Lesson 4: Switching and VLANs

N.BERREHOUMA

Department of Computer Science
8 Mai 1945 University, Guelma

March 2, 2025

Overview

What is a Switch?

- Definition: A network device that connects multiple devices on a local area network (LAN).
- Function:
  - Forwards **data frames** only to the intended recipient(s) based on MAC addresses.
  - Creates separate collision domains, reducing network congestion.
  - Provides a more efficient and scalable way to connect devices on a LAN compared to hubs.

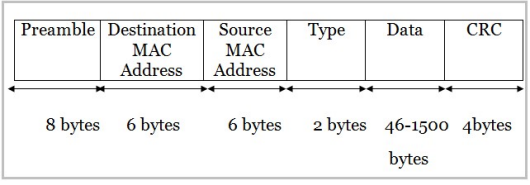


Figure: Ethernet Data Frame

The Switching Process

Key Concepts:

- **MAC Address Table:** Stores MAC addresses and their associated ports.
- **Auto-Learning**: Switch learns MAC addresses by examining the source address of incoming frames.
- **Forwarding:** Switch forwards frames based on the MAC address table.

Step 1: Frame Reception

1: Switch receives a frame on a specific port.
2: Extract the source MAC address (`src_mac`) and incoming port (`in_port`).

Step 2: Auto-Learning

1: Check if `src_mac` is already in the MAC address table.
2: **if** `src_mac` is not in the table **then**
3: Add `src_mac` and `in_port` to the MAC address table.
4: **else**
5: Update the existing entry with the new `in_port`.
6: **end if**

Step 3: Forwarding Decision

1: Extract the destination MAC address (`dst_mac`) from the frame.
2: Check if `dst_mac` is in the MAC address table.
3: **if** `dst_mac` is in the table **then**
4: Forward the frame to the associated port.
5: **else**
6: Flood the frame to all ports except `in_port`.
7: **end if**

Step 4: Frame Transmission

1: **if** Frame is forwarded to a specific port **then**
2: Transmit the frame to the destination device.
3: **else**
4: Transmit the frame to all devices in the network (flooding).
5: **end if**

Step 5: MAC Address Table Aging

1: Periodically check the MAC address table for stale entries.
2: Remove entries that have not been updated within the aging time.

Switching Table Update

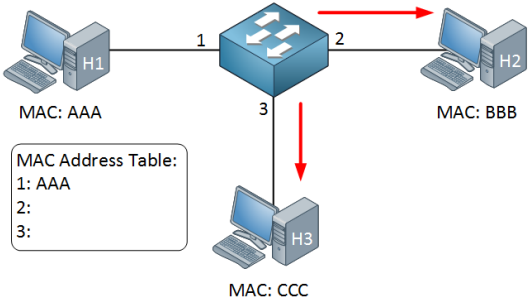


Figure: Switching Table Update

Switching Lab

Demanded Work

- Create the topology →
- configure IP addresses for the three hosts
- try connectivity between hosts with *ping* command
- run switcher CLI to get the forwarding table

```
Switch#show mac-address-table
----------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    000a.f3c4.c813    DYNAMIC     Fa0/3
   1    0060.3e53.29e2    DYNAMIC     Fa0/2
   1    00d0.bad4.2e64    DYNAMIC     Fa0/1
```

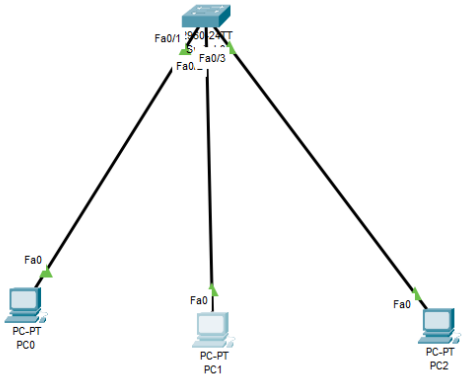


Figure: Lab Topology

Switching Lab

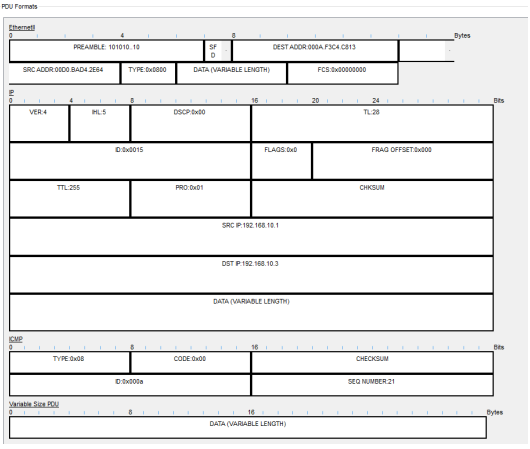
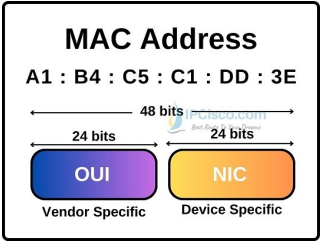


Figure: Captured Traffic obtained through the simulation of ping communication

Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media.
- MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address consists of a 48-bit binary value
- All MAC addresses must be unique to the Ethernet device or Ethernet interface.
- To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).



Address Resolution Protocol (or How to convert IP address to MAC address)

- An IP packet is created with a source and destination IP address carrying the data from an application.
- The IP packet will be encapsulated in an Ethernet frame with a source and destination MAC address.
- The sending computer will of course know its source MAC address but how does it know the destination MAC address? That's where ARP comes into play.

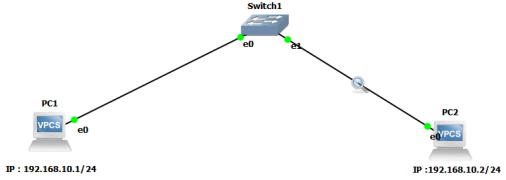


Figure: ARP Protocol Simulation with GNS3

Captured Trafic with WireShark

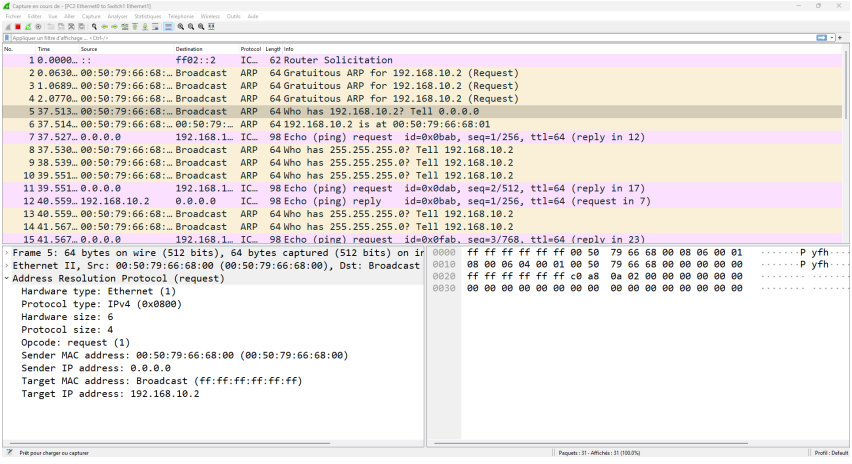


Figure: Wireshark Trafic Capture

ARP Resolution Process

Key Concepts:

- **ARP Request:** Broadcast message to find the MAC address for a given IP address.
- **ARP Reply:** Unicast message containing the MAC address for the requested IP address.
- **ARP Cache:** Stores IP-to-MAC address mappings for future use.

Step 1: Check ARP Cache

1: Device wants to send a packet to a destination IP address (`dst_ip`).
2: Check the ARP cache for an entry matching `dst_ip`.
3: **if** Entry exists in ARP cache **then**
4: Retrieve the corresponding MAC address (`dst_mac`).
5: Proceed to packet transmission.
6: **else**
7: Proceed to **Step 2**.
8: **end if**

Step 2: Send ARP Request

1: Construct an ARP request packet:
2: Sender IP = `src_ip`, Sender MAC = `src_mac`.
3: Target IP = `dst_ip`, Target MAC = `00:00:00:00:00:00`.
4: Broadcast the ARP request to all devices in the local network.

Step 3: Receive ARP Reply

1: The device with `dst_ip` receives the ARP request.
2: Construct an ARP reply packet:
3: Sender IP = `dst_ip`, Sender MAC = `dst_mac`.
4: Target IP = `src_ip`, Target MAC = `src_mac`.
5: Send the ARP reply as a unicast message to `src_mac`.

Step 4: Update ARP Cache

1: The original device receives the ARP reply.
2: Extract `dst_ip` and `dst_mac` from the ARP reply.
3: Add the entry (`dst_ip`, `dst_mac`) to the ARP cache.

ARP Table and How to Retrieve It

- A table stored on devices (e.g., routers, switches, PCs) that contains IP-to-MAC address mappings.
- Used to forward frames within the same subnet.
- Open Command Prompt and run *arp -a* on a host or *show ip arp* on a router
- Automatically learned via ARP requests/replies.
- Dynamic entries expire after a set time (default: 4 hours on many devices).
- To clear the ARP table use *arp -d ** or *clear arp-cache* on a router

Sending an IP Datagram from Machine A to Machine B

Objective: Send an IP datagram from Machine A to Machine B.
Inputs:

- Source IP address (`src_ip`) and subnet mask (`src_mask`).
- Destination IP address (`dst_ip`) and subnet mask (`dst_mask`).
- Default gateway address (`gateway_ip`) for Machine A.

Step 1: Determine if Destination is in the Same Subnet

1: **if** `src_ip&src_mask` == `dst_ip&dst_mask` **then**
2: Destination is in the same subnet.
3: Proceed to **Step 2**.
4: **else**
5: Destination is in a different subnet.
6: Use the default gateway (`gateway_ip`) as the next hop.
7: Proceed to **Step 2**.
8: **end if**

Step 2: ARP Resolution

1: **if** Destination is in the same subnet **then**
2: `target_ip` = `dst_ip`.
3: **else**
4: `target_ip` = `gateway_ip`.
5: **end if**
6: Check the ARP cache for `target_ip`.
7: **if** ARP cache contains `target_ip` **then**
8: Retrieve the corresponding MAC address (`target_mac`).
9: **else**
10: Send an ARP request to resolve `target_ip`.
11: Wait for an ARP reply containing `target_mac`.
12: Update the ARP cache with `target_ip` and `target_mac`.
13: **end if**

Step 3: Construct the IP Datagram

1: Create an IP datagram with:
2: Source IP = `src_ip`, Destination IP = `dst_ip`.
3: Encapsulate the IP datagram in an Ethernet frame with:
4: Source MAC = `src_mac`, Destination MAC = `target_mac`.

Step 4: Send the IP Datagram

1: Transmit the Ethernet frame to `target_mac`.

Step 5: Forwarding (if applicable)

1: **if** Destination is in a different subnet **then**
2: The default gateway forwards the IP datagram to the destination subnet.
3: **end if**

What is a VLAN?

- Definition: A logical grouping of network devices that appear to be on the same broadcast domain, regardless of their physical location.
- Purpose:
  - Segmenting a network into smaller, more manageable broadcast domains.
  - Improving network security by restricting broadcast traffic.
  - Enhancing network performance by reducing network congestion.
  - Supporting different network policies for different groups of users.

VLAN IDs

- Unique identifiers assigned to each VLAN.
- Typically 12-bit numbers, allowing for up to 4096 VLANs.

Tagged and Untagged Frames

- Tagged frames: Contain VLAN information in the frame header.
- Untagged frames: Do not contain VLAN information.

Methods of VLAN Configuration

- Static VLANs: Manually configured by the network administrator.
- Dynamic VLANs: Automatically assigned based on MAC addresses or other criteria.

VLAN Configuration on Switches

- Assigning ports to VLANs.
- Configuring VLAN parameters (e.g., VLAN ID, name).
- Configuring VLAN membership rules (for dynamic VLANs).

Need for Inter-VLAN Routing

- Devices in different VLANs cannot directly communicate with each other.
- A router or a Layer 3 switch is required to route traffic between VLANs.

Methods of Inter-VLAN Routing

- Router-based Inter-VLAN Routing: Using a dedicated router to connect VLANs.
- Layer 3 Switch-based Inter-VLAN Routing: Utilizing the routing capabilities of a Layer 3 switch.

VLAN Trunking

- Encapsulating traffic from multiple VLANs on a single physical link using protocols like 802.1q.
- Enables efficient transmission of traffic between switches.