L&T

APPLIED

INDUSTRIAL IoT

PROJECT

Mahadev Manoj

2363040, 5BTAIML

Batch 7

IMPLEMENTATION OF A SIMPLE LAN AND ANALYSIS OF ARP USING CISCO PACKET TRACER

TABLE OF CONTENTS

Problem Statement

In a Local Area Network (LAN), devices communicate using IP addresses at the network layer. However, the actual delivery of data requires the MAC (Media Access Control) address of the destination device. The Address Resolution Protocol (ARP) provides a dynamic mechanism to map IP addresses to MAC addresses. Without ARP, devices would not be able to discover each other's physical addresses, leading to communication failure.

This project demonstrates the construction of a simple LAN in Cisco Packet Tracer and the analysis of ARP operation in resolving IP-to-MAC mappings.

Aim

To construct a simple Local Area Network (LAN) in Cisco Packet Tracer and understand the concept and operation of the Address Resolution Protocol (ARP).

Theory – Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a network protocol that maps an IP address to its corresponding MAC address within a LAN. It operates at the boundary of the network layer (Layer 3) and the data link layer (Layer 2).

- When a host wants to send data to another host on the same LAN, it checks its ARP cache for the destination MAC address.
- If the MAC address is not present, the host broadcasts an **ARP Request** asking, *"Who owns this IP address?"*.
- The device with the matching IP replies with an **ARP Reply**, providing its MAC address.
- The MAC address is stored in the ARP cache for subsequent communication.

Thus, ARP enables seamless communication by linking logical addresses (IP) with physical addresses (MAC).

Scope of the Solution

- To design and implement a basic LAN using a Cisco switch and PCs.
- To configure static IP addressing on end devices.
- To verify device-to-device communication using ICMP ping.
- To study ARP operation using the commands arp -a and arp -d.
- To visualize ARP broadcast and reply packets in Cisco Packet Tracer Simulation Mode.

Real-World Scope

- In enterprise networks, ARP is essential for enabling seamless communication between hosts, printers, servers, and network devices.
- ARP is critical in troubleshooting network issues such as duplicate IPs, unreachable hosts, and MAC spoofing attacks.
- ARP tables are used in security monitoring and intrusion detection systems to verify legitimate devices.
- ARP is the foundation for advanced protocols such as Proxy ARP, Gratuitous ARP, and is heavily used in Wi-Fi networks, routers, and gateways.
- Cloud and data center environments rely on ARP (or its extensions like GARP) for virtual machine migrations and load balancing.

Required Components

Software

- Cisco Packet Tracer (version 7.x or above)

Hardware (virtualized within Packet Tracer)

- 1 × Cisco 2960 Switch (24-port)
- 2 × PCs (end devices)
- 2 × Copper Straight-Through Cables

Steps Used

1. **Open Cisco Packet Tracer** and create a new project.
2. **Add Devices**: Place two PCs (PC0, PC1) and one Cisco 2960 switch in the workspace.
3. **Connect Devices**: Use Copper Straight-Through cables to connect:
   - PC0 → Switch FastEthernet0/1
   - PC1 → Switch FastEthernet0/2
4. **Assign IP Addresses**:
   - PC0 → IP: 192.168.1.1, Subnet Mask: 255.255.255.0
   - PC1 → IP: 192.168.1.2, Subnet Mask: 255.255.255.0
5. **Verify Connectivity**: On PC0, open Command Prompt and type: ping 192.168.1.2 (Successful replies confirm communication).
6. **Check ARP Table**: On PC0, type: arp -a (This displays PC1's MAC address).
7. **Clear ARP Cache**: On PC0, type: arp-d , Then ping PC1 again to observe ARP resolution.

8. **Visualize in Simulation Mode**: Switch to Simulation mode and observe ARP Request broadcasts and ARP Reply unicasts during the ping process.

Observations

- Successful pings indicate that devices can communicate once IPs are configured.
- The ARP table (arp -a) confirms dynamic IP-to-MAC mapping.
- Clearing the ARP cache (arp -d) causes the next ping to trigger an ARP Request.
- In Simulation Mode, ARP Requests are visible as broadcasts, and ARP Replies are visible as unicasts.

Conclusion

The experiment successfully demonstrated the construction of a simple LAN and the functioning of ARP in resolving IP-to-MAC address mappings. ARP plays a crucial role in enabling communication within a LAN by bridging the gap between IP addresses (logical) and MAC addresses (physical). Cisco Packet Tracer effectively simulated ARP operations, providing both practical and visual understanding of the protocol.

GIT REPO: https://github.com/thefallen7777/ARP-Batch-7-Cisco-Packet-Tracer---2363040