Lab#2: IP ADDRESS & SUBNETORKS (1)

Objectives:

- *Identify IPv4 addresses classes.*
- *Identify the network and host portion of an IP address.*
- *Determine if an address assignment is valid host address*
- *Calculate the sunbetworks in the main nework and the subnetmasks for the subnetwork.*
- *Design a schema of All subnetworks with its valid ranges.*
-

Internet Protocol (IP)

In the 1970's, the Department of Defense developed the Transmission Control Protocol (TCP), to provide both Network and Transport layer functions. When this proved to be an inflexible solution, those functions were separated - with the Internet Protocol (IP) providing Network layer services, and TCP providing Transport layer services. Together, 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. IP Version 4 (IPv4) was the first version to experience widespread deployment, and is defined in RFC 791. IPv4 employs a 32-bit address, which limits the number of possible addresses to 4,294,967,296. IPv4 will eventually be replaced by IP Version 6 (IPv6), due to a shortage of available IPv4 addresses.

IPv4 Addressing

A core function of IP is to provide logical addressing for hosts. An IP address provides a hierarchical structure to both uniquely identify a host, and what network that host exists on. An IP address is most often represented in decimal, in the following format:

158.80.164.3

An IP address is comprised of four octets, separated by periods:

First Octet	Second Octet	Third Octet	Fourth Octet
158	80	164	3

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
10011110	01010000	10100100	00000011

Decimal to Binary Conversion :

The simplest method of converting between decimal and binary is to remember the following table:

128	64	32	16	8	4	2	1

To convert a decimal number of 172 to binary, start with the leftmost column. Since 172 is greater than 128, that binary bit will be set to 1. Next, add the value of the next column (128 + 64 = 192). Since 172 is less than 192, that binary bit will be set to 0. Again, add the value of the next column (128 + 32 = 160). Since 172 is greater than 160, that binary bit will be set to 1. Continue this process until the columns with binary bits set to 1 add up to 172:

Decimal	128	64	32	16	8	4	2	1
Binary	1	0	1	0	1	1	0	0

Binary to Decimal Conversion

Converting from binary back to decimal is even simpler. Apply the binary number to the conversion table, and then add up any columns with binary bits set to 1. For example, consider the binary number of 11110001:

Decimal	128	64	32	16	8	4	2	1
Binary	1	1	1	1	0	0	0	1

By adding 128 + 64 + 32 + 16+ 1, it can be determined that 11110001 equals 241.

The Subnet Mask

Part of an IP address identifies the network. The other part of the address identifies the host. A subnet mask is required to provide this distinction:

158.80.164.3 255.255.0.0

The above IP address has a subnet mask of 255.255.0.0. The subnet mask follows two rules:

• If a binary bit is set to a 1 (or on) in a subnet mask, the corresponding bit in the address identifies the network.

• If a binary bit is set to a 0 (or off) in a subnet mask, the corresponding bit in the address identifies the host.

Looking at the above address and subnet mask in binary:

IP Address: 10011110.01010000.10100100.00000011

Subnet Mask: 11111111.11111111.00000000.00000000

The first 16 bits of the subnet mask are set to 1. Thus, the first 16 bits of the address (158.80) identify the network. The last 16 bits of the subnet mask are set to 0. Thus, the last 16 bits of the address (164.3) identify the unique host on that network. The network portion of the subnet mask must be contiguous. For example, a subnet mask of 255.0.0.255 is not valid.

Hosts on the same logical network will have identical network addresses, and can communicate freely. For example, the following two hosts are on the same network:

Host A: 158.80.164.100 255.255.0.0

Host B: 158.80.164.101 255.255.0.0

Both share the same network address (158.80), which is determined by the 255.255.0.0 subnet mask. Hosts that are on different networks cannot communicate without an intermediating device. For example:

Host A: 158.80.164.100 255.255.0.0

Host B: 158.85.164.101 255.255.0.0

The subnet mask has remained the same, but the network addresses are now different (158.80 and 158.85 respectively). Thus, the two hosts are not on the same network, and cannot *communicate without a router between them. Routing is the process of forwarding packets from one network to another.*

Consider the following, trickier example:

Host A: 158.80.1.1 255.248.0.0

Host B: 158.79.1.1 255.248.0.0

The specified subnet mask is now 255.248.0.0, which doesn't fall cleanly on an octet boundary. To determine if these hosts are on separate networks, first convert everything to binary:

Host A Address: 10011110 . 01010000 . 00000001 . 00000001

Host B Address: 10011110 . 01001111 . 00000001 . 00000001

Subnet Mask: 11111111 . 11111000 . 00000000 . 00000000

Remember, the 1 (or on) bits in the subnet mask identify the network portion of the address. In this example, the first 13 bits (the 8 bits of the first octet, and the first 5 bits of the second octet) identify the network. Looking at only the first 13 bits of each address:

Host A Address: 10011110.01010

Host B Address: 10011110.01001

Clearly, the network addresses are not identical. Thus, these two hosts are on separate networks, and require a router to communicate.

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	---

CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (CIDR) is a simplified method of representing a subnet mask. CIDR identifies the number of binary bits set to a 1 (or on) in a subnet mask, preceded by a *slash. For example, a subnet mask of 255.255.255.240 would be represented as follows in binary: 11111111 . 11111111 . 11111111 . 11110000*

The first 28 bits of the above subnet mask are set to 1. The CIDR notation for this subnet mask would thus be /28. The CIDR mask is often appended to the IP address. For example, an IP address of 192.168.1.1 and a subnet mask of 255.255.255.0 would be represented as follows using CIDR notation: 192.168.1.1 /24 Address Classes vs. Subnet Mask Remember the following three rules:

• The first octet on an address dictates the class of that address.

• The subnet mask determines what part of an address identifies the network, and what part identifies the host.

• Each class has a default subnet mask. A network using its default subnet mask is referred to as ***a classful network****.*

For example, 10.1.1.1 is a Class A address, and its default subnet mask is 255.0.0.0 (/8 in CIDR). It is entirely possible to use subnet masks other than the default.

For example, a Class B subnet mask can be applied to a Class A address: 10.1.1.1 /16 However, this does not change the class of the above address. It remains a Class A address, which has been subnetted using a Class B mask. Remember, the only thing that determines the class of an IP address is the first octet of that address. Likewise, the subnet mask is the only thing that determines what part of an address identifies the network, and what part identifies the host.

<u>Subnet and Broadcast Addresses</u>

On each IP network, two host addresses are reserved for special use:

• The subnet (or network) address

• The broadcast address

Neither of these addresses can be assigned to an actual host. The subnet address is used to identify the network itself. A routing table contains a list of known networks, and each network is identified by its subnet address. Subnet addresses contain all 0 bits in the host portion of the address. For example, 192.168.1.0/24 is a subnet address. This can be determined by looking at the address and subnet mask in binary:

IP Address: 11000000 . 10101000 . 00000001 . 00000000

Subnet Mask: 11111111 . 11111111 . 11111111 . 00000000

Note that all host bits in the address are set to 0. The broadcast address identifies all hosts on a particular network. A packet sent to the broadcast address will be received and processed by every host on that network. Broadcast addresses contain all 1 bits in the host portion of the address. For example, 192.168.1.255/24 is a broadcast address. Note that all host bits are set to 1:

IP Address: 11000000 . 10101000 . 00000001 . 11111111

Subnet Mask: 11111111 . 11111111 . 11111111 . 00000000

Broadcasts are one of three types of IP packets:

• *Unicasts are packets sent from one host to one other host*

• *Multicasts are packets sent from one host to a group of hosts*

•*Broadcasts are packets sent from one host to all other hosts on the local network A router, by default, will never forward a multicast or broadcast packet from one interface to another. A switch, by default, will forward a multicast or broadcast packet out every port, except for the port that originated the multicast or broadcast.*