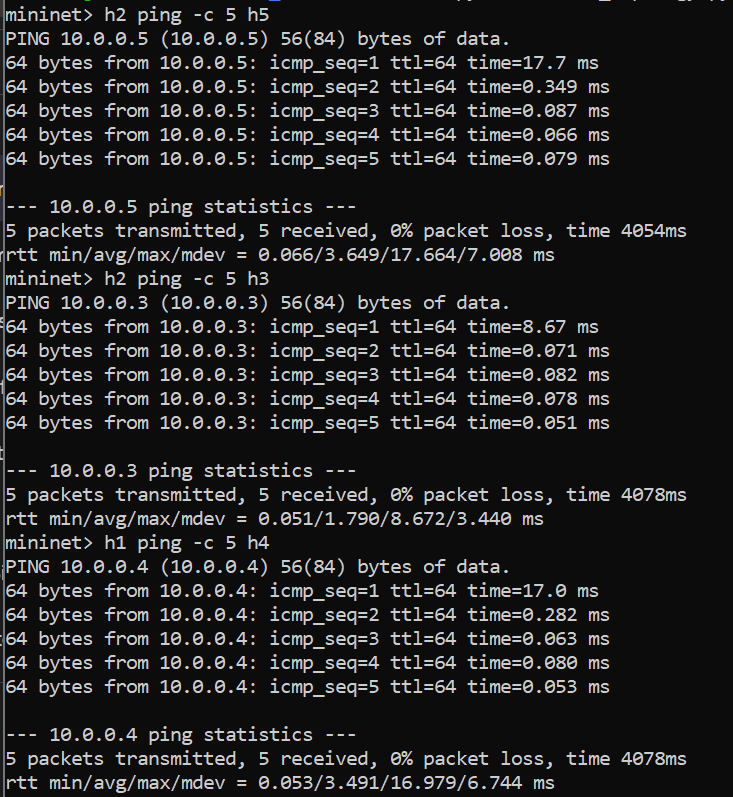
**Programming Assignment 3: SDN and Ryu**

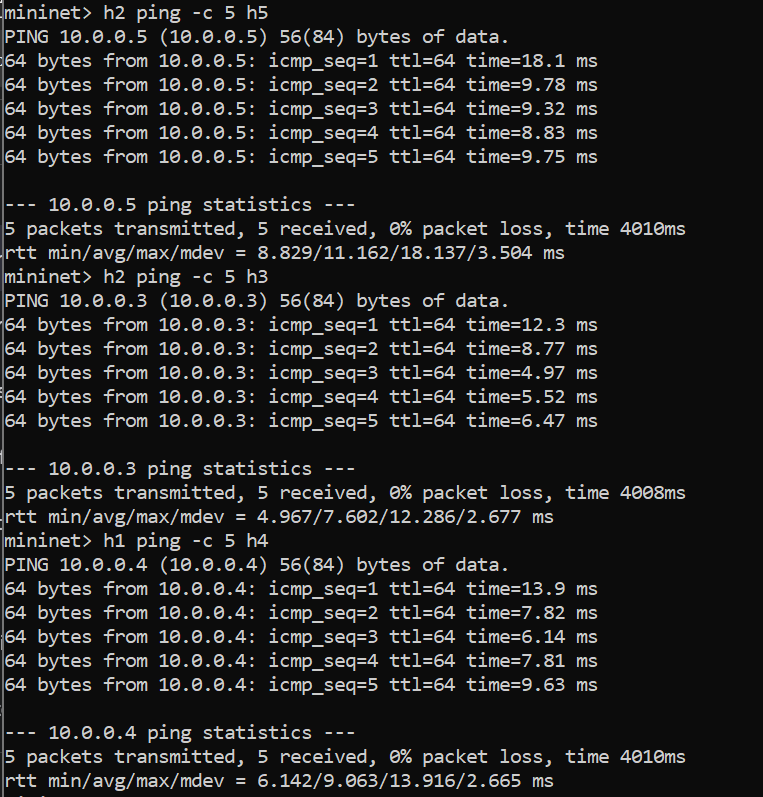
**(jcs232542- SHARATH KUMAR REDDY GANDHAM)**

**Part 1:**

For Learning\_switch:



For Controller\_hub:

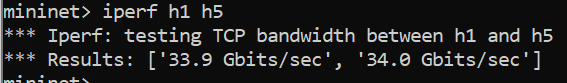


Here we can observe that the latencies for the learning switch are much smaller than the controller hub because the controller hub needs to use the controller to find the way to send the received packet, which overheads the hub to send the packet. Here it does not store anything about the hosts.

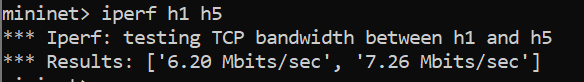
Whereas in the learning switch(it uses layer2 mechanism) at every first-time learning switch also does the same thing done by the hub, but for the next subsequent packets of the same destination it just sends the packet directly without any delay or overhead because here it stores the previous path to send.

**Throughput test:**

Learning Switch:



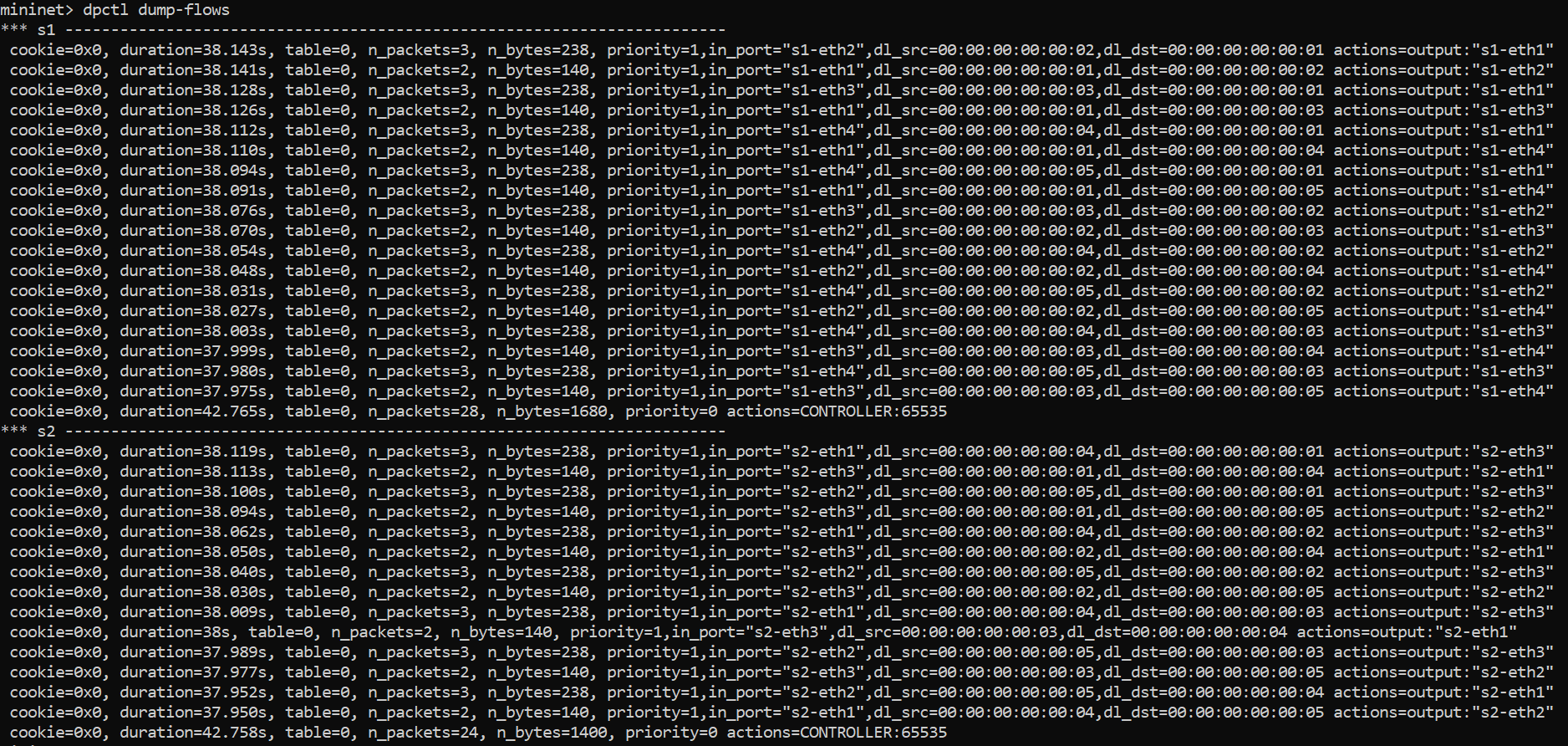
Controller Hub:



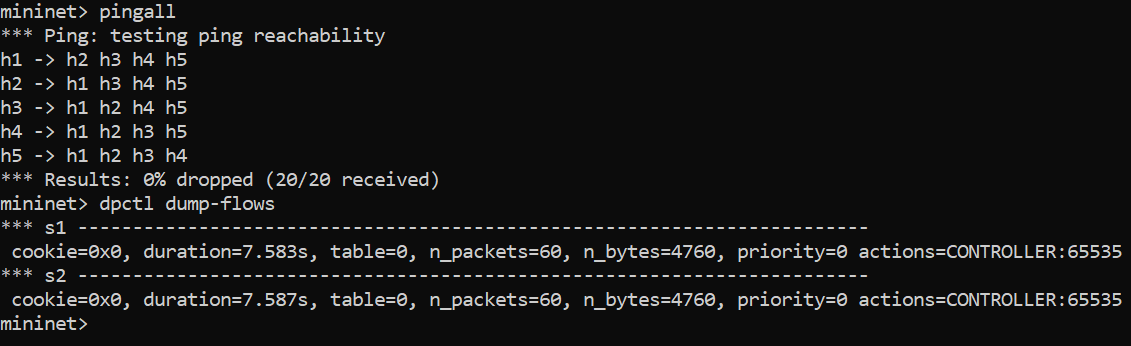
The Learning Switch offers higher local network performance due to its efficient, decentralized operation, while the Controller Hub introduces lower performance but provides more centralized control

After ping all the rules installed:

**Learning\_switch:**

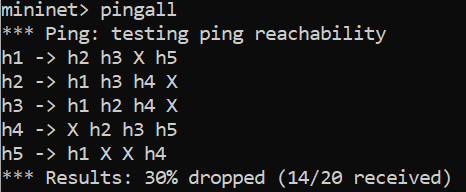


**Controller\_hub:**

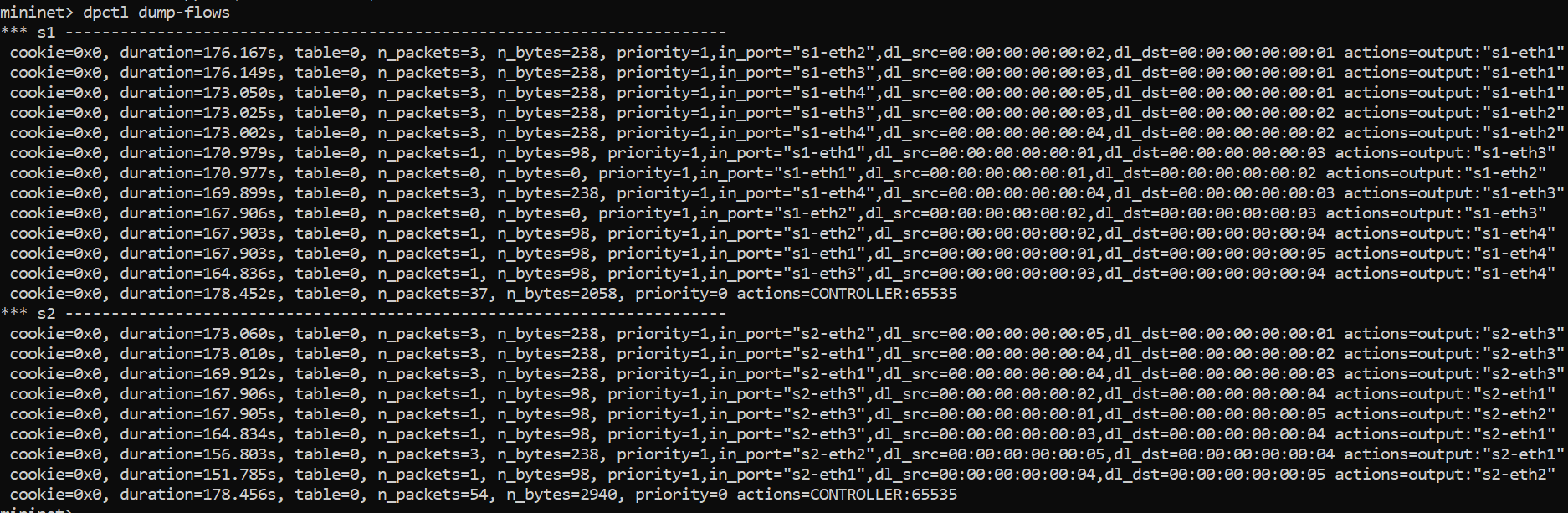


**part-2:**

Firewall and moniter:



**Installed Rules in both switches:**



By the following way we can minimize the number of rules in firewall:

Wildcard Rules: Instead of having specific rules for each pair of IP addresses that you want to block, consider having wildcard rules that cover multiple IP addresses. For example, you can create rules to block entire subnets or address ranges. This reduces the number of rules required.

Use Regular Expressions: Some SDN controllers and switches support regular expressions for matching IP addresses. This allows you to create more flexible and concise rules for blocking traffic.

Rate-Limiting: Instead of blocking traffic completely, you can use rate-limiting to restrict the amount of traffic that can flow between certain IP address pairs. This way, you can avoid creating extensive block rules.

Consolidate Rules: If you have multiple IP address pairs to block that share common characteristics or patterns, you can consolidate them into a single rule. This can be achieved by specifying multiple source or destination addresses in a single rule.

Blacklists and Whitelists: Consider maintaining a dynamic blacklist and whitelist of IP addresses. Instead of static rules, update these lists in real-time based on network activity and policies.

Security Groups or Zones: Group devices into security groups or zones with common characteristics. Apply rules at the group level rather than per device, reducing the number of rules.

Use Layer 4 Rules: If your switch supports layer 4 (transport layer) rules, you can create rules based on ports and protocols, which can be more concise than IP address-based rules.

Prioritize Rules: If you have a large number of rules, prioritize them based on the importance of the traffic. Higher-priority rules can be checked first, and lower-priority rules only if the higher-priority rules don't match.

Rule Optimization: Periodically review and optimize your firewall rules. Remove outdated rules and consolidate rules where possible.

Dynamic Rule Management: Implement dynamic rule management based on policies and security events. This can automatically create or remove rules as needed.

Security Groups: Group devices based on their function or role, and apply firewall rules at the group level. This can reduce the number of rules by applying them to multiple devices at once.