Packet Flow Analysis

Methodology

1. Network Devices

- The packet flow analysis involves examining network devices within the college network. Key devices include routers, switches, and end-user devices.

2. Packet Capture

- Packet capture was performed using the built-in sniffer in Cisco Packet Tracer. Each device's packet capture settings were configured to collect data for analysis.

3. Packet Headers

- Analysis of packet headers revealed crucial information. Ethernet headers provided details on MAC addresses, while IP headers showcased changes in source and destination IP addresses.

4. Changes and Alterations

- Notable changes in packet headers occurred as packets traversed routers, indicating routing decisions and changes in network segments.

Findings

1. Path of Packet Flow

- The packet flow originated from student devices, passed through switches, and traversed routers before reaching the external network.

2. Layered Analysis

- Observations aligned with the OSI model layers. Ethernet headers pertained to Layer 2, while IP headers reflected Layer 3 routing decisions.

3. Network Design Impact

- The packet flow analysis provided insights into the efficiency of the network design, emphasizing the role of routers in directing traffic.

Observations

1. Curvature and Direction

- No significant curvature was observed, indicating a well-designed network. Directional changes were evident at routers, influencing the packet's path.

2. Layer 3 Device Impact

- Layer 3 devices (routers) played a crucial role in determining the packet's route. Changes in IP headers highlighted the impact of routing decisions.

Conclusion

The packet flow analysis unveiled the efficient design of the college network, emphasizing the importance of routers in directing traffic. Understanding changes in packet headers provides valuable insights into network behavior.