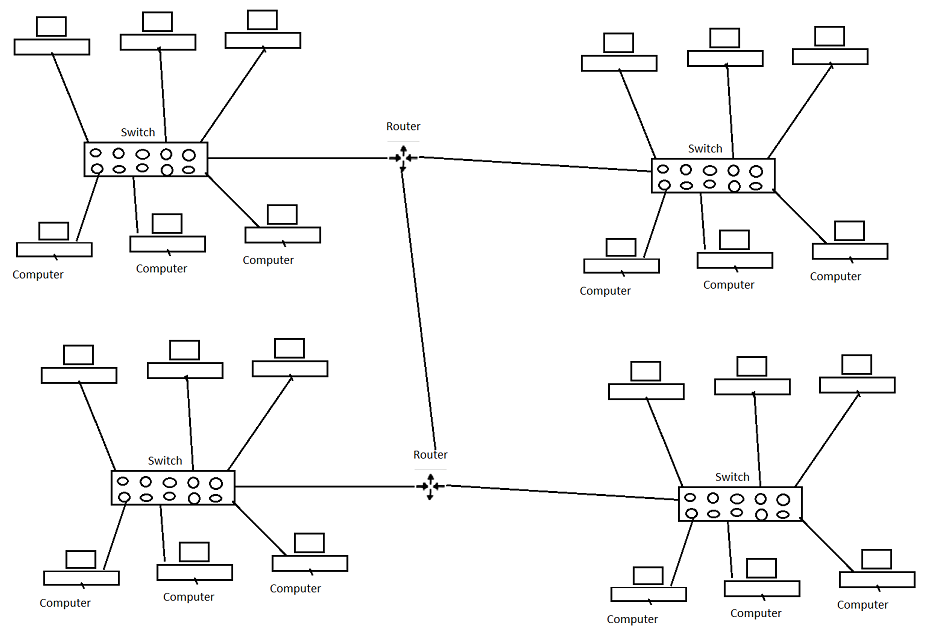
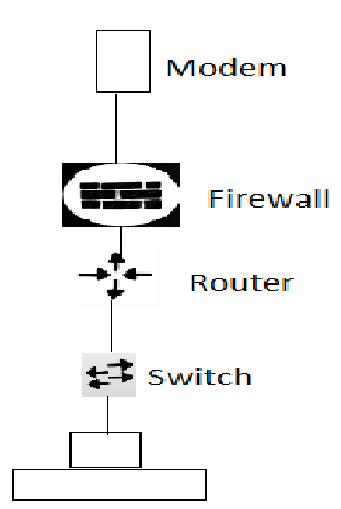
**Network**

Normally, computers are connected to switches. Every lan has to have a switch so that computers can communicate with each other via switch. Then we can connect our lan to another network via Router and etc. So this is the Internet the world’s largest network.

Switches are layer 2 devices.





WAP –wireless access point is used to broadcast the network over the air waves.

Before switches, people used hubs. But they are dump because it sends the information to every device that it is connected to. Hubs just repeat electrical signal.

A switch stores all the mac addresses of each computer connected to it in its CAM table.

CAM stands for content addresable memory. MAC-Media access control (layer 2 data link layer). Every single device has the mac address.

When a swtich receives information from a computer it becomes a frame. Then the receiver gets the message it becomes a packet because there is an ip address (layer 3) involved. In other words, we send frames (with source MAC address, which is used to populate CAM table, and destination MAC address) to switches and we send packets to routers.

Switches use destination mac addresses to make forwarding decisions.

**Routers**

Roters are layer 3 devices meaning that they can see 3 layers: Physical layer, data link layer (mac address), network layer (ip address).

The default gateway is the path used to pass information when the device doesn't know where the destination is. A default gateway makes it possible for devices in one network to communicate with devices in another network. If a computer, for example, requests a web page, the request goes through the default gateway before exiting the local network (LAN) to reach the internet.

**The default gateway is the ip address of our router.**



The ip address of the device is 192.168.31.55

Our device knows if the request is between the range of

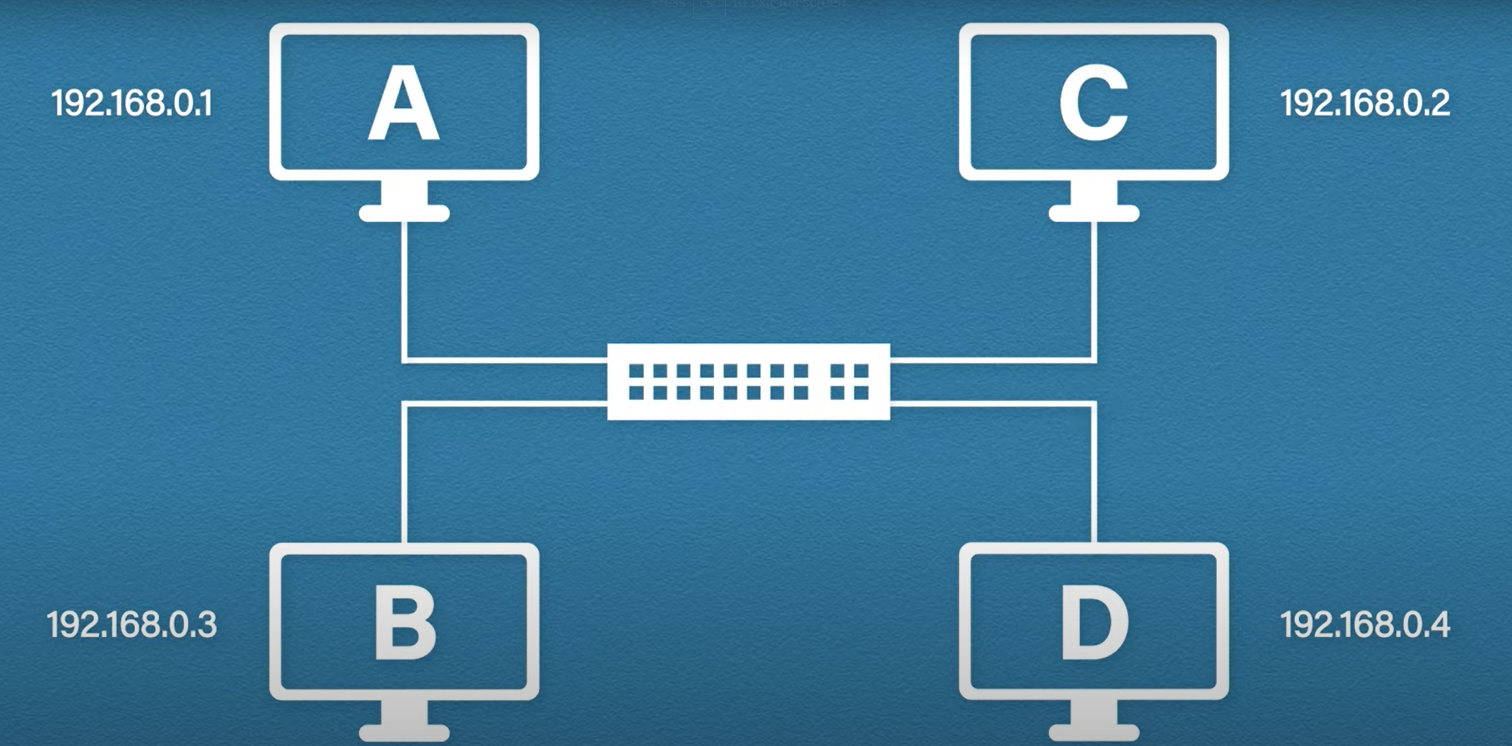
192.168.31.0 ---192.168.31.255 then it is in our network. Otherwise, it is in another network. And it will exit our LAN with the default gateway.

So when one of the devices exit the LAN it uses the default gateway. When they see unknown ip address they know that they have to exit their network.

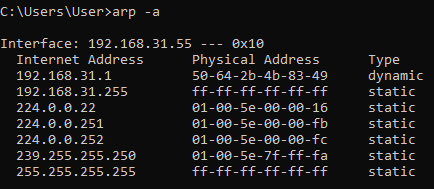
ARP – Address Resolution Protocol is used to discover mac addresses and map them to an ip address.

Let’s say that we have a network and 3 devices are connected A, B and C. Let’s say there is a new device D that just has been connected to the network. It will be given an ip address.

Now host A wants to communicate with host D. Since A only has the ip address of D it will have to first figure out the mac address of D. A will look at the ARP cache to see if D’s mac address is there. Since it is a new device A will have to send a broadcast message (asking everyone who is 192.168.0.4?). Then D responds and after this A stores the mac address of D in its ARP cache. Then they will be able to communicate because A knows the mac address of D.

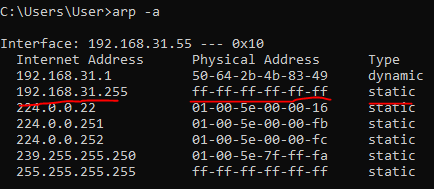


ARP cache 🡪



Dynamic types are created by arp itself when we make requests (the one that we just saw). But static ones are created manually and they are not deleted. In contrast, dynamic types get removed after sometime to make space.

So ARP is used to translate from 32 bits (ip address) into 48 bits (mac address).

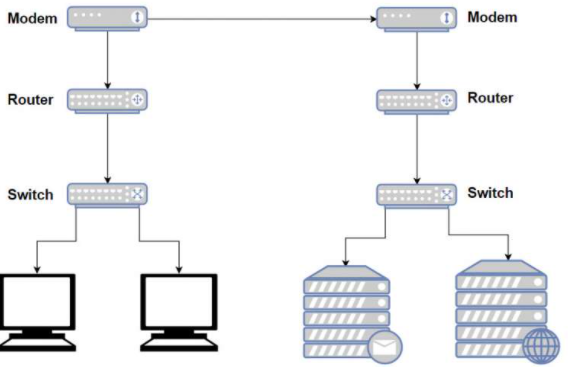


The first top static type is called direct broadcast address. We can know that it is a broadcast message from the physical address (FF-FF-FF-FF)

And also the Ip address is the last ip address in the network because of 255.

When we send a get request, let’s say for example we want to communicate with another server (facebook etc.), first what happens is our device will compare its ip address with the searched one to see if that ip address is in our network. Knowing that it is from outside of the network, it will have to go off our network. To do this, it will look at the ARP cache to find the default gateway ip address to get the mac address of our router. If it is not there then it will send a broadcast message to find our router. Then it will populate the arp cache table and after this our device will take the destination mac address (router’s) and go to it. When the router receives our request it will ses its mac addres as well as the ip address of the website (or server in this case).

So the entire process 🡪



If host A wants to communicate with host B then host A first looks at its ARP table to find the mac address of the host B. if it is not there then it sends a broadcast message. When our ARP populates host B’s mac address then it will be able to communicate with host B.

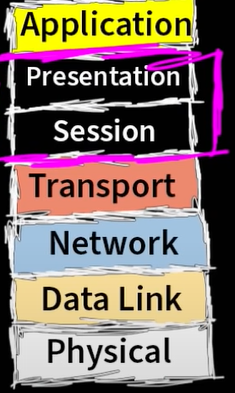
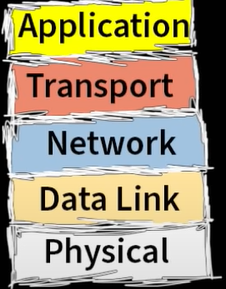
If we want to communicate with another server then we get off our network through the default gateway. The same process goes. host A first looks at its ARP table to find the mac address of our router. if it is not there then it sends a broadcast message. The gateway is the IP address of our router. After this host A sends a request through the default gateway.

Our computer needs the mac address of our router so that it is sent through the switch.

**TCP/Ip**

TCP/IP is just a list of guidelines, rules, standards on how diffrerent computers (Windows,MAc) can communicate. The functions are divided into layers.

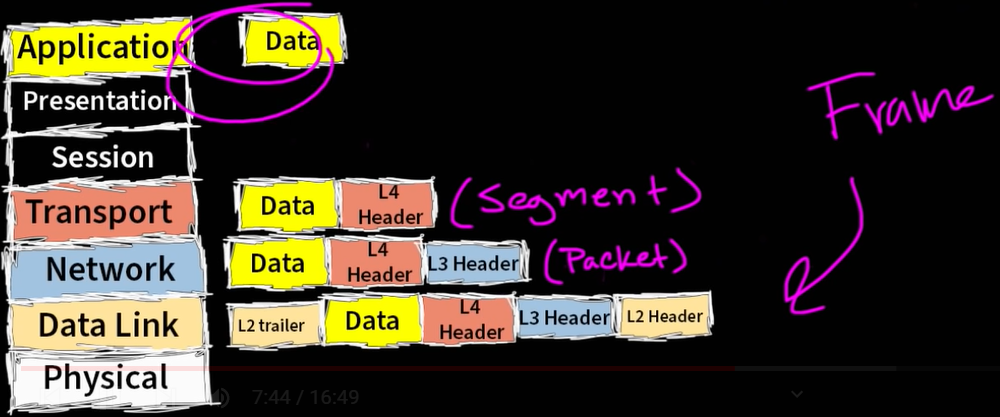
TCP/IP OSI(Open system’s interconnection)



TCP/IP and OCI networking models that define as to how we connect to our computers.

As it goes down to other layers from the layer 7, it gets encapsulated. 🡪 In layer 4 (transport) we have TCP and UDP.

And as devices receive our packages (all the layers) they will decapsulate our package. If it is a switch then it will only be able to see layer 2 and etc.



Presentation layer (layer 6) deals with the following tasks:

Data Format – file types such as .html, xml , jpg

Data encryption

Presentation layer (layer 6) deals with the sessioning. This tells if the whether the communication should continue or not.

All these layers (session and presention) are just one layer in TCP/IP model.