Performance Optimization of Service Chain for vCPE in Small Size Network with OpenFlow Switch

Nen-Fu Huang* Chia-An Li*, Chi-Hsuan Li*, Chia-Chi Chen*, I-Hsien Hsu*,
Che-Chuan Li *, Ching-Hsuan Chen† and, I-Ju Liao*
* Department of Computer Science National Tsing Hua University, Hsinchu, Taiwan
† Institute of Communication Engineering National Tsing Hua University, Hsinchu, Taiwan

Abstract—In the last decade, along with the continuously developing of SDN, numerous SDN applications have played important roles in modern network. vCPE is one of potential applications can make game change because it can reduce OPEX and CAPEX in the same time. This service compose of many technologies with complex architecture like NFV, VNF and Service Chaining. Many researches discuss algorithm or mechanism to link multiple VNFs as a single NFV then connect NFVs as a service chain in cloud. Nevertheless, the hardware resource and characteristic of SDN switch that never mention before may waste in this architecture. In this paper, a vCPE framework with multiple flow table management based on cloud is implemented. The proposed of vCPE framework is to create a SDN-enabled VNF using both resoures in SDN switch and on cloud and these VNFs can be deployed as edge. The system is also integrated with an application identification engine based on machine learning algorithms thus providing flow control in vCPE framework with confidence. Experimental results show that the framework provide performance in VNF compete over single table SDN application.

Index Terms—SDN, vCPE, VNF, NFV, OpenFlow

I. INTRODUCTION

SDN[1], [2] has been developing almost a decade since the first Openflow article had be presented in 2008[3]. Openflow[4] gives a brand new viewpoint on network research, and makes innovation on industries. This technic proposed not just a novel architecture but also bring out more methods of flexible traffic engineering. After tons of implementations and researches had been proposed, this architecture exposed some weakness in performance. The main concept of this architecture is separating data plane and control plane that put smart control and multi-path into real world. But legacy hardware design eventually put this perfect design into reality. To achieve high speed packet exchange, ternary content-addressable memory (TCAM) plays an important role in legacy fabric switching. This hardware design speed up the packet switching but it also cause high cost and less size problems. In the beginning, most of SDN switch used legacy hardware design and just add software API support for temporary solution. The smaller TCAM size comes the less flow control rules but it can keep high performance in packet switching. It brings out inter-datacenter dynamic traffic routing because that scenario doesnt need much flow entries. At the same time as SDN was developed, Network Function Virtualization (NFV)[5],[6],[7] has been introduced by Telco operators. Operators want to reduce their cost on maintaining old telco platform which may has been operated in 50 years. To replace the old platform with high maintenance cost, they use virtual machine (VM) based on new computers as solutions. This method can really save a lot of money in maintaining old platform but not all of operators have the same requirement as AT&T; there is another idea about reducing OPEX and CAPEX in enterprise networks that is vCPE which was innovated by NEC[8]. vCPE manage network functions on operation side to reduce cost which was deployed on cloud [9]. Although both of technical ideas are perfect, it still address two critical problems. The first one is the lack of hardware support because these ideas need large size of flow tables to achieve multi VNF support. And the other is VM based on cloud may slow down the high speed network exchanging network[10],[11]. From Pica8[12] finished their first OpenFlow switches, there are so many implementation method on a SDN switch. Even Open Network Foundation (ONF)[13] has a series of testing processes, it cant shows completely testing result of SDN switch especially performance. Let us take flow entries as example, there are single flow table and multiple flow table architectures much more based on hardware or software. Bandwidth control APIs have been an option in OpenFlow 1.3 but there are many switches still didnt support these API. Even it did support, there are still at least two implementation methods should be noticed. Meters and per queue show different ways controlling bandwidth not mention to accuracy of bandwidth. Service chain[14] is another concept with vCPE framework because enterprise will apply a bulk of network services. This technic inherit weakness of SDN switches and vCPE so there is no standard to unified interface to link all services. Its hard to combine and link all switches and cloud service in such complex situation. Different services on cloud must be working fine with different SDN switches and we believe thats why most of service chain was implemented in VM on the cloud.

Therefore, the purpose of this paper can be summarized as follows:

1) To achieve extremely speed of packet exchanging of vCPE in small size network, this study proposed a mechanism to control OpenFlow tables which is in different

hardware switches such as Lagopus[15], Pica8[12] and Edgecore[16]. It supports single table and multi-table implementation in different switches and sends status and information message to Ryu controller. This mechanism brings out a novel implementation method of VNF that combine hardware and software operations. It not only makes hardware usage more efficiency but also stays maximum flexibility in NFV deployment.

2) To cover most of NFV framework, this vCPE framework offer a multi cloud management feature. It can working with OpenDaylight[17] on OpenStack[18] and Ryu[19] on Docker[20] perfectly. Users can deploy their NFV features in any kind of VM system even in public cloud, and monitor it in same system.

3) To control flows with confidence, an application identification algorithm might be in consideration. The first thing comes out must be Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) but there are 2 major weakness of this two kind of technic. The first is it spends a lot of time to identify connections, and network speed may hang on IPS. The other is it may cant figure out encryption connections because not all of IDS or IPS have key matching feature. Most of modern cloud applications use https protocol as basic communication method which makes matter even worse. This study gives an algorithm to identify applications with statistical method with machine learning. The algorithm only use connection attributes to train an identification models such as packet direction, packet length. Afterward, the algorithm can identify network applications by this model. Even encryption connection can be identified with high accuracy because the algorithm monitor packet in statistical way instead of trying to decode it.

4) To analysis performance of this vCPE framework, this study integrate all of functions mention above to evaluate it compare with the single-table mechanism.

This paper is structured as follows. Section II introduce the overall architecture of the framework what this study proposed. Section III describe multi table management mechanism in the beginning. Rest of section will show how to implement VNF with the mechanism. Section IV considers application identification in SDN because system can do nothing if the system doesnt know what kind of application running on the network. Section V analytically performance of vCPE framework what we proposed include comparison with traditional network devices. Conclusion and future works will summary in the last section.

II. System Description

A. Overview of Network Function

With the concept of SDN-enabled VNFs[21][22], SDN technology work not only for traffic steering but also as a part of network functions. In this idea, network functions have been achieved by the synergies between computer infrastructures(NFV) and network infrastructures(NFVI)[23],[24], shown in Fig. 1. The former is a VNF controller, mainly
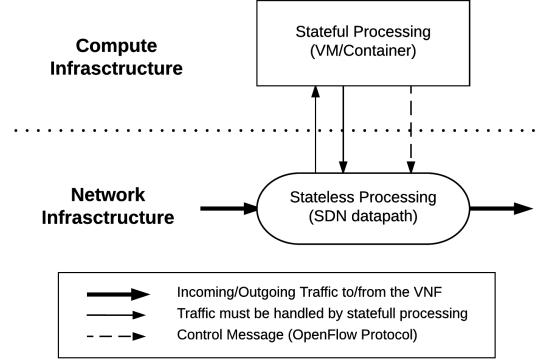

Fig. 1: Overview of network function.

responsible for dealing with stateful processing. The latter is a SDN switch used for stateless processing.

1) Stateful Processing Component (VNF controller in container): This component have to control the workflow, keep the state associated with the VNF, and provide interface for service providers or customers to configure and update the behavior of the stateless datapath processing component. We use SDN controller to implement the NFV controller and its worth noting that we use southbound APIs of SDN controller framework to handle the interface between the stateful and stateless component with OpenFlow protocol, which was originally designed for this.

2) Stateless Processing Component (SDN datapath): Stateless processing component, are implemented by SDN datapath resources, which is optimized for data plane traffic processing. Since SDN switch have decoupled the control plane and data plane, so it can accept the control message from the stateful processing component.

Using the advantages of this architecture, we can assign stateless or light-weight state work to the SDN switch, for example, packet filtering and packet counting, to load-off the computing resources. If we want to update our service, we just need to update the stateful component, since the stateless component just follow the command from stateful components

B. Service Deployment Model

Different from some related works are discussed about virtualizing network functions located in PE devices[25], we come up with a network function service deployment model, with architecture mentioned in Fig. 1 based on the NetFATE (Network Function at the Edge) approach[26]. Because computing infrastructures handles the algorithm and policies, and the generic network devices only do stateless processing, the customer just need to buy a general SDN switch at their home gateway and will have a different network function service by subscribing different the NFV controller through our vCPE platform.

Fig. 2 illustrates the service deployment model. Each green area is a local network domain of customer. At the gateway of this domain, theres a SDN-enabled switch. The customer can subscribe to our vCPE service through our dashboard.
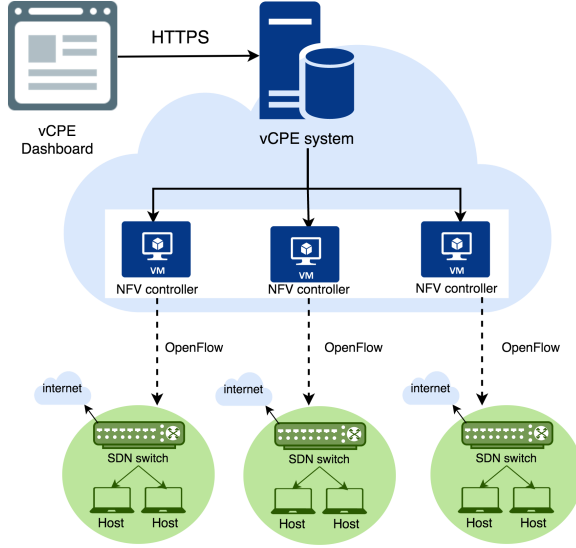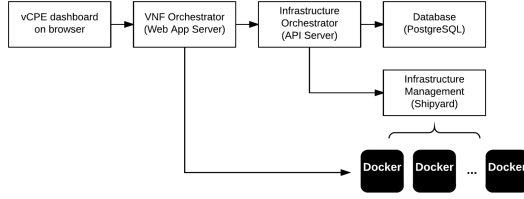
Fig. 2: Service deployment model.

Fig. 3: Architecture of the vCPE framework.

After subscribing, the vCPE system will create a new docker container, in which running a SDN controller we developed. The customer only need to setup the gateway SDN switch to connect the SDN controller by the OpenFlow protocol, then the switch will handle these service.

C. Architecture of the vCPE System

The architecture of the vCPE system is adapted from [27], shown in Fig. 3, including of a Infrastructure Controller, Infrastructure Orchestrator, Cloud Database, VNF Controllers and VNF Orchestrator. The Infrastructure Orchestrator, VNF Orchestrator and Cloud Database are web servers Each component is introduced in the subsection below.

1) Infrastructure Controller: The infrastructure controller is a composed Docker management server with the ability to manage the Docker resources like containers and images. The infrastructure doesn't handle the customer authentication or maintaining the state of running service, it just follows the request from the infrastructure orchestrator to create, delete, start, stop and inspect containers.

2) Infrastructure Orchestrator: The infrastructure orchestrator plays the key role of our system. It connecting and automating of workflows when we deploy our services. When a customer subscribes, the infrastructure orchestrator authenticates the customer first, next it will call the infrastructure controller to create a container for this customer, and update

information in database afterwards. It handle the entire lifecycle of our vCPE service.

3) Cloud Database: The cloud database is used for restoring the of our vCPE services, which include each customers credential, customers container settings and virtual CPE service states. The cloud database is using PostgreSQL, which is a open source, easily customized and object-relational database system. Only Infrastructure Orchestrator has permissions to access cloud database.

4) VNF Controllers: VNF Controllers contains a SDN controller developed with ryu framework[19] and a remote launcher module. The SDN controller does not have a remote launcher module to remotely execute a SDN controller. We built a light-weight server as a launcher module to resolve the remotely execution issue. The remote launcher module monitor the SDN controller process ID (PID) and properly kill the SDN controller process ID when on demand. When the infrastructure controller once create the container, the remote module will run up initially, waiting request from VNF Orchestrator. The details of SDN controller design will be presented at section III.

5) VNF Orchestrator: The VNF Orchestrator is a Web application server hosting on Amazon Web server, being online for customer and provide a dashboard for virtual CPE and containers management and configuration. Through the web UI provided by the VNF Orchestrator, the customers can subscribe to the desired service and without typing any command via the command line interface (CLI). After receiving the subscribing message, the VNF orchestrator will request the infrastructure orchestrator to create a new VNF controller, and then send the virtual CPE configuration to the new VNF controller. Based on configuration demands under different conditions, the network administrator is able to select any of the listed network functions on the dashboard such as Firewall, NAT, DHCP and QoS management.

D. Network Functions

The proposed vCPE service provides following network functions.

1) Firewall: The firewall service could filter the packets based on packet header fields, including MAC address, IP, and layer4 protocols. The network manager can add new rules or remove rules to the access control list through our vCPE GUI.

2) NAT: The NAT service is a network function that can remap IP address to another one. The Source NAT (SNAT) is typically used by internal users (inside private network) to access the Internet (outside network). The network function uses the action Set-Field, which deined by OpenFlow protocol for rewriting packet header fields. Via vCPE GUI interface, the network manager can set up the WAN port of SDN switch, public IP, default gateway, and local network address when using this function.

3) DHCP: DHCP service allocates IP addresses to hosts dynamically. To implement the function, the SDN controller cope with UDP packets which use port 67 and 68. It generates DHCP offer and DHCP acknowledge to reply DHCP discovery and DHCP request received from the hosts.

4) Forwarding: Forwarding Service is a basic service that forward traffic to its destination and we use the Mac address learning concept to implement our forwarding function.

5) QoS: Quality of Service (QoS) are always used to control the traffic flows of a network and prevent the traffic to exceed the network capacity and cause traffic congestion. Therefore we implement the bandwidth management using meter which is defined within OpenFlow protocol 1.3 to set the limitation of the bandwidth. Beside achieving network functions virtualization with SDN technology, we also make the network administrator manage and monitor a network more easily. As a result, we can offer the user the best network quality in the limited network resource without traffic congestion. In this paper, our QoS integrates with a flow classification engine and offers the two ways of bandwidth management.

- For a specific host.
- For a specific application.

E. Application Identification

Application identification is to identify each flow as an application name to enable QoS management system to do bandwidth control or distribution at application level[28][29]. The application name means the name of application which establishes the flow. A flow is defined by 5-tuple (source IP, source port, destination IP, destination port, and transport layer protocol). Applications include desktop applications, native mobile applications, and web applications, such as Facebook, Skype, YouTube, Instagram, Line and WeChat. We use supervised machine learning and a method based on inspecting domain name service (DNS) responses to do flow classification. After application identification system classifies a flow as an application name, it sends the classification result to a server with database. The server stores the classification result into the database, and waits for requests from QoS management system. The detail will be described in section IV.

III. NETWORK FUNCTION WITH MULTIPLE FLOW TABLE MANAGEMENT MODEL

A. Multiple Flow Tables Strategy

In subsection II-A, the vCPE service design architecture have been introduced. The network functions are handled by the cooperation between SDN controller on cloud and SDN switch at the local network gateway. The controller transform the network functions to series of OpenFlow rules requests and send to SDN switch. Following the orders from controller, the SDN switch inserts rules to its flow tables, checks incoming packets against the flow entry match fields, and execute the actions in matching rules. The flow table[30] defines all matching and corresponding processing, thus playing an important role to executive network function.

Since the flow table is a crucial component, and we find that single flow table binds us to implement our network functions. The[31] also mentioned two condition for single flow table is too restrictive. The first is a single packet need to perform independent actions based on matching different fields. The second is that the packet needs two-stage processing. Involves into both situation, our network functions implemented by multiple flow tables strategy.

In multiple flow tables strategy, the most important question is: which flow table should we insert rules into? We use the network function as a demarcation, that is, SDN applications which are responsible for specific network functions will only insert rules to one specific flow table, so we can focus on the design of the network function itself. In this way, however, the order of flow table become crucial. Should we put this network function at first, or the other? The answer is about the type of match and action in the rules generated by the network function

The network functions of vCPE services including Firewall, NAT, DHCP, Forwarding and QoS. We have determined the order of each function, shown in 4. (Notice that the flow tables are counting from zero) In the following subsections, we will introduce how to implement these network functions, which type of rules will be inserted to SDN switch, and how these rules affect our decision of the order of flow tables.

B. Service Control

Service control is about which service we want to enable or disable. To enable a service, we need to modify the table-miss rule. We always put a packet-in rule in the flow table of the last active service as a table-miss in case that there isn't any corresponding rule. To make our service chain possible, the rules of each service except the last service contains an additional action, go to next flow table, so the packets can continue to pass through all active services.

To disable a service, we not only need to modify the table-miss rule but also have to add an enforce rule. Each enforce rules has maximum priority and the action is goto next flow table. It means that packets will still pass through the disabled service's table, and the only thing they do in this flow table is ignoring other rules and go to next flow table.

C. Firewall

Firewall service is able to block traffic dynamically, and in this service, the packets will not cause any packet-in event.

On the dashboard, we can specify the blocking policies. There are 3 kinds of policies:

- Block any traffic from a source IP or destination IP.
- Block traffic based on known layer 4 protocols, such as SSH, HTTP, etc.
- Block traffic to customize layer 4 ports of a host.

For different policies, the controller applies corresponding rules to the SDN switch. After the policies are set, the blocking rules will be installed immediately. Then any traffic that hit the blocking rules will be dropped. For normal traffic, they will not be affected.

As shown in Table I, all the actions of flow entries are drop. The first rule illustrates that SSH connection with source IP address 192.168.2.1 would be blocked. The second rule shows the flow entry would block the Telnet protocol.
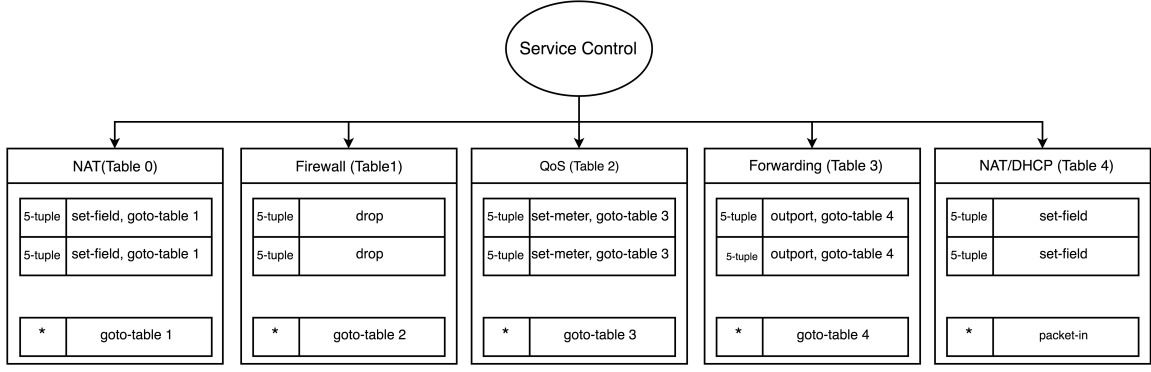
Service Control

NAT(Table 0)	
5-tuple	set-field, goto-table 1
5-tuple	set-field, goto-table 1
*	goto-table 1

Firewall (Table1)	
5-tuple	drop
5-tuple	drop
*	goto-table 2

QoS (Table 2)	
5-tuple	set-meter, goto-table 3
5-tuple	set-meter, goto-table 3
*	goto-table 3

Forwarding (Table 3)	
5-tuple	outport, goto-table 4
5-tuple	outport, goto-table 4
*	goto-table 4

NAT/DHCP (Table 4)	
5-tuple	set-field
5-tuple	set-field
*	packet-in

Fig. 4: The flow table order of vCPE service.

In our multiple flow tables model, the firewall service is located in the flow table 1, since once packets are caught by the blocking rules, they doesn't need to apply any other services. The packets which match the rules will be dropped immediately, and their journey in the flow table ends here. To other no-blocked packets, they pass all blocking rules and finally match the table-miss rule, which will let the packets go on the next flow table. The action of firewall is different from other services, since in other services, no matter what actions are taken to the packets, the packets have to go to the next flow table.
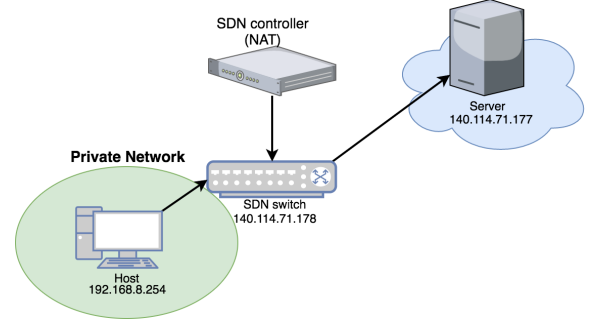
D. NAT

The NAT service could allow a lot of hosts to use one public IP address to connect the network. In order to achieve this thing, SDN controller have to set the packet header filed. Because the SDN switch would set the field, the first packet have to go to controller. And controller would add the flow to SDN switch, after that the packet would not go to controller. It can decrease the burdens of the controller.

Below is a examples to show how the NAT service modify the IP address and port number. For outgoing packet, the SDN switch doesnt have any flow entry in flow table, so the Packet-in event will be triggered at the beginning. The packet that is sent by private network host will be sent to SDN controller, and the packet header fields are modified by Set-Field action. The source IP address and source port number of outgoing packet will be modified to public IP address and remaped a new port number for NAT. For ingoing packet, the destination IP and destination port number are modified to fit private IP and port number. And then SDN controller add these flow entries to SDN switch, it cant avoid that all the packet sent to controller.

Fig. 5 show the public IP address of NAT is 140.114.71.178 and a host private IP is 192.168.8.254 and port number 7878. The client sent the packet to a server with IP address 140.114.71.177 and port number 9898.

As shown in Table II, when host sent the packet to server (outgoing), the Packet-in will be trigger, and then packet to controller. The Set-Field action would modify the Source IP to public IP address of NAT is 140.114.71.178 and source port to 2000. when the server sends back to the client (ingoing),

SDN controller (NAT)

Private Network

Server 140.114.71.177

SDN switch 140.114.71.178

Host 192.168.8.254

Fig. 5: The flow table order of vCPE service.

the packet header field would be modified. The destination IP address and destination port number would be modified to 192.168.8.254 and 7788.

In the single flow table framework, we have to add the two rules to SDN switch to match the outgoing and ingoing situation. At the first, we predict the NAT service to be put one the last table in the multiple flow tables framework. Because the NAT service need to set the packet header fields and play a role of connection to the outside network. And the most important thing is that the SDN switch is according to order of table to match. We have to consider the outgoing and ingoing situations. As a result of all the above factors combined, the NAT service is located at the first and the last table in our multiple flow table framework.

E. DHCP

DHCP service implements DHCP protocol to dynamically assign IP addresses to hosts. DHCP operation uses UDP protocol. The clients use port 68 as the source port and 67 as the destination port. On the contrary, the server use port 67 as the source port and 68 as the destination port. Our system is able to handle these packets to realize DHCP service.

The service follows these steps:

1) The controller adds a DHCP rule for DHCP packets when the service is enabled.
2) All packets match this DHCP rule cause packet-in.
3) The controller checks if a packet is a DHCP discovery packet. If so, the controller assigns an IP address, and generate a DHCP offer then do packet-out. If not, the

TABLE I: Firewall rules in Flow Entry

IP proto	IP Src	IP Dst	L4 sport	L4 dport	Action
TCP	192.168.2.1	*	*	22	Drop
TCP	*	*	*	23	Drop

Symbol * represents wildcard (match any value).

TABLE II: Flow entry for modifying the packet header fields of packets

	IP Src	IP Dst	L4 src port	L4 dst port	Action
1. outgoing	192.168.8.254	140.114.71.177	7878	9898	IP Src → 140.114.71.178; L4 src port → 2000
2. ingoing	140.114.71.177	140.114.71.178	9898	2000	IP Dst → 192.168.8.254; L4 dst port → 7878

controller then checks whether it's a DHCP request. If the result is positive, the controller generate a DHCP acknowledge then do packet-out.

Our system support multiple flow table, but a specific flow table for DHCP service is not required. The reason is that only one rule will be installed for all hosts who request for DHCP service. When the service is disabled, the DHCP rule will be deleted, and the packets will continue to pass through our service chain. Following DHCP packets can reach other DHCP servers without entering our service chain since our controller will automatically flood out broadcast packets.

F. Forwarding

In this service, when the first packet in a new connection incoming, it will cause a packet-in event because there is no corresponding rule. When controller receives the packet, it will record IP-layer information, including source IP, destination IP, input port number, source mac address and destination mac address. With the recorded information, the controller is able to install a 5-tuple forwarding rule for this connection and following packets dont need to packet-in again. The 5-tuple is source IP, destination IP, network layer protocol, source layer 4 port, and destination layer 4 port.

In order to gather per-session statistics information, 5-tuple rules are needed. This is why we dont add rules based on mac address. The controller installs a pair of dummy rules for every connection, and then request the switch to get current flow statistics every second. In this way, we can get the real-time bandwidth statistics of each connection by just subtracting the byte count from byte count of last second.

G. QoS

QoS service is mainly for traffic control and we provide two management funtion for QoS service. We will introduce these two strategy first and then discuss the flow table order of QoS service in multiple table model.

1) Rate Limitation of Hosts: When some hosts take up a lot of bandwidth of network, it will make other hosts in slow speed or make traffic congestion. To prevent this, rate limiting is used to control the rate of traffic from a host. For implementing the host rate limitation, we create a meter for desired bandwidth first and then add a flow, of which match is hosts mac address and action is the meter we just created.
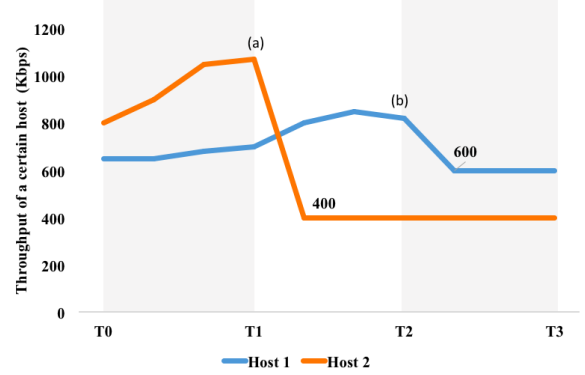

Fig. 6: Illustration of rate-limiting for a certain host

The concept of this option is shown in Fig. 6. In T0, host 1 and host 2 are not limited yet. Since host 2 takes up a lot of bandwidth from network in T0 to T1, the network administrator sets host 2 rate-limited under 400 Kbps. When controller receive this request, marked as (a), it will create a new meter with meter id = 1 and bandwidth = 400 Kbps, and set the rule in the flow table with destination MAC address = MAC address of host 1 and meter = 1. According to our flow table, it will limit the rate of the target host. Then the traffic from host 2 will reduce and be limited with 400Kbps immediately. The similar situation also occurs to host 1 in T2. The administrator chooses to set host 1 under 600 Kbps, marked as (b), and then traffic from host 1 will be limited with 600Kbps.

2) Rate Limitation of Applications: There are more and more networks applications used such as online games, video streaming, conference call, etc. Therefore, there are massive traffic working in the network. Consequently, we integrate with a flow classification engine to identify the flow belongs which application is. The integration scenario will be shown as Fig. 9.

In order to rate limit for a certain application, we need to gathering per-flow statistics information first. When a connection is created, the first packet of this connection will be handled by the forwarding service and add 5-tuple rules into SDN switch, so we can get the bandwidth information of per-flow connection. (See subsection III-F for details). With the classified result of application identification, we can know the application type of each connection.
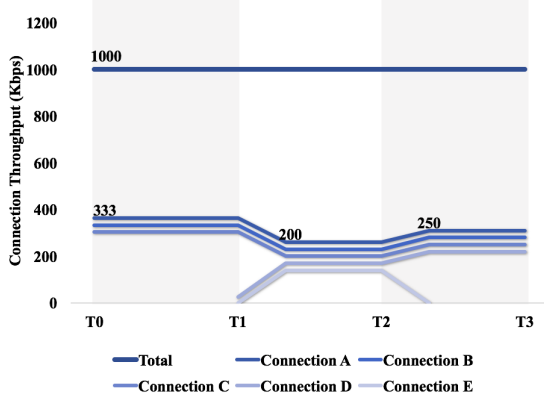
Fig. 7: Illustration of rate-limiting for a certain application.

Fig. 8: Architecture of our application identification system in training phase.

When network administrator request to rate limit a certain application to a certain bandwidth, we will equally distribute the bandwidth to each connection of the application. The controller set all flows belong to the same application into the same meter, and modifying the bandwidth of meter to achive our goal. For instance, if there is an application and we can find out which flows belong to this application through the flow classification engine and we want to limit this application to 1000Kbps. As Figure. 7, in T0, we know there are 3 connections belong this application and we will set the bandwidth of meter to each link with 1000/3 = 333Kbps. In T2, there are more two connections added to this application and we will reset the bandwidth of meter to each links with 1000/5 = 200Kbps. In T2, there is a connection ended by this application, we will reset the bandwidth of meter to each links with 1000/4 = 250Kbps, therefore. Whereas, the sum of bandwidth from this application is always being 1000 Kbps. That is, the bandwidth will be dynamically adjusted according the numbers of connections.

It is worth mentioning that we would not change any rules in flow table and we only change the bandwidth of the correspond meter in the meter table. Therefore, there only have a little overhead to switch and controller.

3) The Flow Table Order of Forwarding and QoS Service: Since the location of NAT, DHCP and firewall are determined. Here we only need to decide the arrangement of QoS and forwarding. Let's consider the scenario that we put the QoS flow table after the forwarding flow table. Plus, we have only two services enabled, forwarding and QoS, then suppose a host is not limited by QoS policies. The very first packet will not be affected in both arrangement. For the following packets, the difference can be observed. The packets which has matched the rules of the forwarding flow table will still cause packet-ins when they go to QoS flow table. This is not supposed to happen, since the host is not restrained by QoS policies and any packet-in increase the controller's load. To reduce the burden of the controller, we put QoS flow table ahead of forwarding flow table. In this scenario, all packets that pass through QoS flow table will continue to go to forwarding flow table without matching any QoS rules. Then the packets except the very first packet will just be forwarded by forwarding
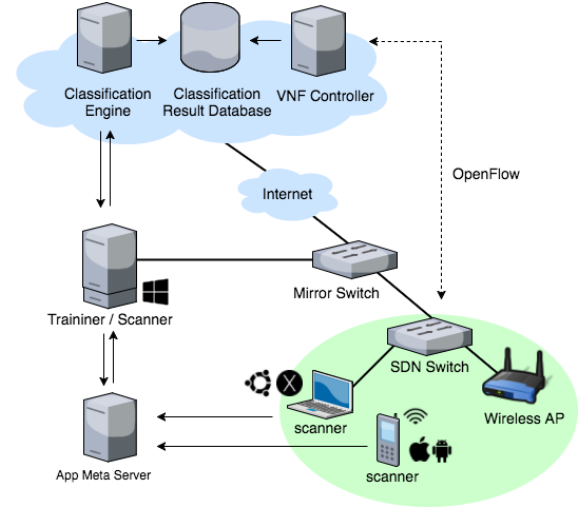
service instead of causing packet-ins. Hence the controller's load will decrease. To use our system, the forwarding service is necessary, so there is no such scenario that users enable QoS and disable forwarding.

IV. APPLICATION IDENTIFICATION METHOD

In order to let QoS management system be able to control or distribute bandwidth at application level, we designed and implemented an application identification system (also called flow classification system) to judge each flow is established by what application. In other words, the application identification system can classify each flow as an application name in real time, rather than a rough category or a transport layer protocol. The corresponding application name of a flow means the name of the application which establishes the flow. We use supervised machine learning (ML) and a method based on inspecting domain name service (DNS) responses to do flow classification. The system analyzes the packets whose transport protocol are TCP or UDP. Except for DNS responses, the system only reads headers to get transport layer information of packets without inspecting their payload.

A. Architecture of Application Identification System

There are training phase (also called preparation phase) and classifying phase, their architectures are shown in Fig. 8 and Fig. 9 respectively. These architectures can be integrated, and do training and classifying in the same time.

B. Overall Procedure of Application Identification

In training phase, we generate some data needed by our proposed method. In classifying phase, if a flow meet some requirement, we use the method based on inspecting DNS response to classify; otherwise, we use supervised ML to classify.
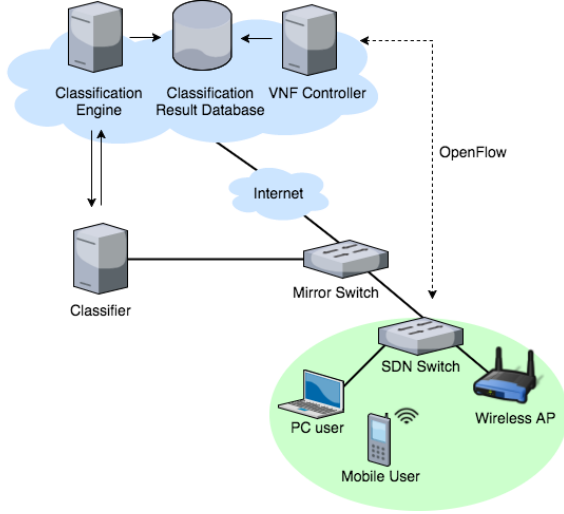
Fig. 9: Architecture of our application identification system in classifying phase.

Fig. 10: Multiple Table Performance Evaluation Scenario

Fig. 11: Result of Multiple Table Performance Evaluation

C. Procedure of Supervised ML

In training phase, the architecture is show in Fig. 8. Flow classification engine is to build classification model by training data from Trainer, and update the model when new training data comes. Trainer is to analyze traffic from mirror port to get flow attributes. After Trainer finishes calculating flow attributes of a flow, it gets ground truth of the flow from Scanner or App Meta Server to generate training data, and sends training data to flow classification engine. App Meta Server is to store mappings of 5-tuple and ground truth from Scanner, and accept queries from Trainer. Scanner is to get mappings of 5-tuple and ground truth from OS. In classifying phase, the architecture is shown in Fig. 9. Flow classification engine is to use flow attributes from Classifier and classification model to get a classification result, and sends classification result to Classifier. Classifier is to analyze traffic from mirror port to get flow attributes. After Classifier finishes calculating flow attributes of a flow, it use flow attributes to ask flow classification engine for classification result if needed.

D. Flow ttributes of Supervised ML

In ML, when system calculates flow attributes, we only use transport layer information of packets which have payload. We use Application Round (APPR) proposed by[32] to analyze flow behavior. We use number of packets, packet sizes, transmission time, transmission direction, throughput, and APPR to define flow attributes. There are 69 attributes in total, as defined in our previous work[33].

E. Algorithms of Supervised ML

We use algorithms implemented by Weka, a famous open source ML tool developed at the University of Waikato. We call Weka Java API to build classification model. We use three algorithms, namely RandomSupSpace with RandomTree[34], FilterClassifier with discretization and RandomTree, and RandomCommittee with RandomTree.
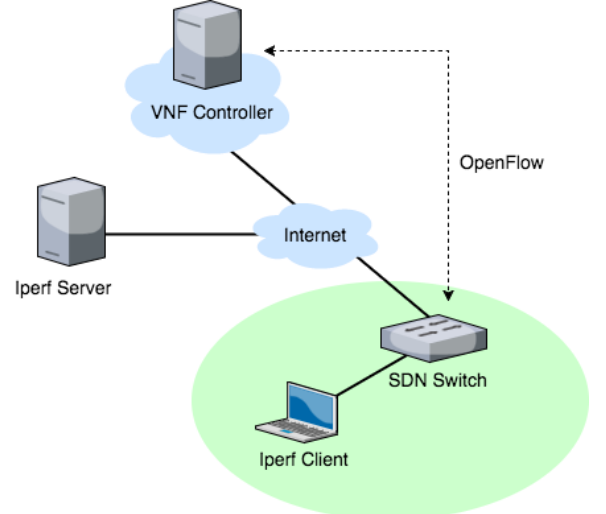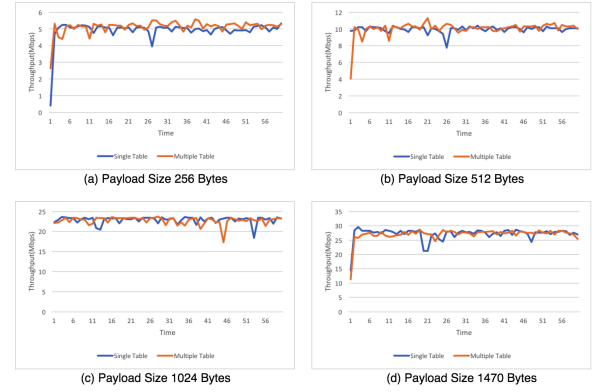
F. Procedure of a Method Based on Inspecting DNS Response

In training phase, we collect the mappings of server IP and application name. A mapping of server IP and application name means the application has ever established connection with the server whose IP is the server IP, and the server IP has ever occurred in any DNS response we have captured. In classifying phase, we do not use those server IPs which have more than two corresponding applications among the mappings to classify. We only use server IPs which have one corresponding application in the mappings to classify. When system detect a flow, we check whether source IP or destination IP of the flow match any of these server IPs. If it matches, we regard corresponding application name as classification result; otherwise, we use flow attributes of the flow and classification model of supervised ML to classify.

V. PERFORMANCE EVALUATION

A. Multiple Table Performance

The single flow table framework implementation is easier than multiple flow table framework, but the multiple flow table framework is more flexible. To verify the efficacy of multiple flow table vCPE framework, this experiment use the NAT

service to compare the throughput between single flow table vCPE and multiple flow table vCPE.

To begin with, an overview of the experiment environment is shown in Fig. 10. The NFV controller run on the Dell PowerEdge R630 Rack Server, and the SDN switch use the Pica8 P-3290 switch[12]. We use the iPerf2[35] to generate the network traffic. The iperf server would connect the public IP address with 140.114.71.178, and then the iperf client connect to the SDN switch, and is controlled by NFV controller. NFV controller run the NAT service, but use the different framework that are single flow table and multiple flow table.

We use the iPerf to generate the UDP packets and send to server from client, and set the fixed value to bandwidth at 100Mbps. These experiments would use diffrent payload sizes to inspect their performances. As shown in Fig. 11, the throughput value show that the performances of large packets such as 1024 bytes and 1470 bytes is better than small packets. Because the NAT service need to set the packet header field and small payload size would send more packets to server at the same time, the performance of larger packets is well. We can see that the throughput value of multiple table framework is close to single table framework. So we can realize the multiple table framework is more flexible than single table framework, and the performance is close to each other, which shown as Fig. 11.

B. Accuracy of Application Identification

1) Testing Data Set: Testing data set are mappings of flow attributes and ground truth. These mappings are also called rules. This testing data set were generated by our system in our lab in National Tsing Hua University in Taiwan. We manually operated applications to generate traffic. Each platform of an application took around 50 minutes. When the application identification system generated rules, it exported them into a file, because we wanted to do 10-fold cross validation on a testing data set. There are 14659 rules in total, and there are 137 applications if we count each platform version of an application as one application. The testing data set does not contain all of platform version of each application which is in this testing data set.

2) Validation Method: Although the system can do online training and classifying, we do offline training and classifying, shown as Fig. 12. More specifically, when we did online training to analyze traffic, get ground truth, and export the rules into a file. We do 10-fold cross validation on the rules. There are 10 rounds in 10-fold cross validation. We split the data set into 10 subsets. At each round, we used 1 of 10 subsets as a classifying data set and the union of the other subsets as a training data set. Then we did 10 rounds, and each subset acted as the classifying data set exactly once. We implemented Classifier Light and Trainer Light, acting as Classifier and Trainer respectively without the function of analyzing traffic. Because there are labels in classifying data set, we can calculate accuracy.

3) Mapping of Category Names: Mapping of category names: At each round of 10-fold cross validation We do name mapping on training dataset before we use training
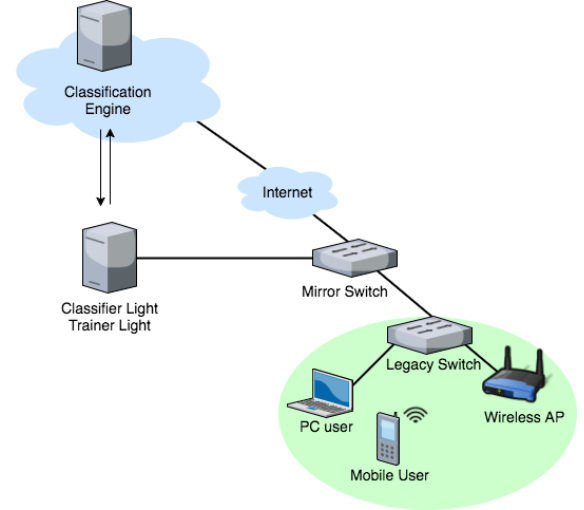

Fig. 12: Evaluation of Application Identification.

data set to build classification model, and do name mapping on classifying data set before we use classifying data set to calculate accuracy. The main reason is that some application have different ground truth in different operating system. After name mapping, there are 99 categories in testing data set.

4) Accuracy Matrices and Results: To evaluate accuracy, we used precision, recall and F-measure (also called F1 score), as shown in Eq. (1), Eq. (2), and Eq. (3)[36]. In each round in 10-fold cross validation, we calculate precision and recall of each category to calculate F1 score of each category. After ten rounds, we calculate average F1 score of each category in 10 rounds. Table I shows F1 score of each category in top 40 most popular applications in testing data set. Next, we calculate average F1 score of all categories in 10 rounds, and we get 0.9062. The result (Table. III) shows it achieved high accuracy, which makes QoS possible to do bandwidth control or distribution at application level.

$$Precision = \frac{True\ positive}{True\ positive\ +\ False\ positive} \quad (1)$$

$$Recall = \frac{True\ positive}{True\ positive\ +\ False\ negative} \quad (2)$$

$$F1\ score = \frac{2 \times Precision \times Recall}{Precsion + Recall} \quad (3)$$

C. Integration Evaluation: QoS Limit Host bandwidth Evaluation

We choose a way to verify our function is downloading the file in that it is a situation always takes up the network recourse in real world. We decide to download the image of Ubuntu 14.04 which is about 1GB size.

As shown in Fig. 9, The NFV controller run on the Dell PowerEdge R630 Rack Server, and would excute the QoS service. And the OpenFlow-enable switch use the the Edge-Core AS5712-54X[16] switch that operating system is PicOS TM r2.6.

TABLE III: 40 POPULAR APPLICATIONS AVERAGE F1 SCORE IN 10 ROUNDS

| Application name	Average F1 score	Application name	Average F1 score
OneDrive	0.991255	Trello	0.988889
gamerAnimad	0.985714	Dropbox	0.985714
AmazonMusi	0.977461	MEGAsync	0.968889
MEGAsync	0.968889	BattleNet	0.967812
Udacity	0.966667	Lity	0.966427
Tumblr	0.964624	Asana	0.963492
Skype	0.963117	Twitch	0.963117
TeamViewer	0.946667	FileZilla	0.946429
Agoda	0.944764	TripAdvisor	0.942075
Pinterest	0.936026	BBCNews	0.931049
LINE	0.923904	Slack	0.920985
Twitter	0.917906	Youku	0.913925
Evernote	0.912381	Snapchat	0.912221
Weibo	0.910872	WeChat	0.906349
GoogleDrive	0.896612	Trivago	0.895406
iTunes	0.890464	Netflix	0.876234
Facebook	0.868641	Telegram	0.862222
Airbnb	0.857029	Spotify	0.856971
Instagram	0.833465	TED	0.829277
Tmall	0.799747	YouTube	0.713084
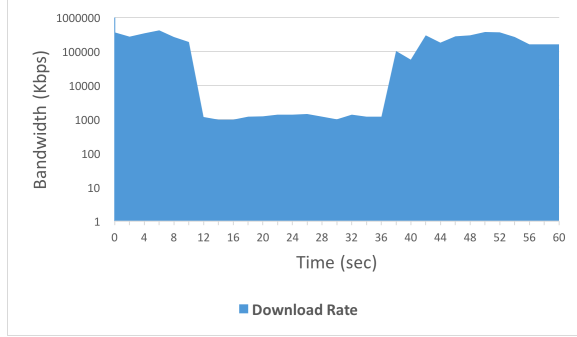
Fig. 13: Limit the download rate to a host.

We used a desktop computer to be the experimental host and record the bandwidth in every 2 seconds. As shown in Fig 13, we start downloading the file without limiting and the rate is between 190000 Kbps to 410000 Kbps in the beginning. At 10th seconds, we wanted to limit this hosts bandwidth to 1024Kbps and we added the rule the destination MAC address is matching this desktop computer with a meter of 1024Kbps. Then we can find out the bandwidth from this host is decrease and be limited to about 1024Kbps immediately.

At 36th seconds, we cancel the limit to this host. That is, removing the meter field from the rule in the flow table. Obviously, we also observed the bandwidth of download from this host is rising rapidly and without limiting.

D. Integration Evaluation: QoS Limit Application Bandwidth Evaluation

There are a lot of people using the streaming applications nowadays and those applications always take up an amount of networks source. We integrated with application identification to classify each flow belongs what the application is, consequently.

In our experiment environment, as shown in Fig. 9. We use a mirror switch to replicate the whole traffic form SDN switch
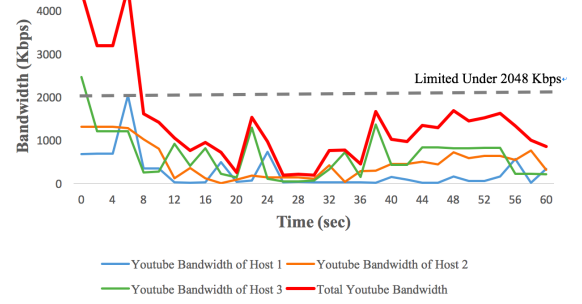

Fig. 14: Limit the Youtube rate to a network domain.

and provide the application identification system to classify the flows belong which applications. Application identification system will upload the result of identification to database. Then the controller will get the result from the database and update the flow information of application. Therefore, we can use the flow information (5-tuple and the result of identification) to complete our limitation to application.

We choose YouTube to verify our limitation function of applications and there are 3 hosts (host 1, host 2 and host 3) in the same network domain. Then we will limit the Youtubes bandwidth of this network domain, that is, the sum of bandwidth from Youtube of host 1, host 2 and host 3.

As shown in Figure. 14, in the beginning without limitation, the total bandwidth of this network is about 3000 Kbps to 4000 Kbps. At 8th seconds, we limited the total bandwidth from Youtube to 2048 Kbps in this network domain. Therefore, we can find out the total traffic of Youtube from this network domain is reducing immediately. Clearly, the total traffic from Youtube will not exceed the limited bandwidth (2048Kbps) since we limited the Youtube to this network domain.

When using our limitation function of application, we can guarantee the traffic of this network domain will not over the network capacity and prevent the traffic congestion in short.

VI. CONCLUSION

The proposed vCPE framework enables deploying NFVs as edge of network and these VNFs are implpemented with multiple flow table management model. In this way, the customers only need a SDN switch at local network, and some network functions that could not have been done by single table machanism are also resolved. The experimental results show that the framework provide performance in VNF compete over single table SDN application. The integration evaluation also show its flexibility to integrate with any bonus applicaion identification system, IDS or IPS.

REFERENCES

[1] O. N. Foundation, "Software-defined networking: The new norm for networks," tech. rep., 2012.

[2] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, pp. 14–76, jan 2015.

[3] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, pp. 69–74, Mar. 2008.

[4] "Openflow switch specification." https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.0.pdf, June 2012.

[5] "Network functions virtualisation: An introduction, benefits, enablers, challenges and call for action, white paper.." http://portal.etsi.org/NFV/NFV_White_Paper.pdf.

[6] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2016.

[7] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: Rapid prototyping for software-defined networks," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, Hotnets-IX, (New York, NY, USA), pp. 19:1–19:6, ACM, 2010.

[8] "NEC's vCPE solutions." http://www.nec.com/en/global/solutions/tcs/vcpe/.

[9] J. Soares, M. Dias, J. Carapinha, B. Parreira, and S. Sargento, "Cloud4nfv: A platform for virtual network functions," in *2014 IEEE 3rd International Conference on Cloud Networking (CloudNet)*, Institute of Electrical and Electronics Engineers (IEEE), oct 2014.

[10] M. C. Luizelli, L. R. Bays, L. S. Buriol, M. P. Barcellos, and L. P. Gaspary, "Piecing together the NFV provisioning puzzle: Efficient placement and chaining of virtual network functions," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Institute of Electrical and Electronics Engineers (IEEE), may 2015.

[11] H. Moens and F. D. Turck, "VNF-p: A model for efficient placement of virtualized network functions," in *10th International Conference on Network and Service Management (CNSM) and Workshop*, Institute of Electrical and Electronics Engineers (IEEE), nov 2014.

[12] "Pica8 OpenFlow-enabled switches." http://www.pica8.com/products/pre-loaded-switches.

[13] "Open Networking Foundation." https://www.opennetworking.org/index.php.

[14] J. Blendin, J. Ruckert, N. Leymann, G. Schyguda, and D. Hausheer, "Position paper: Software-defined network service chaining," in *2014 Third European Workshop on Software Defined Networks*, Institute of Electrical and Electronics Engineers (IEEE), sep 2014.

[15] "Edge Core switches." http://www.lagopus.org/.

[16] "Edge Core switches." http://www.edge-core.com/productsKind.php?cls=1.

[17] "OpenDayLight." https://www.opendaylight.org/.

[18] "OpenStack." https://www.openstack.org/.

[19] "Ryu SDN framework." http://osrg.github.io/ryu/.

[20] "Docker." https://www.docker.com/.

[21] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-enabled NFV architecture," *IEEE Communications Magazine*, vol. 53, pp. 187–193, apr 2015.

[22] R. Mijumbi, J. Serrat, and J.-L. Gorricho, "Self-managed resources in network virtualisation environments," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Institute of Electrical and Electronics Engineers (IEEE), may 2015.

[23] NFV, "Gs nfv 003 - v1.2.1 - network functions virtualisation (nfv); terminology for main concepts in nfv," tech. rep., dec 2014.

[24] NFV, "Gs nfv-inf 004 - v1.1.1 - network functions virtualisation (nfv); infrastructure; hypervisor domain," tech. rep., jan 2015.

[25] P. Minoves, O. Frendved, B. Peng, A. Mackarel, and D. Wilson, "Virtual CPE: Enhancing CPE's deployment and operations through virtualization," in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, Institute of Electrical and Electronics Engineers (IEEE), dec 2012.

[26] A. Lombardo, A. Manzalini, G. Schembra, G. Faraci, C. Rametta, and V. Riccobene, "An open framework to enable NetFATE (network functions at the edge)," in *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*, Institute of Electrical and Electronics Engineers (IEEE), apr 2015.

[27] NFV, "Gs nfv-man 001 - v1.1.1 - network functions virtualisation (nfv); management and orchestration," tech. rep., dec 2014.

[28] N.-F. Huang, I.-J. Liao, H.-W. Liu, S.-J. Wu, and C.-S. Chou, "A dynamic QoS management system with flow classification platform for software-defined networks," in *2015 8th International Conference on Ubi-Media Computing (UMEDIA)*, Institute of Electrical and Electronics Engineers (IEEE), aug 2015.

[29] N.-F. Huang, S.-J. Wu, I.-J. Liao, and C.-W. Lin, "Bandwidth distribution for applications in slicing network toward SDN on vCPE framework," in *2016 18th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Institute of Electrical and Electronics Engineers (IEEE), oct 2016.

[30] M. Kuniar, P. Pereíni, and D. Kosti, "What you need to know about sdn flow tables," in *Passive and Active Measurement*, pp. 347–359, Springer Science + Business Media, 2015.

[31] O. N. Foundation, "The benefits of multiple flow tables and ttps," tech. rep., 2015.

[32] N.-F. Huang, G.-Y. Jai, C.-H. Chen, and H.-C. Chao, "On the cloud-based network traffic classification and applications identification service," in *2012 International Conference on Selected Topics in Mobile and Wireless Networking*, Institute of Electrical and Electronics Engineers (IEEE), jul 2012.

[33] C.-C. Chou, "A Cloud based Application Classification Service Platform with Machine Learning Algorithms," Master's thesis, National Tsing University, Taiwan, 2013.

[34] T. K. Ho, "The random subspace method for constructing decision forests," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 832–844, 1998.

[35] "iPerf." https://iperf.fr/iperf-doc.php.

[36] N. Chinchor, "Muc-4 evaluation metrics," in *Proceedings of the 4th Conference on Message Understanding*, MUC4 '92, (Stroudsburg, PA, USA), pp. 22–29, Association for Computational Linguistics, 1992.

Nen-Fu Huang

PLACE
PHOTO
HERE

Chia-An Lee was born in 1988. He received the B.S. degree in Undergraduate Program of Computer Science in 2010 from National Tsing Hua University, Hsinchu, Taiwan. Currently he is a Ph.D student of the Department of Computer Science in National Tsing Hua University. His research include Software Define Network ,Network Function Virtualization, Moocs, and data analytics.

PLACE
PHOTO
HERE

Chi-Hsuan Li received the B.S. degree in Undergraduate Program of Electrical Engineering and Computer Science in 2015 from National Tsing Hua University, Hsinchu, Taiwan. Currently she is a graduate student of the Department of Computer Science in National Tsing Hua University. Her research interest is Software Define Network and Network Function Virtualization.

Chia-Chi Chen was born in 1994 and received the B.S. degree in Computer Science in 2016 from National Tsing Hua University, Taiwan. He is a graduate student and major in Computer Science from National Tsing Hua University now. Mr. Chen research chiefly focuses on Software Defined Network in High Speed Network Lab at National Tsing Hua University.

I-Hsien Hsu was born in 1994 and received the B.S. degree in Computer Science in 2016 from National Tsing Hua University, Taiwan. He is a graduate student and major in Computer Science from National Tsing Hua University now. His research mainly focuses on Software Defined Network in High Speed Network Lab at National Tsing Hua University.

PLACE
PHOTO
HERE

Che-Chuan Li was born in Tainan City, Taiwan, in 1993. He received the B.S. degree in computer science from National Tsing Hua University, Hsinchu, Taiwan, in 2015. He is currently pursuing the M.S. degree in computer science at National Tsing Hua University, Hsinchu, Taiwan.

Ching-Hsuan Chen received the bachelor degree in Computer Science department in 2016 from National Tsing Hua University, Hsinchu, Taiwan. Now he is a graduate student of the Institute of Communications Engineering in the same university, National Tsing Hua University. His research mainly focuses on Software Define Network and Network Function Virtualization.

PLACE
PHOTO
HERE

I-Ju Liao