Subnetting Your Network – What, When and How

What is Subnetting?

Subnetting is essentially the modification of a single IP network to create 2 or more logically visible sub-sections. It entails changing the subnet mask of the local network number to produce an even number of smaller network numbers, each with a corresponding range of IP addresses.

When is subnetting necessary?

Subnetting is required when one network number needs to be distributed across multiple LAN segments. This may be the case in instances when:

- a company uses two or more types of LAN technology (i.e. Ethernet, Token Ring) on their network.
- two network segments are restricted by distance limitations (i.e. remote offices linked via point-to-point circuit).
- segments need to be localized for network management reasons (accounting segment, sales segment, etc.).
- hosts which dominate most of the LAN bandwidth need to be isolated.

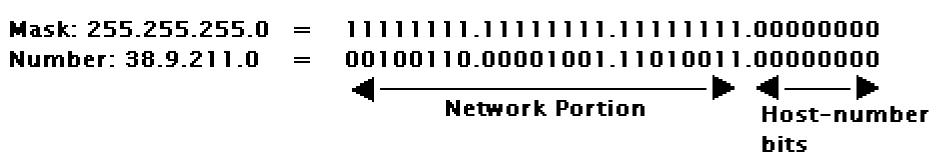
Advantages and Disadvantages

Hopefully your decision to subnet happened before your workstations were assigned IP addresses. This will allow for much more flexibility in your segment layout. Subnetting can provide you with easier network management capabilities and also lends itself to faster troubleshooting. Additionally, subnetting keeps the size of the Internet's routing tables down, since you won't be adding an additional network number for each segment.

The routing announcement of your network to the outside world will still be based on your single network number. Keep in mind, though, that subnetting will decrease the total amount of IP addresses available to you, and may require purchasing additional hardware, such as a router.

How It Works

An IP address is a 32 bit number divided into 4 sections of 8 bits, called octets. Each octet is usually converted from binary to decimal form and separated with a dot to make it readable. The address can also be split into a network and host portion. The network portion always remains fixed for a particular network, while the remaining bits which make up the host portion can be altered to give the range of addresses to assign to hosts. In order to determine where the network portion ends and the host portion begins, a subnet mask (or netmask, or just mask) is used to fix the network portion and allow the host portion to be changed. As an example, we will use the IP number 38.9.211.0 with a subnet mask of 255.255.255.0. Changing to binary, we get:



A binary 1 will "mask" the bit, and a 0 will deem it variable. So, for this case, we refer to the netmask as 24 bits, or /24 (**38.9.211.0/24)**.

The fixed bits become the network portion and the remaining bits become the host portion, so in this case there are 8 host bits which account for a range from 0-255. IP protocol standards dictate that we use addresses of all 0's to refer to the network as a whole, and addresses of all 1's to refer to the broadcast of all hosts on the network, so these host addresses may not be used. This limits our host range from 1 - 254.

- 38.9.211.0/24 — the entire /24 network
- 38.9.211.1 - 38.9.211.254 — range of valid hosts
- 38.9.211.255 — broadcast address of all hosts on the network

Once you receive your network number, whether it's a /24, /25, or /27, you have the ability to extend the network portion further into the host-number field by lengthening the netmask. The number of bits that you extend into the original host portion determines how many segments, or subnets, you will produce. To be specific, lengthening the mask by n bits will produce 2^n subnets. Let's illustrate what would happen if we used 2 subnet bits. The host portion would be reduced to six bits. There are 4 different combinations of arranging the 2 subnet bits, so we arrive at 4 unique subnets.

Subnet 1	00000000 - 00111111	(.0 - .63)
Subnet 2	01000000 - 01111111	(.64 - .127)
Subnet 3	10000000 - 10111111	(.128 - .191)
Subnet 4	11000000 - 11111111	(.192 - .255)

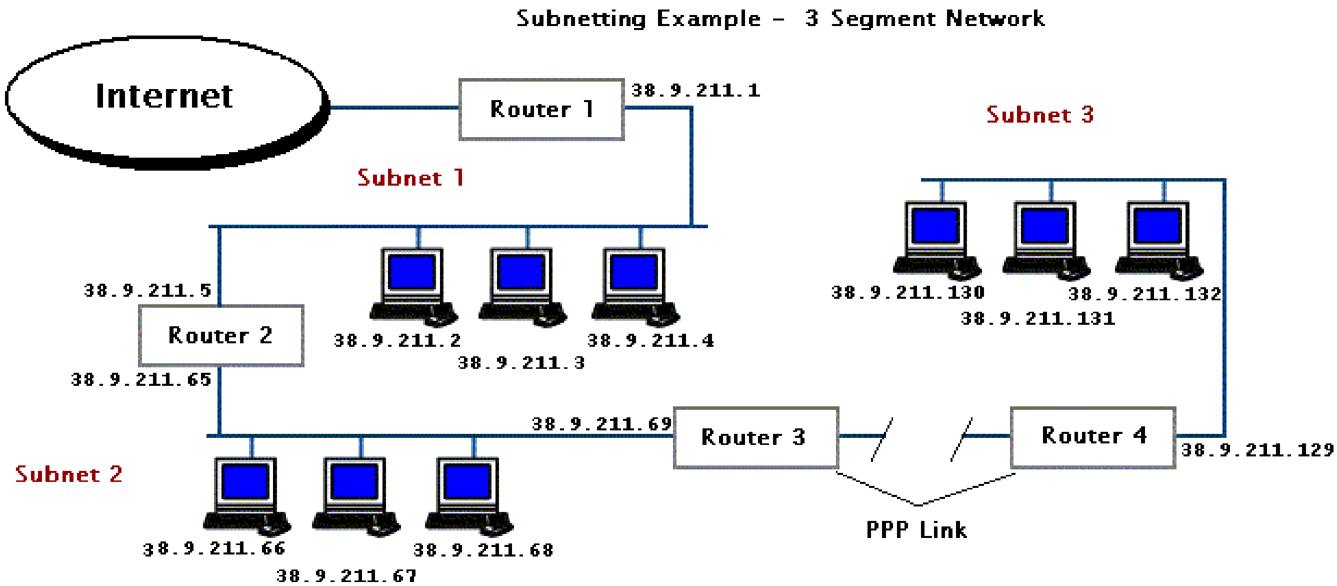
What we have accomplished is creating 4 network numbers from 1. Once again, adhering to our rule that all 0's is a network, and all 1's is a broadcast, we can see where each subnetwork begins and ends.

Network	Host Ranges	Broadcast
**38.9.211.0/26	38.9.211.1 - 38.9.211.62	38.9.211.63
38.9.211.64/26	38.9.211.65 - 38.9.211.126	38.9.211.127
38.9.211.128/26	38.9.211.129 - 38.9.211.190	38.9.211.191
**38.9.211.192/26	38.9.211.193 - 38.9.211.254	38.9.211.255

**An Important Note

Some older routers do not send subnet masks for every announced route. These routers do not understand the all 0's and all 1's subnets, so they may not be used. However, if you are using an assigned number from our net 38 block (i.e. 38.x.x.x), or if your router allows you to provide netmasks in its routing table, these subnets are routable.

Subnetting Your Network – What, When and How



Sample Topology

The figure above illustrates a topology which can route the same network number over 3 segments, one of which is linked across a PPP connection. The /24 network was split into 4 subnets (since you may only produce 2^n subnets) using a /26 mask.

Configuration

Each router and workstation will use a 255.255.255.192 subnet mask in its IP configuration. The default gateway will always be the IP address of the closest router to the Internet on the segment.

TCP/IP Config

Subnet 3 - 38.9.211.128/26
The following use 38.9.211.129 as a default gateway:
- 38.9.211.130
- 28.9.211.131
- 38.9.211.132

Subnet 2 - 38.9.211.64/26
The following use 38.9.211.65 as a default gateway:
- 38.9.211.69
- 38.9.211.68
- 38.9.211.67
- 38.9.211.66

Subnet 1 - 38.9.211.0/26
The following use 38.9.211.1 as a default gateway:
- 38.9.211.5
- 38.9.211.4
- 38.9.211.3
- 38.9.211.2

Subnetting Your Network – What, When and How

Static vs. Dynamic Routing

Internal routing may be accomplished statically or dynamically. For dynamic routing, an internal protocol such as rip may be used. Each router will create its own routing table based on rip announcements. If static routing is preferred, the tables will need to be created manually. The table below illustrates what the routing table will look like on each router. The default gateway is identified by
the 0.0.0.0 route which refers to any route that is not explicitly matched in the routing table.

Router 4 (38.9.211.129)
0.0.0.0 via PPP WAN link

Router 3 (38.9.211.69)
0.0.0.0 via 38.9.211.65
38.9.211.128 255.255.255.192 via PPP WAN link

Router 2 (38.9.211.5)
0.0.0.0 via 38.9.211.1
38.9.211.128 255.255.255.192 via 38.9.211.69
38.9.211.64 255.255.255.192 via 38.9.211.65

Router 1 (38.9.211.1)
0.0.0.0 via WAN link or POP IP address
38.9.211.128 255.255.255.192 via 38.9.211.5
38.9.211.64 255.255.255.192 via 38.9.211.5
38.9.211.0 255.255.255.0 via 38.9.211.1 (Full /24 announcement)