## 3.8 Classless Inter-Domain Routing (CIDR)

CIDR is basically the method that ISPs (Internet service providers) use to allocate a number of addresses to a company, a home, and a customer. They provide addresses in a certain block size.

CIDR Values

| Subnet Mask | CIDR Value | |
|---|---|---|
| 255.0.0.0 | /8 | Class A |
| 255.128.0.0 | /9 | |
| 255.192.0.0 | /10 | |
| 255.224.0.0 | /11 | |
| 255.240.0.0 | /12 | |
| 255.248.0.0 | /13 | |
| 255.252.0.0 | /14 | |
| 255.254.0.0 | /15 | |
| 255.255.0.0 | /16 | Class A & B |
| 255.255.128.0 | /17 | |
| 255.255.192.0 | /18 | |
| 255.255.224.0 | /19 | |
| 255.255.240.0 | /20 | |
| 255.255.248.0 | /21 | |
| 255.255.252.0 | /22 | |
| 255.255.254.0 | /23 | |
| 255.255.255.0 | /24 | Class A , B & C |
| 255.255.255.128 | /25 | |
| 255.255.255.192 | /26 | |
| 255.255.255.224 | /27 | |
| 255.255.255.240 | /28 | |
| 255.255.255.248 | /29 | |
| 255.255.255.252 | /30 | |

The /8 through /15 can only be used with Class A network addresses. /16 through /23 can be used by Class A and B network addresses. /24 through /30 can be used by Class A, B, and C network addresses. This is a big reason why most companies use Class A network addresses. Since they can use all subnet masks, they get the maximum flexibility in network design

## General Notes for Subnetting:

The subnetting is a process of dividing a single network into subnets, the default subnet mask can be shown in table 3.2.

***Table 3.2 Shows subnets with their network, host range and broadcast addresses***

| Class | Format | Default Subnet Mask | Network Range |
|---|---|---|---|
| A | N.H.H.H | 255.0.0.0 | 0.0.0.0 /8 to 127.0.0.0 /8 |
| B | N.N.H.H | 255.255.0.0 | 128.0.0.0 /16 to 191.255.0.0 /16 |
| C | N.N.N.H | 255.255.255.0 | 192.0.0.0 /24 to 223.255.255.0/24 |

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and broadcast addresses of a subnet that the mask provides, all you need to do is answer five simple questions:

- How many subnets does the chosen subnet mask produce?
- How many valid hosts per subnet are available?
- What are the valid subnets?
- What's the broadcast address of each subnet?
- What are the valid hosts in each subnet?

In a Class C address, only 8 bits are available for defining the hosts. Remember that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

| Binary | Decimal | CIDR |
|---|---|---|
| 00000000 = | 0 | /24 |
| 10000000 = | 128 | /25 |
| 11000000 = | 192 | /26 |
| 11100000 = | 224 | /27 |
| 11110000 = | 240 | /28 |
| 11111000 = | 248 | /29 |
| 11111100 = | 252 | /30 |

For example, we have 11000000 and we want to answer above five big questions:

- *How many subnets?* $2^x$, where $x$ is the number of masked bits or the 1s. So the number of 1s gives $2^2$= 4 subnets.

- *How many hosts per subnet?* $2^y$-2, where $y$ is the number of unmasked bits or the 0s. So, the number of 0s gives $2^6$-2= 62 host per subnet.

- *What are the valid subnets?* 256 – subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64. Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64, 128, 192.

- *What's the broadcast address for each subnet?* Since we counted our subnets in the last section as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet. For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64. The 64 subnet has a broadcast address of 127 because the next subnet is 128. And so on.

- *What are the valid hosts?* Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s. For example, if 64 is the subnet number and 127 is the broadcast address, then 65 – 126 is the valid host range it's *always* the numbers between the subnet address and the broadcast address.

## 3.9 Private and Public Addresses

***Private IP address*** of a system is the *IP address* that is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

***Public IP address*** of a system is the IP address that is used to communicate outside the network. A public IP address is basically assigned by the *ISP (Internet Service Provider)*. The differences between private and public addresses can be shown in table 3.3.

***Table 3.3 Shows some of differences between private and public addresses***

| No. | Private Address | Public Address |
|---|---|---|
| 1 | The scope of Private IP is local | The scope of Public IP is global |
| 2 | It is used to communicate within the network | It is used to communicate outside the network |
| 3 | It works only on LAN | It is used to get Internet service |
| 4 | Private IP can be known by entering "ipconfig" on the command prompt | Public IP can be known by searching "what is my Ip" on google |
| 5 | Range:<br>10.0.0.0 – 10.255.255.255,<br>172.16.0.0 – 172.31.255.255,<br>192.168.0.0 – 192.168.255.255 | Range:<br>Besides private IP addresses, the rest are public. |
| 6 | Example: 192.168.1.10 | Example: 17.5.7.8 |
| 7 | Private IP addresses are secure | Public IP address has no security and is subjected to attack |
| 8 | Private IP addresses require NAT to communicate with devices | Public IP does not require a network translation |