Fr. Conceicao Rodrigues College of Engineering

Department of Computer Engineering

Academic Term : July-Nov 2023-24

Class : T.E. (Computer B)
Subject Name: Computer network Lab
Subject Code : CSL 502

Experiment No:	7
Date of Performance:	31/08/2023
Roll No:	9614
Name of the Student:	AQIB FIRDOUS KHAN

AIM: To simulate ARP protocol using Packet Tracer

THEORY:(write in brief theory of ARP) :
The Address Resolution Protocol (ARP) is a fundamental networking protocol used in Ethernet and IP networks to map an IP address (Layer 3) to the corresponding physical MAC address (Layer 2) on a local network segment. ARP is crucial for the functioning of modern computer networks, and here's a short detailed note on how it works and its significance:

Address Resolution Purpose:

ARP is used when a device in a local network needs to communicate with another device within the same network segment.
It resolves the issue of how to identify the hardware address (MAC address) associated with a known IP address.
ARP Operation:

When a device wants to send data to another device on the same local network, it first checks its ARP cache. This cache stores recently resolved IP-to-MAC address mappings.
If the needed mapping is not in the cache, the requesting device sends out an ARP request broadcast frame to the entire network. This broadcast contains the target IP address that the sender is trying to reach.
Devices on the network receive the ARP request and check if the target IP address matches their own. If it does, they respond with an ARP reply.
The ARP reply contains the MAC address of the target device, and the requesting device updates its ARP cache with this information.
ARP Table:

Each device on a network maintains an ARP table (also known as an ARP cache) to store IP-to-MAC address mappings.

This table helps in reducing ARP broadcasts, as devices can quickly reference it before initiating ARP requests.
ARP Spoofing and Security:

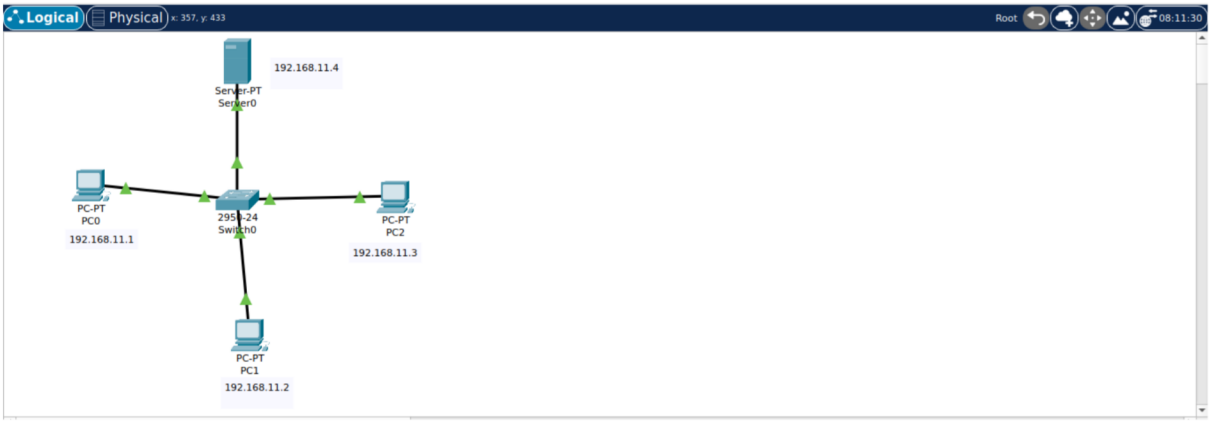
ARP is a stateless protocol, making it susceptible to ARP spoofing or ARP poisoning attacks. In these attacks, malicious entities can provide false IP-to-MAC mappings, leading to traffic interception or redirection.
To mitigate ARP spoofing, various security mechanisms like ARP cache timeouts, static ARP entries, and ARP inspection have been developed.
ARP and Routing:

ARP operates within the local network segment, so it's primarily used for local communication.
Routers and Layer 3 devices use ARP only for devices within their own subnets. For communication with devices in other subnets, routers rely on ARP for the local segment and their own ARP tables for remote segments.
IPv6 and ARP:

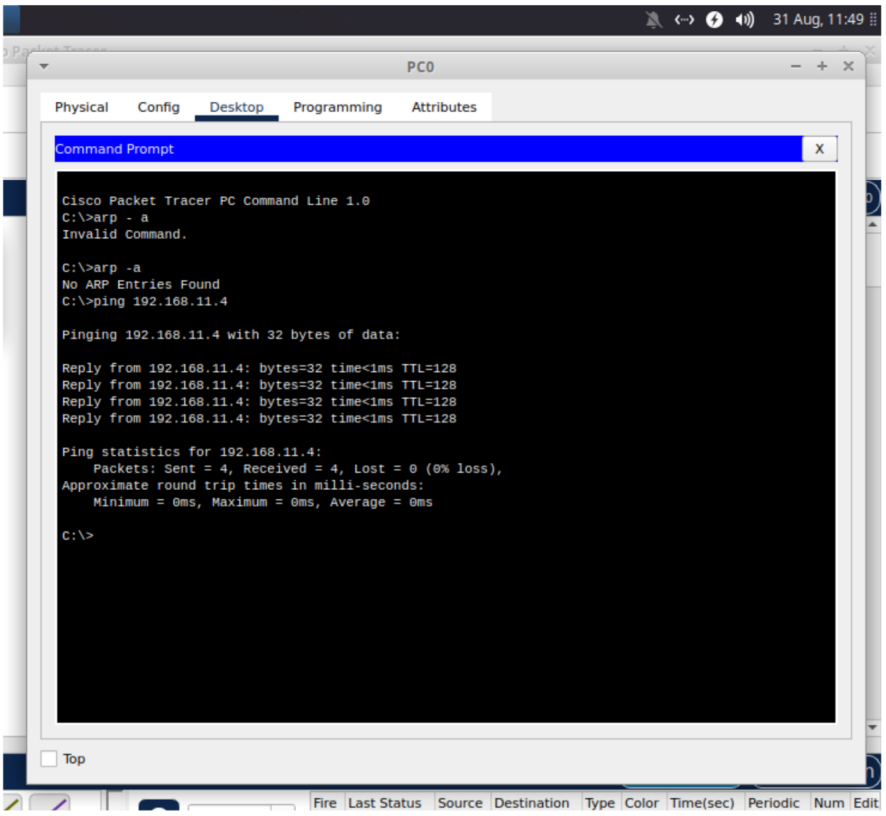
In IPv6 networks, ARP is replaced by the Neighbor Discovery Protocol (NDP), which serves similar functions but with improvements and security enhancements.

Steps: Write down the steps with screenshot

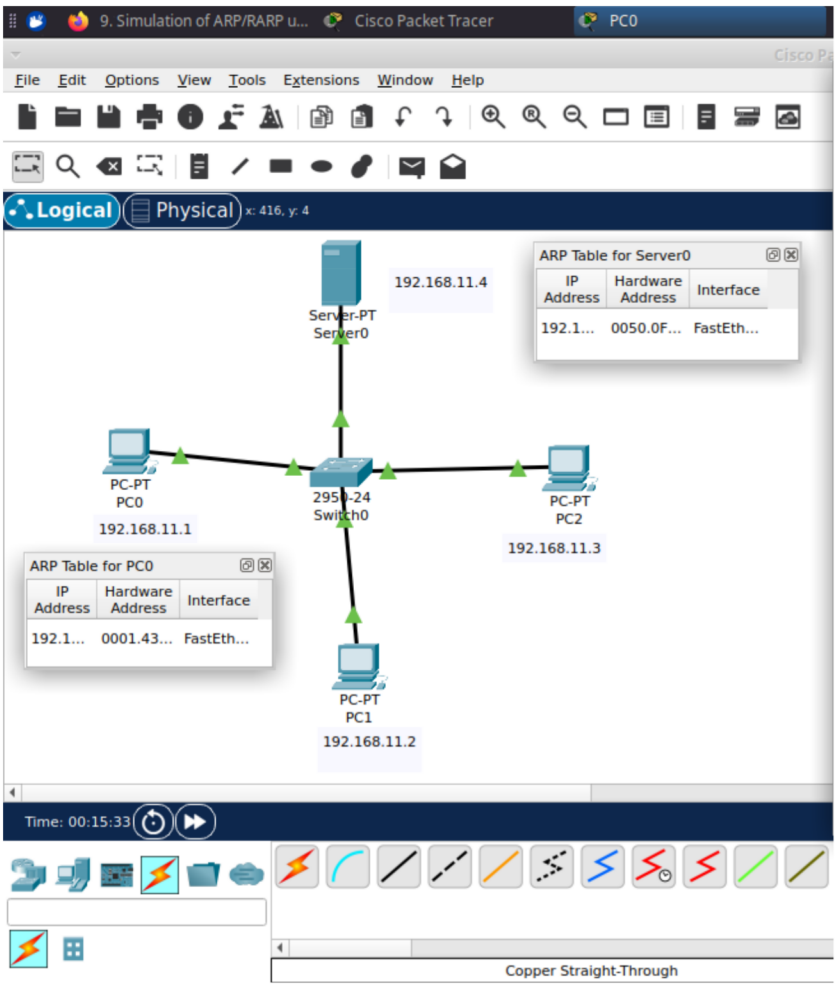
STEP 1 : Select Server- PT and set an IP address.
STEP 2 : Select 3 PC's and set their IP address respectively.
STEP 3 : Select SWITCH 2950-24 and set an IP address for it as well.



STEP 4 : Connect the computers to the SWITCH with Copper straight-through wire.
STEP 5 : Connect the SWITCH to the server.
STEP 6 : Open the command prompt of PC0
STEP 7 : Type the following Commands:-



STEP 8 : Choose the Inspect icon and check whether the message has been sent from PC0 to the Server- PT



Conclusion:

In packet tracer we observed how arp works by enabling devices to map ip addresses to MAC addresses in order to send and receive data packets.