Experiment 2.1

Student Name: Jeetendra Patel **UID:22BCS12228**
Branch:BE/CSE **Section/Group:702_DC-B**
Semester:5th **Date of Performance:12/08/24**
Subject Name: Computer Networks **Subject Code: 22-CSH-312**

1. **Aim:** Implement Data link Layer Protocols such as CSMA,CSMA/CD etc

2. **Requirements(Hardware/Software):**

S/W Requirement :- Packet Tracer
H/W Requirement :-
• Processor – Any suitable Processor e.g. Celeron
• Main Memory - 128 MB RAM
•Hard Disk – minimum 20 GB IDE Hard Disk
• Removable Drives–1.44 MB Floppy Disk Drive
–52X IDE CD-ROM Drive
•PS/2 HCL Keyboard and Mouse

3. **Theory:**

Implementation of Data Link Layer Protocols

1. Data Link Layer Overview

The Data Link Layer (Layer 2) of the OSI model is pivotal in managing how data packets are transferred across a local network. It provides essential functions such as framing, error detection and correction, and flow control, ensuring data integrity and efficient communication between network devices.

- Framing: The Data Link Layer encapsulates packets from the Network Layer into frames. This framing includes adding headers and trailers to the packet to prepare it for transmission over the Physical Layer.
- Error Detection and Correction: It detects and sometimes corrects errors that occur during transmission, ensuring that the data received is accurate and complete.
- Flow Control: This function regulates the rate of data transmission between devices to prevent overwhelming the receiver.
- Access Control: It manages how multiple devices share the same communication medium, ensuring that data is transmitted without interference.

2. Carrier Sense Multiple Access (CSMA) Protocol

Carrier Sense Multiple Access (CSMA) is a protocol used to control access to a shared communication medium. The fundamental principle of CSMA is to reduce collisions by having network devices listen to the channel before transmitting:

- Carrier Sensing: Devices check if the channel is idle or busy before attempting to send data. If the channel is clear, they proceed with transmission.
- Collision Avoidance: If the channel is busy, devices wait for a random period before rechecking the channel and attempting transmission again.

The randomness helps minimize the chance that multiple devices will attempt to transmit at the same time, thereby reducing the likelihood of collisions.

3. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD is an extension of CSMA designed to manage collisions more effectively, primarily in Ethernet networks:

- Collision Detection: While transmitting data, devices also listen to the channel to detect if another device is transmitting simultaneously. If a collision is detected, the transmitting devices halt their transmission.
- Collision Handling: After a collision, the devices involved wait for a random backoff period before attempting to retransmit. This reduces the chance of repeated collisions.

CSMA/CD is effective in wired Ethernet networks where the medium is shared among all devices connected to a hub.

4. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

CSMA/CA is used in wireless networks, such as Wi-Fi, to avoid collisions in environments where collision detection is not feasible:

- Collision Avoidance: Instead of detecting collisions, CSMA/CA tries to prevent them by ensuring that the channel is clear before transmission and using acknowledgment frames to confirm successful data receipt.
- RTS/CTS Mechanism: The Request to Send (RTS) and Clear to Send (CTS) signals are used to reserve the channel before data transmission. This exchange helps manage access to the channel, particularly in scenarios where hidden nodes may exist.

By using these mechanisms, CSMA/CA improves the efficiency of wireless networks and minimizes the likelihood of data collisions.

5. Comparison of CSMA/CD and CSMA/CA

- CSMA/CD: Used in wired Ethernet networks where devices share a common medium (hub). It detects and handles collisions during data transmission. Effective in environments where collision detection is possible.
- CSMA/CA: Used in wireless networks where collision detection is not practical. It employs techniques to avoid collisions before they occur, making it suitable for environments with multiple wireless devices.

4. Procedure:

1. Set Up Network:
- Open Cisco Packet Tracer.
- Add a hub and three PCs to the workspace.
- Connect each PC to the hub using copper crossover cables.

2. Configure IP Addresses:
- On each PC, go to the Desktop tab and select IP Configuration.
- Assign static IP addresses (e.g., PC1: 192.168.1.1, PC2: 192.168.1.2, PC3: 192.168.1.3).

3. Switch to Simulation Mode:
- Click on the Simulation Mode tab to observe data transmission and collision behavior.

4. Initiate Data Transmission:
- Use the Command Prompt on one PC to ping another PC and start data transmission.
- Observe how data frames are transmitted and how collisions are managed by the CSMA/CD protocol.

5. Analyze and Compare:

- Document how the data frames travel through the hub and how collisions are handled.
- If applicable, simulate wireless transmission using CSMA/CA .

5. Output:

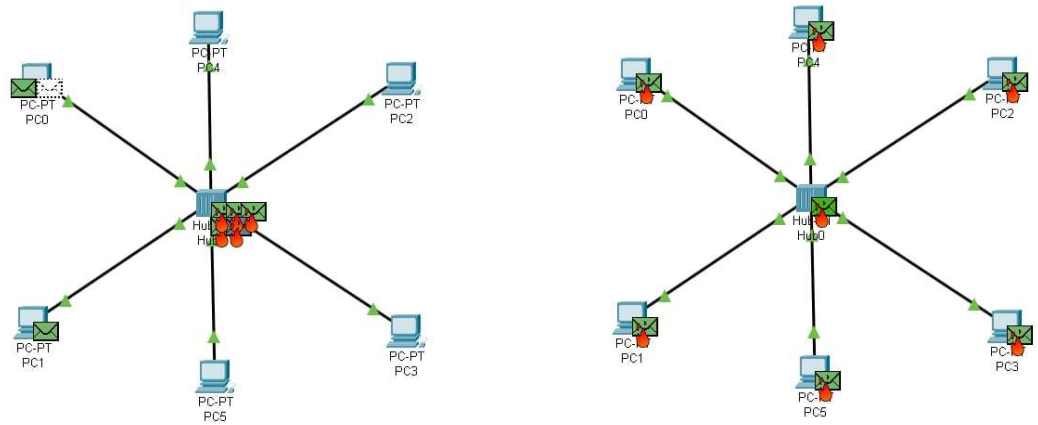

Fig 1. Collision of messages

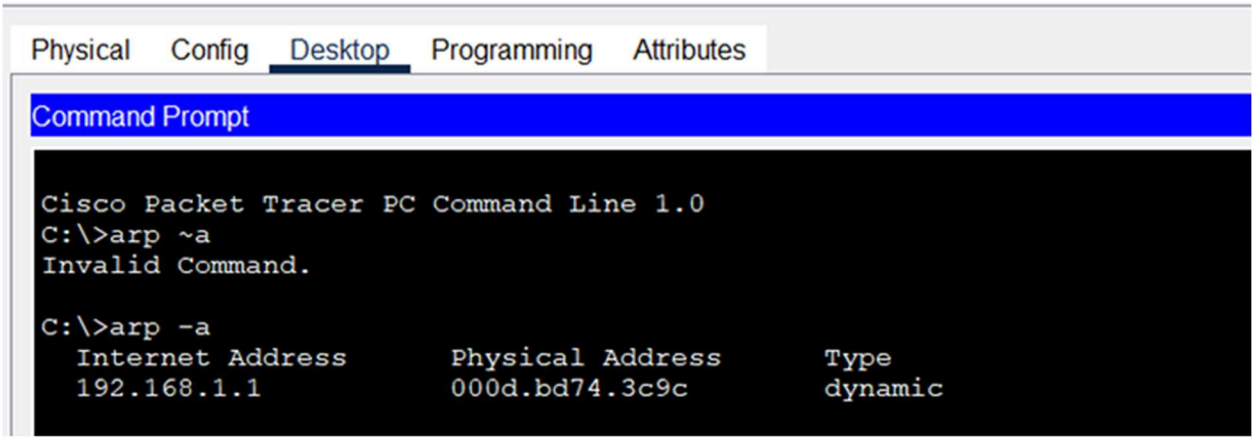

Fig 2. General configuration of PCs

6. Learning Outcome:

1. Understanding Collision Management:

- Gain insight into how CSMA/CD and CSMA/CA protocols manage network collisions and ensure efficient data transmission.

2. Network Device Configuration:

- Learn how to configure network devices and assign static IP addresses using Cisco Packet Tracer.

3. Data Transmission Observation:

- Observe the behavior of data transmission through a hub and understand the impact of shared medium on network performance.

4. Protocol Performance Analysis:

- Compare the performance and efficiency of CSMA/CD in wired networks versus CSMA/CA in wireless networks.

5. Collision Detection and Avoidance:

- Analyze how CSMA/CD handles collisions through detection and retransmission, and how CSMA/CA avoids collisions using RTS/CTS mechanisms.