How Network Address Translation Works

by Jeff Tyson

If you are reading this article, you are most likely connected to the Internet and viewing it at the HowStuffWorks Web site. There's a very good chance that you are using **Network Address Translation** (NAT) right now.

Special thanks to **Cisco** for its support in creating this article.

The Internet has grown larger than anyone ever imagined it could be. Although the exact size is unknown, the current estimate is that there are about 100 million hosts and more than 350 million users actively on the Internet. That is more than the entire population of the United States! In fact, the rate of growth has been such that the Internet is effectively doubling in size each year.

So what does the size of the Internet have to do with NAT? Everything! For a computer to communicate with other computers and Web servers on the Internet, it must have an **IP address**. An IP address (IP stands for Internet Protocol) is a unique 32-bit number that identifies the location of your computer on a network. Basically, it works like your street address -- as a way to find out exactly where you are and deliver information to you.

When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have 4,294,967,296 unique addresses (2^{32}). The actual number of available addresses is smaller (somewhere between 3.2 and 3.3 billion) because of the way that the addresses are separated into classes, and because some addresses are set aside for multicasting, testing or other special uses.

With the explosion of the Internet and the increase in home networks and business networks, the number of available IP addresses is simply not enough. The obvious solution is to redesign the address format to allow for more possible addresses. This is being developed (called **IPv6**), but will take several years to implement because it requires modification of the entire infrastructure of the Internet.
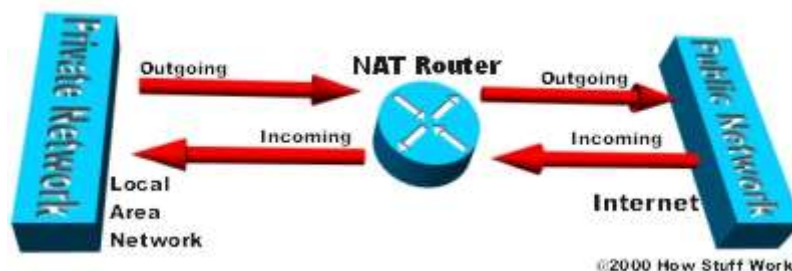
The NAT router translates traffic coming into and leaving the private network.

This is where NAT (RFC 1631) comes to the rescue. Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers.

But the shortage of IP addresses is only one reason to use NAT. In this edition of **HowStuffWorks**, you will learn more about how NAT can benefit you. But first, let's take a closer look at NAT and exactly what it can do...

What Does NAT Do?

NAT is like the receptionist in a large office. Let's say you have left instructions with the receptionist not to forward any calls to you unless you request it. Later on, you call a potential client and leave a message for that client to call you back. You tell the receptionist that you are expecting a call from this client and to put her through.

The client calls the main number to your office, which is the only number the client knows. When the client tells the receptionist that she is looking for you, the receptionist checks a lookup table that matches your name with your extension. The receptionist knows that you requested this call, and therefore forwards the caller to your extension.

Developed by Cisco, Network Address Translation is used by a device (firewall, router or computer) that sits between an internal network and the rest of the world. NAT has many forms and can work in several ways:

- **Static NAT** - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.


In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.

- **Dynamic NAT** - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.
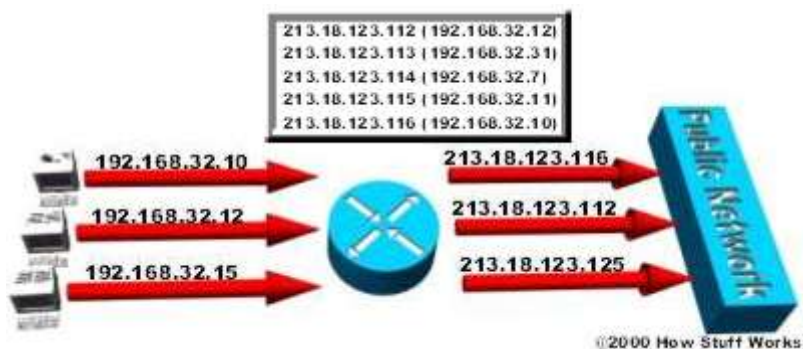

In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150.

- **Overloading** - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.
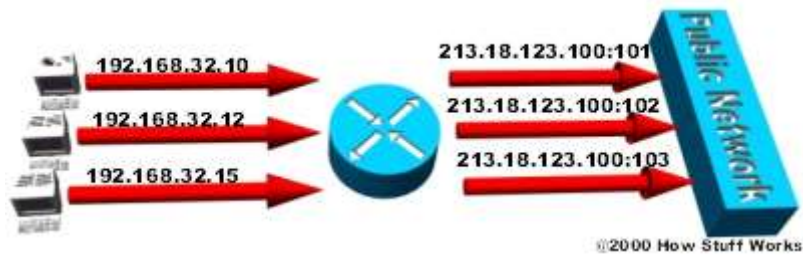
In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment.

- **Overlapping** - When the IP addresses used on your internal network are registered IP addresses in use on another network, the router must maintain a lookup table of these addresses so that it can intercept them and replace them with registered unique IP addresses. It is important to note that the NAT router must translate the "internal" addresses to registered unique addresses as well as translate the "external" registered addresses to addresses that are unique to the private network. This can be done either through static NAT or by using DNS and implementing dynamic NAT.
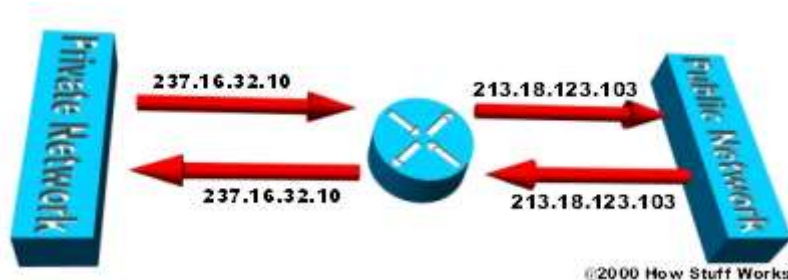

The internal IP range (237.16.32.xx) is also a registered range used by another network. Therefore, the router is translating the addresses to avoid a potential conflict with another network. It will also translate the registered global IP addresses back to the unregistered local IP addresses when information is sent to the internal network.

The internal network is usually a **LAN (Local Area Network)**, commonly referred to as the **stub domain**. A stub domain is a LAN that uses IP addresses internally. Most of the network traffic in a stub domain is local, so it doesn't travel outside the internal network. A stub domain can include both registered and unregistered IP addresses. Of course, any computers that use unregistered IP addresses must use Network Address Translation to communicate with the rest of the world.

NAT can be configured in various ways. In the example below, the NAT router is configured to translate unregistered (inside, local) IP addresses, that reside on the private (inside) network, to registered IP addresses. This happens whenever a device on the inside with an unregistered address needs to communicate with the public (outside) network.

- An ISP assigns a range of IP addresses to your company. The assigned block of addresses are registered, unique IP addresses and are called **inside global addresses**. Unregistered, private IP addresses are split into two groups. One is a small group (**outside local addresses**) that will be used by the NAT routers. The other, much larger group, known as **inside local addresses**, will be used on the stub domain. The outside local addresses are used to translate the unique IP addresses, known as **outside global addresses**, of devices on the public network.
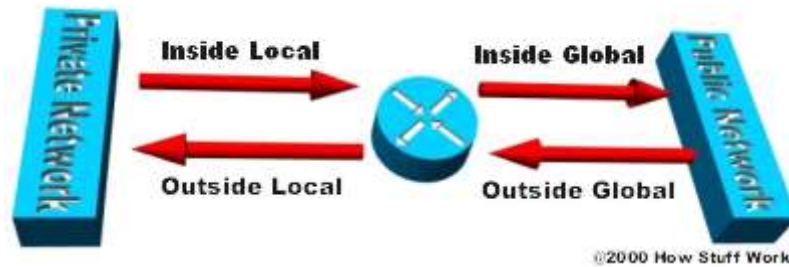
IP addresses have different designations based on whether they are on the private network (stub domain) or on the public network (Internet), and whether the traffic is incoming or outgoing.

- Most computers on the stub domain communicate with each other using the inside local addresses.
- Some computers on the stub domain communicate a lot outside the network. These computers have inside global addresses, which means that they do not require translation.
- When a computer on the stub domain that has an inside local address wants to communicate outside the network, the packet goes to one of the NAT routers.
- The NAT router checks the routing table to see if it has an entry for the destination address. If it does, the NAT router then translates the packet and creates an entry for it in the address translation table. If the destination address is not in the routing table, the packet is dropped.
- Using an inside global address, the router sends the packet on to it's destination.
- A computer on the public network sends a packet to the private network. The source address on the packet is an outside global address. The destination address is an inside global address.
- The NAT router looks at the address translation table and determines that the destination address is in there, mapped to a computer on the stub domain.
- The NAT router translates the inside global address of the packet to the inside local address, and sends it to the destination computer.

NAT overloading utilizes a feature of the TCP/IP protocol stack, **multiplexing**, that allows a computer to maintain several concurrent connections with a remote computer (or computers) using different TCP or UDP **ports**. An IP packet has a header that contains the following information:

- **Source Address** - The IP address of the originating computer, such as 201.3.83.132
- **Source Port** - The TCP or UDP port number assigned by the originating computer for this packet, such as Port 1080
- **Destination Address** - The IP address of the receiving computer, such as 145.51.18.223
- **Destination Port** - The TCP or UDP port number that the originating computer is asking the receiving computer to open, such as Port 3021

The addresses specify the two machines at each end, while the port numbers ensure that the connection between the two computers has a unique identifier. The combination of these four numbers defines a single TCP/IP connection. Each port number uses 16 bits, which means that there are a possible 65,536 (2^{16}) values. Realistically, since different manufacturers map the ports in slightly different ways, you can expect to have about 4,000 ports available.

Dynamic NAT and Overloading

Here's how **dynamic NAT** works:

- An internal network (stub domain) has been set up with IP addresses that were not

specifically allocated to that company by **IANA** ([Internet Assigned Numbers Authority](#)), the global authority that hands out IP addresses. These addresses should be considered **non-routable** since they are not unique.

- The company sets up a NAT-enabled router. The router has a range of unique IP addresses given to the company by IANA.
- A computer on the stub domain attempts to connect to a computer outside the network, such as a Web server.
- The router receives the packet from the computer on the stub domain.
- The router saves the computer's non-routable IP address to an **address translation table**. The router replaces the sending computer's non-routable IP address with the first available IP address out of the range of unique IP addresses. The translation table now has a mapping of the computer's non-routable IP address matched with the one of the unique IP addresses.
- When a packet comes back from the destination computer, the router checks the destination address on the packet. It then looks in the address translation table to see which computer on the stub domain the packet belongs to. It changes the destination address to the one saved in the address translation table and sends it to that computer. If it doesn't find a match in the table, it drops the packet.
- The computer receives the packet from the router. The process repeats as long as the computer is communicating with the external system.

Here's how **overloading** works:

- An internal network (stub domain) has been set up with non-routable IP addresses that were not specifically allocated to that company by IANA.
- The company sets up a NAT-enabled router. The router has a unique IP address given to the company by IANA.
- A computer on the stub domain attempts to connect to a computer outside the network, such as a Web server.
- The router receives the packet from the computer on the stub domain.
- The router saves the computer's non-routable IP address and port number to an address translation table. The router replaces the sending computer's non-routable IP address with the router's IP address. The router replaces the sending computer's source port with the port number that matches where the router saved the sending computer's address information in the address translation table. The translation table now has a mapping of the computer's non-routable IP address and port number along with the router's IP address.
- When a packet comes back from the destination computer, the router checks the destination port on the packet. It then looks in the address translation table to see which computer on the stub domain the packet belongs to. It changes the destination address and destination port to the ones saved in the address translation table and sends it to that computer.
- The computer receives the packet from the router. The process repeats as long as the computer is communicating with the external system.
- Since the NAT router now has the computer's source address and source port saved to the address translation table, it will continue to use that same port number for the duration of the connection. A timer is reset each time the router accesses an entry in the table. If the entry is not accessed again before the timer expires, the entry is removed from the table.

Look at this table to see how the computers on a stub domain might appear to external networks.

Source Computer	Source Computer's IP Address	Source Computer's Port	NAT Router's IP Address	NAT Router's Assigned Port Number
A	192.168.32.10	400	215.37.32.203	1

B	**192.168.32.13**	**50**	**215.37.32.203**	**2**
C	**192.168.32.15**	**3750**	**215.37.32.203**	**3**
D	**192.168.32.18**	**206**	**215.37.32.203**	**4**

As you can see, the NAT router stores the IP address and port number of each computer in the address translation table. It then replaces the IP address with it's own registered IP address and the port number corresponding to the location, in the table, of the entry for that packet's source computer. So any external network sees the NAT router's IP address and the port number assigned by the router as the source-computer information on each packet.

You can still have some computers on the stub domain that use dedicated IP addresses. You can create an access list of IP addresses that tells the router which computers on the network require NAT. All other IP addresses will pass through untranslated.

The number of simultaneous translations that a router will support are determined mainly by the amount of **DRAM** (Dynamic Random Access Memory) it has. But since a typical entry in the address-translation table only takes about 160 bytes, a router with 4 MB of DRAM could theoretically process 26,214 simultaneous translations, which is more than enough for most applications.

IANA has set aside specific ranges of IP addresses for use as non-routable, internal network addresses. These addresses are considered **unregistered** (for more information check out RFC 1918: Address Allocation for Private Internets, which defines these address ranges). No company or agency can claim ownership of unregistered addresses or use them on public computers. Routers are designed to discard (instead of forward) unregistered addresses. What this means is that a packet from a computer with an unregistered address could reach a registered destination computer, but the reply would be discarded by the first router it came to.

There is a range for each of the three classes of IP addresses used for networking:

- Range 1: Class A - 10.0.0.0 through 10.255.255.255
- Range 2: Class B - 172.16.0.0 through 172.31.255.255
- Range 3: Class C - 192.168.0.0 through 192.168.255.255

Although each range is in a different class, your are not required to use any particular range for your internal network. It is a good practice, though, because it greatly diminishes the chance of an IP address conflict.

Security and Administration

Implementing dynamic NAT automatically creates a **firewall** between your internal network and outside networks, or between your internal network and the Internet. NAT only allows connections that originate inside the stub domain. Essentially, this means that a computer on an external network cannot connect to your computer unless your computer has initiated the contact. You can browse the Internet and connect to a site, and even download a file; but somebody else cannot latch onto your IP address and use it to connect to a port on your computer.

In specific circumstances, Static NAT, also called **inbound mapping**, allows external devices to initiate connections to computers on the stub domain. For instance, if you wish to go from an inside global address to a specific inside local address that is assigned to your Web server, Static NAT would enable the connection.

Static NAT (inbound mapping) allows a computer on the stub domain to maintain a specific address when communicating with devices outside the network.

Some NAT routers provide for extensive filtering and traffic logging. Filtering allows your company to control what type of sites employees visit on the Web, preventing them from viewing questionable material. You can use traffic logging to create a log file of what sites are visited and generate various reports from it.

NAT is sometimes confused with **proxy servers**, but there are definite differences between them. NAT is transparent to the source and to destination computers. Neither one realizes that it is dealing with a third device. But a proxy server is not transparent. The source computer knows that it is making a request to the proxy server and must be configured to do so. The destination computer thinks that the proxy server **IS** the source computer, and deals with it directly. Also, proxy servers usually work at layer 4 (transport) of the OSI Reference Model or higher, while NAT is a layer 3 (network) protocol. Working at a higher layer makes proxy servers slower than NAT devices in most cases.
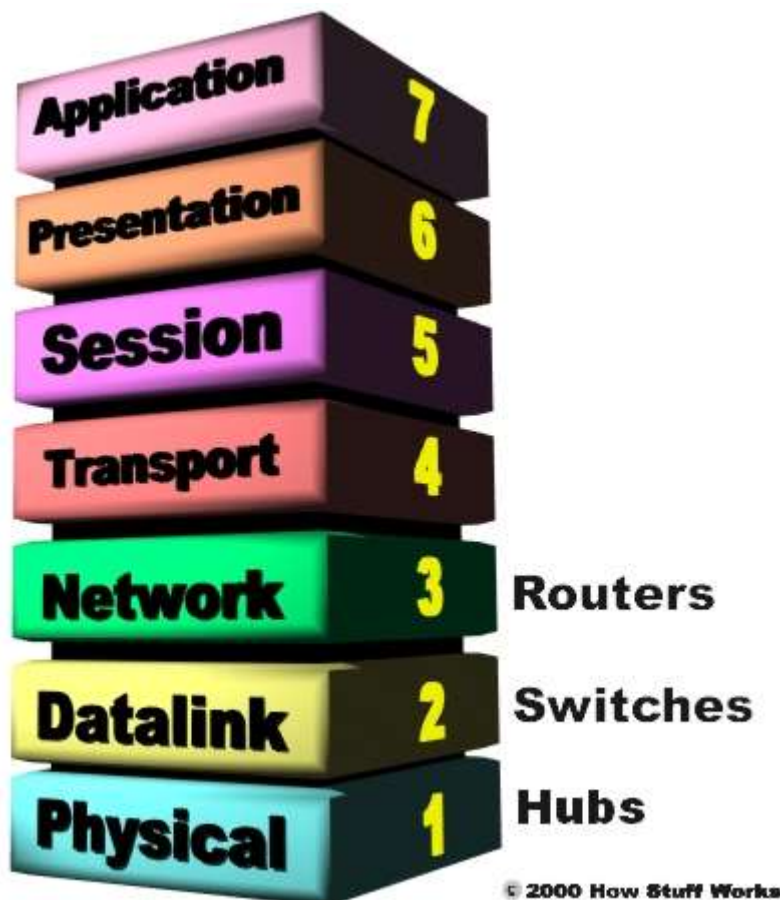
NAT operates at the Network layer (layer 3) of the OSI Reference Model -- this is the layer that routers work at.

A real benefit of NAT is apparent in **network administration**. For example, you can move your Web server or FTP server to another host computer without having to worry about broken links. Simply change the inbound mapping at the router to reflect the new host. You can also make changes to your internal network easily, because the only external IP address either belongs to the router or comes from a pool of global addresses.

NAT and DHCP (dynamic host configuration protocol) are a natural fit. You can choose a range of unregistered IP addresses for your stub domain and have the DHCP server dole them out as necessary. It also makes it much easier to scale up your network as your needs grow. You don't have to request more IP addresses from IANA. Instead, you can just increase the range of available IP addresses configured in DHCP to immediately have room for additional computers on your network.

Multi-homing

As businesses rely more and more on the Internet, having multiple points of connection to the Internet is fast becoming an integral part of their network strategy. Multiple connections, known as **multi-homing**, reduces the chance of a potentially catastrophic shutdown if one of the connections should fail.

In addition to maintaining a reliable connection, multi-homing allows a company to perform **load-balancing** by lowering the number of computers connecting to the Internet through any single connection. Distributing the load through multiple connections optimizes the performance and can significantly decrease wait times.

Multi-homed networks are often connected to several different **ISPs** (Internet Service Providers). Each ISP assigns an IP address (or range of IP addresses) to the company. Routers use **BGP** (Border Gateway Protocol), a part of the TCP/IP protocol suite, to route between networks using different protocols. In a multi-homed network, the router utilizes **IBGP** (Internal Border Gateway Protocol) on the stub domain side, and **EBGP** (External Border Gateway Protocol) to communicate with other routers.

Multi-homing really makes a difference if one of the connections to an ISP fails. As soon as the router assigned to connect to that ISP determines that the connection is down, it will reroute all data through one of the other routers.

NAT can be used to facilitate scalable routing for multi-homed, multi-provider connectivity. For more on multi-homing, see Cisco: Enabling Enterprise Multihoming.