data moves through networks based upon 3 tables:

- MAC address table, mapping of switch port to MAC address

- ARP table/cache, mapping of IP address to MAC address

- routing table, mapping of IP network to interface or IP to next router (all routes to networks that the router knows about)

A computer screen shot of a cloud computing diagram

AI-generated content may be incorrect.

This example has 3 routers and 3 hosts, each host exists within a network, and each device has its own IP address within its network. Each of the wires are connected to NIC’s so each device has a NIC meaning they have MAC addresses. The switch does not require a MAC address or IP address because data is not being sent to it nor is data being sent from it, we are only sending traffic through the switch. The switch only has 2 switch ports.

The switch only needs a MAC address table which maps switch ports to device MAC addresses. All 3 routers have both an ARP table and a routing table. Each host also has an ARP table and a routing table. Both ARP tables and MAC address tables will be populated as traffic goes through the network, while the routing tables will be populated beforehand. This is because if a router receives a packet with an unknown destination IP address, the packet will be dropped.

Each host needs only one route in the routing table and that is the default route (0.0.0.0 /0) which points towards its default gateway (its local routers IP address).

Each router will have 2 routes, one of them being DC which is the network that they are attached to, then each router will have a default route that is connected to the internet. Usually that default route would point to another router on the internet, but for simplicity we will point it to the internet.

Host A wants to send data to host B, the first thing that will happen is that a layer 3 header will be formed to account for end-to-end delivery. SRC 11.8.8.11 DST 22.7.7.22 (SRC host A IP address DST host D IP address). Now host A will compare the DST IP address to its own IP address and subnet mask to determine that the DST IP address is on a foreign network. Therefore, the packet needs to be sent to host A’s default gateway which is found in host A’s routing table. Host A’s ARP table is empty which means that host A does not know router 1’s MAC address meaning it cannot make the layer 2 header to deliver the packet to the router.

Current layer 2 header:

Data:

Layer 2 header:

SRC a1a1

DST ????

Host A must do ARP to figure out R1’s MAC address. The ARP request will have a layer 2 header, SRC a1a1 DST ffff. This is the broadcast MAC address which means the ARP request will be sent to everyone on the network. When host A puts it on the wire, it will arrive at the switch. Whenever a switch receives data, it will learn to MAP the senders MAC address to port mapping. In this case the senders SRC MAC address is a1a1 and it went through the switch from port 4. So, the MAC address table will be updated with the entry: 4--->a1a1. Then the switch will look at the DST MAC address and notice that it is the broadcast MAC address so it will do the flooding action, and it will send the frame to all ports. Router 1 then receives the ARP request and learns that the 11.8.8.11 IP address is mapped to the a1a1 MAC address and puts this entry in its (R1) ARP table, then R1 and sends back an ARP response with the SRC MAC address of its own so eee1 and a DST MAC address of the ARP requests sender which is host A so a1a1. ARP response: SRC eee1 DST a1a1. This is a unicast. When this ARP response gets put on the wire, the switch receives it and since the switch received something on port 5, it learns that the e1e1 MAC address is connected to port 5. So, the entry 5--->a1a1 is put on the MAC address table.

Then the switch will look at the DST MAC address and look in its MAC address table and see that the DST MAC address is on port 4, so it will send the frame to port 4. Host A will then receive the frame, host A will learn the MAC address associated with the 11.8.8.1 (R1 IP address) IP address, and it will add that entry (11.8.8.1--->eee1) to its ARP table. Now host A can create the layer 2 header to send the frame to the router. The layer 2 header: SRC a1a1 DST eee1.

Data:

Layer 2 header:

SRC a1a1

DST eee1

Layer 3 header:

SRC 11.8.8.11

DST 22.7.7.22

Now host A can do its first hop which is from host A to R1. Host A will send the frame to the switch, the switch will check the SRC MAC address and see if it can learn a new MAC address to port mapping but, in this case, it already knows it so the switch checks the DST MAC address and sees that eee1s port mapping is to be sent through to port 5. R1 will receive the frame and discard the layer 2 header.

Updated image:

A computer screen shot of a cloud computing diagram

AI-generated content may be incorrect.

R1 will now check it’s the data’s DST IP address and notice that it matches the default route, this means that R1 will have to send the packet to the internet. Normally this route would point to another router because the internet is just a bunch of routers connected to each other; this packet will be passed from router to router across the internet until it gets to R2. Then R2 will check its routing table to figure out what to do with the packet, and it can see in its routing table that its DST IP address matches the DC route. R2 is unable to form a layer 2 header because its ARP table is currently empty. So R2 will have to do ARP, the ARP request: SRC eee2 DST ffff. The frame will be put onto the wire and host B will receive it, then host B will learn that the MAC address eee2 matches the IP address 27.7.7.1. meaning that host B will learn the IP to MAC mapping of the sender of the ARP request so that entry can be inserted into host B’s ARP table.

Then host B will generate a response: SRC b2b2 DST eee2. R2 will receive the ARP response and learn that the MAC address of the packets DST IP address. So R2’s ARP table will have the entry: 27.2.2.22--->b2b2. Now R2 can create the layer 2 header for the packet. The layer 2 header: SRC eee2 DST b2b2. Host B then receives the frame, then it will discard the MAC address, then it will discard the IP address and process the data. Usually in the network 27.7.7.x /24 network, the host wouldn’t be connected directly to the router, it’d be connected to a switch or even multiple switches, but this is just for simplicity as we went through the process of how it would work with a switch in the 11.8.8.x /24 network.

Now host B can generate a response back to host A. the data will have a layer 3 header with the SRC IP address of its own and the DST IP address of host A: SRC 27.7.7.22 DST 11.8.8.11.

Updated image:

A computer screen shot of a cloud computing diagram

AI-generated content may be incorrect.

Since this packet is being sent to a foreign network, the packets first hop must be to host B’s router. At this point in time, host B already has the ARP mapping for R2 (it has R2’s MAC address) meaning it can create the layer 2 header:

Data:

Layer 2 header:

SRC b2b2

DST eee2

Layer 3 header:

SRC 22.7.7.22

DST 11.8.8.11

R2 will then receive the frame, then it will strip off the layer 2 header. R2 will check the DST IP address then check its (R2) routing table and see that the DST IP address matches the default route which points to the internet. The packet will be handed from router to router across the internet and eventually it will arrive at R1. R1 will then look at its own routing table and determine that the DST IP address matches the DC route so R1 knows that this DST IP address is the final hop for this packet. R1 also knows the MAC address for the DST IP address by looking at its (R1) ARP table. So now R1 can create a layer 2 header to take the packet across the final hop to host A. The layer 2 header: SRC eee1 DST a1a1. R1 will put the packet onto the wire. The switch will receive it, and the switch will try to map the receiving switch port which is 5 to the SRC MAC address of the frame but it already has that mapping so nothing happens. Then the switch will look at the DST MAC address and realise that it has that mapping to port 4 so it will forward the frame to port 4 where the frame will be received by host A. host A will then receive the frame, then host A will strip off the layer 2 header, then it will strip off the layer 3 header, then it will process the data.

Now host A will send some data to host C, picture updated here:

A computer screen shot of a cloud computing diagram

AI-generated content may be incorrect.

The first thing that happens is that a layer 3 header is created, the SRC IP address is host A’s IP address and the DST IP address is host C’s IP address. Since host A knows that this packet will be sent to a foreign network, it will look at the default route in its routing table to determine the default gateway IP address which is R1. Since host A has the ARP mapping for its default gateways IP address, it can create the layer 2 header which will take the packet to R1. The layer 2 header: SRC a1a1 DST eee1.

NEXT PAGE

Data:

Layer 2 header:

SRC a1a1

DST eee1

Layer 3 header:

SRC 11.8.8.11

DST 33.6.6.33

Host A will put the frame onto the wire, and the switch will receive it, since the switch already knows all the mappings for its network there isn’t any updated entries. The switch will check the DST MAC address and determine that the frame is meant to go through port 5. Then R1 will receive the frame, then R1 will strip off the layer 2 header. R1 will look at its routing table and determine that the DST IP address matches the default route which points to the internet. R1 will send this packet across the internet where it will end up on R3. R3 will look at the DST IP address and realise that it matches the DC route in its (R3) routing table. R3 knows that it needs to create a layer 2 header which matches the DST MAC address associated with the DST IP address. But at this point, R3 does not know the ARP mapping of the DST IP address so it can’t make the layer 2 header. R3 will do an ARP request, SRC eee3 DST ffff. This broadcast DST MAC address will ensure that everyone on the network receives the ARP request. When host C receives the ARP request, host C learns the ARP mapping (MAC address) of R3. So, host C’s ARP table will include the entry 33.6.6.1-->eee3. Host C will send an ARP response: SRC c3c3 DST eee3. Then R3 will receive the ARP response and learn that the MAC address of the DST IP address it was looking for was c3c3 so R3’s ARP mapping will be updated with the entry: 33.6.6.33--->c3c3. Now R3 can make the layer 2 header: SRC eee3 DST c4c4. R3 will put the frame onto the wire and host C will receive it, host C will strip off the layer 2 header, then host C will strip off the layer 3 header, then host C will process the data.

Now host C will send a response back to host A, updated image:

A computer screen shot of a cloud computing diagram

AI-generated content may be incorrect.

Host C will create a layer 3 header with the SRC IP address as itself (33.6.6.33) and the DST IP address of host A (11.8.8.11). Host C knows that it’s trying to speak to something on a foreign network. So, host C checks its routing table and knows that it must deliver the packet to the default route which points to the default gateway which is R3. Host C has the ARP mapping of the default gateway in its ARP table so it can create the layer 2 header: SRC c3c3 DST eee3.

Data:

Layer 2 header:

SRC c3c3

DST eee3

Layer 3 header:

SRC 33.6.6.33

DST 11.8.8.11

R3 will then receive the data and R3 will strip off the layer 2 header. Then R3 will look at its routing table to determine where to take the packet. R3 can see that the packet is destined to the default route which points to the internet. So R3 will send the packet across the internet, and it will arrive to R1. R1 will look at its routing table and confirm that the DST IP address matches the DC route. R1 knows that this is the final hop to deliver the packet. R1 checks its ARP table, and it knows the ARP mapping of the DST IP address so it can create the layer 2 header: SRC eee1 DST a1a1. The frame will get put on the wire where the switch receives it. The switch can’t make any new entries onto its MAC address table, but it determines the DST MAC address matches port 4 so it forwards the packet to port 4. Then host A will receive the packet, host A will strip off the layer 2 header, host A will strip off the layer 3 header, host A will process the data.

A diagram of a cloud computing system

AI-generated content may be incorrect.

To explain what happens when you type [www.google.com](http://www.google.com), imagine when host A sending data to host B was a DNS request, then the DNS server responds back with the IP address to the website, then host A speaking to host C was a HTTP/HTTPS request, host A was requesting the website and the web server responded with the html page.