Ethernet LAN Switching Cheat Sheet

by xavierjackson6940 via cheatography.com/184463/cs/38482/

What is a LAN?

A LAN stands for local area network. These are devices that are confined to a limited area. For example, a SOHO, or an office department etc. A LAN in its basic form can just be two computers plugged together. However, in most enterprise or office's, these LAN's are created by something called a switch. End-hosts are typically plugged into switches. These end hosts could be PC's or servers.

What is a Switch?

A switch is a Layer 2 device. (Based on OSI Model) Switches typically have a lot of ports on them, unlike routers which typically do not have many interfaces on them. This makes switches great to plug into end hosts. The function of a switch is to forward traffic WITHIN LAN's. A router on the other hand will forward traffic BETWEEN LAN's.

Ethernet Switching

Ethernet Switching is when a switch forwards traffic to the correct end host within a LAN based upon MAC addresses.
Ethernet itself is a Layer 2 protocol in the OSI Model, also known as the Data Link Layer.
The PDU (Protocol Data Unit) at Layer 2 is known as a Frame. Thus Ethernet Frames are what are sent when sending traffic within LAN's.

Ethernet Frames

The Minimum size for an Ethernet Frame is 64 Bytes. 1 Byte = 8 Bits, so 64 Bytes = 512.
An Ethernet Frame will include an Ethernet header, a packet (encapsulated from Layer 3) and a trailer. This would make the minimum size if everything included to 64 bytes.
Minimum PAYLOAD size is 46. If <46 padding bytes are added to the frame to add upto 46. (Below explains why)

Ethernet Header: (Without 802.1Q)

The Ethernet Header is comprised of 4 main sections (There are optional ones, like VLAN 802.1q which isnt explained here). These are Preamble & SFD, Destination & Source, Type, and CRC.

Preamble & SFD: The preamble is 7 bytes long. (56 bits) Its main purpose is to allow devices to sync their reciever clocks. The SFD is 1 byte long (8 bits) and is used to mark the end of the rest of the frame. The preamble & SFD are usually not considered part of the ethernet frame. So, without this, the ethernet payload is 64-18 (Preamble +SFD) = 46. So, if it is <46 padding is added.

Destination & Source: These sections indicate the source & destination of where the frame is headed too. Inside these it includes MAC addresses, which are 6 bytes in length. So it will be 6 bytes for both the Destination & the Source. In ethernet frames destination comes before source, because of something called ARP.

Type/Length: 2 Bytes in Length. (16 Bits) A value of 1500 or less indicates the length of the encapsulated packet. A value of 1536 or higher indicates the TYPE of encapsulated packet. For example IPv4 = 2048, IPv6 = 34,525.

MAC Addresses

MAC Address stands for Media Access control.
Its 6 bytes in Length. Its usually assigned/-burnt into the device when it is manufact-ured. (Usually to the NIC).
The first 3 bytes are the OUI (Organizatio-nally Unique Identifier, which is assigned to the company making the network device.
The Last 3 bytes are unique to the device itself.
It is also written is hexadecimal. (Not included here)

MAC Address Table

A Switch will have a MAC address table. This is what it uses to record the MAC address of the device it receives a frame from.
It will note the MAC address of the device & the interface.
This is known as Dynamically Learned MAC address.
Statically Learnt is when the MAC address is manually configured to the switch.

Unicast/Unknown Unicast

A unicast frame is one that is intended for a single target. If this end host is known, then its all good and traffic will end up where it should.
However, if the switch does not know the MAC address of the end host, then it will flood the frame out of all its interfaces besides the interface it received it on. This is so it can find out what end host the frame is for. This is known as an Unknown Unicast Frame.

Unicast/Unknown Unicast (cont)

Once a flood happens, all devices that receieve the frame will de-encapsulate it upto the data link layer to see if its MAC address matches the destination MAC Address of the frame. If it does, then it sends a unicast reply back to the switch. If not, it drops the packet.

Known Unicast/Forwarding

If a Switch has already sent traffic (or has statically assigned MAC addresses) then there is no need to send out an Unknown unicast if it has that devices MAC address already.
It will just forward the frame. This is Known Unicast Frame.
So essentially, Unknown Unicast = flooding, known = Unicast

ARP

ARP stands for address resolution protocol.
ARP is used to discover the layer 2 address (MAC) of a known layer 3 address. (IP address)
Consists of an ARP Request & ARP Reply.
ARP Request = Broadcast Ethernet frame, sent to all hosts on the network.
ARP Reply = Unicast. Sent to only one host. (The host that sent the request.)
All F's is a broadcast MAC Address.
Switches will have an ARP Table. We can also see the ARP table in windows via 'ARP - a', or in Cisco IOS via 'Show ARP'

Ping

Ping is a network tool that is used to test reachability. So if an end host is reachable.
Measures the round trip time.
Ping uses ICMP Echo Request & ICP Echo Reply.
ICMP Echo Request needs the MAC address of the destination host before an echo request can be sent.
Thus we need ARP first.
Command to use ping is: 'ping (IP Address)'
Usually when pinging the first packet will drop due to ARP, but the rest should work if everything is configured correctly. If not, then all packets will drop.