Home Networking, Routers and IP Addresses

by Andy Pepperdine

Introduction

This paper is about the way IP addresses are interpreted, and how a home network uses them as well as the wider Internet.

It will restrict itself entirely to IPv4, since the next generation of network addressing (IPv6) is implemented properly in the UK by less than a handful of ISPs, and there are almost no routers that support IPv6 for the home yet. When that situation changes, we can re-visit IP addressing and networks. Suffice it to say that when it does become commonplace, the Linux systems being distributed now have all the support in them ready.

What is an IP address?

When a message is sent from one machine on a network to another, it must have some means of addressing the message so it goes to the right place – in the same way as when you put an address on a letter, the postman knows where to take it. This address is called the IP (Internet Protocol) address and consists of a 32-bit number conventionally written as four decimal numbers separated by full stops. Each number is an 8-bit value in the range [0-255].

In addition, it can be interpreted as the number of a particular host on a specific sub-network. The left hand part of the number is the identification of the network, and the right side is the host identification. How many bits are to be used to identify the subnetwork is defined by the network mask.

For example, if you look at the connection information on your PC, you may see something like this:

IP address: 192.168.0.8
Subnet mask: 255.255.255.0

This means that 24 bits (three 8-bit values) are being used to define the subnetwork. Whenever any router sees this address, it knows which network to send it to (192.168.0...), and which host on that network (8). If you like, it knows which street it is on, and then, on that street, which house. The address is sometimes written as 192.168.0.8/24 which is a more compact way of showing both the network and host IDs.

[On Linux machines, to see this information, click on the connection icon, probably in a status bar. Whether you left click or right click depends on the window manager you are using.]

MAC address (Media Access Control address)

To be more precise, the IP address is not the address of a particular machine, but the address of a specific hardware connection on that machine. Typically if you connect via wireless you will probably see a different IP address from when you connect via cable. There is no reason why a machine cannot be connected to two different networks through these different connectors, and so they will be given different addresses.

A network connection is associated with the specific MAC address of the hardware that connects. So a wireless connection and a cable connection use different hardware components and so will use different MAC addresses, too.

For example, the IP address given above is associated with the MAC address: AC:81:12:16:8B:5F and is the wireless connection for my laptop. MAC addresses should be unique for all pieces of equipment and is assigned to it when is made, although some manufacturers may allow them to be changed after sale.

If I connect the laptop via a cable instead and look at the connection information, I might see:

IP address: 192.168.0.2
Subnet mask: 255.255.255.0
MAC address: F0:DE:F1:2E:45:5E

which is the information associated with the ethernet connector on the laptop.

More about IP addresses

The IP address you see on that connection is the address within the local network. What about the wide internet world?

There are several sites that will tell you what your IP address is. For example, if you go to https://www.whatismyip.com/ you may see it reports something like: 91.85.34.83. Why is it not the same as that reported by the connection information locally?

The answer is that you have connected to the wider network through a router. The router has the task of bridging between your local network (with an address in the range 192.168.0.0/24) and the wider world.

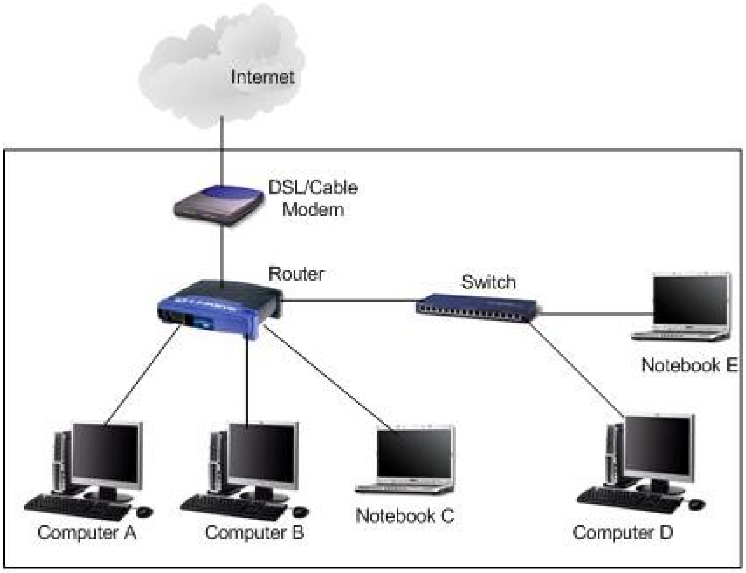
In order for this to work, the complete range of addresses have been divided up by agreed standard, and some of them are restricted to particular uses. You can see which addresses have been reserved for special uses here: https://en.wikipedia.org/wiki/Reserved_IP_addresses

One of these is the range 192.168.0.0/16, which is reserved for local private networks. This explains why when you look at your network information in your home, you may see the same IP address as someone else in their home. You are both connected to different local networks. To the outside world, however, your routers have different addresses.

Where do the IP addresses come from?

A typical small home network will look like this the digram below. In practice, the connections to the router may be via cable, or wireless, it makes no difference to this discussion. There may also be other devices on the network, like printers. All of them will see their IP addresses in the same network range (e.g. 192.168.0.0/24).

So far as the hardware is concerned, these days, the DSL modem is almost certainly contained inside the router itself, so there is only one box and not the two as in the picture.



When you switch on your PC, laptop, etc. it has no idea which network it is attached to, nor what its identifier is. All it does know is the MAC address, since that is part of the hardware it has. So the first thing it does is to send out a message to everyone it can asking for some help: “Is there anyone out there can tell me where I am, please?” Home routers, these days, will support a protocol known as DHCP (Dynamic Host Configuration Protocol), which means that they take it upon themselves to administer the network they can see on the home side of their operation. They will respond to the plea for help, and answer with information giving the machine its network and host IDs, i.e. its full IP address – on its local network.

It is also important that only one device on a network can assign addresses, or clashes could occur.

The external IP address

The router, however, also sees the wider world. How does it get its address?

Essentially in the same was as your PC. When it is switched on, it send out a plea for information about where it is, but this time, only on the outbound side of its connections, that is to the ISP (Internet Service Provide) (e.g. Virgin, TalkTalk, BT, etc.) The ISP then responds with a suitable external IP address selected from the set of addresses which have been allocated to that ISP.

The hardware at your ISP is controlling its subnetwork in the same way that your router is controlling your local network.

Your router is effectively acting as a bridge between your local network and the wider Internet.

One other address

There is one other address that you may see, and that is the special one 127.0.0.1. This is by far the most common one allocated in the subnetwork 127.0.0.0/24, and these address are reserved never to be routed outside a machine. They are used to act as test addresses for diagnostics, and target addresses for failed packets and other errors. In effect, it is a “loopback” which routes a message back into the originating machine without ever hitting any hardware to transfer it elsewhere. The address 127.0.0.1 is sometimes known as the “home” address, because it always refers to itself.

Routing

How does the postman work? How does each router in the network know where to send a message it receives?

There are a set of tables which define what a piece of equipment, whether it be a switch, router, o your PC, will do with a message that arrives. The device will consult the address given on the front of the message, and see if it is to be handled locally (e.g. it’s a reply to a message you sent out), forwarded to somewhere else (e.g. a router sending a message from you to your mail server), rejected with an error response to the sender (e.g. the forward link has broken temporarily), or dropped on the floor and forgotten (e.g. a broadcast message that is none of your business).

These tables are known as iptables in Linux machines, and change over time.

If you have more than one person on your home network all browsing on the Internet, they have their own IP addresses on the local network, but so far as the outside world is concerned, they all come from the IP address assigned by the ISP to your router. The router must keep track of where a message came from when forwarding it to the ISP, so that when it receives a reply, it knows which message has been replied to and forwards the reply to the right machine on the local network.

Further information

You may think that in a local network with the address 192.168.0.0/24, you will have 256 devices possible. In fact, that is not the case. There are two addresses that are special and cannot be used for a device. One has the host ID all zeros, and that refers to the network itself, and the other where the host ID is all ones, and that is for broadcasting in the local network. If you are interested, details are here: http://www.tcpipguide.com/free/t_IPAddressesWithSpecialMeanings-2.htm

Details of how to manipulate the iptables were not covered, but here are two useful links if you are interested:
https://www.linode.com/wiki/index.php/Netfilter_IPTables_Mini_Howto
http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch14_:_Linux_Firewalls_Using_iptables