

# Overview of Layer 2 Switched Networks and Communication

---

## General Overview of Layer 2

Layer 2 is Data Link Layer (DLL) as per OSI Model. As we know function of each layer is to provide services to above layer, so DLL provide various services to Layer 3: Network Layer. Various services which DLL provides are:

1. Framing network layer data packets.
  2. Flow Control
  3. Multiple Access control using CSMA/CD (Carrier Sense Multiple Access / Collision Detection) in wired network and CSMA / CA (Collision Avoidance) in wireless network.
  4. Physical Addressing
  5. Switching
  6. Quality of Service (QoS)
  7. Virtual LAN's (VLAN)
- & some more.

Data Link Layer is basically divided into two sub-layers:

- **Logic Link Control (LLC):** Provide services to upper layer.
- **Media Access Control (MAC):** Perform Layer 2 functions like switching, physical addressing etc.

Basically what I am going to explain in this article is, how inter-communication happens in data network between two devices at Layer 2 (Switching).

## Physical Addressing and Switching

Network is a group of devices connected to each other. On Layer 2, devices can communicate within a single network only. Layer 2 devices cannot span multiple networks, for multiple networks Layer 3 support is required.

Each device in a single network needs to be identified uniquely. At Layer 2, unique identification is done via physical addressing scheme. Device hardware (NIC Card) which provides interconnection has unique physical address assign to it known as MAC Address. MAC address is of 48 bits, written in hexadecimal form separated after 8 bits with either colon (:) or hyphen (-). Example address: **00:80:48:5C:1A:52**. So each machine will have unique physical address by which machine is identified. Total MAC Address is of 6 bytes. Each manufacturer is allotted with first 3 bytes of MAC Address which act as series prefix for all the NIC's by that company, last 3 bytes are unique within one series. By this way no MAC address of one company can clash with another nor within company series.

Communication among devices at layer 2 is done via some interconnecting device, which forms connection between each host machine or network devices (router, wireless, etc). Switch is that device which provides interconnection. Switch has ports (physical interface) at which wires from various network devices or host machines connect. All devices in a network are connected to a switch which interconnects them; this is Layer 1 (inter-connection).

Now let's get into deep understanding about how communication is done after interconnection. For this we need to understand working of switch.

### *Working of Switch*

Switch is an interconnecting device with 16 or 24 ports in common. All other devices are connected to these ports. Whenever any machine sends packet to any other machine, source machine send packet to switch, switch then forwards it to destination machine. Each packet which comes to switch contains source and destination physical address in it, on basis of which switch forwards packet to other machine. Switch always sent packet based on destination MAC address. Its process is as follows: (process also known as Switching)

1. When switch receives a packet from any device, it checks for its destination MAC address.
2. Then switch compares destination MAC address with its MAC Address Table for corresponding MAC address.
  - a. If MAC Address is found, packet is sent out to port against which MAC Address was matched.

- b. If entry is not found, Unknown unicasts (when the switch doesn't have a port mapping for a destination mac address in the frame) are treated like broadcasts by Layer Two devices, and are flooded out of all ports except the port on which the frame originated.

Now question comes, how does switch knows on which port destination machine is connected? For this switch uses one table in its cache memory called MAC Address table or Forwarding Table in which switch stores that at which port which machine is connected by storing its physical address (MAC Address). So table contains two columns (Physical Address and Port Number) and rows equal to number of ports in switch.

When switch is turned ON, by default there is no entry in MAC address table, as communication starts, based on devices involved entries are created in table.

### *Working of Address Resolution Protocol (ARP)*

ARP is a layer 2 protocol, used for obtaining MAC address of any devices within a network. Host machines use ARP protocol to obtain MAC Address. ARP protocol in conjunction with Layer 3 IP Protocol addressing (IP Address).

Host machine uses ARP because when machine needs to send packet to another device, destination MAC address is needed to be written in packet sent, so host machine should know the MAC Address of destination machine. Operating Systems also maintain ARP Table (MAC Address Table).

To obtain MAC address, ARP performs following process: (ARP request by host machine)

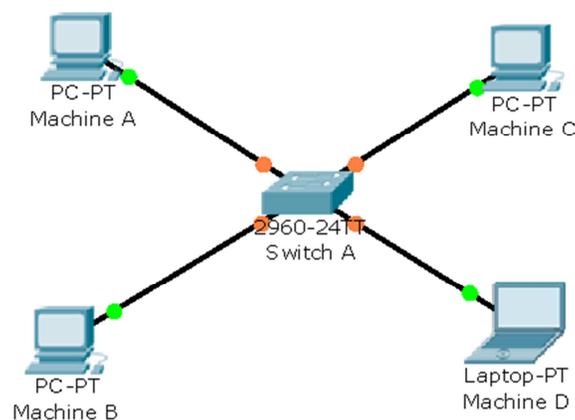
1. Source machine generate ARP REQUEST packet with source MAC address (of this machine), source IP address (of this machine) and destination IP address and forwards this packet to switch.
2. Switch receives the incoming packet and reads the source MAC address and checks its MAC address table, if entry for packet at incoming port is found then it checks its MAC address with the source MAC address and updates it, if entry not found then switch add and entry for incoming port with MAC address.

3. All ARP REQUEST packets are broadcasted in network, so switch broadcast ARP REQUEST packet in network, because destination for ARP packet will be 255.255.255.255.  
(Broadcast are those packets which are sent to everyone in network except the sender, only in network to which it belongs, it cannot span multiple networks)
4. All devices in network receives ARP packet and compare their own IP address with the destination IP address in that packet.
5. Only the machine which matches the both will reply with ARP reply packet. This packet will have source IP of this machine (which was destination machine in previous packet, as now its replying this machine will be the source machine) , source MAC address, destination MAC address (same as source MAC address in REQUEST packet) and destination IP address (same as source IP address in REQUEST packet).
6. Then switch reads the ARP reply message and add entry in its MAC Address Table for port number on which it has received packet by reading its source MAC address field and forwards that packet to destination machine (source machine in REQUEST packet) as its MAC is in destination MAC address.
7. Further host machine add destination machine entry into its ARP table.

This using ARP resolution switch and other devices in network obtain MAC address of any other device in a network. Remember ARP works on broadcast, so it works only in single network.

## Final Layer 2 Communication Process

Now finally let's see how devices communication occur at Layer 2:



Suppose Machine A needs to communicate with Machine D, following will be the process at Layer 2:

### Summary Process

1. Machine A lookup's for Machine D MAC address in its ARP table.
  - a. If MAC Address found then packet is formed and sent to Switch A.
  - b. If MAC address not found then ARP Request is generated and MAC address is obtained.
2. Switch A receives packet and checks for MAC Address in its MAC Address Table.
  - a. If MAC Address matched it will forward packet on matched port number.
  - b. If MAC Address not found then the packet is broadcasted to all ports, except on which it has received the packet.
3. Machine D receives packet from Switch A which was sent by Machine A.
4. When Machine D will reply, same process will be followed as switching is done.

### Detailed Process

1. Machine A lookup's for Machine D MAC address in its ARP table. If MAC address is not found, machine A will send ARP Request for MAC address of machine D (using Machine D IP Address) and sends packet of Switch A.
2. Switch A will receive and read packet and add Machine A physical address in its MAC Address table to which Machine A is connected.
3. After that, switch will broadcast ARP Request packet in network..
4. All machines in network except Machine A will receive ARP Request packet. Then all machines will check for Destination IP address and compare with its own IP Address.
5. Only Machine D IP address matches with destination IP address as packet was intended for that machine.
6. Machine D will reply with its MAC Address (as per ARP working).
7. Switch A receives ARP Reply packet, and will add physical address of Machine D in its MAC Address table against corresponding port on which it received request.
8. After adding entry it will check for destination MAC Address and compare it with its MAC address table.
9. Based on MAC Address table entry, it will forward packet to corresponding port number against which successful match was found.
10. Host machine will receive ARP Reply and add MAC address to its ARP table.

11. Then machines forms complete data packet and sends it to Switch A.
12. Switch A receives packet and updates it's MAC Address Table and based on Destination MAC Address match with its MAC Address Tables, forwards packet on corresponding port.
13. In same manner other machine will reply and same process will repeat as point 12 and 13.