up for the router within that subnet. So if you had a subnet mask of 255.255.255.252 which would give you 2 devices. One would be your router to the internet and the other your internal connection device like a workstation or a Firewall.

NAT

If you have a High-Speed Internet Connection at home, chances are that you have a Dynamic TCP/IP address associated with that connection. There are hundreds of Internet service providers and many of them are connected to their own type of device. AT&T offers U-Verse, Comcast offers Cable connections, and many offer DSL connections while others offer pure Wireless.

The way it works is that they give you a Modem or a Router with that internet connection. It usually has a set of numbers that would allow you to connect 254 machines to it. However, it

usually is a subnet of private numbers or Private Network. Private Network numbers are a set of Non-Routable numbers that will not route out to the Internet. These numbers were setup during the creation of IPv4 and there are even more private networks defined in IPv6. We are just going to discuss IPv4 in this article for right now.

The private numbers are as follows:

IP Range			Number of Addresses
10.0.0.0	-	10.255.255.255	16,777,216
172.16.0.0	-	172.31.255.255	1,048,576
192.168.0.0	-	192.168.255.255	65,536

So the outside internet and every device out there will not Route a Private IP Address past its own subnet. This is what saved us from running out of numbers and why were are still on IPv4 for the most part. There are much more computers out there than there are TCP/IP numbers in version 4. Most people at home or at work do not need a real TCP/IP number. Those numbers are usually called Static IP numbers because their machines do not hosts services for the internet like webpages or file shares.

So usually they receive the above mentioned Router and it translates to a private number. This is called Network Address Translation or NAT for short. The NAT'ed number is usually a 192.168.x.x number for smaller networks. So for example you might have a modem or a router that takes your real TCP/IP number connected to the Wide Area Network Port called "WAN" for short, (let's say 23.67.231.27 as an example). It translates that connection to a private TCP/IP number. 192.168.0.1 Number for example. Your Router or Modem will then offer connections to all other numbers within that range starting from the 192.168.0.2 until the end of that subnet all the way to 192.168.0.254. That is called "Dynamic Host Configuration Protocol" or DHCP for short.

All packets from your workstation translate up to your real IP Address through your router. Routers are called Routers because they route packets from one subnet to another subnet. In closing, your private subnet at home cannot be accessed from the outside through your router unless there is a rule that can allow that access.

Firewalls

In most businesses, you would have a router accepting your connection from your Internet Service Provider (ISP) which would have a Static IP number. That connection would go straight to a Firewall which would do many things. Besides Stateful Packet Inspection, it might also have services like Anti-Virus Protection, Spyware Prevention and Intrusion Prevention and maybe Content Filtering.

Your Firewall can also have Rules and NAT policies which would allow an outside connection to go through your Router and Firewall to allow connections to your local website or email server. Usually connections like this in a business are connected to a private zone called a Demilitarized

Zone or DMZ for short. This protects your Local Area Network or LAN from outside connections.

On your Home device, you might have a connection accepting your TCP/IP address and you can create a Pinhole that can do a pass-through to connect straight to one of your machines through your router with only one IP address. The way it works is that your real Static IP address of your router can accept many Service Ports. Let's say you have a Web Server that you want people to look at that is on your private network. You can have your router forward port 80 to a local machine internal to display that website. You can only use on Port Number per Port-Forward. So in this case you cannot have two Port 80's however, you can assign a Port 81 to go to a different website using Port Forwarding.

Hope this explains Network Address Translation and how it pertains to your local network.