COL334 Assignment 3

Abhinav Rajesh Shripad Entry Number: 2022CS11596
Jahnabi Roy Entry Number: 2022CS11094

October 6, 2024

Part 1: Controller Hub and Learning Switch

Flow Table Comparison

Switch Rules

- **Comparison from Switch S1**

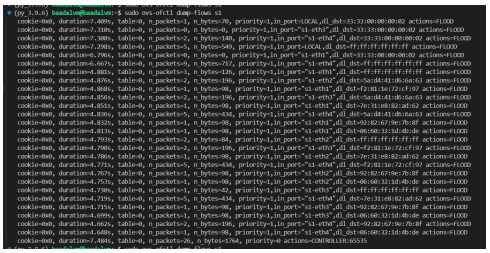

Figure 1: S1 - Hub Controller

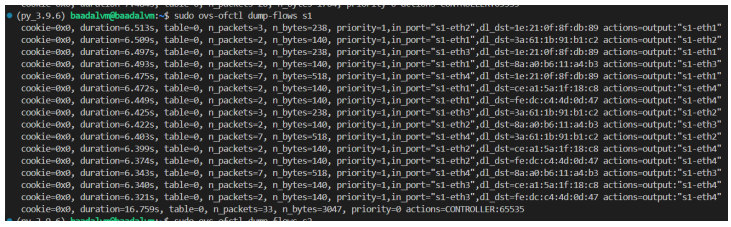

Figure 2: S1 - Learning Switch

- **Comparison from Switch S2**

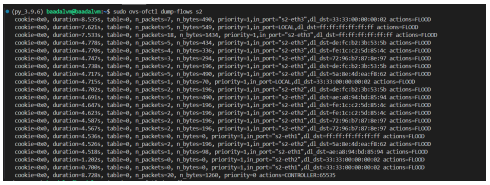

Figure 3: S2 - Hub Controller

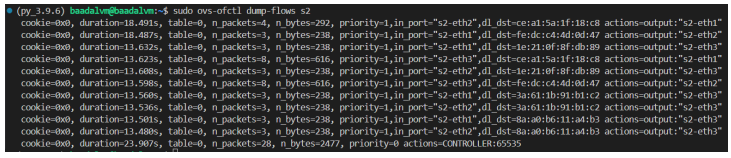

Figure 4: S2 - Learning Switch

- The flow rules indicate hub controller behavior, with all actions being either "FLOOD" or "CONTROLLER," meaning packets are either flooded to all ports or sent to the controller.
- The use of "FLOOD" actions confirms that the switches behave like hubs, flooding traffic to all ports irrespective of the destination. This ensures full connectivity but leads to inefficient network utilization.
- A hub controller floods traffic without learning MAC addresses, unlike a learning switch, which creates forwarding rules based on MAC addresses.
- In learning switch mode, both S1 and S2 have learned the MAC addresses of all hosts and created specific flow entries, forwarding packets to appropriate ports.
- S1 directs traffic to H1-H3 via specific ports, and traffic to H4-H5 through the link to S2 (S1-eth4).
- S2 directs traffic to H4-H5 via specific ports and traffic to H1-H3 through the link to S1 (S2-eth3).
- Both switches have a default rule (priority=0) that sends unmatched packets to the controller, allowing them to learn new MAC addresses and update their flow tables.
- Unlike the hub controller, the learning switch forwards packets to the necessary ports, reducing latency after the learning phase.

Comparing Bandwidth

- **Hub Controller and Learning Switch Bandwidth Calculations using iperf**

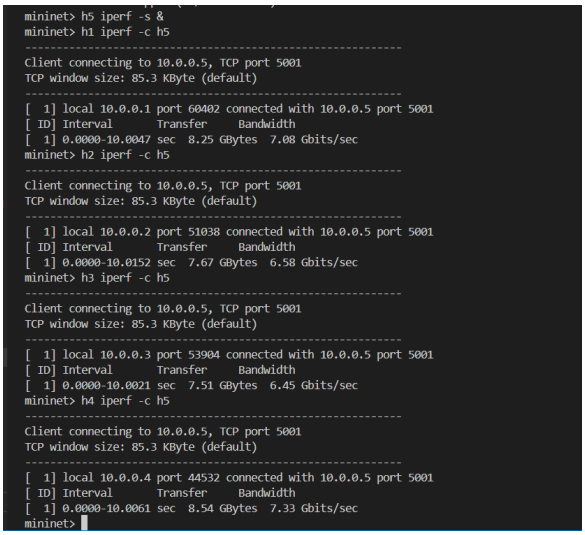

Figure 5: Hub Controller Bandwidth

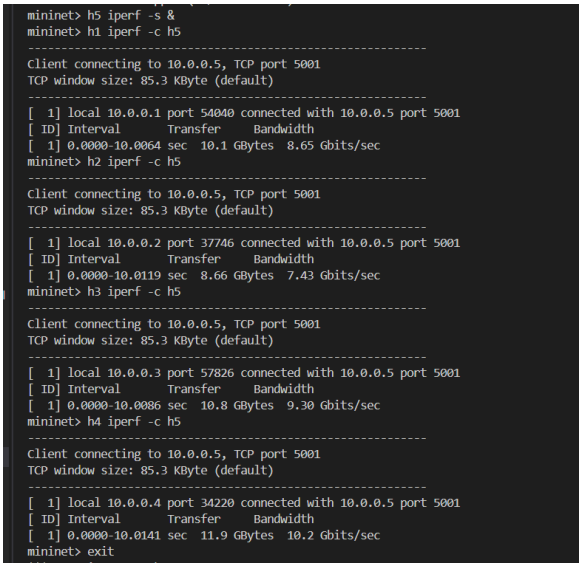

Figure 6: Learning Switch Bandwidth

Host Pair	Learning Switch (Gbits/sec)	Hub Controller (Gbits/sec)
H1 to H5	8.65	7.08
H2 to H5	7.43	6.58
H3 to H5	9.30	6.45
H4 to H5	10.2	7.33

Table 1: Throughput Results for Learning Switch and Hub Controller

- The learning switch shows higher average throughput than the hub controller.
- Throughput variability is higher in the learning switch due to network paths and forwarding decisions.
- H4 to H5 (same switch) has the highest throughput (10.2 Gbits/sec) in the learning switch, as no inter-switch link is needed.
- The learning switch utilizes network capacity more efficiently, achieving throughput closer to the theoretical maximum.

Pingall

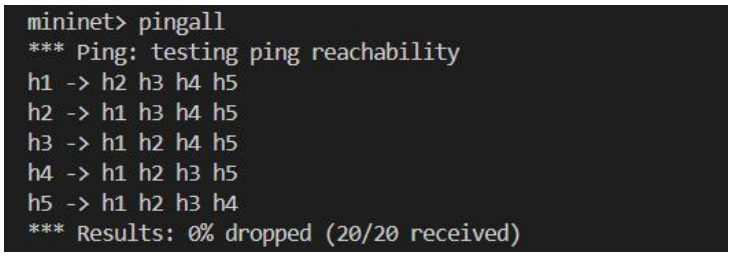

Figure 7: Pingall Result

Part 2: Spanning Tree and MAC Address Learning

A spanning tree ensures that all switches in a network are connected in a loop-free topology. This ensures no packet is forwarded to multiple ports and the bandwidth gets lost.

Spanning Tree Formation

The formation of a spanning tree begins by identifying all the links (edges) between the switches. These edges represent the physical connections between the switches in the network. Once the complete set of links is available, we use BFS with neglecting the back edges to compute a spanning tree. The goal of this step is to create a tree that connects all switches while avoiding loops. This is $O(n + m)$ process where n is the number of switches and m is number of links between them.

Creating Forwarding Table

After the spanning tree is established, for each switch (say s_i) we traverse along the spanning tree and for each switch (say s_j) on out path, we update the forwarding table for s_i on which port to forward to reach s_j . Here we must run this process for all s_i and each process will take $O(n)$, the whole step will take $O(n^2)$.

Blocked Ports

The ports on a switch which are not the part of the spanning tree, we add them to the list of blocked ports on this switch.

Learning Process

Upon receiving a frame, the switch records the source MAC address and the port through which the frame arrived. This process, known as *MAC address learning*, allows the switch to associate each MAC address with a specific port. As a result, when future frames are destined for that MAC address, the switch knows exactly which port to forward the frames to.

Forwarding Decision

When the switch receives a frame that is destined for a specific MAC address, it consults its forwarding table. If the destination MAC address is found in the table, the switch forwards the frame only to the corresponding port. This prevents the frame from being flooded across all ports, which would consume unnecessary bandwidth and create inefficiencies in the network. If no port is found for the destination address, we flood the message on each port of the switch except the input port and the blocked ports.

```
Forwarding Table: {1: {4: 3, 2: 2, 3: 2}, 2: {1: 2, 4: 2, 3: 3}, 3: {2: 2, 1: 2, 4: 2}, 4: {1: 3, 2: 3, 3: 3}}
Blocked Ports: {3: {3}, 4: {2}}
```

Figure 8: Forwarding Table and the blocked ports on the sample topology

```
*** Ping: testing ping reachability
h1 -> h2 h3 h4
h2 -> h1 h3 h4
h3 -> h1 h2 h4
h4 -> h1 h2 h3
*** Results: 0% dropped (12/12 received)
mininet>
```

Figure 9: Successful pingall in p2_topo

Part 3: Shortest Distance Routing

Shortest distance routing ensures that data packets are forwarded along the most efficient paths in a network, minimizing latency.

Cost Metrics Calculation

We measure the link delays in each link and this denotes the edge of the weights on our graph. We use LLDP Packets for this.

Routing Table Formation

For each switch we apply Dijkstra's algorithm to compute the shortest paths to other switches. We then update the port on which to forward the packet if one wants to reach a particular switch. Each run of Dijkstra's Algorithm takes $O(n \log(n))$, thus the total process takes $O(n^2 \log(n))$

Learning Process

Upon receiving a frame, the switch records the source MAC address and the port through which the frame arrived. This process allows the switch to associate each MAC address with a specific port.

Forwarding Decision

When a router receives a data packet, it checks the destination MAC address and consults its routing table. If the destination address is found in the table, the router forwards the packet to the corresponding next-hop address. This targeted forwarding prevents unnecessary flooding of packets across the network, thereby conserving bandwidth and improving efficiency.

If the destination address is not in the routing table, the packet may be sent to a default gateway or dropped, depending on the configuration of the routing protocol and the network policy.

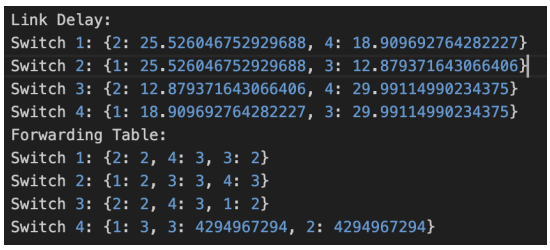

Figure 10: Forwarding Table and Link Delays

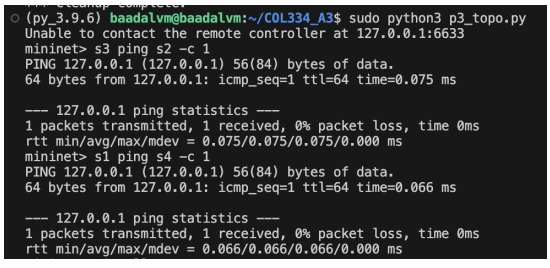

Figure 11: Switches Successful Pings

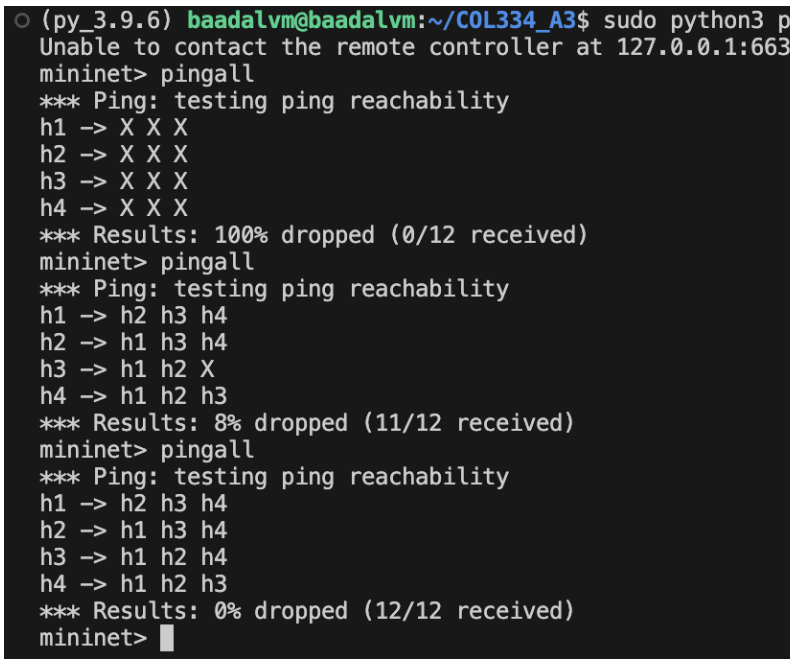

Figure 12: Hosts Learning Process and Eventual Successful Ping

Part 4: Congestion-aware Shortest Path Routing

Shortest distance routing ensures that data packets are forwarded along the most efficient paths in a network, minimizing latency.

Cost Metrics Calculation

We measure the link delays in each link and this denotes the edge of the weights on our graph. We update the link delays at a periodic interval of 30 seconds. We use **EMA(Exponential Moving Average)** to calculate the link delays with the parameter $\alpha = 0125$

Routing Table Formation

For each switch we apply Dijkstra's algorithm to compute the shortest paths to other switches. We then update the port on which to forward the packet if one wants to reach a particular switch. Each run of Dijkstra's Algorithm takes $O(n \log(n))$, thus the total process takes $O(n^2 \log(n))$

Blocked Ports

The ports on a switch which are not use to reach any other switch, we add them to the list of blocked ports on this switch.

Learning Process

Upon receiving a frame, the switch records the source MAC address and the port through which the frame arrived. This process, known as **MAC address learning**, allows the switch to associate each MAC address with a specific port. As a result, when future frames are destined for that MAC address, the switch knows exactly which port to forward the frames to.

Forwarding Decision

When a router receives a data packet, it checks the destination IP address and consults its routing table. If the destination address is found in the table, the router forwards the packet to the corresponding next-hop address. This targeted forwarding prevents unnecessary flooding of packets across the network, thereby conserving bandwidth and improving efficiency.

If the destination address is not in the routing table, the packet may be sent to a default gateway or dropped, depending on the configuration of the routing protocol and the network policy.