Packet Tracer Lab

Instructions for Submission:

- The lab should be documented in a report format and submitted as a PDF file.
- The report should include screenshots for each step demonstrating the progress and completion of the tasks.
- Ensure that screenshots clearly display the Packet Tracer interface, configurations, and test results.
- A separate image of the badge from the course link provided earlier must also be submitted. This image should not be included in the report but submitted as a separate file.
- **Deadline (23-February-2022, 12:00 pm)**

Objectives

- Develop an understanding of Packet Tracer's functions.
- Prototype a network with two PCs connected to a switch and configure basic settings.
- Observe network traffic behavior, including ARP and ICMP messages.
- Validate network configurations using connectivity tests.
- Troubleshoot basic network issues using Packet Tracer's simulation tools.

Step 1: Set Up the Network Topology

a) Add two PCs and a Cisco 2950T switch to the workspace.

b) Use straight-through cables to connect the devices:

- Connect PC0 to interface Fa0/1 on Switch0.
- Connect PC1 to interface Fa0/2 on Switch0.

Step 2: Configure the Devices

a) Click PC0, open the Config tab, and set:

- Display Name: PC-A
- IP Address: 192.168.10.10
- Subnet Mask: 255.255.255.0

b) Click PC1, open the Config tab, and set:

- Display Name: PC-B
- IP Address: 192.168.10.11

- Subnet Mask: 255.255.255.0

Step 3: Observe Data Flow Using Simulation Mode

a) Switch to **Simulation Mode** by selecting the stopwatch icon in the bottom-right corner.

b) Click **Edit Filters** and deselect all filters. Select **ARP** and **ICMP** filters.

c) Select **Simple PDU (closed envelope icon)** and click PC-A as the source, then PC-B as the destination.

- Two envelopes should appear beside PC-A (ARP and ICMP).
- The Event List in the Simulation Panel will show their type.

Step 4: Run and Analyze Network Traffic

a) Click **Auto Capture / Play** to observe packet movement.

b) Click **Capture / Forward** to analyze the process step by step.

c) Click **Power Cycle Devices** and confirm the reset.

- Both ARP and ICMP packets should reappear.

Step 5: Verify and Troubleshoot Network Connectivity

a) Click PC-A > Desktop > Command Prompt.

b) Type: ping 192.168.10.11 and press Enter.

- A successful ping should resemble:

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time=70ms TTL=128

Reply from 192.168.10.11: bytes=32 time=72ms TTL=128

Reply from 192.168.10.11: bytes=32 time=68ms TTL=128

Reply from 192.168.10.11: bytes=32 time=71ms TTL=128

Ping statistics for 192.168.10.11:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)

Approximate round trip times: Min = 68ms, Max = 72ms, Avg = 70ms

c) If the ping fails, verify cable connections and IP configurations.

Step 6: View and Analyze ARP Tables

a) Run arp -a on PC-A and PC-B to view the ARP table.

b) Verify that each PC has the MAC address of the other device in its ARP table.

c) Close all configuration windows and confirm the correct setup.

interface Fa0/2
switchport mode access
switchport access vlan 20
exit
d) Verify VLAN configuration using:
show vlan brief