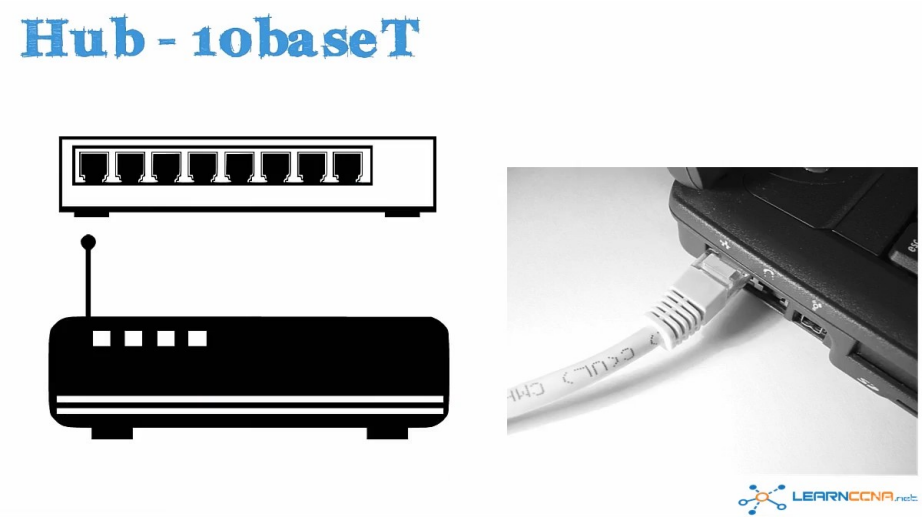
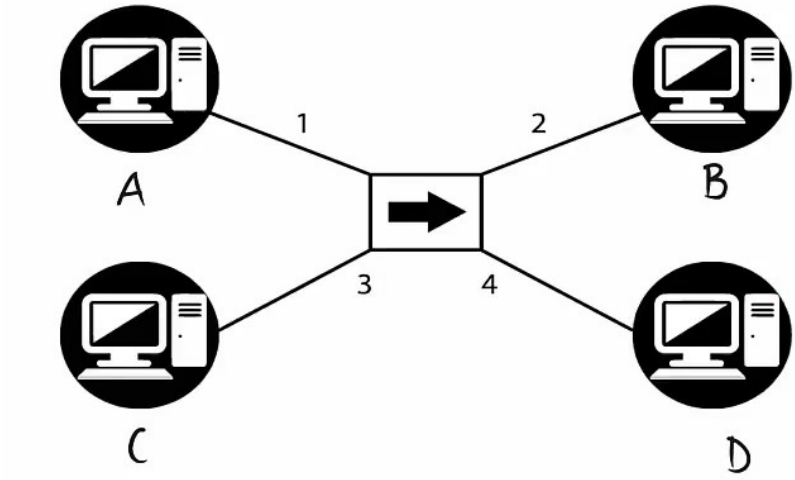
Network Devices

Hubs



Physical Layer Device - Layer 1 Device in the OSI model
Not intelligent, does not understand the frames going through it.
Essentially just a multiport repeater – will amplify the signal coming through it
Frames coming in one port, go out all other ports
Uses a CAT 5 Cable (w/ rj45 connector) to connect NIC on a laptop to a port on the Hub
Deprecated – replaced by switches
Wireless (WiFi operates in the same way as a hub)
Physical Toplogy of a Hub is called a STAR topology

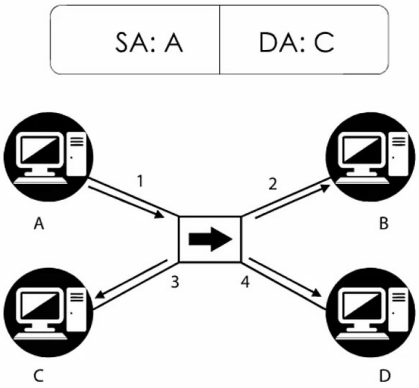
HUB example - -Star Topology



In a star topology, you have a central device which in this case is a hub and devices hanging off that central device, called spokes.
Each “Spoke” device is connected to the central device with its own cable, and all transmission or communications between devices are though the central device.
For a A to comm with C, the traffic flows though the hub through to C

There were some major advantages to using Hubs and Unshielded Twisted Pair as opposed to 10base2.
The first advantage is a cable break.
Should a cable between Device A and the hub break, the whole network does not go down, rather only device A is taken offline.
Advantage 2: You can extend to further distance easily. A device to the hub can only extend 100 meters, but by adding a second hub (multiport repeater), which repeats and amplifies the signal, you can add an additional 100 meters to the network per hub.

What does a hub do with received Traffic?



Source Mac Address: A on Device 1
Destination MAC Add: C on Device 3

1. **Device 1 Sends a frame to Device 3 and the frame first leaves 1 and arrives at the HUB**
2. **From the HUB, the frame is then sent out of all ports (except the receiving port)**
3. **Devices 2,3,4 receive the frame and read the destination MAC address (B,C,D), since the Destination MAC in the frame is for C (DA:C) Devices 2 (B) and 4 (D) will drop the frame**
4. **The NIC for device 3 (C) will see the frame is destined for itself and will then accept and process the frame (strip the Layer 2 Headers (SA: DA: mac addresses) and pass the frame to the higher layer protocols.**
5. **Assuming Device 1(A) sent a ping to Device 3(C) a return frame would be sent.**
6. **Device 3 sends a frame with a SA:C and a DA: A back to the hub.**
7. **The hub then sends this frame to all ports (except the receiving Port)**
8. **B and D drop the Frame and Device 1 (Mac: A) will then accept the frame, remove the layer 2 headers and process the higher layer protocols**

Hub
Physical topology is a star (Central devices and spoke devices)
Logical Topology is a Bus – All devices receive a frame (except the sender)

Very important to realize there is a difference between the physical and logical topologies of a network.
The way a network is physically cabled isn't necessarily the way the network is going to operate.

A hub is a <u>single collision domain</u> – a collision anywhere will cause devices to backoff, send a jamming signal, and then resend the frame.
A hub is also a <u>single broadcast domain</u> – all devices need to process broadcasts sent by every other device tin the network . Broadcasts flood the entire network, interrupting the CPU of every device (not ideal)

From a bandwidth PoV this may be 10 base T, but that 10mbps is shared between all devices. There is also a max utilization of 30% of that 10mpbs. So

4 devices on the network, slow the per device speed by 10/4 = 2.5mbps x 3/10 = ~.75mbps per device

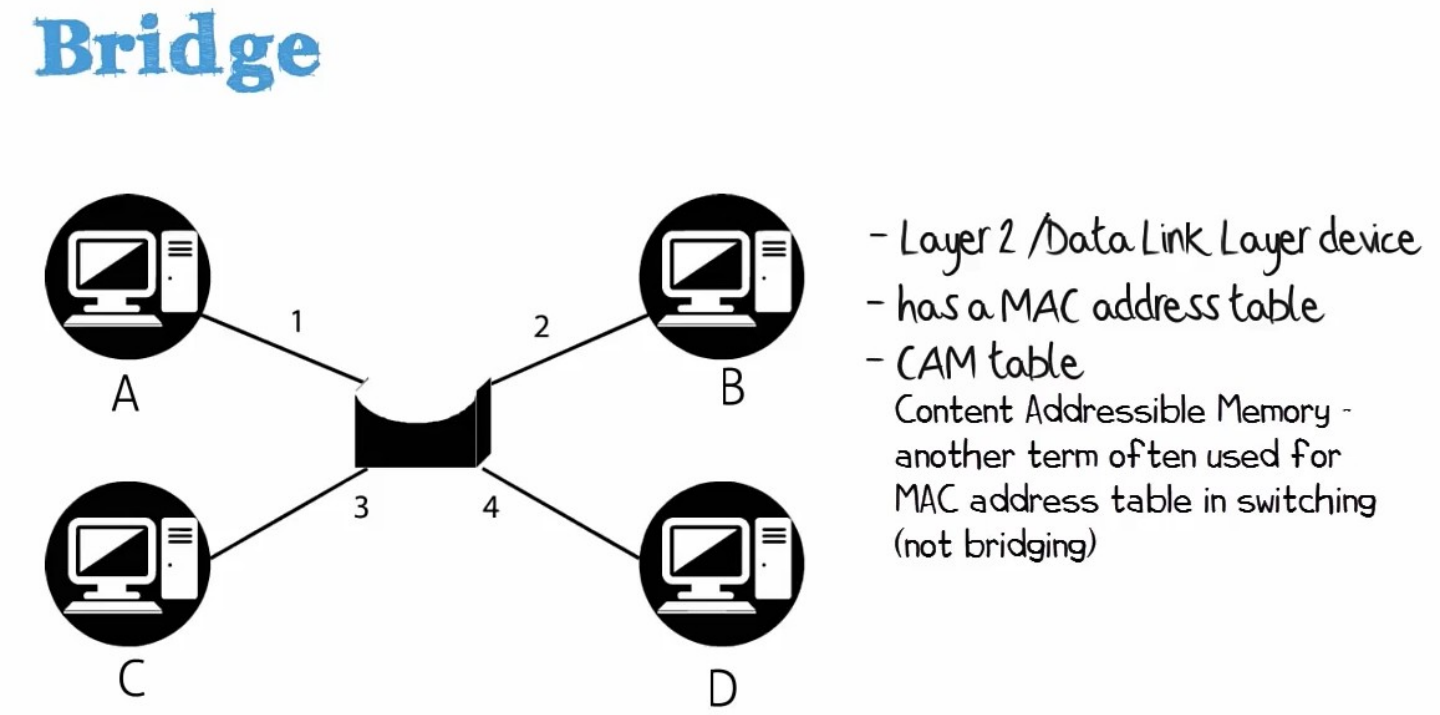
OSI Model Overview

Layer 1 – Physical

Layer 2 – Data Link
- **Mac address**

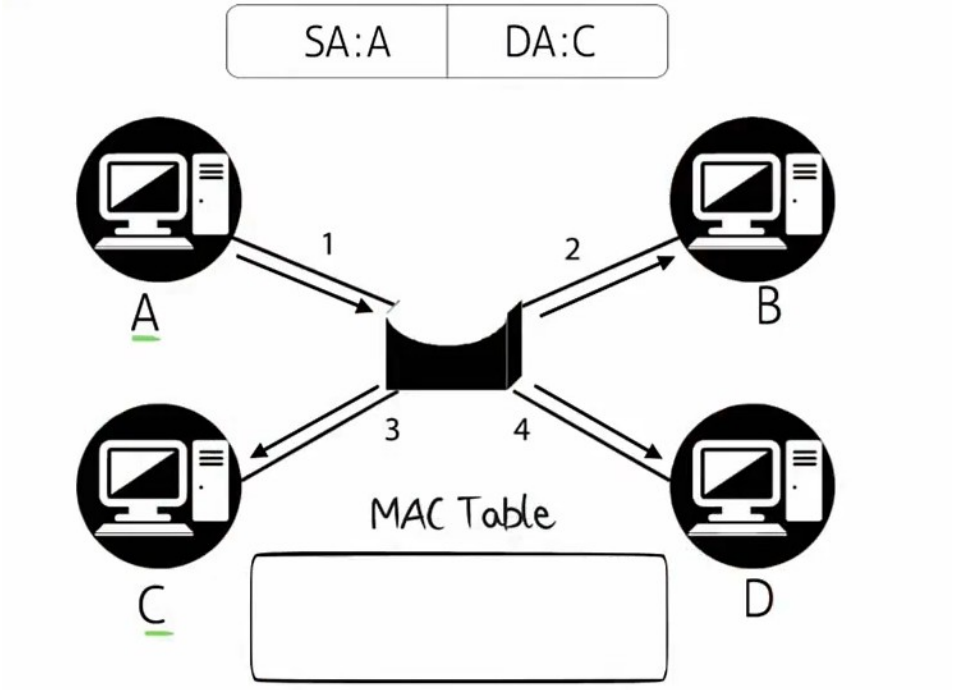
Layer 3- Network
- **IP addresses**

Layer 4 – Transport
- **TCP/UDP**



Physical Topology – Star
Logical Topology –
Bridges store MAC addresses in the MAC address table and that is stored in Software
Bridges are very slow compared to switches.
Bridges and Switches operate in a similar way, but bridges do the processing in software (slow) where as Switches do their processing in Hardware (fast).
Switches use ASICs (Application Specific Integrated Circuits) which allow for high throughput, very quick table lookups, and the forwarding of traffic often at line rate (meaning the processing of traffic is not slowed because the traffic went through the switch).
Bridges are the predecessors to Switches and did things in software (slower than Hardware based ASIC), however from a forwarding PoV, bridges and switches forward traffic on layer 2 in the same way.

What does a Bridge do when it receives a frame?



Device 1 (MAC Add: A) is sending data through a Bridge to Device 3 (Mac Add: C)

When a bridge boots, its MAC address Table is empty. (i.e. it does not contain dynamically learned Mac Addresses).
When a frame arrives on PORT 1 (of the Bridge) – sent by Host A, the bridges learns that Host A is connected to Bridge Port 1 and updates its MAC Table.
A – port 1
However, it is unaware of where port C is. So it flood the frame out of all ports (except the port that received it) to ensure that C receives the frame.
B and D drop the frame as the DA: is for C
Host C – receives the frame – deletes the layer 2 headers and send it up the OSI model to higher layer protocols.
Lets assume Device A was pinging C, so C replies.
The Bridge updates its MAC address Table so it knows that Device C is connected ot port 3 of the bridge.
Since C's reply has a DA: of A the bridge knows that that is connected on Port1 of the bridge and its then forwards the frame directly though port 1 to Device A.

Bridge – received frames are flooded to all ports (except the receiving port)
The Bridge notes the MAC address of the receiving port
The frame is received by the appropriate device which then replies
The bridge updates its MAC Address table and forwards the reply to the port that it already noted in its MAC table

Each interface on a bridge is a separate collision domain

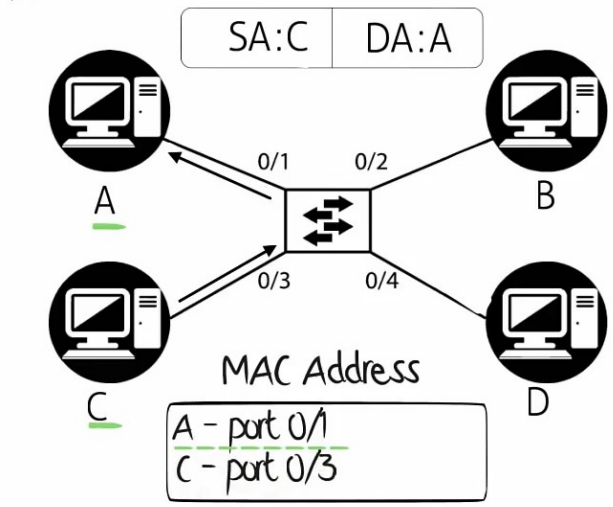
All interfaces are part of a single broadcast domain – so if A sends a broadcast, it would be received by everyone in the topology,

All devices will receive the broadcast, which is some cases is a good thing, but in most case's it is not.
In networking we want to restrict/contain the amount of broadcast traffic.
When there are too many broadcasts, it can slow down all devices on the network and in the worst case scenario, bring down the entire network (Broadcast Storm)

Bridges – process information in software
Switches – Process frames in hardware
The number of ports on a bridge is also limited when compared to switches
The number of ports on a bridge is also limited when compared to switches,
In today's environments, switches have replaced bridged.

Switches
Reside at Layer 2 (like bridges)
Advantage of Switches over Bridges
Processing is done in Hardware (ASICs)
The number of ports supported by switches is much higher (into the hundreds for one switching device)
Switching is done at wire speed, so there is no degradation of performance between two devices

What does a Switch do when it receives a frame?



Think of a Switch as a much more powerful and quick bridge
If you had a problem in a bridged environment and replaced the bridge with a switch, you would still have the same issues, but the issues would occur much quicker.
Bridge problems are not solved by switches, Switches simply increase the performace

A sends a frame to C
The switch receives the frame and notes which port A is on in the MAC address Table

The frame is then broadcast to all ports except A.
C then replies to the frame which goes back thought swich, which updates its MAC address table to note where C is.
The frame is then sent directly to A. Now A and C can communicate directly though the switch with no further broadcastings
Speed / Duplex
With Switches the Speed rating is dedicated to each individual port, rather than shared by all ports on the devices
So if you add more devices on the switch, it doesn't degrade the throughput each device gets
In addition, you can increase the speed by changing the Duplex
By setting this to Full Duplex you actually get 20 MPBS

Hubs operated by using CSMA/CD which is very similar to 10base2 - Half Duplex
Shared bandwidth, single collsion domain, single broadcast domain

Half-Duplex vs Full Duplex
Full Duplex, send and receive traffic at the same time
Half Duplex is like a walkie talkie, where only one side can send at any given time

Switches can use full duplex – both the PC and the Switch can send and receive at the same time.
Note that when using full duplex, Collision detection is disabled and only CSMA is used. This is because no collisions can occur when both sides are able to comm simultaneously.

Issues will arise if one side is set to full and the other is set to half Duplex. So check both sides of a connection to ensure that duplex has been negotiated correctly. You wont be able to tell if you only look at one side.

In theory, Full duplex gives you twice the bandwidth (10 downstream and 10 upstream), but you will only see your uploads/downloads operate at 10mpbs).

Be aware that Wireless access points tend to operate like hubs, meaning they have a shared infrastructure with share bandwidth. Where as switched devices had dedicated bandwidth

Conclusion
Hubs are Layer 1 devices
- **A hub is a <u>single collision domain</u>**
- **A hub is also a <u>single broadcast domain</u>**
- **Physical topology is a star (Central devices and spoke devices)**
- **Logical Topology is a Bus – All devices receive a frame (except the sender)**
- **Uses CSMA/CD**

Bridges are Layer 2 devices

A Bridge is a single collision domain

A Bridge is a single broadcast domain

Switches are Layer 2 Devices

Each port is its own collision domain,

Still part of a single broadcast domain.

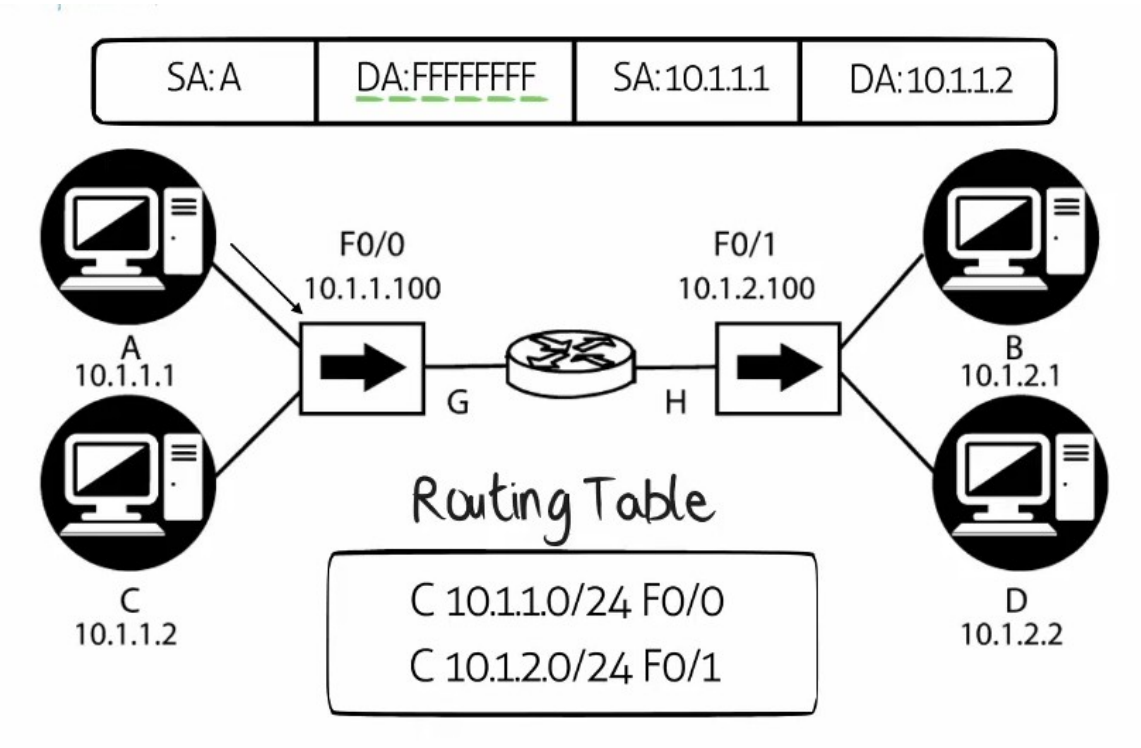
Switches use ASICs to process frames in Hardware at lIne speed, basically the frames travel just as fast as if there were no switch in their way.

Switches offer faster throughput and much greater Scalability.

Switches can also operate at Layer 3 (thus Layer 3 Switches) but unless otherwise stated operate at Layer 2

Routers

When a device wants to comm with another device in the same subnet, the first device will send a broadcast onto the local segment to find the mac address of the device its looking to communicate with using the target IP address.



1. **A sends a frame to the HUB**
2. **HUB (multiport repeater) floods the broadcast out of all ports (except the one that received it)**
3. **Both the Router and Host C receive the frame.**
   (note: NICs will only accept unicast traffic destined to their MAC address or they'll accept broadcast traffic / multicast traffic (must be subscribed to the multicast).
4. **The router will drop the frame as it can tell the ARP request is not for one of its IP Addresses.**
   (note: router's do not forward broadcasts)
5. **The NIC on PC "C" receives the broadcast and sees this Is an "ARP request" for its IP address**
6. **PC C will then reply with an "ARP reply" and the PC will update its ARP cache,**
   to show that IP add (10.1.1.1) is associated with MAC address (A)
7. **PC C's "ARP reply is received by the HUB and the HUB will send the frame out of all ports (except the receiving port).**
8. **The Router will receive a frame destined for MAC add: A | does not match its interfaces – frame drop**
9. **PC A receives the ARP Reply and accepts the frame. It then updates its ARP cache (10.1.1.2 = C)**

Pinging a Device on a remote Subnet

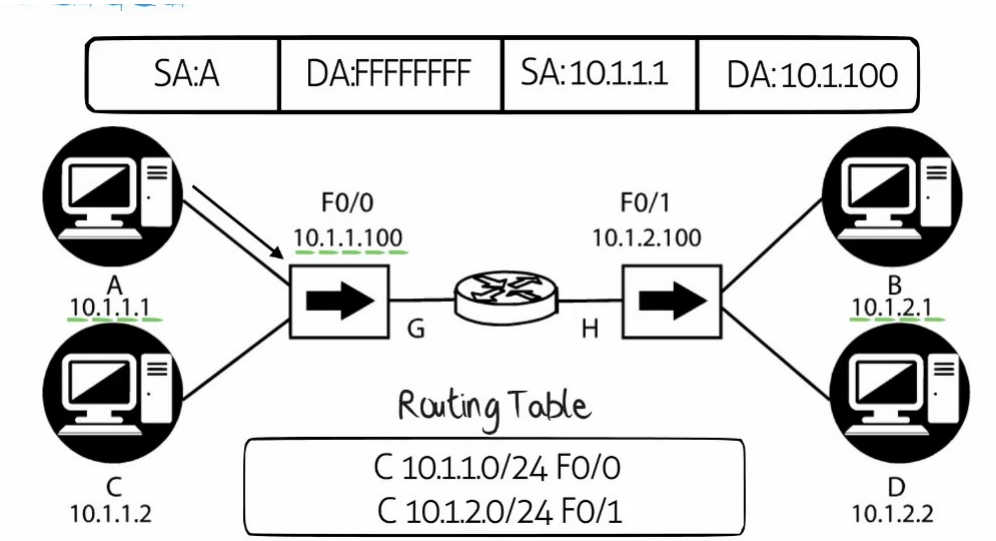
PC A with an IP address of 10.1.1.1 /24 wants to ping 10.1.2.1 /24

The first step it would take is to check to see if the remote IP is on its same subnet by seeing if the network portion of its address matches.

A /24 network has a subnet mask of 255.255.255.0 where the first 3 octets (filled with 1's)

(1111 1111 = 255) is the network portion of the address. Since they don't match, the local PC knows the target device is on a separate subnet and will therefore send the traffic to its default-gateway to get to the target device through the gateway/router.

Prior to sending data through the def gateway to the target device, the PC needs to verify that it has the def gateway's MAC address in its ARP cache. (Note: Since this is an ethernet segment, a layer 2 MAC address is required)



PC A doesn't have the MAC address of its default gateway (only knows its IP address)

PC A sends an ARP request (broadcast) onto the segment asking: Who has 10.1.1.100? Tell PC A

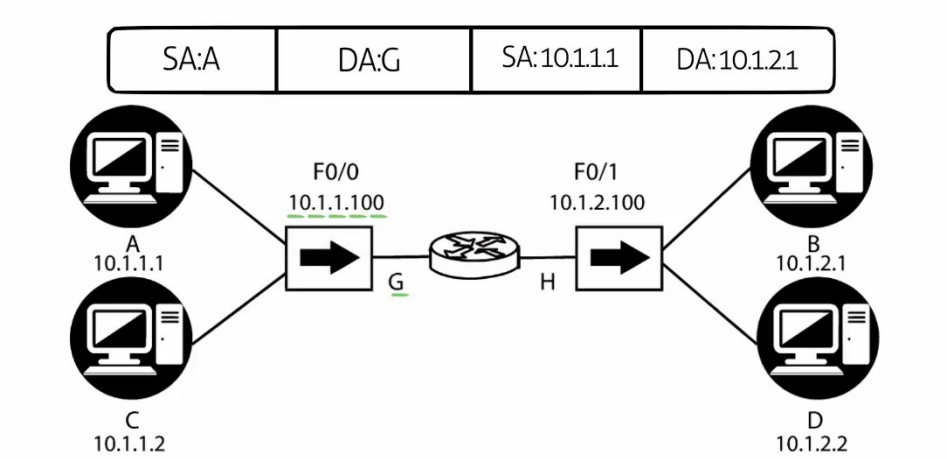
The hub repeats the frame out of all ports (except the receiving port) and PC C drops the frame.

The router sees that the frame is meant for itself, processes the frame, updates it mac cache, and reply with an ARP reply)

The hub forwards the ARP reply out of all ports (except the receiving port), PC C's NIC will drop the Frame.

PC A's NIC will accept the frame at layer 2, strip the L2 headers and forward the frame to the upper layer protocols for further processing. PC A will update its ARP cache: 10.1.1.100 = G

Sending Traffic to a separate subnet



Layer 2

SA: A (PC A)

DA:G (PC A's def gateway)

Layer 3

SA: 10.1.1.1 (PC A)

DA: 10.1.2.1 (PC B)

Note: the Layer 2 frame goes to the router, hence the L2 information contains the Local segment MAC Addresses.

Layer 3 information contains the IP address of the Remote host and the local host's IP address

PC A sends a ping seeking PC B on the other subnet

The hub floods the frame…

The Router will receive the frame at L2, it will then strip the L2 headers from the frame and read the L3 info

The Layer 3 Info shows the Source IP address (PC A) and the destination IP address (PC B)

The router checks if the destination IP address is local to the router. It not

The router then checks its routing table, from here the router sees that DA:10.1.2.1 is located in the subnet 10.1.2.0 /24 out of fa 0/1. The router therefore knows to get traffic to 10.1.2.1 it will need to send out of Fa0/1.

The router would then check its ARP cache to see if it knows the MAC add of 10.1.2.1

Assuming, the router does not have this MAC in its ARP cache. To get this MAC address, the Router broadcasts an ARP Request asking who is 10.1.2.1? Tell R1. The gateway forwards as per usual, PC D drops the frame.

PC B sends an ARP Reply stating its MAC add is “B” and updates is ARP cache: R1 (10.1.2.100 = H)

The ARP Reply from PC B gets back to the router, the Router updates its ARP Cache.

Now that the ARP cache is updated, the router can send the og Ping traffic to PC B

The Ping will now have a the following SA’s and DA’s

L2 L3

SA: H (Fa0/1 on the router) SA: 10.1.1.1 (the original source IP stays in PLACE)

DA: B SA: 10.1.2.1

Note: When Packets traverse a router / L3 Switch (e.g. going from 1 VLAN to another), the Layer 2 information is rewritten, where as the Layer 3 information stays the same)