**SUBNETS, SUBNET MASKS AND NAT**

Subnetting is basically dividing a big network into smaller networks.

An IP address has 2 components –

|  |  |
| --- | --- |
| Network address (or Network ID) | Host address (or Host ID) |

Subnetting a network further divides the host address part of the network into Subnet ID and Host ID.

|  |  |  |
| --- | --- | --- |
| Network ID | Subnet ID | Host ID |

An IP address is a 32 bit number.

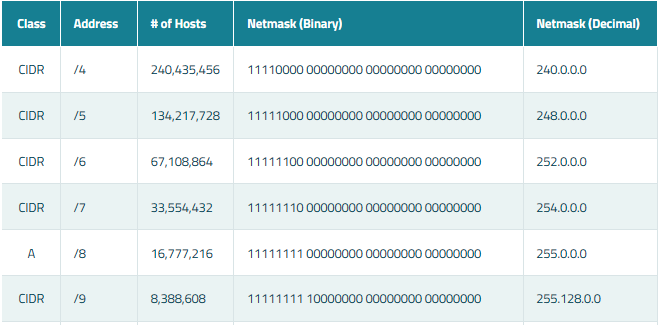
If the first 8 bits is reserved for the NID part, this IP address is a part of a class A network.

If the first 16 bits is reserved for NID, this IP address is part of a class B network.

If the first 24 bits is reserved for NID, this IP address is part of a class C network.

A subnet mask is to extract the network address given an IP address from the network.

A subnet mask is made by setting the network bits to all 1’s and host bits to all 0’s. When a subnet mask is applied to an IP address (by AND operation), the result is the NID part will remain intact and the HID part will remain zero.



Here, when AND operation is performed between the netmask and an IP address of the network, we get the network address.

REASON BEHIND SUBNETTING

For practical applications as in industries, management of big networks is very difficult.

Suppose in a company, there are 4 departments

1. Development
2. Testing
3. Maintenance
4. HR

Consider there is a code server in the development department. Via subnetting, we can divide the network into smaller networks for each department. In this way, we can ensure protection of the code server from the other departments.

Also, it is easier to manage smaller networks via subnetting than manage a big network.

SUBNETTING NETWORK

Here is another scenario where subnetting is needed. Pretend that a web host with a Class C network needs to divide the network so that parts of the network can be leased to its customers. Let's assume that a host has a network address of 216.3.128.0 (Note that the host ID part is zero). Let's say that we're going to divide the network into 2 and dedicate the first half to itself, and the other half to its customers.

216 . 3 . 128 . (0000 0000) (1st half assigned to the web host)

216 . 3 . 128 . (1000 0000) (2nd half assigned to the customers)

The digit after 128 is the subnet ID part.

When the SID is 0 (Range of IP addresses 216.3.128.00000000 to 216.3.128.01111111) these IP

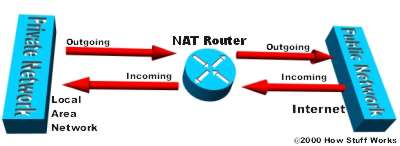
addresses are part of a network assigned to web hosts.

When the SID is 1(Range of IP addresses 216.3.128.10000000 to 216.3.128.11111111) these IP addresses are part of a network assigned to customers.

DISADVANTAGE OF SUBNETTING

If subnetting is implemented in a big network, it takes longer for a message to reach the host compared to a host in a network where subnetting is not done.

NAT



For a computer to communicate with other computers and [Web servers](http://computer.howstuffworks.com/web-server.htm) on the Internet, it must have an IP address.

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](http://computer.howstuffworks.com/internet/basics/question549.htm) (232). 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](http://computer.howstuffworks.com/home-network.htm) 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.

­ This is where NAT ([RFC 1631](http://www.faqs.org/rfcs/rfc1631.html)) comes to the rescue. Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.

The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network, like workstations needing access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them. This is where NAT comes into play.

Internet requests that require Network Address Translation (NAT) are quite complex but happen so rapidly that the end user rarely knows it has occurred. A workstation inside a network makes a request to a computer on the Internet. Routers within the network recognize that the request is not for a resource inside the network, so they send the request to the firewall. The firewall sees the request from the computer with the internal IP. It then makes the same request to the Internet using its own public address, and returns the response from the Internet resource to the computer inside the private network. From the perspective of the resource on the Internet, it is sending information to the address of the firewall. From the perspective of the workstation, it appears that communication is directly with the site on the Internet. When NAT is used in this way, all users inside the private network access the Internet have the same public IP address when they use the Internet. That means only one public addresses is needed for hundreds or even thousands of users. There are other uses for Network Address Translation (NAT) beyond simply allowing workstations with internal IP addresses to access the Internet. In large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network. Additional rules can be added, including which ports can be accessed at that IP address. Using NAT in this way allows network engineers to more efficiently route internal network traffic to the same resources, and allow access to more ports, while restricting access at the firewall. It also allows detailed logging of communications between the network and the outside world.

Additionally, NAT can be used to allow selective access to the outside of the network, too. Workstations or other computers requiring special access outside the network can be assigned specific external IPs using NAT, allowing them to communicate with computers and applications that require a unique public IP address. Again, the firewall acts as the intermediary, and can control the session in both directions, restricting port access and protocols.

NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.