

Subnet Masks

A subnet mask allows users to identify which part of an [IP address](#) is reserved for the network and which part is available for host use. By looking at the IP address alone, especially now with classless inter-domain routing, users cannot tell which part of the address is which. Adding the subnet mask or netmask gives users all the information needed to calculate network and host portions of the address with ease. In summary, knowing the subnet mask can allow users to easily calculate whether IP addresses are on the same [subnet](#) or not.

There are two fundamental rules when subnetting:

- If a bit in a subnet mask has a value of one, then the bit is part of the network prefix in the corresponding IP address.
- If a bit in a subnet mask has a value of zero, then the bit is part of the host suffix in the corresponding IP address.

Determining Network and Host Portions of an IP Address with a Subnet Mask

To determine what the [network address](#) is for any given IP address, users merely have to convert both octal addresses into binary and do a bitwise AND operation. Here is an example of using an IP address of 156.154.81.56 with a network mask of 255.255.255.240:

IP Address:	10011100.10011010.01010001.00111000
Subnet mask:	11111111.11111111.11111111.11110000
Bitwise AND	-----
Result:	10011100.10011010.01010001.00110000

255.255.255.252 252 = 11111100

Subnets						Hosts	
1	1	1	1	1	1	0	0
128	64	32	16	8	4	2	1
32	16	8	4	2	1	2	1

subnets = 62 (64 - 2)

hosts = 2 (4 - 2)

The network address for the IP address and subnet mask in question is 156.154.81.48. To determine how many hosts can be on this same subnet, it is a simple operation. Count the number of bits from the right until the first "1" in the binary network address display is reached. That number will be the power raised to 2 for the calculation of possible number of hosts. Also, subtract two from the result because one address is reserved for broadcast and

network addresses. This results in the final algorithm of 2^{n-2} . In this case there are 4 bits of 0 in the network address, leaving 2^{4-2} hosts possible or 14 hosts. This means that the network address is 156.54.81.48, that there is a range of addresses available to hosts from 156.154.81.49 – 156.154.81.62, and that the broadcast address for this network is 156.154.81.63.

Default Subnet Mask

When applying the two rules of subnetting to classful addresses, the default subnet mask for different classes of the ip addresses are:

- Class A = 255.0.0.0
- Class B = 255.255.0.0
- Class C = 255.255.255.0

Where 255 represents network prefix and 0 represents host suffix. In the above table 255.0.0.0 is a standard class A subnet mask, since the first bit are all once (network) and the last three bites are all zeros (host). When this subnet mask is applied to a class A network, no subnetting is performed.

How to Change Subnet Mask?

The subnet mask is a value that basically differentiates the network and host portion of your networking device. If you can change the subnet mask of your computer for some purpose you can change by two different methods either by using graphical tools or by using command line interface.

Following are the details of both the methods in the Microsoft Windows Operating System:

- In the properties tab of Local Area Connection you should have to select [TCP/IP](#) and click the properties tab of TCP/IP. Click once on the field of subnet mask and delete the old subnet mask, then configured the new subnet mask and click on OK tab and then click OK. Check the new subnet mask with the command "ipconfig".
- You should have to execute the command "set address local static ip address subnet mask" in the netsh interface ip> mode of your Microsoft Windows computer.

Defining Variable Length Subnet Masking

With classful subnetting, all subnets have the identical number of host addresses. This could present issues if you need certain subnets to have a small number of IP addresses, and you need other subnets to have a large number of IP addresses. The solutions listed below; to

solving this issue does not however optimize the network configuration. This is mostly due to IP addresses being wasted:

If you require a large number of host addresses, you can create subnets that have numerous numbers of host addresses.

- If you require a small number of host addresses, you can create subnets that have small numbers of host addresses.

Previously, a single [subnet mask](#) was used in the entire network, and was shared by all hosts in that particular network. When one subnet mask is used, and the network is divided into subnets, then all subnets have the identical number of host addresses.

Variable length subnet masks (VLSMs) allow subnets to be further subnetted, and also enable routers to handle different subnet masks. VLSMs provide the flexibility needed to optimize the network configuration by allowing you to configure network subnets that meet the requirements of your organization.

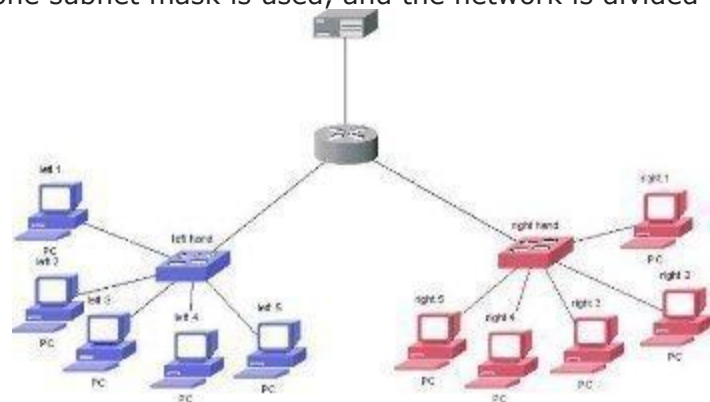
No IP addresses are wasted. VLSMs (nonclassful subnetting) can be defined

as the process whereby which subnets are divided into smaller segments of various sizes. The name used to describe the process wherein subnets are continuously subdivided, is recursive subnetting.

For VLSM to allow subnets to be further subnetted, it utilizes the subnet mask to distinguish between the network address and the host address of the IP address. The process of dividing a subnet into further segments starts with the subnet mask used on the original subnet. The default subnet mask is not the starting point.

When you use VLSM to divide a network into different sized subnets, a definite pattern of subnet IDs with trailing 0s have to be used. The trailing 0s actually prevent the subnet address spaces from overlapping with each other. With a Class C network, a maximum of seven subnets can be defined. This concept is illustrated below:

- Subnet 1:
 - Subnet ID: 0



- Subnet Mask: 255.255.255.128
- Hosts per Subnet: 126
- Subnet 2:
 - Subnet ID: 10
 - Subnet Mask: 255.255.255.192
 - Hosts per Subnet: 62
- Subnet 3:
 - Subnet ID: 110
 - Subnet Mask: 255.255.255.224
 - Hosts per Subnet: 30
- Subnet 4:
 - Subnet ID: 1110
 - Subnet Mask: 255.255.255.240
 - Hosts per Subnet: 14
- Subnet 5:
 - Subnet ID: 11110
 - Subnet Mask: 255.255.255.248
 - Hosts per Subnet: 6
- Subnet 6:
 - Subnet ID: 111110
 - Subnet Mask: 255.255.255.252
 - Hosts per Subnet: 2
- Subnet 7:
 - Subnet ID: 111111
 - Subnet Mask: 255.255.255.252
 - Hosts per Subnet: 2

From the above illustration, you can notice that the last two subnets, Subnet 7 and Subnet 6 are the same size. Subnet 7 is differentiated by a subnet ID that has all 1s. No trailing 0s are used to define Subnet 7. You can utilize this configuration at any subnet level to replace each of the subnets beneath that particular subnet.

While RFC 1812 allows you to use subnets that are all 0s or all 1s, you should first verify that each host and router on your network supports this particular configuration. Even today, not all hosts and routers support RFC 1812. Before you can implement subnets with all 0s or all 1s, you have to meet the following requirements:

- A [routing protocol](#) which supports RFC 1812 must be running within your network environment. [Routing](#) protocols that support RFC 1812 are:
 - Border Gateway Protocol version 4 (BGPv4)
 - Open Shortest Path First (OSPF)
 - [Routing Information Protocol](#) version 2 (RIPv2)
- You have to configure your hosts and routers to support all 0s or all 1s subnets. If you have hosts and routers running Windows Server 2003, the use of 0s or all 1s subnets is automatically supported. You do not need to perform any further configuration.

Are Subnet Masks Necessary?

Subnet masks are critical to communications on an IP network. Network devices use the IP address targets and defined netmask to determine if the network the host is on is a local subnet or a [remote network](#). This is important because devices act differently depending on the result. If the subnet is local, the device will send an [ARP](#) request to retrieve the [MAC or hardware address](#) of the system in question to communicate over the [data-link layer](#). If the address is found to be on a [remote network](#), then the network device [routes](#) packets to the gateway in its [routing table](#) that is set to handle that network. If no routing table entry matches that network, the packets are routed to the default route. If no default route is defined, the packets are dropped with nowhere left to go.

Source: <http://www.tech-faq.com/subnet-mask.html>