Subnetting

Subnetting is the process of breaking down an IP network into smaller sub-networks called "subnets." Each subnet is a non-physical description (or ID) for a physical sub-network (usually a switched network of host containing a single router in a multi-router network).

In many cases, subnets are created to serve as physical or geographical separations similar to those found between rooms, floors, buildings, or cities.

There could be more than one definition for subnetting but perhaps the best explanation is that by default a network id has only one broadcast domain. Subnetting is a process of segmentation of a network id into multiple broadcast domains.
Subnetting originally referred to the subdivision of a class-based network into many subnetworks, but now it generally refers to the subdivision of a CIDR block in to smaller CIDR blocks. Subnetting allows single routing entries to refer either to the larger block or to its individual constituents. This permits a single routing entry to be used though most of the Internet, more specific routes only being required for routers in the subnetted block.

Most modern subnet definitions are created according to 3 main factors. These include:

1. The number of hosts that needs to exist on the subnet now and in the future.
2. The necessary security controls between networks.
3. The performance required for communications between hosts.

Subnet Mask Notation

There are two forms of subnet notation, standard notation and CIDR (Classless Internet Domain Routing) notation. Both versions of notation use a base address (or network address) to define the network's starting point, such as 192.168.1.0. This means that the network begins at 192.168.1.0 and the first possible host IP address on this subnet would be 192.168.1.1.
In standard subnet mask notation, a four octet numeric value is used as with the base address, for example 255.255.255.0. The standard mask can be calculated by creating four binary values for each octet, assigning the binary digit of .1. to the

network portion, and assigning the binary digit of .0. to the host portion. In the example above this value would be 11111111.11111111.11111111.00000000. In combination with the base address is a subnet definition. In this case the subnet in standard notation would be 192.168.1.0 255.255.255.0.

In CIDR notation, the number of 1.s in the mask's binary version is counted from the left and that number is appended to the end of the base address following a slash (/). In the example here, the subnet would be listed in CIDR notation as 192.168.1.0/24.

Network Subnetting

In a subnetted network, there is an extended network portion. For example, a subnet mask of 255.255.255.0 would subnet a class B IP address space using its third byte. Using this scheme, the first two octets of an IP address would identify the class B network, the next octet would identify the subnet within that network, and the last octet would select an individual host. Since subnet masks are used or bit-by-bit

bases, masks like 255.255.224.0 (three bits of subnet and thirteen bits of host) are perfectly normal.
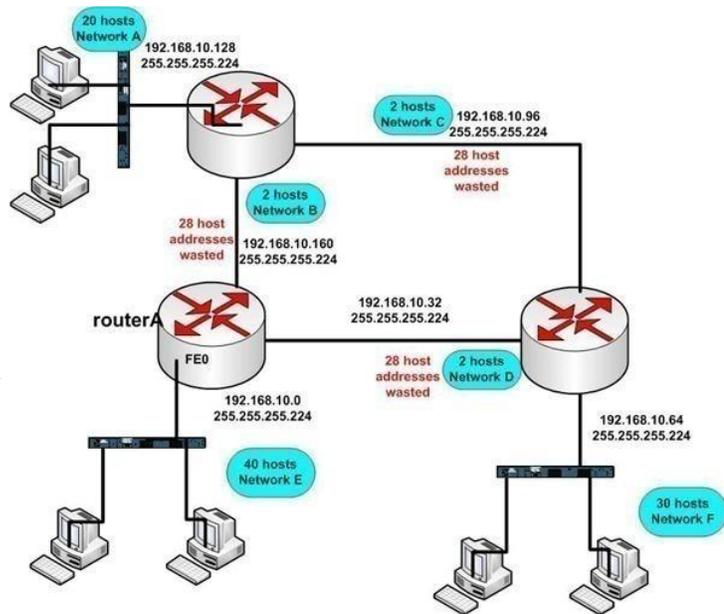
There are several restrictions applied in a traditional subnetted network. Many of these restrictions have been lifted by CIDR, VLSM and more flexible IP routing protocols such as EIGRP and OSPF. However, if other routing protocols such as IGRP and RIP are used, the two restrictions must still be observed are as follow:

- All subnet masks must be of a fix length. Since IGRP and RIP routing updates do not include subnet mask information, a router must assume that the subnet mask with which it has been configured is valid for all subnets. Therefore, a single mask must be used for all the subnets of a given classful network and different subnet masks can be used for different classful network addresses. This rule is referred to as the rule of FLSM (Fixed Length SubnetMask). Based on the

assumption of FLSM, router can exchange subnet route with other routers within the network. Since the subnet masks are identical across the network, the routers will interpret these routes in the same manner. However, routers not attached to the subnetted network can not interpret these subnet routes, since they lack the subnet mask. Therefore, subnet route are not relayed to router on other networks. This leads to second restriction.

- A subnetted network can not be split into isolated portions. All the subnets must be contiguous, since subnet routing information can not be passed to non-members. All the subnets must be able to reach all other subnets with in a network without passing traffic through other networks.

Class C Subnetting

The Class C subnetting is less complicated then the other two classes of IP Addresses. There is comparatively less calculations you have to do in this type of subnetting. For example your company is using a single class C network of 192.168.0.0 with a default subnet mask of 255.255.255.0. The company has six departments of 30 hosts each and the requirement of your company is to segment them and broke the single broadcast domain for security reasons and to increase the maximum availability of bandwidth. You have to do three bits of subnetting using the formula 2n -2 where n is the value of subnet bits. The subnet bits would change the host portion of the subnet mask which is now 255.255.255.224 after subnetting. This can also be written in bit count format such as 192.168.0.0/27. A common subnetwork environment is too inflexible when you require various types of subnet mask for the same network address. For example, consider a large organization with a single class C address of 192.168.0.0. Its headquarters site is made up of one subnet with 120 hosts on this subnet. The same organization has three regional offices, with a single LAN with less then 30 hosts each. Finally, this organization has six field offices. Each field office has a single segment with less then five hosts each. Which of the following subnet mask is best for this organization?

- A 25 bit subnet mask yielding 2 subnets with each subnet yields 128 valid host addresses each (255.255.255.128).
- A 26 bit subnet mask yielding 4 subnets with each subnet yields 62 valid host addresses each (255.255.255.192).

- A 29 bit subnet mask yielding 30 subnets with each subnet yields 6 valid host addresses each (255.255.255.248).

The answer is the 25 bit subnet mask can be deployed at then central site. The 26 bit subnet mask can be deployed at the branch offices while the 29 bit mask can be deployed at the field offices. This is an example of a Variable Length Subnet Mask. However, the FLSM environment can not accommodate deploying all of these different length subnet masks for a single classful network prefix.

There are two types of subnetted environment such as Fixed Length Subnet Mask (FLSM) and Variable Length Subnet Mask (VLSM). The selection of routing protocol also determines whether you are stuck with a FLSM environment or whether you can deploy VLSM.

How to Compute the Maximum Number of Hosts for a Subnet Mask

To compute the maximum number of hosts for a subnet mask, take two and raise it to the amount of bits allocated to the subnet (count the number of 0.s in the subnet mask binary value) and subtract two. Subtract two from the resulting value because the first value in the IP address range (all 0s) is reserved for the network address and the last value in the IP address range (all 1s) is reserved for the network broadcast address. For example, DSL networks commonly use 8 bits for their subnets. The amount of allowable hosts for such a DSL network could be computed by the following formula: max hosts = $(2^8)-2 = 254$ hosts.

As users subnet networks, the number of bits that the subnet mask represents will decrease. Decrease the octets in order starting from the rightmost value and proceed left toward a zero value. Mask values decrease by a power of two each time a network is split into more subnets. Values are 255, 254*, 252, 248, 240, 224, 224, 192, 128. Each decrease indicates that an additional bit has been allocated. After 128, the next bit allocated will reduce the fourth octet to 0, and the third octet will follow same 8-number progression.

For instance, a subnet mask dotted decimal number of 255.255.255.255 indicates that no bits have been allocated and that the maximum number of hosts is 1 $(0^1=1)$. The subnet mask 255.255.255.128 indicates that the maximum number

of hosts is 128. And the subnet mask 255.255.128.0 indicates that the maximum number of hosts is 32,786.

* 254 is not a valid number for the fourth octet because no addresses are available for hosts. i.e. (2^1)-2 = 0.

Subnetting Calculators

Subnetting calculator is a very useful tool that is available on subnetting tutorials offered by various websites. We can utilize it by downloading from any website for subnetting practice. The subnetting of Class A and B Addresses is comparatively more difficult and complicated then Class C Address. Subnet calculator makes it easier.

Implementing Subnetting

The Important factors that should be clarified when determining the requirements of your subnetting scheme are:

- The number of required network IDs. A network ID is needed for each subnet, and for each WAN connection.
- The number of required host IDs. A host ID is needed for each TCP/IP based network device

Using the information above, you can create

- A subnet mask for the network.
- A subnet ID for every physical network segment
- A range of host IDs for every unique subnet

You implement subnetting by assigning a subnet address to each machine on a particular physical network. While you cannot change the network address segment of an IP address, you can change the host address segment. With subnetting, you take part of the host address and reuse it as a subnet address. This is done by taking bit positions from the host ID and then changing it to the subnet identifier. The number of host IDs are therefore reduced when you implement subnetting.

When you start the subnetting process, the bit position taken from the host ID reduces the number of hosts by a factor of 2. For instance, in a Class B network, you can have 65,534 possible host addresses or IDs. If you start subnetting the number of hosts which you can have is about half that figure. This is calculated as 65,534 / 2.

If the network has been subnetted, you can use the following equation to determine the number of host IDs you can have for each subnet:

- 2x – 2
  - x = number of bits in the host ID

Legacy Subnets

Legacy subnets were not flexible because they had predefined limitations on their size and numbers. These were called "classful" networks because each network could be easily identified and placed into a specific class, A to E. Shown below is a table containing the original "classful" definitions for IP addresses:

IP Address Range	CIDR Equivalent	Purpose	RFC	Class	Total # of Addresses
0.0.0.0 – 0.255.255.255	0.0.0.0/8	Zero Addresses	1700	A	16,777,216
10.0.0.0 – 10.255.255.255	10.0.0.0/8	Private IP addresses	1918	A	16,777,216
127.0.0.0 – 127.255.255.255	127.0.0.0/8	Localhost Loopback Address	1700	A	16,777,216
169.254.0.0 – 169.254.255.255	169.254.0.0/16	Zeroconf / APIPA	3330	B	65,536
172.16.0.0 – 172.31.255.255	172.16.0.0/12	Private IP addresses	1918	B	1,048,576
192.0.2.0 – 192.0.2.255	192.0.2.0/24	Documentation and Examples	3330	C	256
192.88.99.0 – 192.88.99.255	192.88.99.0/24	IPv6 to IPv4 relay Anycast	3068	C	256
192.168.0.0 - 192.168.255.255	192.168.0.0/16	Private IP addresses	1918	C	65,536
198.18.0.0 – 198.19.255.255	198.18.0.0/15	Network Device Benchmark	2544	C	131,072
224.0.0.0 – 239.255.255.255	224.0.0.0/4	Multicast	3171	D	268,435,456
240.0.0.0 - 255.255.255.25	240.0.0.0/4	Reserved	1700	E	268,435,456

5					

Classless IP Addresses

With the advent of CIDR (Classless Inter-Domain Routing), the "classful" definition of subnet divisions was lifted. Any network address could be defined just as any of the "classful" subnet of the past could be defined. All that is required is enough neighboring address space to cover all the IP addresses needed. Classless addresses also assist in reducing the overall size of the global routing tables on network devices.

When is Subnetting Used?

The advantages associated with subnettng a network are summarized below:

- Through subnetting, you can reduce network traffic and thereby improve network performance. You only allow traffic that should move to another network (subnet) to pass through the router and to the other subnet.
- Subnettiing can be used to restrict broadcast traffic on the network.
- Subnetting facilitates simplified management. You can delegate control of subnets to other administrators.
- Troubleshooting network issues is also simpler when dealing with subnets than it is in one large network.

A subnet is usually composed of a network router, a switch or hub, and at least one host.

Source: http://www.tech-faq.com/subnetting.html