**SUBNET, SUBNET MASKS AND NAT**

**Introduction**

A subnetwork or subnet is a logical subdivision of an IP network(TCP/IP model). The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the "rest" field or host identifier.

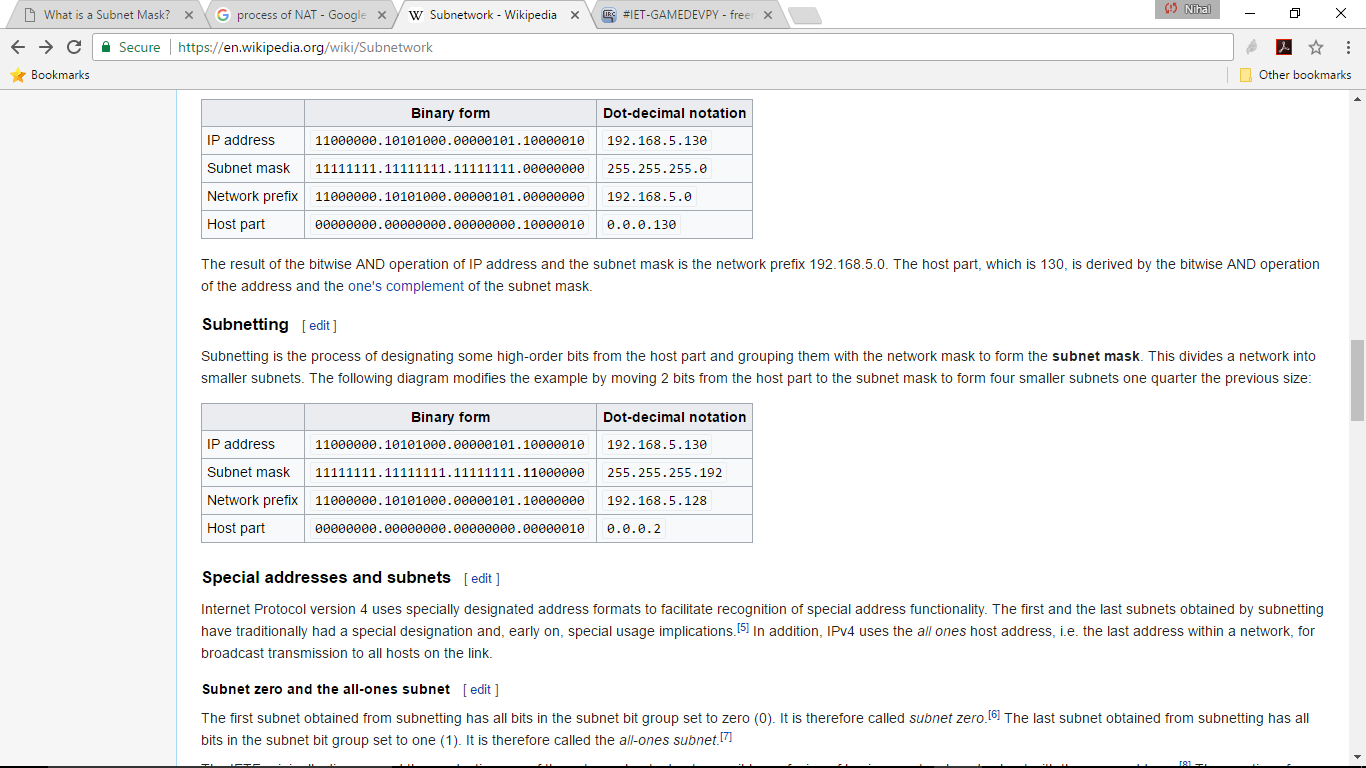
For IPv4, a network may also be characterized by its subnet mask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix.

In computer science, a mask is data that is used for bitwise operations, particularly in a bit field. Using a mask, multiple bits in a byte, nibble, word (etc.) can be set either on, off or inverted from on to off (or vice versa) in a single bitwise operation.

**Subnet Mask**

A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>) if additional subnetwork is needed. . It is called a subnet mask because it is used to identify network address of an IP address by perfoming a bitwise AND operation on the netmask.

Subnetting an IP network is to separate a big network into smaller multiple networks for reorganization and security purposes. All nodes (hosts) in a subnetwork see all packets transmitted by any node in a network. Performance of a network is adversely affected under heavy traffic load due to collisions and retransmissions.

Applying a subnet mask to an IP address separates network address from host address. The network bits are represented by the 1's in the mask, and the host bits are represented by 0's. Performing a bitwise logical AND operation on the IP address with the subnet mask produces the network address.

**NAT**

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 4,294,967,296 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.

By

Nihal Haneef

16CO128