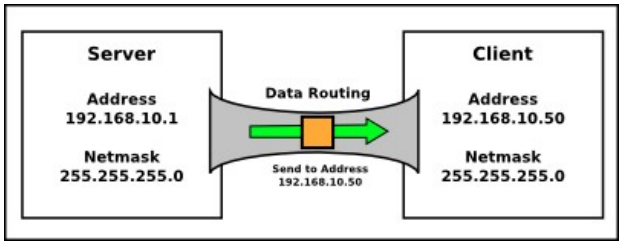
Networking Basics – Overview Sheet

Network Interface

A network interface (NIC) is a hardware port which can be configured to talk on the network. This can be ethernet, wireless or some other networking infrastructure. A computer can have more than one network interface at the same time, allowing it to be on more than one network.

IP Addresses

In order to send a packet of information somewhere, each destination interface needs an internet protocol address (IP address). The IP address of an interface must be unique.
The address is a set of numbers split up into four 8bit integer numbers (octets) separated by dots (for IPv4) or six 16bit hexadecimal numbers (for Ipv6), for example:



IPv4 Example Address: 192.168.10.30
IPv6 Example Address: fe80:10:21b:38ff:fed6:8f6b

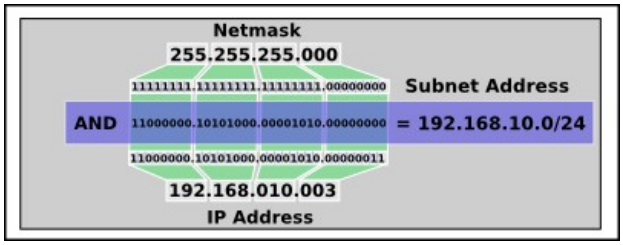
A static IP address is one that is configured on the machine that hosts the interface.

A dynamic IP-address address is usually generated using DHCP. Instead of having a pre-configured IP-address, the computer will send a broadcast message to the network asking to be assigned an IP-address by a central managing computer. The response should give the interface a free address from a range of addresses as well as other information such as DNS servers and internet router IP-address.

Subnet Masks

Computers can be connected to each other in hierarchical ways so each interface's IP Address is grouped into networks by their "subnet mask". This allows all interfaces which are members of that group to be able to talk to each other; but not to non-members, even when they're plugged into the same network infrastructure.

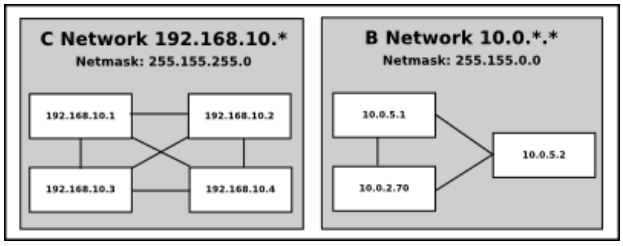
A subnet mask is a 'bit-wise' AND mask used on the IP address to generate the subnet address. The subnet address of the host's interface and the incoming address have to be the same for communications. The subnet address is marked with the number of bits that apply to it, for instance 192.168.10.0/24 has 24 of the full 32 bits as the subnet address and the remaining 8 bits for host addresses.



In IPv4, there are 3 standard classes of subnet : A, B, C.

Class C Subnet Example: 255.255.255.0 (notated by /24 in the subnet address)

Take the IP address 192.168.10.1 and its subnet mask is 255.255.255.0. If we apply the subnet mask then our subnet address is 192.168.10.0/24 and we can communicate with any computers with the same first 3 numbers but any remaining last number. For instance 192.168.10.2 or 192.168.10.3. On the other hand we would not be able to talk to 192.168.9.2 because the subnet mask would differ.

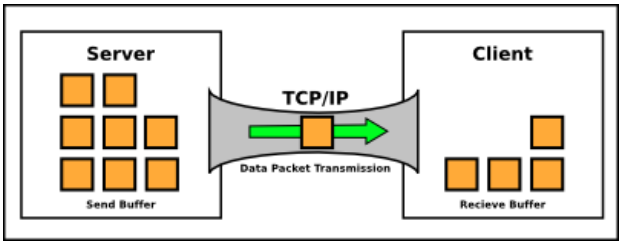


Class B Network Example: 255.255.0.0 (notated by /16) can contain 65 thousand addresses.
Class A Network Example: 255.0.0.0 (notated by /8) can contain 16 million addresses.

Addresses 0 and 255 are reserved for the "network" and "broadcast" functions. Sending information to a broadcast address will send packets to all computers in that network at once. So these are always unavailable.
For a computer to communicate across a network, the packets must go through a router (explained below).

Packets

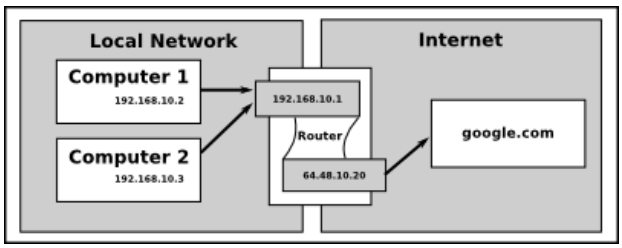
When computers are connected via some physical medium, they need to send information to each other that can be traced, routed and managed. Any given communication, such as a file, is split up into multiple packets. Each packet contains a section of information from the whole file and also contains a header which contains its routing information: where it's going to, what it was in response to and what data in the file it represents. This protocol is called IP (Internet Protocol).



For any given packet there can be a number of different transmission protocols. The standard transmission protocol is called TCP (Transmission Control Protocol) and an alternative protocol is UDP (User Datagram Protocol). Each with their own features and advantages. Normally, network traffic is done over TCP/IP, a combination of IP and TCP protocols. Each packet will either make it's way to the destination or possibly be dropped somewhere along the way. TCP packets that are dropped can be repeated if necessary but obviously this causes a loss in performance in the network. The main difference between TCP and UDP is that if a UDP packet is dropped, it is never repeated. This makes it perform better than TCP, but at the expense of the occasional packet. UDP is typically used for streamed content such as videos, music or voice over IP (VoIP) internet telephones.

Routing/Gateways

A computer can only send packets to interfaces in its own network. If a packet needs to get to another network, then we need a special computer/device called a router or gateway. This has two or more networks configured for two different networks and translates the packets from one to the other.



Consider the simplified example (see diagram) that our computer needs to see the google.com web page. First it will resolve google.com to an IP address, perhaps 64.48.10.21. Then it will send an ARP (address resolution protocol) request to its broadcast address. The ARP request will simply say “Who has 64.48.10.21?”. Because it's a router and because it has an interface in that network, the router will reply “I have 64.48.10.21” and our computer will start sending the request for the web page to the router. The router, in turn will be able to talk to 64.48.10.21 because it has an interface in that network, 64.48.10.20.

A router can't have an interface in every possible network, so there is a “default gateway”. The computer's default gateway is the router, while the router's default gateway might be the ISP's router. The ISP's router's default gateway might be a core router in the LINX, whose default gateway is a trans-atlantic hop to its American equivalent. By using default gateways, packets can hop from router to router – this is the core concept of the internet.

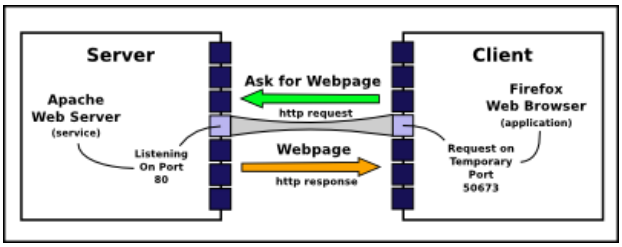
Domain Names

Typing in an IP address every time we wanted to get to a website or send an email would be difficult remembering them and keeping up with their changes. So we use human recognisable names that resolve to IP addresses called Domain Names and there are special servers which are used to record or route all the domain names for the network called Domain Name Servers (DNS servers). At the top level there is a controlling server (.) which documents the top level domain names (TLDs) for instance .com .org .uk and so on. These then point to other machines which are controlled by different people who have a list of sub domains under those top ones, for instance google.com. or co.uk. And those can then point to other servers which further sub domains such as `mail.google.com` until the human readable domain name is finally resolved to an IP address.

The Internet

The internet is simply a network of every public facing computer with its own IP address and the routers which connect them all together. Most of the computers are clients (personal computers or phones) and the rest are servers which provide various services such as E-Mail, web pages, internet relay chat or instant messaging. The internet is commonly confused with the world wide web (www) which is a single service of many running over the internet.

Services and Ports



At each computer there is a list of internal numbers (ports) which connect running programs with each other. Ports are opened and closed by programs as required. A service is a program which is always running and listening on given ports for requests, it then services these requests as required. For example, a web server is always listening on port 80 (by default) and when you type a URL into your web browser, the browser is making a connection to the web server you typed on that port.

Firewalls

There are two types of firewall, hardware and software. A hardware firewall is a special router which is able to intentionally drop or accept packets before they get to their destination service, based on a set of rules. The rules can be as simple as 'drop all packets on port 137' to complex chains of multiple accept/drop rules based on IP address destinations and sources. For example, a mail server might have a firewall protecting it which says “drop any traffic destined for this mail server that isn't running on port 25 (which is the port for SMTP mail traffic).

Software firewalls run on a computer as a service and prevent that computer's NIC from sending or receiving certain types of traffic, again based on a set of rules.

Firewalls are not a replacement for the security of disabling services which you don't use: they can only define precise rules about when a service is allowed to be used on the computer.

Network Hardware

Ethernet

Ethernet is the standard physical networking wiring. Using Cat6 cables and RJ45 connectors, it can go up to speeds of 1Gb/s. It's the most common network connector (see ports sheet). Ethernet has a maximum cable length of 90 metres.

Wireless (802.11)

WiFi networks are networks which use radio waves instead of ethernet cables. The computer will communicate using its WiFi NIC to a WiFi base station which is cabled to to the physical network. The physical network a base station is connected to is identifed by the stations SSID. Communication is secured using either WEP or WPA protocols.

Routers

A networking device dedicated to routing, and optionally firewalling, dns lookups and dhcp allocation. It's normally used to quickly get a local network onto the internet and doesn't always have to be a full blown personal computer with two network cards.

Switches

Switches are devices that allow many computers to be connected together. A switch has no concept of routing. It simply passes the traffic along its connected cables based on ARP requests. A switch will only connect two devices this way when they have shown a need to do so via ARP. This means packets to other computers won't get in the way and traffic isn't bouncing around the whole network.

Hubs

A hub is like a switch but without the ARP segregation. Bandwidth on a hub is shared between all computers on the network. If the network can only handle 100Mb/s and you have 10 computers, that means each computer will only get 10Mb/s. Packets can also “collide” as they are being sent through the network causing more packets to be rejected. It is not recommended to use hubs and instead switches should be used. Hubs are increasingly rare in today's markets due to these limitations and the relative cost of switches.

Modems

A modem is a device which converts analogue signals to digital and visa versa. They are used to transmit digital computer network packets over analogue phone lines. The old modems using the RJ11 connector had a maximum speed of 56k/s, where as newer modems used for A/DSL can go many times faster.

Networking Command Line Tools

- ifconfig – Address configuration and view.
- dhclient – a tool used for request DHCP IP addresses.
- iwconfig - a wireless (WiFi) configuration tool.
- iwlist – a tool to list all Wireless (WiFi) networks.
- ping – send an ICMP packet to the host to see if it is available (“up”, or “alive”).
- arp – tool to view a computer's ARP cache.
- nslookup / whois / host / dig – Name Server lookup tools.
- traceroute / mtr – tools to show how networks are connected.
- Iptables / ufw – manage the internal linux firewall.
- tcpdump – realtime view of the traffic on a NIC.
- netsend – for sending a file to another computer over the network.