## **Computer Networks Lab: Exploring Network Behavior with Hubs and Switches**

**Abstract:** This laboratory exercise investigates the fundamental differences in traffic forwarding between network devices operating at Layer 1 (hubs) and Layer 2 (switches). Through packet analysis and observation, we will examine the concept of broadcast domains and the initial learning process of a switch's MAC address table. This lab also introduces the concept of Virtual Local Area Networks (VLANs) as a mechanism for segmenting broadcast domains in switched networks.

**1. Introduction**

This lab explores the basic principles of network communication using hubs and switches. Hubs operate at the physical layer and simply repeat incoming signals out of all other ports. Switches, operating at the data link layer, learn the MAC addresses of connected devices and forward traffic based on this information. Understanding these fundamental differences is crucial for designing and troubleshooting computer networks. This lab also provides a foundational understanding of broadcast domains and the role of VLANs in network segmentation.

**2. Objectives**

Upon completion of this lab, the student will be able to:

* Describe the forwarding behavior of a network hub.
* Describe the initial forwarding behavior of a network switch with an empty MAC address table.
* Identify the devices that receive traffic in a hub-based network.
* Identify the devices that initially receive traffic in a switch-based network.
* Explain the concept of a broadcast domain.
* Determine the number of broadcast domains in a given network topology.
* Understand the basic concept and benefits of VLANs.

**3. Equipment and Software**

* Cisco Packet Tracer software
* The provided Packet Tracer topology file

**4. Procedure**

**4.1 Network 1: Hub-Based Network Analysis**

1. **Topology Verification:** Open the provided Packet Tracer file and examine Network 1. Note the IP addresses assigned to PCs PC1 through PC4 and their connection to the hub (Hub1).
2. **Simulating Reboot:** To ensure all device states are reset, use the "Power Cycle Devices" button in Packet Tracer (if available, otherwise simply restarting the simulation will suffice for this observation).
3. **Pinging from PC1 to PC4:** Initiate a ping from PC1 to PC4 (IP address 10.1.1.4) using the command prompt on PC1: ping 10.1.1.4.
4. **Packet Analysis (Simulation Mode):** Switch to Simulation Mode in Packet Tracer. Observe the first packet generated by PC1.  
   * **Question 1:** When PC1 pings PC4, what type of packet is sent to the hub initially? Can you prove it?  
     + **Proof:** The initial packet generated by a ping command is an **ICMP Echo Request** packet. You can verify this by examining the details of the packet in the Simulation Event List. Look for the "Details" column for the first event initiated by PC1. The OSI Layer 3 PDU (Protocol Data Unit) will show information about the ICMP protocol and the "Echo Request" type.
   * **Question 2:** Who receives the packet?  
     + **Proof:** In Simulation Mode, observe the animation of the packet leaving PC1 and arriving at the hub (Hub1). Then, observe where the hub forwards this packet. You will see that the hub **floods** the incoming packet out of all its other ports. Therefore, **PC2, PC3, and PC4** will receive a copy of the ICMP Echo Request packet.
   * **Question 3:** Who receives the return traffic from PC4 to PC1?  
     + **Proof:** When PC4 receives the ICMP Echo Request, it generates an **ICMP Echo Reply** packet destined for PC1 (10.1.1.1). Observe the simulation as this packet travels from PC4 to the hub. The hub will again **flood** this packet out of all its other ports. Therefore, **PC1, PC2, and PC3** will receive the return traffic.
   * **Question 4:** When ping traffic is sent from PC1 to PC4, who receives the traffic?  
     + **Proof:** As demonstrated in the previous steps, the initial ICMP Echo Request from PC1 is received by **PC2, PC3, and PC4**. The subsequent ICMP Echo Reply from PC4 is received by **PC1, PC2, and PC3**.

**4.2 Network 2: Switch-Based Network Analysis**

1. **Topology Verification:** Examine Network 2. Note the IP addresses of PCs PC5 through PC8 and their connection to the switch (Ashish Switch).
2. **Simulating Reboot:** Again, use the "Power Cycle Devices" button or restart the simulation to clear the switch's MAC address table.
3. **Pinging from PC5 to PC8:** Initiate a ping from PC5 to PC8 (IP address 10.1.1.8) using the command prompt on PC5: ping 10.1.1.8.
4. **Packet Analysis (Simulation Mode):** Switch to Simulation Mode and observe the first packet generated by PC5.  
   * **Question 5:** Assume that the Switch's MAC address table is empty. When PC5 pings PC8, what type of packet is sent to the switch initially? Can you prove it?  
     + **Proof:** Similar to the hub-based network, the initial packet generated by the ping command is an **ICMP Echo Request** packet. Examine the packet details in the Simulation Event List to confirm the OSI Layer 3 PDU and ICMP type. The destination MAC address in the Layer 2 header will be the broadcast MAC address (FF:FF:FF:FF:FF:FF) because PC5's Address Resolution Protocol (ARP) process will not yet know the MAC address of PC8 (assuming no prior communication).
   * **Question 6:** Who receives the packet?  
     + **Proof:** With an empty MAC address table, the switch doesn't yet know the location of PC8's MAC address. Therefore, upon receiving the ICMP Echo Request, the switch will **flood** the packet out of all its other ports (except the port it received it on). Thus, **PC6, PC7, and PC8** will receive the initial ICMP Echo Request. The switch will also learn the MAC address of PC5 and the port it is connected to and record this in its MAC address table.
   * **Question 7:** Who receives the return traffic from PC8 to PC5?  
     + **Proof:** When PC8 receives the ICMP Echo Request, it generates an ICMP Echo Reply destined for PC5. The destination IP address is 10.1.1.5, and now PC8 will know the MAC address of PC5 (it would have learned it from the broadcast ICMP request or a prior ARP request). The switch, having learned the MAC address of PC5 in the previous step, will now **forward** the ICMP Echo Reply **only to the port connected to PC5**. Therefore, only **PC5** will receive the return traffic.
   * **Question 8:** When ping traffic is sent from PC5 to PC8, who receives the traffic?  
     + **Proof:** The initial ICMP Echo Request (due to an empty MAC table) is received by **PC6, PC7, and PC8**. The subsequent ICMP Echo Reply is received only by **PC5**. For subsequent pings between PC5 and PC8, the switch will forward the traffic directly between the ports connected to these two PCs, and no other devices will receive it.

**4.3 Broadcast Domains**

* **Question 9:** How many broadcast domains are there in Network 1? Can you prove it?
  + **Proof:** In a hub-based network, all devices connected to the hub share the same collision domain and the same broadcast domain. When a broadcast frame is sent by one device, the hub repeats it out of all other ports, and every connected device receives it. Therefore, **Network 1 has one broadcast domain**. You can prove this by initiating a broadcast (e.g., an ARP request) from any PC in Network 1 in Simulation Mode and observing that all other PCs in Network 1 receive it.

**5. Discussion**

This lab highlighted the fundamental differences in how hubs and switches handle network traffic. Hubs act as simple repeaters, leading to a single broadcast domain and potential collisions. Switches, on the other hand, learn MAC addresses and forward traffic more intelligently, limiting the scope of broadcast domains implicitly.

The concept of a broadcast domain is crucial for network design. Large broadcast domains can lead to increased network congestion and reduced efficiency due to unnecessary broadcast traffic being sent to all devices. VLANs provide a mechanism to create multiple logical broadcast domains within a single physical switch, improving network performance, security, and organization. By logically grouping ports into different VLANs, broadcast traffic is contained within that specific VLAN. While not explicitly configured in this lab, the presence of a multilayer switch in Network 2 indicates the capability for VLAN implementation in future network expansions.

**6. Conclusion**

This lab provided a practical understanding of basic network connectivity and the behavior of hubs and switches. We observed the broadcast nature of hubs and the initial learning process of a switch. Furthermore, we introduced the concept of broadcast domains and the importance of VLANs in segmenting these domains for better network management and efficiency.

**7. Further Exploration**

Experiment with sending different types of traffic (e.g., ARP requests) in both networks and observe the behavior.

* Research the limitations of hubs in modern network environments.
* Investigate how switches handle unknown destination MAC addresses after the initial flooding.
* In a future lab, explore the configuration and benefits of VLANs on the multilayer switch in Network 2.