NETWORK CONFIGURATION AND OPTIMIZATION

IP ADDRESSING

Physical Addressing

A physical address uniquely identifies a host within a local network. The physical address is a function of the Data-Link layer of the OSI model, Layer-2. The Ethernet utilizes 48-bit MAC address as its physical address. The MAC address is often hardcoded on the physical network interfaces, though some interfaces support changing the MAC address using special utilities. In virtualized environments, it is common to dynamically assigning MAC addresses.

MAC addresses are often represented in hexadecimal number system, using any of the following two accepted formats:

i) 00:43:AB:F2:32:13

ii) 0043.ABF2.3213

The first six hexadecimal digits of a MAC address identify the manufacturer of the physical network interface. This is referred to as the Organizational Unique Identifier, OUI. The last six digits uniquely identify the host itself, and are referred to as the host ID.

Drawbacks associated with MAC addresses.

The shortcoming associated with the MAC address is that it contains no hierarchy. The MAC address provides no mechanism to create boundaries between networks hence no way to distinguish one network from another. The lack of hierarchy poses significant difficulties to network scalability. For example, if only Layer-2 physical addressing existed on the network interface, all hosts would technically exist on the same network. Then internetworks such as the Internet would not exist, because it would be impossible to separate one network from the other.

Logical Addressing

Logical addressing is a function of the Network layer, layer 3, of the OSI Model, and provides a hierarchical structure to separate networks. The addresses are never hardcoded on physical network interfaces, and therefore are dynamically assigned and changed freely. The address contains two components:

- Network ID – identifies which network a host belongs to.
- Host ID – uniquely identifies the host on that network.

Examples of logical addressing protocols include Internetwork Packet

Exchange (IPX) and Internet Protocol (IP). The IPX was predominantly used on Novell networks, but is now almost entirely obsolete. The IP is the most widely-used logical address, and is the backbone protocol of the Internet.

Internet Protocol (IP)

In the 1976, the Department of Defense of the United State of America developed the Transmission Control Protocol (TCP), to provide both Network and Transport layer of the OSI layer functions. When it proved to be an inflexible solution, the functions were separated - with the Internet Protocol (IP) providing Network layer services, and TCP providing Transport layer services.

However both TCP and IP provide the core functionality for the TCP/IP or Internet protocol suite.

IP provides two fundamental Network layer services:

- Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.
- Routing – determines the best path to a particular destination network, and then routes data accordingly.

IP was originally defined in RFC 760, and has been revised several times.

IPv4 Addressing

The core function of IP is to provide logical addressing for hosts, that is, a hierarchical structure to both uniquely identify a host, and the network unto which that host exists.

The IP address is most often represented in decimal, in the format; 178.60.124.5. It comprises of four octets, separated by periods.

First Octet	Second Octet	Third Octet	Fourth Octet
178	60	124	5

Each octet is an 8-bit number, resulting in a 32-bit IP address. The smallest possible value of an octet is 0, or 00000000 in binary. The largest possible value of an octet is 255, or 11111111 in binary.

The above IP address represented in binary would look as follows:

First Octet	Second Octet	Third Octet	Fourth Octet
10110010	00111100	01111100	00000111

Classful IP Addressing

IP Addressing standardization in September 1981 necessitated that any network device that needed to communicate through the internet needed to be assigned a unique IP Address to its network interface. That unique network interface IP address needed to possess two parts; one to identify the network and the other part to identify the network device (host) to the network identified in the first part of the IP address. That created a two-level address hierarchy, one addressing the network unto which a device reside and the other one uniquely defining an identity of the device on the network address created in the first part of the hierarchy. For example, such is an IP address and the two-level hierarchy:

Network Number (Prefix)	Host Number

In the defined addressing scheme, all hosts on a given network share the same network prefix but must have a unique host number. Similarly, any two hosts that are on different networks must have different network numbers (prefixes) although they may possibly possess the same host number.

IP Address Classes

The IPv4 address space has been structured into several classes. The value of the first octet of an address determines the class of the network:

Class	First Octet Range	Default Subnet Mask
Class A	1 - 127	255.0.0.0
Class B	128 - 191	255.255.0.0
Class C	192 - 223	255.255.255.0
Class D	224 - 239	-
Class E	- Reserved for experimentation and future expansion.	

Class A networks (/8 Prefixes)

Pronounced as '/8s' or 'slash eights' or 'simply as eights', the Class A networks have an 8-bit network prefix ranging from 1 to 127. This means they have a defined set of 126 networks. To arrive at 126 networks, the computation requires that 2 is subtracted from 2^7(128) because address 0.0.0.0 is reserved for use as the default route while 127.0.0.0 is reserved for the loop back function.

The class has 16,777,214, i.e. 2^{24}- 2 hosts per network. To arrive at this, the computation requires that 2 is subtracted because all 0s and all 1s host numbers are not assigned to individual hosts. Reasons advanced for this restriction was to avoid situations that could potentially confuse classful routers given that routers can be both classless and classful at the same time i.e. could be running classful and classless protocols at the same time. The default subnet mask is 255.0.0.0.

Class B Network(/16)

Simply referred to as '/16s', Class B networks are 16-bit prefix networks ranging from 128 to 191. The default subnet mask for this class is 255.255.0.0. The first two octets of the network define the network with a maximum of 16,384 (2^{14}) networks, while the last two octets define the hosts with a maximum of 65,534 (2^{16}-2) hosts per network. That is 1,073,741,824 (2^{30}) addresses.

Example of a Class B address:

Address: 172.16.5.195

Subnet Mask: 255.255.0.0

Class C Networks (/24)

This /24 or Class C networks are 24-bit networks ranging from 192 to 223. The default subnet mask is 255.255.255.0. The first three octets define the network with a maximum of 2,097,152 (2^{21}) networks, and the last octet defining 254 (2^8-2) hosts per network.

Example of a Class C address:

Address: 197.26.153.6

Subnet Mask: 255.255.255.0

Class D Networks

Class D networks are reserved for use in supporting multicasting traffic. The addresses do not have subnet masks.

Class E Networks

Class E networks are reserved for experimental purposes only.

The Dotted-Decimal Notation

To simplify the utilization of the internet protocol address to humans, the address had to be addressed in four dotted notations of 8bits to represent the 32bit figure required. For instance;

10101100	.	10000	.	101	.	11000000
↓		↓		↓		↓
172	.	16	.	5	.	195