How Subnets Work in Practice

Fred Marshall
Coastal Computers & Networks

Background

There's lots of literature available on how the bit structure of an address can be split up using the subnet mask. Generally, any address is split up between what's referred to as a "network address" part and a "host address" part.

It's assumed that all computers are either on the "network" – meaning that they all have the same network address – or they aren't.   Here are some examples:

Computer #1 IP: 192.168.1.101 Subnet Mask: 255.255.255.0

Computer #2 IP: 192.168.1.130 Subnet Mask: 255.255.255.0

Computer #3 IP: 205.160.3.222 Subnet Mask: 255.255.255.240

Here, computers #1 and #2 have private range IP addresses and have the same subnet address.
They are said to be on network 192.168.1.0 which has 254 usable addresses from 192.168.1.1 to 192.168.1.254

Computer #3 isn't on the same network.
It is on network: 205.160.3.208 which has 14 usable addresses from 205.160.3.209 to 205.160.3.222

All of this sort of thing you can read about all day by Googling "how does a subnet mask work?" But, after a while you might want to understand just a bit more about how the subnet mask works – how it makes things happen (and not happen) in a real network.

Packets

All communications of interest here are accomplished by the transmission and reception of "packets" of data. Each packet has a "source address" (where it's coming from) and a "destination address" (where it's intended to end up). NOTE: there is no subnet mask included in the packet!! This means that no computer on the network "knows" what the source or destination subnet masks are. It only knows what its own subnet mask is!!

The implication of this is that a computer (or router or ……) only uses its subnet mask after it has received a packet.

Routing

When a packet leaves your computer it is either sent to a "next hop" address or it's sent directly to the destination address. This is important.
If a packet is destined for an address on the same "network" <u>as defined by its own subnet mask</u>, then the packet is just "put on the wire"; i.e. it's sent directly to the intended destination and there isn't any "next hop" really. Or, if you like, the "next hop" IS the destination.

In contrast, if a packet is destined for an address that is not on the same "network" <u>as defined by its own subnet mask</u>, then the packet is forwarded to an interim computer or device which would be the logical "next hop".

Most networks have at least one "gateway" router that is the normal "next hop" device for any packets that aren't on the source computer's network. It's the router's job to "route" the packets it receives to the proper physical port or connection and on to the next "next hop" in gettting to the destination.

Note that routing of packets beyond the "next hop" is outside the control of the originating source computer.

A typical small router has two "ports" to which it might send packets:
- a WAN or Internet port
- a LAN port or switch with multiple physical ports
If neither the WAN or the LAN are appropriate launch points to a next hop, then the packet is dropped. So, there are 3 possible outcomes when a packet reaches the router:
-    go to a next hop from the WAN port; so perhaps on to the internet,
-    go to a next hop (likely the destination) from the LAN port,
-    disappear.

Each computer and each router (just another computer) have a "routing table" that it uses to decide how packets are to be handled. If you open a command line window and type something like:

route print

you'll see the routing table for your computer. Let's say it's Computer #1 from above. Among the table entries you'll see:

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.101	20
192.168.1.0	255.255.255.0	192.168.1.101	192.168.1.101	20

Default Gateway: 192.168.1.1

Here, as it says, the default gateway is the router with LAN address 192.168.1.1.

Note that this doesn't tell us what the subnet mask for the router LAN might be!! Anyway, the way to read the table is this:

The "interface" column says that all of these packets go out from network interface on the computer which is 192.168.1.101

A network destination of 0.0.0.0 pretty much means "any other address" should be routed to the gateway router. So, really there are no dropped packets here – they either go on the wire directly or to the gateway router. Now, if a packet is destined for a computer that's turned off, then it's lost as there's no computer to receive it.

A network destination of 192.168.1.0 means any address in *my* subnet just goes out on the wire directly to the destination address. Note the difference in the routing table "gateway". In this case it's simply the network interface on the computer 192.168.1.101 while for any other address it's 192.168.1.1, the router.

There are plenty of better and more detailed explanations of routing tables – so one can look them up.

- - - -

OK. So now let's consider what happens when a packet arrives at the router:

As above, the router has a routing table of its own.

In the router, there are more choices than we see in the computer's routing table. As above, the packets can go to the WAN/internet interface, they can go to the LAN interface or they can be dropped – not going to either interface. It's really beyond the intent of this paper to get into all the rules.

How Subnet Settings Interact

OK. So now we have some background on packets and routing. The key question we want to address here is:

What happens if computers and devices using different networks and subnet masks are physically connected together? Can they communicate? Will they?

Note: This has nothing to do with the operating system on any of the computers. At least it's not intended to!

Let's take a couple of examples:

Example 1: One computer on a network that's a subset of the other computer and the router:

Computer "A" 192.168.1.101 Subnet Mask: 255.255.255.0

Computer "B" 192.168.1.130 Subnet Mask: 255.255.255.128

Router LAN: 192.168.1.1   Subnet Mask: 255.255.255.0
Router WAN: 205.160.3.222 Subnet Mask: 255.255.255.240

Source	Destination	Next Hop	Result
192.168.1.101	192.168.1.130	192.168.1.130	Single hop
192.168.1.130	192.168.1.101	192.168.1.1	
192.168.1.130	192.168.1.101	192.168.1.101	Double hop
192.168.1.101	192.168.0.1	192.168.1.1	Packet dropped in router

In the first case, Computer "A" sees the address of Computer "B" as inside its own network and sends the packet directly to Computer "B".

In the second case, Computer "B" sees the address of Computer "A" as outside its own network and sends the packet to the router. The router sees the packet as belonging to its LAN network and puts the packet back out on the LAN; this time it's addressed to Computer "A" – while on the first hop it was addressed to the router.

In the third case, Computer "A" sees the address 192.168.0.1 as outside its own network and sends the packet to the router.   The router doesn't have an interface configured that will accept this address as a destination and the packet is dropped.

Example 2: One computer on a network that's a superset of the other computer and the router:

Computer "A" 192.168.1.101 Subnet Mask: 255.255.255.0

Computer "B" 192.168.1.130 Subnet Mask: 255.255.255.128

Router LAN: 192.168.1.1   Subnet Mask: 255.255.255.128
Router WAN: 205.160.3.222 Subnet Mask: 255.255.255.240

Source	Destination	Next Hop	Result
192.168.1.101	192.168.1.130	192.168.1.130	Single hop

192.168.1.130	192.168.1.101	192.168.1.1	Packet dropped in router
192.168.1.101	192.168.0.1	192.168.1.1	Packet dropped in router
192.168.1.101	192.168.1.102	192.168.1.102	Packet put on the wire

In the first case, Computer "A" sees the address of Computer "B" as inside its own network and sends the packet directly to Computer "B".

In the second case, Computer "B" sees the address of Computer "A" as outside its own network and sends the packet to the router. The router doesn't have an interface configured that will accept this address as a destination and the packet is dropped.

In the third case, Computer "A" sees the address 192.168.0.1 as outside its own network and sends the packet to the router.   The router doesn't have an interface configured that will accept this address as a destination and the packet is dropped.

In the fourth case, Computer "A" sees the address of 192.168.1.102 as inside its own network and sends the packet directly to that address. If the subnet mask of Computer "A" is set in error and the intent was for it to go to the router then this packet might be lost.

The fourth case shows how a group of computers could communicate on a LAN without involving the router and be somewhat isolated from other computers on the same physical LAN by the choice of subnet mask on the router.

Example 3: The router is on a network that's a superset of any of the computers and the router:

Computer "A" 192.168.1.101 Subnet Mask: 255.255.255.128

Computer "B" 192.168.1.130 Subnet Mask: 255.255.255.128

Computer "C" 192.168.0.1   Subnet Mask: 255.255.255.0

(Computers "A" and "B" are on different subnets.

Router LAN: 192.168.1.1   Subnet Mask: 255.255.0.0
Router WAN: 205.160.3.222 Subnet Mask: 255.255.255.240

Source	Destination	Next Hop	Result
192.168.1.101	192.168.1.130	192.168.1.1	
192.168.1.101	192.168.1.130	192.168.1.130	Double hop
192.168.1.130	192.168.1.101	192.168.1.1	
192.168.1.130	192.168.1.101	192.168.1.101	Double hop

| 192.168.1.101 | 192.168.0.1 | 192.168.1.1 | |
| 192.168.1.101 | 192.168.0.1 | 192.168.0.1 | Double hop |

In the first case, Computer "A" sees the address of Computer "B" as outside its own network and sends the packet to the router. The router sees the address of Computer "B" as inside its own network and puts the packet back out on the LAN, addressed for Computer "B".

In the second case, Computer "B" sees the address of Computer "A" as outside its own network and sends the packet to the router. The router sees the address of Computer "A" as inside its own network and puts the packet back out on the LAN, addressed for Computer "A".

In the third case, Computer "A" sees the address 192.168.0.1 as outside its own network and sends the packet to the router.   The router sees the address of Computer "C" as inside its own network and puts the packet back out on the LAN, addressed for Computer "C".

Conclusions

Either packets go out directly "on the wire" or to the router. No computer will put packets out "on the wire" unless the destination address is within that computer's own network range as defined by its own address and its subnet mask.

If a packet is "on the wire" then it will reach its destination if such a destination exists.

If a packet goes to the router then:

- If the router sees that the packet is on its LAN network (as defined by the router's own LAN subnet mask), then it will put the packet back out on the LAN.

- If the router sees that the packet is not on its LAN network (and assuming that other rules allow it), it will put the packet out on the WAN.

This means that subnetting doesn't necessarily yield separation between computers. There are two simple ways that a computer can be reached from a computer on a different subnet:

1) If the originating computer is on a network that includes the destination computer then it doesn't matter what the subnet of the destination computer is. And, it's only the destination computer that "knows" what its subnet is. Accordingly, this condition is completely out of the control of the destination computer. The originating computer can (and will) send packets to the destination computer.

2) If there's a router in the picture then if the originating computer is on a network that is a subset of the LAN network of the router, the router will redirect packets back to the LAN that are within the larger router network.

There are practical implications of this:

One can set the subnet mask of a computer so that it's on a very small network compared to the other computers on a LAN.
- all packets destined for this computer will arrive just fine even if the source computers are in a larger network.
- return packets from this computer will be sent to its gateway / router and presumably back out on the LAN.

One can set the subnet mask of a computer so that it's on a very large network compared to the other computers on a LAN.
  - any packets destined for computers on this larger network, but are actually on another LAN, will be lost because they aren't sent to the router.
  -