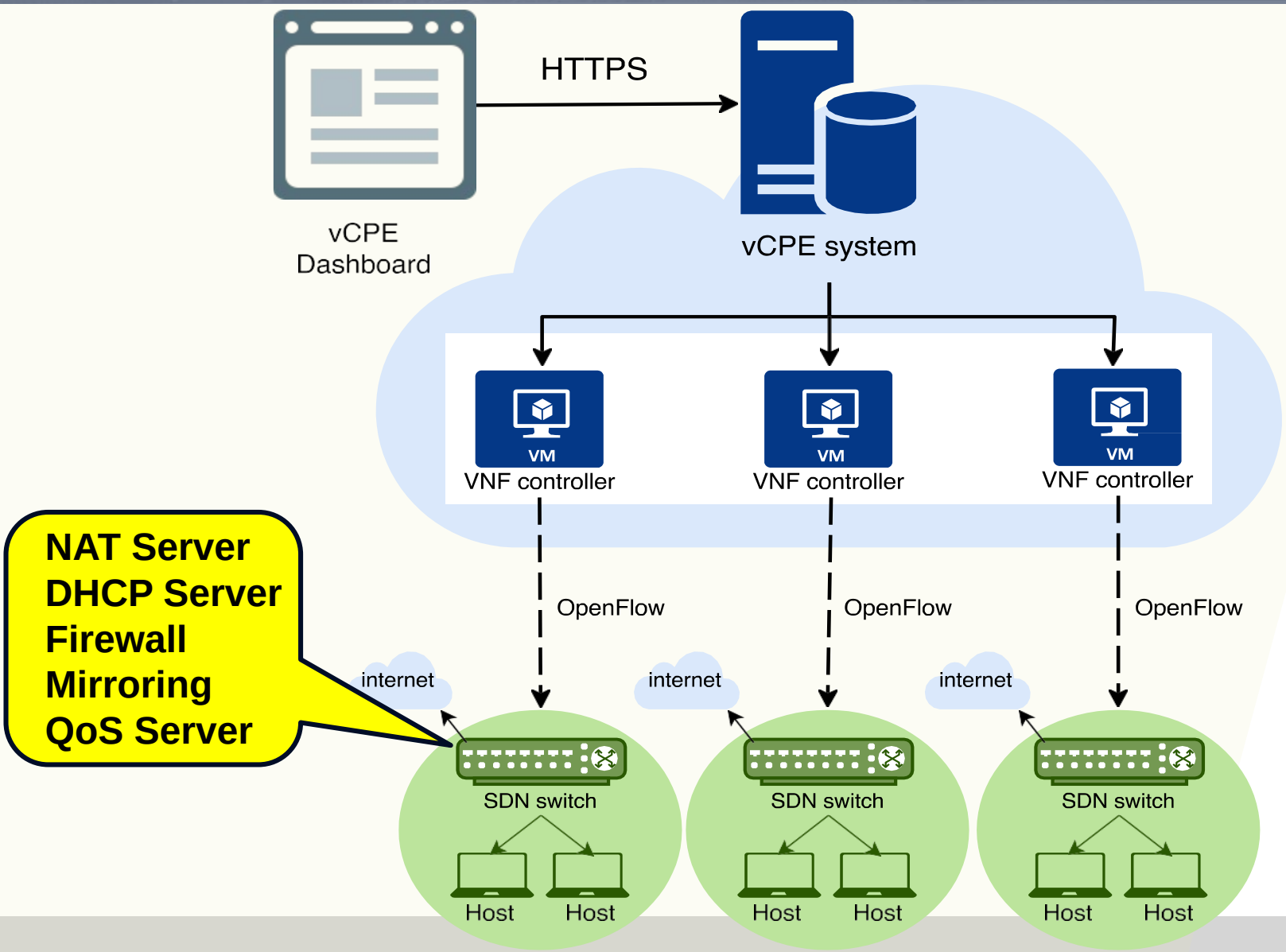
A Novel vCPE Framework for Enabling Virtual Network Functions with Multiple Flow Tables Architecture in SDN Switches

Nen-Fu Huang, Chi-Hsuan Li, Chia-chi Chen, I-Hsien Hsu, Che-Chuan Li, Ching-Hsuan Chen
Department of Computer Science, National Tsing Hua University,
Hsinchu, Taiwan
Seoul, Korea, APNOMS 2017

Outline

- Introduction
- System Design and Implementation
- Experimental Results
- Conclusion

Virtual CPE Platform System Overview



Introduction(1/2)

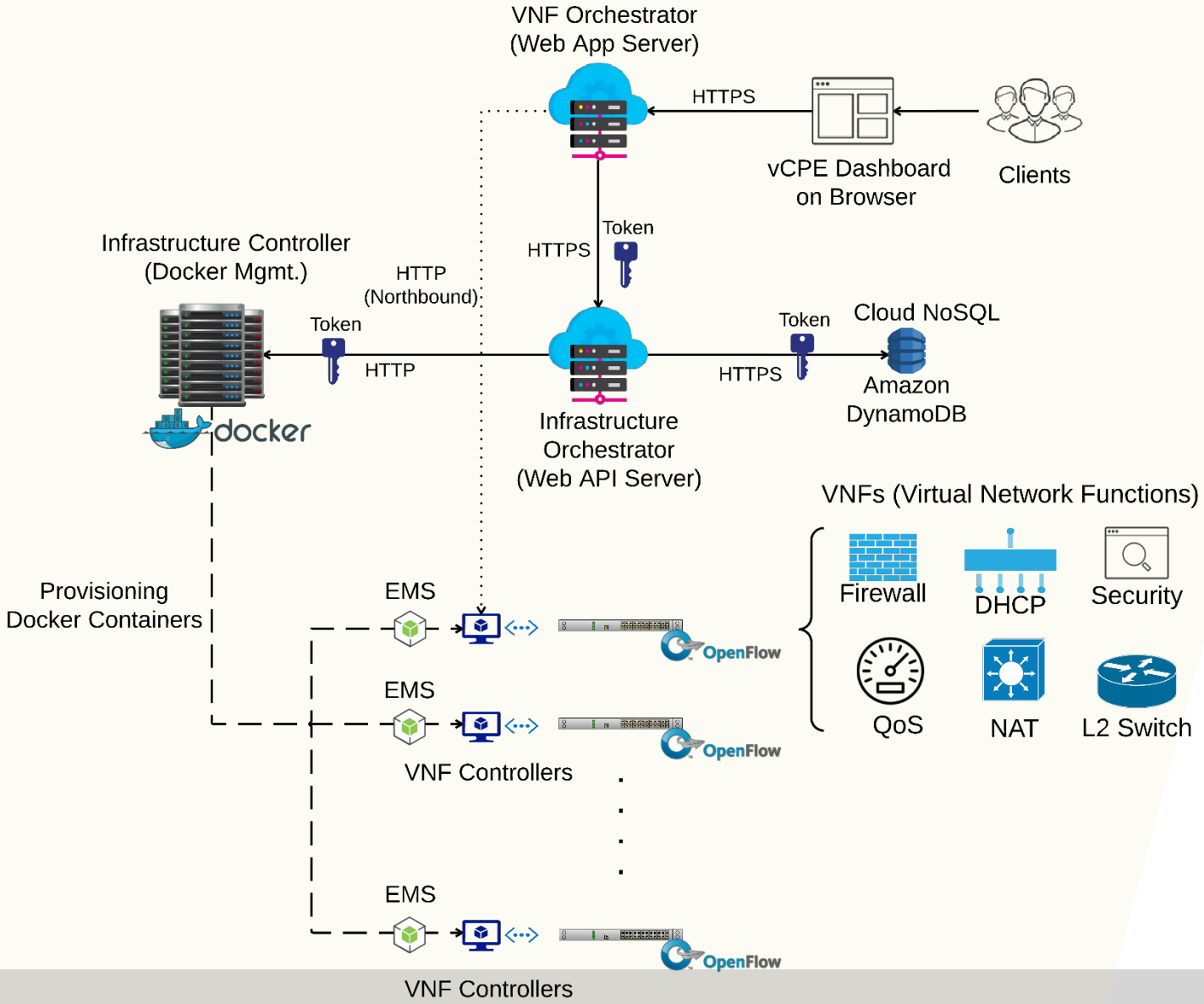
❖ Motivation

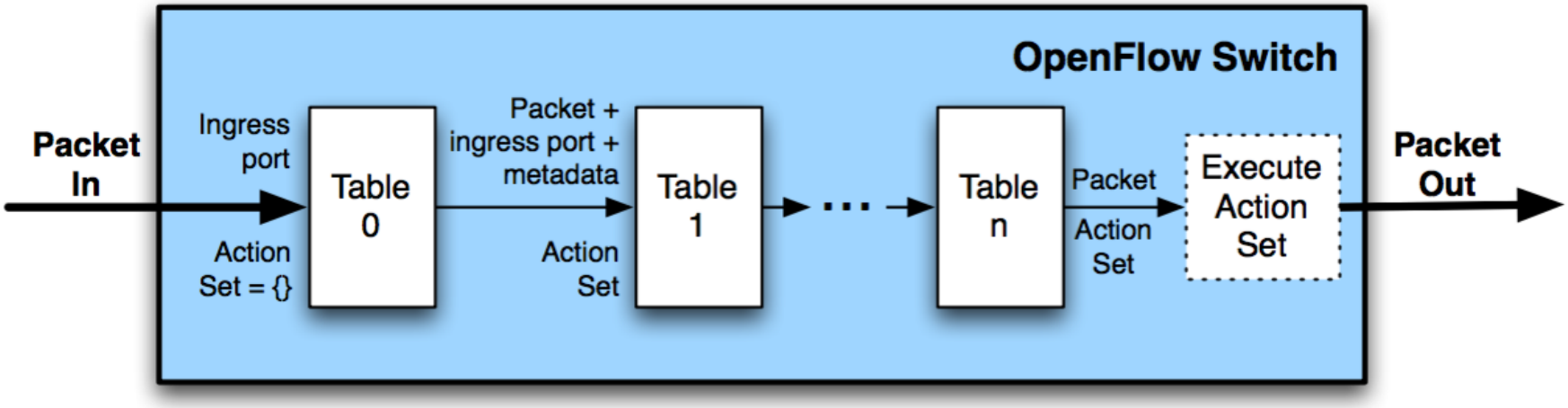
- When the vCPE network functions, such as firewall, NAT, DHCP, forwarding, traffic mirroring, and QoS (bandwidth) management are performed by an SDN switch, we usually face the restrictions of Single Flow Table:
  - (1) Network functions involve performing independent actions based on matching different fields of packet.
  - (2) The incoming packet may require two-stage processing (or even more stages).

Introduction(2/2)

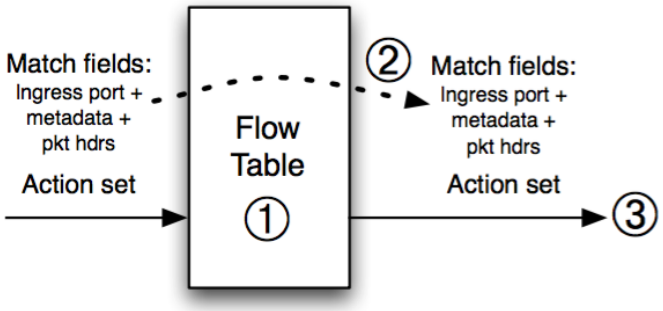
- **The main contributions of this paper are**
  - **A multiple flow table (MFT) mechanism is proposed to implement network functions in the SDN switch.**
  - **The proposed CPE provides several functions: firewall, NAT, DHCP, forwarding, traffic mirroring, and QoS management at the same time.**
  - **Compared to the single-table mechanism, the performance of the proposed MFT mechanism is still good.**

Virtual CPE Platform System Overview





Packets are matched against multiple tables in the pipeline.



① Find highest-priority matching flow entry

② Apply instructions:
- i. Modify packet & update match fields (apply actions instruction)
- ii. Update action set (clear actions and/or write actions instructions)
- iii. Update metadata

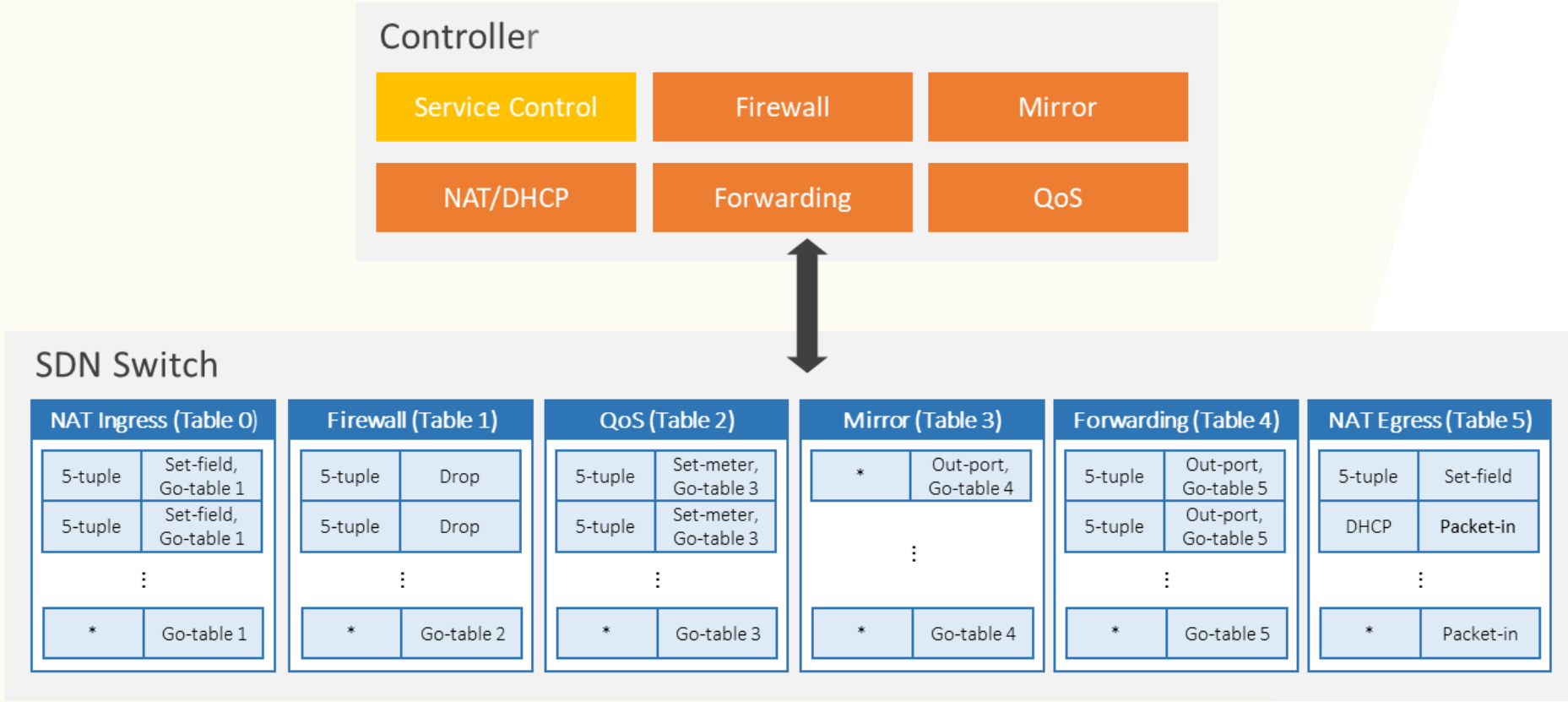
③ Send match data and action set to next table

The workflow of handling packet through the pipeline

System Design and Implementation

- **Service Control in the proposed MFT mechanism**
- **Network Services**
  - **NAT**
  - **Firewall**
  - **Forwarding**
  - **Mirroring**
  - **QoS (bandwidth) management**

Multiple Flow Tables Mechanism

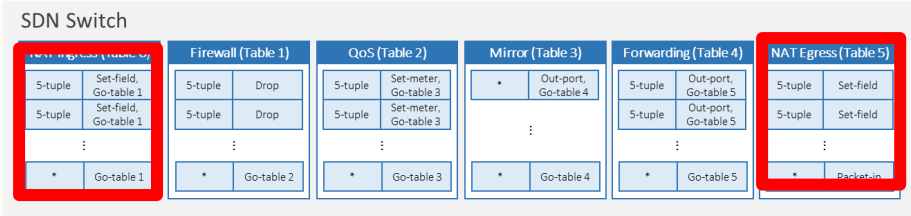


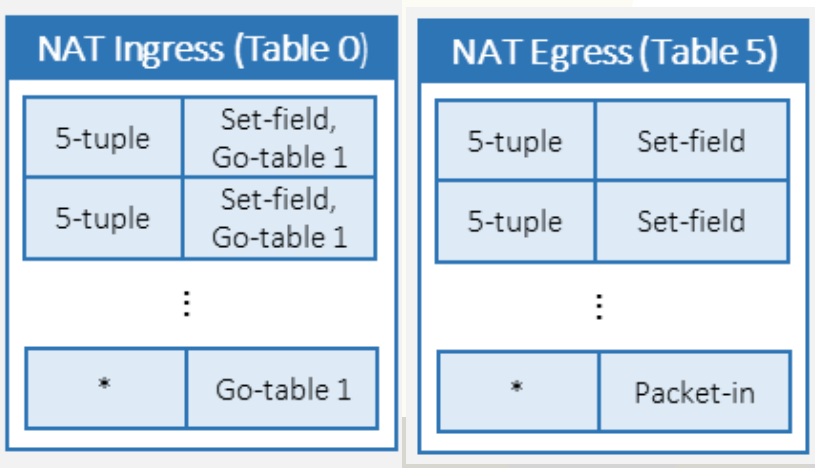
Service Control

- Our MFT mechanism is achieved by the **table-miss rules with GOTO-TABLE action**, which enables the packets to **pass through all active services.**
- **Disable a service**
  - **Add a force-ignoring rule (highest priority) into the table of the service.**
- **Enable a service**
  - **Remove the force-ignoring rule.**

NAT

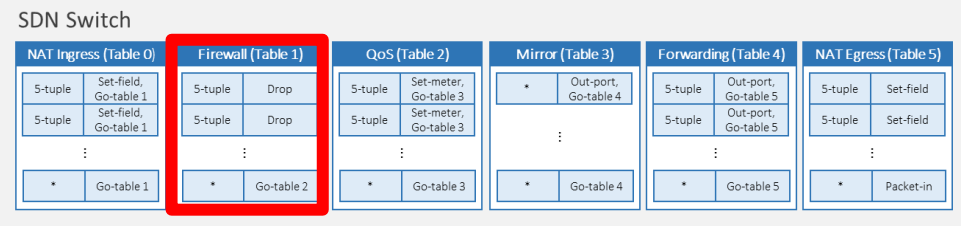
- For a new connection:
  1. The first outgoing packet doesn't match any flow entry in SDN switch, so it will be sent to controller by the PACKET-IN action in the last table.
  2. The controller will modify the source IP to public IP and the source port to an un-used port.
  3. Then, the controller will send a pair of rules to SDN switch: one is for egress traffic and the other is for ingress traffic.

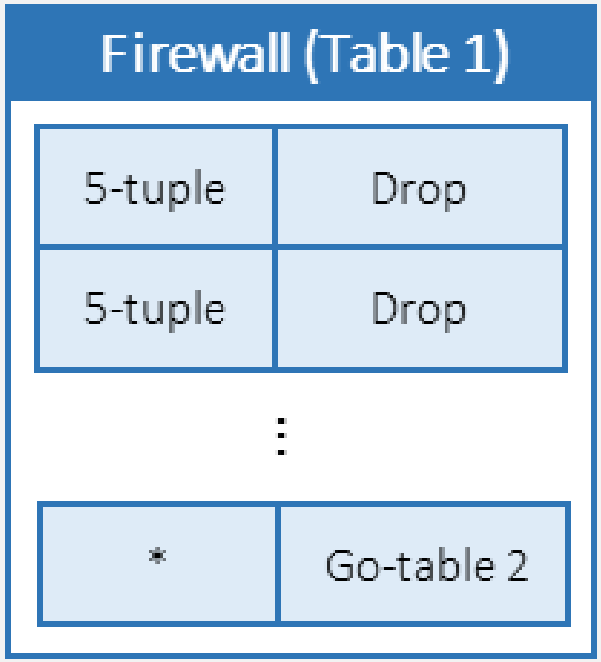




Firewall

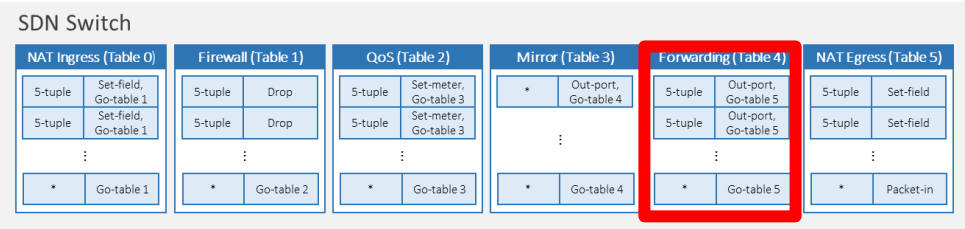
- The firewall service is located in flow table 1 because once packets are detected by the blocking rules, they are immediately dropped.
- The other unblocked packets satisfy the table-miss rule
  - go on to the next flow table.

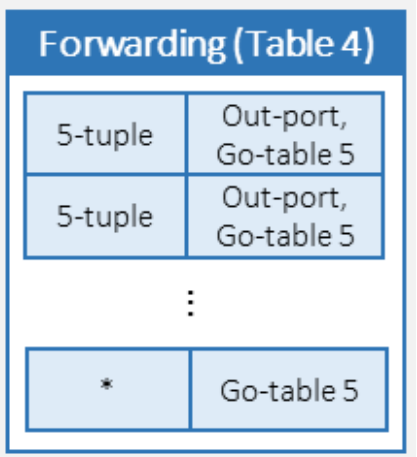




Forwarding

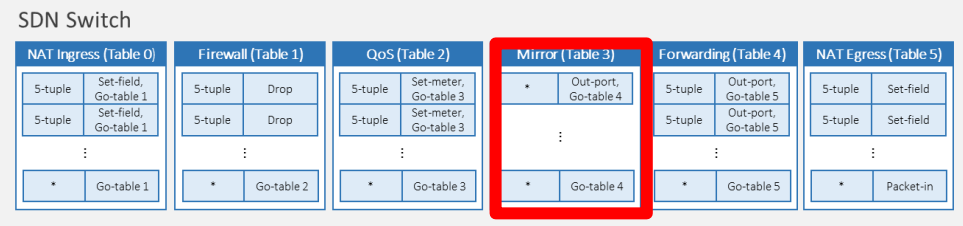
- **For a new connection**
  1. **The first packet PACKET-IN to controller.**
  2. **When the controller receives the packet, it records the IP-layer information to build up topology records:**
     - **(source IP, destination IP, input port , source MAC, destination MAC)**
  3. **The controller can install a 5-tuple forwarding rule with OUT-PORT action for this connection to gather per-session information**
     - **(source IP address, destination IP, Transport layer protocol, source port, and destination port).**

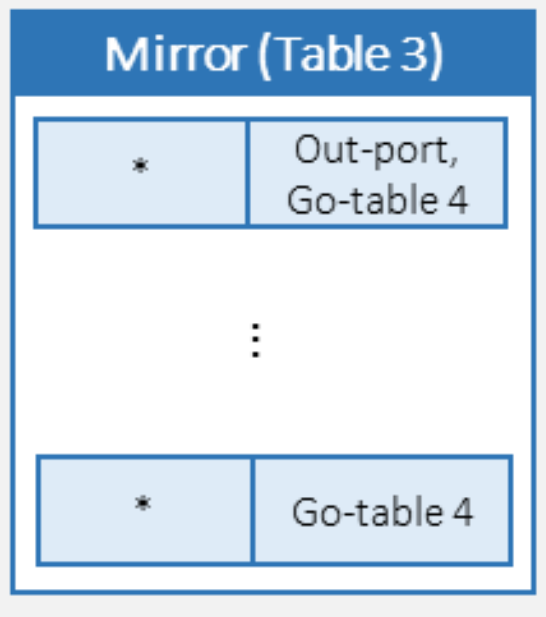




Traffic Mirror

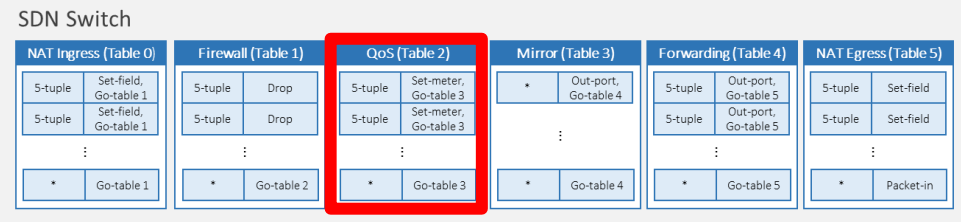
- A wildcard match with **OUT-PORT action** to make all packets mirroring to mirror port.
- We mirror the packet flow to a **flow classification system** for identifying the application (such as Line, FileZilla, WeChat, Youtube, Spotify, Skype, on line games, …)
- The QoS service then uses the classified result to limit the application bandwidth.

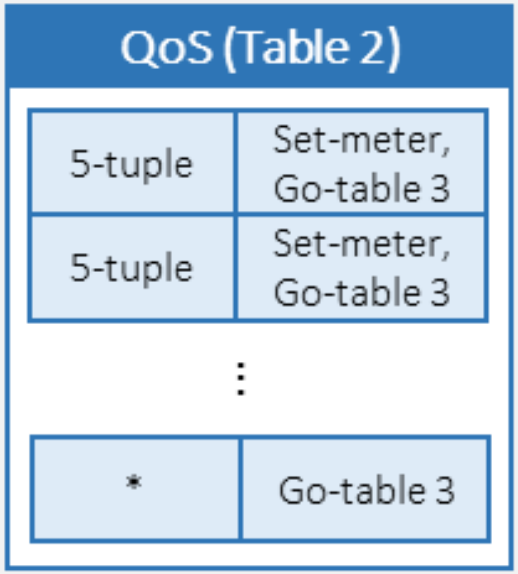




QoS Management (bandwidth limitation)

- To implement the rate limiting for hosts, we use **meter table** to set the bandwidth limitation.
- Two strategies
  - **Rate Limitation of Host**
  - **Rate Limitation of Applications**
    - The 5-tuple information is used to classify for a certain application and then add set-meter based on the classification results.

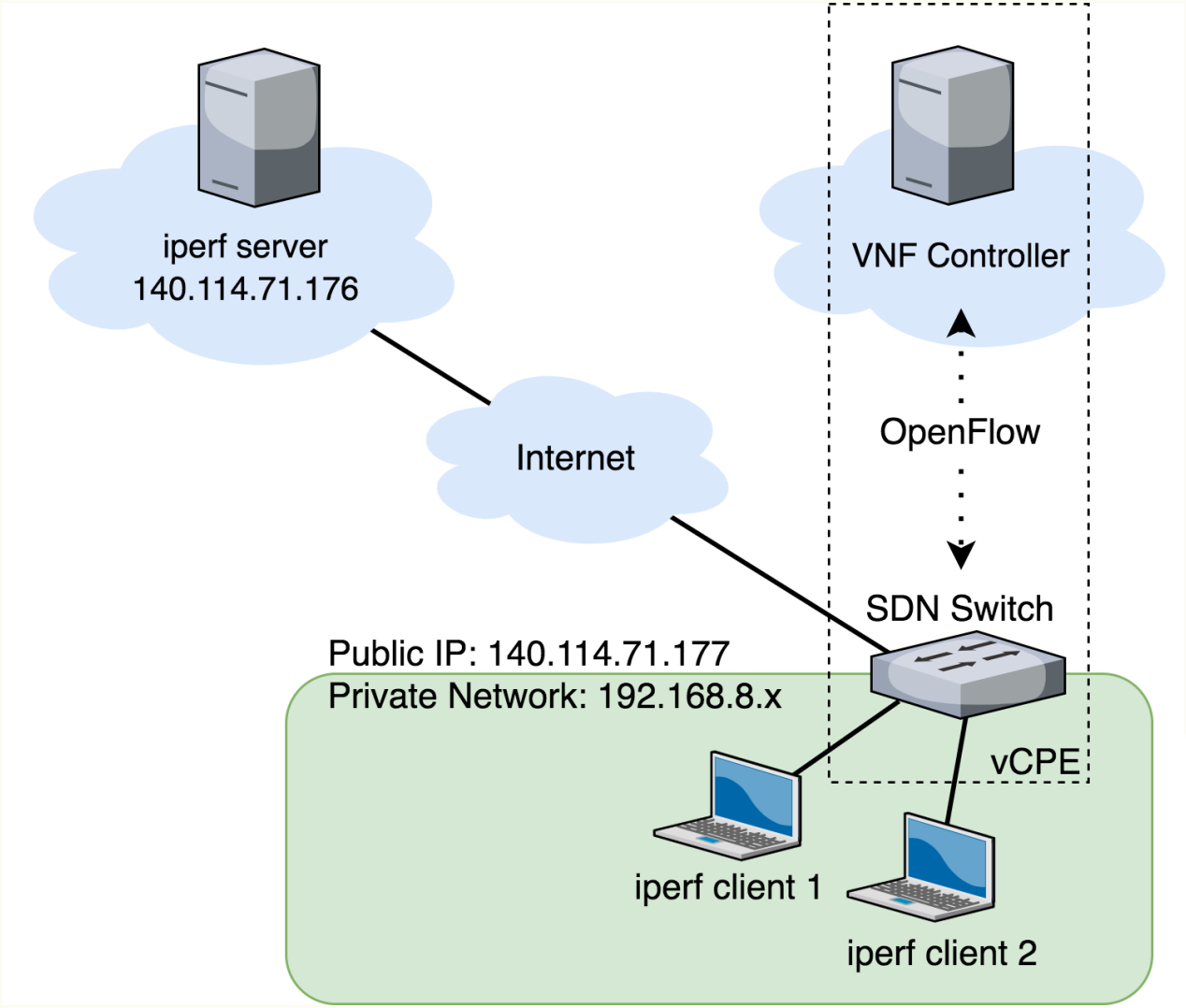




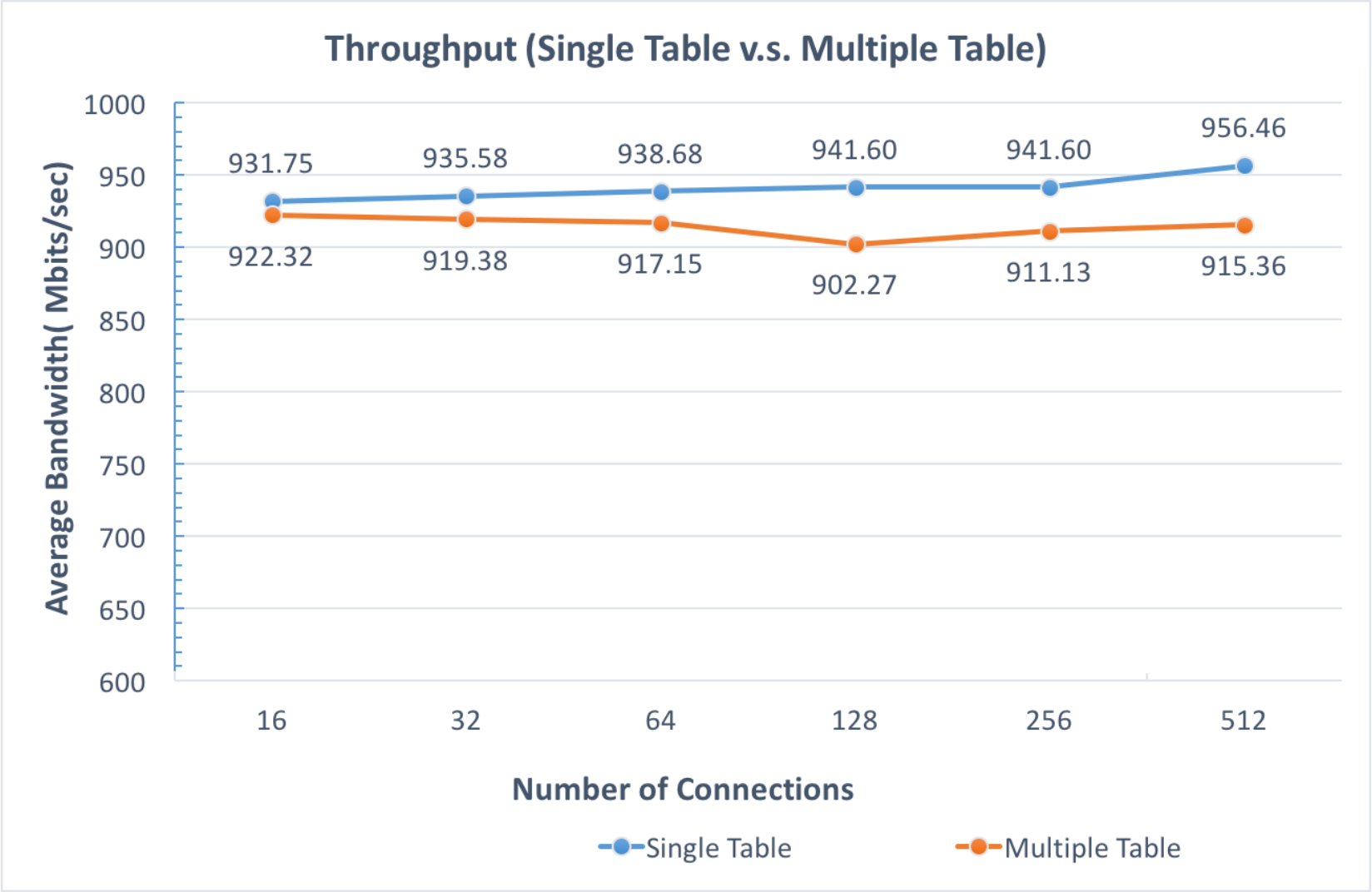
Experimental Results

- **Multiple Table Performance Evaluation**
  - **iPerf is employed to test NAT service performance**
- **Integration Evaluation**
  - **Integrate with application classification system**
  - **Host rate limitation**
  - **Application rate limitation**

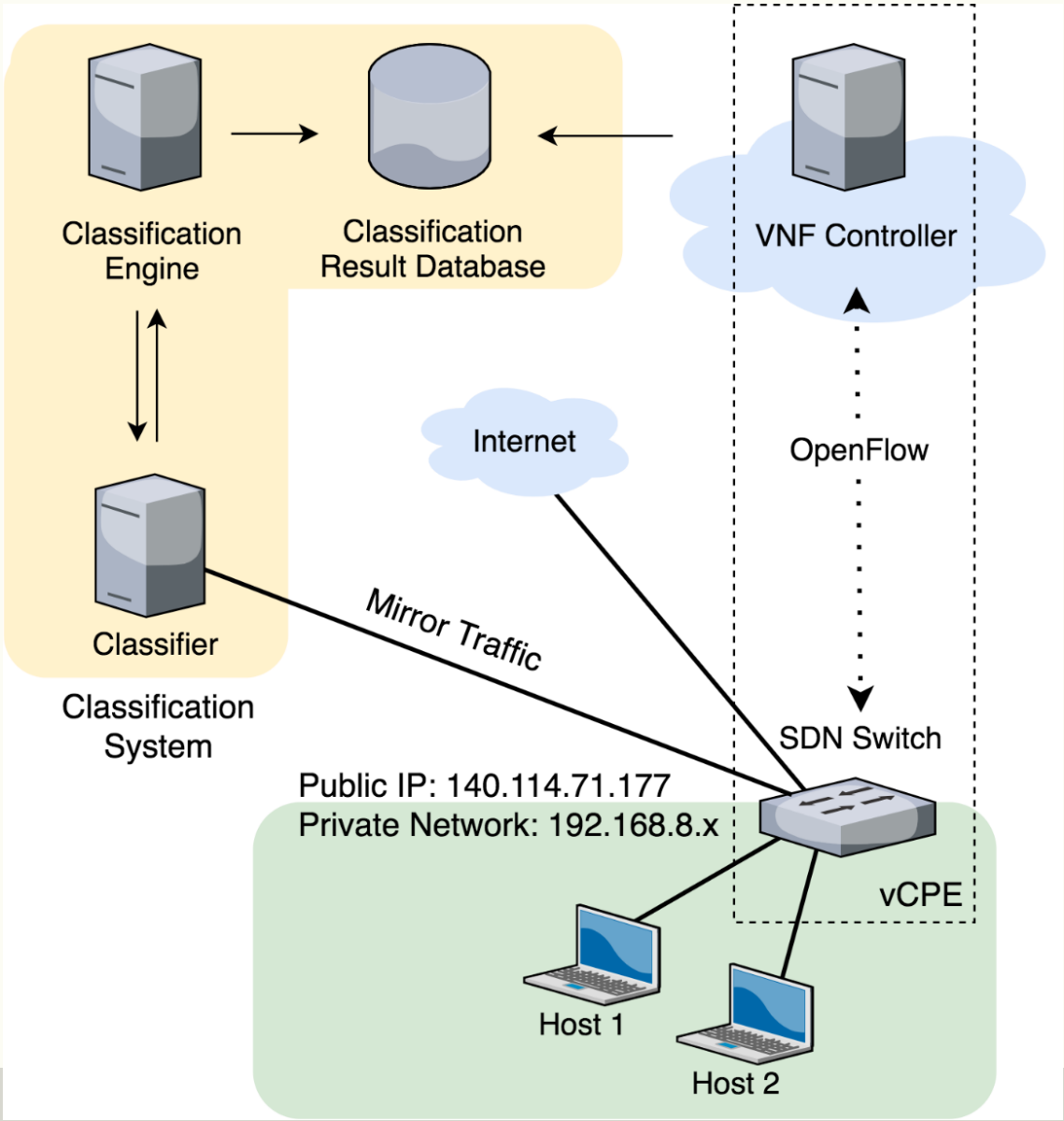
Multiple Table Performance(1/2)



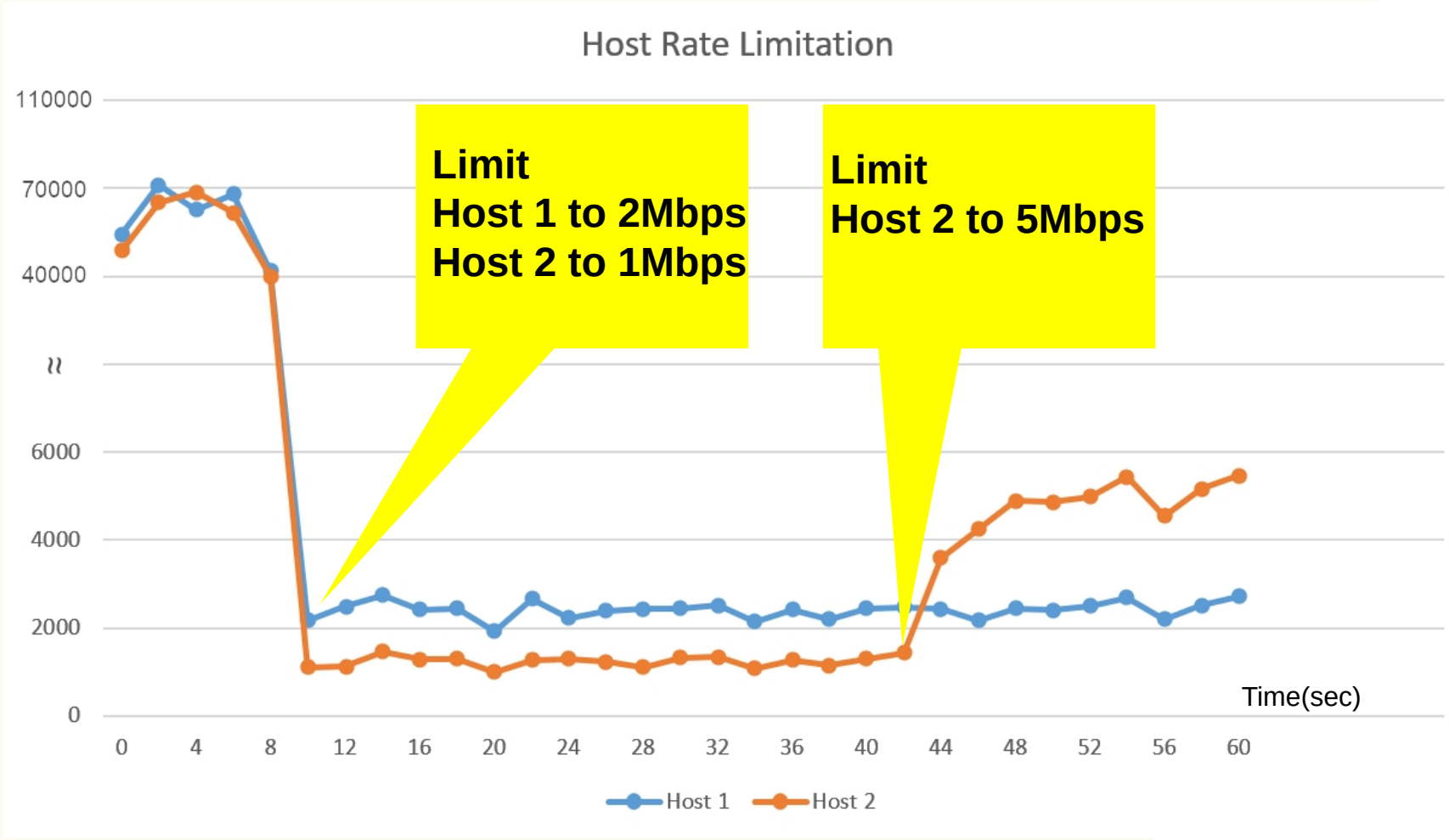
Multiple Table Performance(2/2)



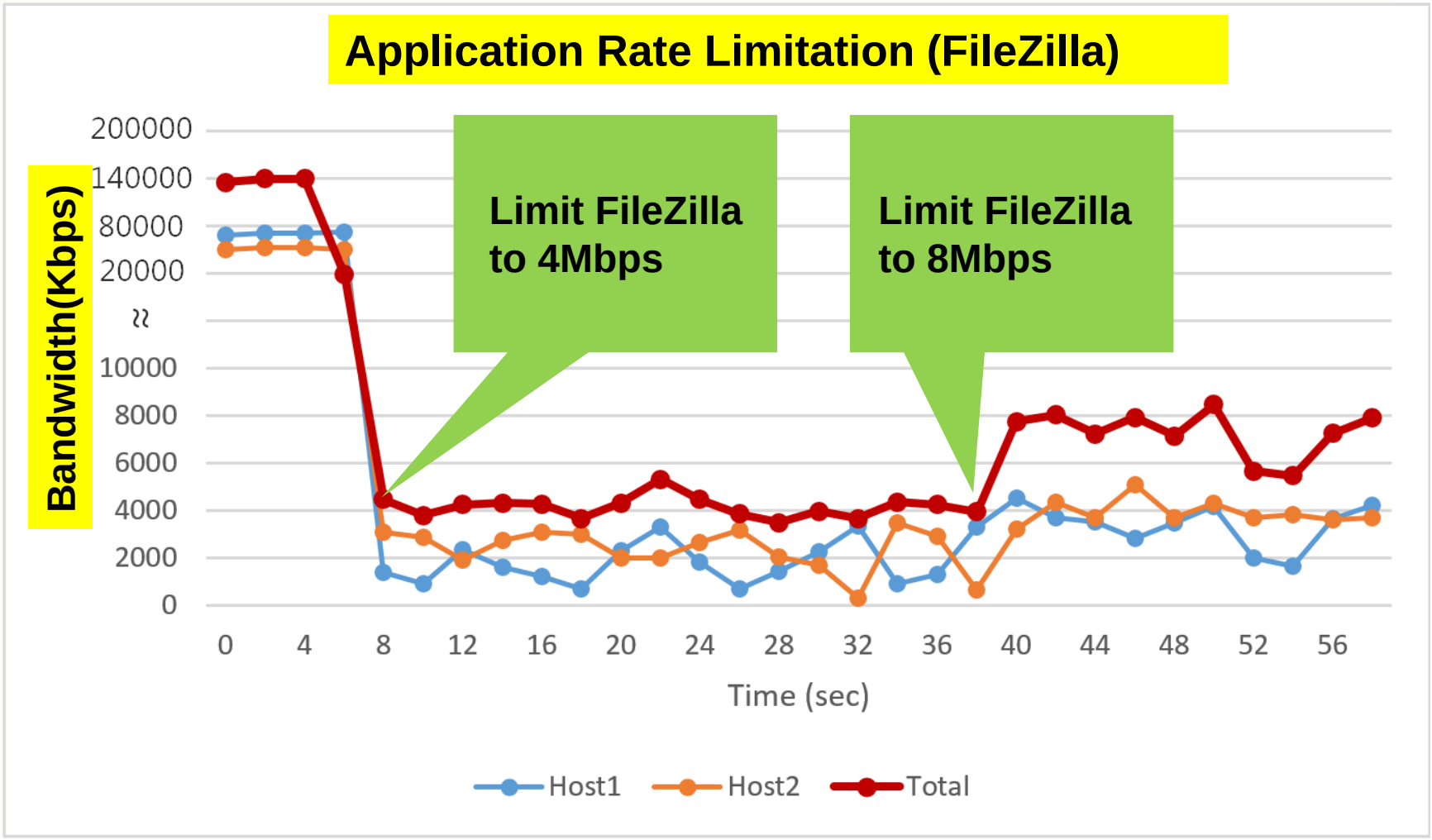
Integration Evaluation(1/3)



Integration Evaluation(2/3)



Integration Evaluation(3/3)



Conclusion

- In this paper, a multiple flow table (MFT) mechanism is proposed to implement network functions in the SDN switch.
- The proposed CPE provides several functions: firewall, NAT, DHCP, forwarding, traffic mirroring, and QoS management at the same time.
- A friendly web-based dashboard for subscribing services is also provided.
- Compared to the single-table mechanism, the performance of the proposed MFT mechanism is still good.

Thank you for your attention!