Networks

# Layers

Most networks are built up from the seven layer OSI model of networking:

Layer 1

Layer 1 is the phyical layer of a network, built up of cables and electrical signals.

Layer 2

Layer 2 is the datalink layer and provides the means for delivering data frames between nodes (devices) on the same level of network (local network). Messages are routed by the layer 2 address for each device which is defined by the devices Media Access Code (MAC) address.

Layer 3

Layer 3 is the network layer and provides the means for transfering variable length network packets, via one or more networks. Layer 3 packets are routed by Internet Protocol (IP) address, which is an address given to each device on the network for the purpose of identificaion and location. In an isolated network each IP address will be unique to allow for accurate routing.

# Components

Hubs

Network hubs are dumb relays for network messages. When a message is received on a phyical port, it is relayed to all other connected ports on the hub. Since messages are not relayed directly to correct recipient, this causes many collisions, slowing down network speed and reducing privacy.

Switches

Switches are similar to hubs however they have Content Addressable Memory (CAM) in which they can store a table relating the devices on the network to which port they are connected to on the switch. This allows switches to direct messages receieved from a device to it specific reciepent on the network.

Network switches operate on layer 2, transmitting only frames defined by their MAC address.

The CAM table is populated by source addresses, since these are definitive.

# Utilities

Ping

Ping is a network utility used to test the reachability of a host on an IP network. Ping operates by sening Internet Controler Message Protocol (ICMP) echo request packets to the target host, then waiting for an ICMP echo reply. Pinging a host can provide various details about the network connection, such as:

* round trip time (ping time)
* packet loss
* errors
* standard deviation of ping time
* reponse times

Most opertating systems have a ping ultilty built into their command line. For example, the linux CLI for ping is:

ping -c <number-of-probes> <host-address>

# Routers

General

A router's, also called a gateway, job is to connect networks with different ip address groups.

ARP Requests

When newly connecting to a local network, the local machine may only know the ip address of a host it is trying to connect to, yet layer 2 switches can only route using MAC addresses. Therefore, the local machine must discover the MAC address for the desired host using an Address Resolution Protocol (**ARP**) request. The ARP message is simply a message sent to the switch with a MAC address of FFFF:FFFF:FFFF and the host IP address, which is then broadcasted to all other devices connected to the switch. If a connected device matches the IP address of the ARP message, it will reply to the swtich, returning the MAC address to the local machine, allowing for future frames to be sent to the correct address.

However, when the IP address is not within the range of the local network, the ARP request from the local machine will be sent to the network router (gateway) IP address. The router replies with its own MAC address, and the local machine will start sending its data frames to the router. The new data frames will be transmitted by the switch over layer 2 to the router, but they will also the layer 3 address details which the router can use to forward the message on to the external network. If the router does not already know the MAC address for the IP address for which the received packets is addressed to, it will also send out ARP requests to find it in its local network.

In modern internet networks there are many routers and therefore networks chained together. So, sending packets to IP addresses external to the local network, will often result in a chain of ARP requests being sent across the internet. While this first connection may be slow, once the MAC to IP address relation is processed, it is saved in the router cache, making the process of sending future packets very fast.

NAT

NAT - Network Address Translation is the process of remapping one IP address space to another by modifying the network address information in the IP header of the packet. In routing one public IP address is exposed for the network, and the router perform NAT on each packet to convert its local IP to public IP and vice versa. To manage multiple connections, the router opens up a new external port for every connection it is requested to route and stores this link to the local connection in the translation table. The server will then respond to the request on the new port and the router can link it to a local machine in the translation table, then perform NAT on the packet and forward it on.