SUBNET MASK

A subnet mask is a number that defines a range of IP addresses that can be used in a network. (It is not something you wear on your head to keep subnets out.) Subnet masks are used to designate subnetworks, or subnets, which are typically local networks LANs that are connected to the Internet. Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router Therefore, subnetworks can be used to partition multiple networks and limit the traffic between them.

A subnet mask hides, or "masks," the network part of a system's IP address and leaves only the host part as the machine identifier. A common subnet mask for a Class C IP address is 255.255.255.0. Each section of the subnet mask can contain a number from 0 to 256, just like an IP address. Therefore, in the example above, the first three sections are full, meaning the IP addresses of computers within the subnet mask must be identical in the first three sections. The last section of each computer's IP address can be anything from 0 to 255. For example, the IP addresses 10.0.1.201 and 10.0.1.202 would be in the same subnet, while 10.0.2.201 would not. Therefore, a subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used).

If your system is connected to a network, you can typically view the network's subnet mask number in the Network control panel (Windows) or System Preference (Mac OS X). Most home networks use the default subnet mask of 255.255.255.0. However, some office networks may use a different subnet mask such as 255.255.255.128, which can be used to split a network into two subnets. Large networks with several thousand machines may use a subnet mask of 255.255.0.0. This is the default subnet mask used by Class B networks. The largest Class A networks use a default subnet mask of 255.0.0.0.

NETWORK ADDRESS TRANSLATION

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.

When IP addressing first came out, everyone thought that there were plenty of addresses to cover any need. Theoretically, you could have 4294967296 unique addresses (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 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) 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.