APAC Telecom Innovation Initiative

Work Project #3 Final Report

- Flexible Access Network Virtualization -

Date of Submission: December 17th, 2019

(Last Updated: December 10th, 2019)

Table of Contents

1. Summary

ATII Work Project #3 (WP3) has conducted a three-parties joint lab-trial about flexible access network virtualization technologies under the condition of the joint experiment agreement that was contracted between Nippon Telegraph and Telephone Corporation (NTT), PT Telekomunikasi Indonesia, Tbk. (TELKOM) and Viet Nam Posts and Telecommunications Group (VNPT).

By establishing a testbed based on international Virtual Private Network (VPN) connections between three laboratories, each of which is located in Indonesia, Viet Nam and Japan, a trial system has been built in an office of TELKOM in Bandung, Indonesia, an office of VNPT in Hanoi, Viet Nam and the NetroSphere PIT of NTT in Tokyo, Japan. By using this system, WP3 has conducted the joint Proof of Concept (PoC) on access network virtualization. Through the PoC, WP3 has obtained a lot of useful findings and insights from experimental results.

WP3 has successfully verified that it is technically possible to enhance existing services by applying flexible access network virtualization technologies. We have mainly studied three attractive use cases: simple line opening operation for zero-touch provisioning, Internet Protocol version 6 (IPv6) services, and virtual firewall (vFW) on Central Office Re-architected as a Datacenter (CORD) in a Box (CiaB, now Software Defined Network (SDN) Enabled Broadband Access (SEBA) in a Box). This WP3 final report describes our holistic experimental results, key findings, and future works obtained through joint PoC.

2. Work Project Name

Flexible Access Network Virtualization

3. Objectives and Overview of Activity

This activity aims to propose new service concepts based on flexible access network virtualization technologies over carriers' network platforms with various network functions, and to verify the feasibility by conducting PoC in collaboration with Asia-Pacific (APAC) major telecom carrier members.

WP3 has jointly studied the scope of work, target use cases, technologies

to be studied through the activity, configurations of the joint PoC and so on. WP3 also jointly builds the common experimental platform to conduct WP3 PoC by connecting each lab in three countries: Indonesia, Viet Nam, and Japan. By conducting experiments, performance of use cases is evaluated. The effectiveness and issues are discussed in this report, and those are finally reported as WP3 activity to the Board of ATII by submission of this WP3 final report.

4. Members

Chair:

Hiroo Suzuki, NTT

Members:

I Gede Astawa, TELKOM

Trinh Minh Tri, VNPT

Manabu Yoshino, NTT

5. Scope

WP3 agreed upon the scope of work on zero-touch provisioning basis. WP3 made and released a white paper, “Flexible Access Network Virtualization [1-3].” This White Paper describes requirements and a lot of use cases utilizing access network virtualization concept. WP3 members chose one of the use cases through discussions as the basic model of our PoC (Use case 17: Activation multi-play services).

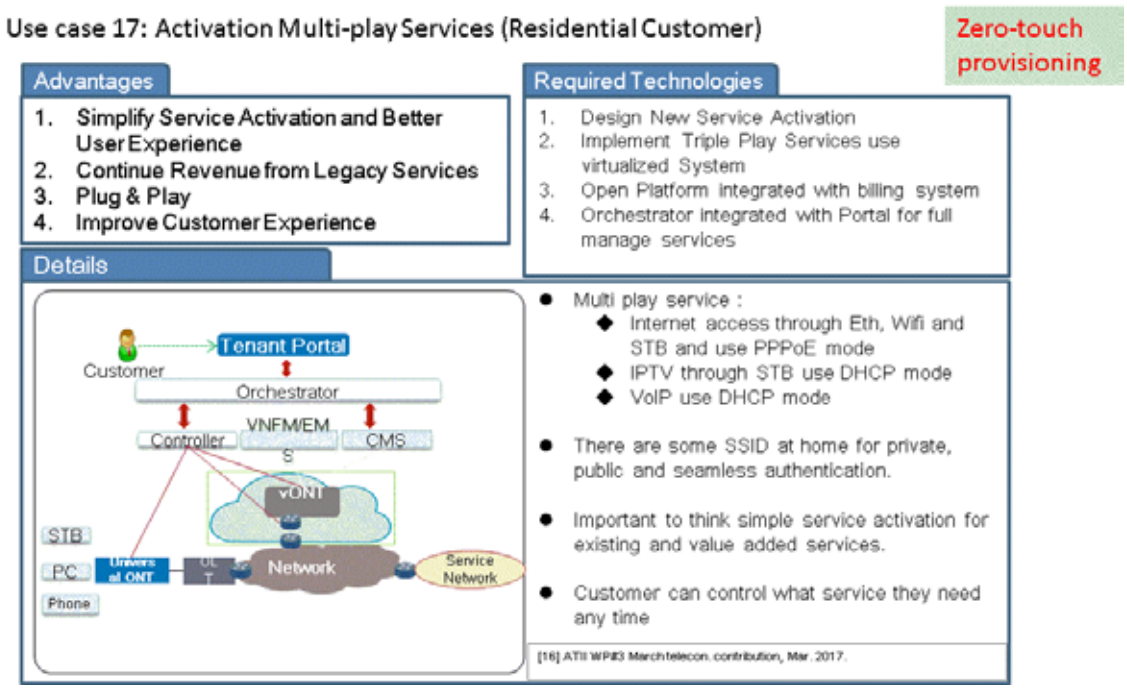

Figure 1: Scope of the work

6. Processes and Timelines

WP3 started to construct a common testbed environment in April, 2018 and completed joint PoC using it in December, 2019.

7. Environment and Target Use Cases of Joint PoC

Based on the use cases we chose, WP3 members discussed what we aim to do and how to do it. As a result, in this joint PoC, WP3 were focused on three use case demonstrations considering zero-touch provisioning: simple line opening operation for zero-touch provisioning, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) and vFW on CiaB. A pluggable module-type Optical Line Terminal (OLT) and Optical Network Unit (ONU) s were used and located in order to study simple line opening operation for zero-touch provisioning in NetroSphere PIT of NTT in Tokyo, Japan. and experimental setup on DHCPv6 functions were mainly set in an office of TELKOM in Bandung, Indonesia and a vFW on CiaB function was placed in an office of VNPT in Hanoi, Viet Nam. Each experimental system was connected by VPN over the Internet.

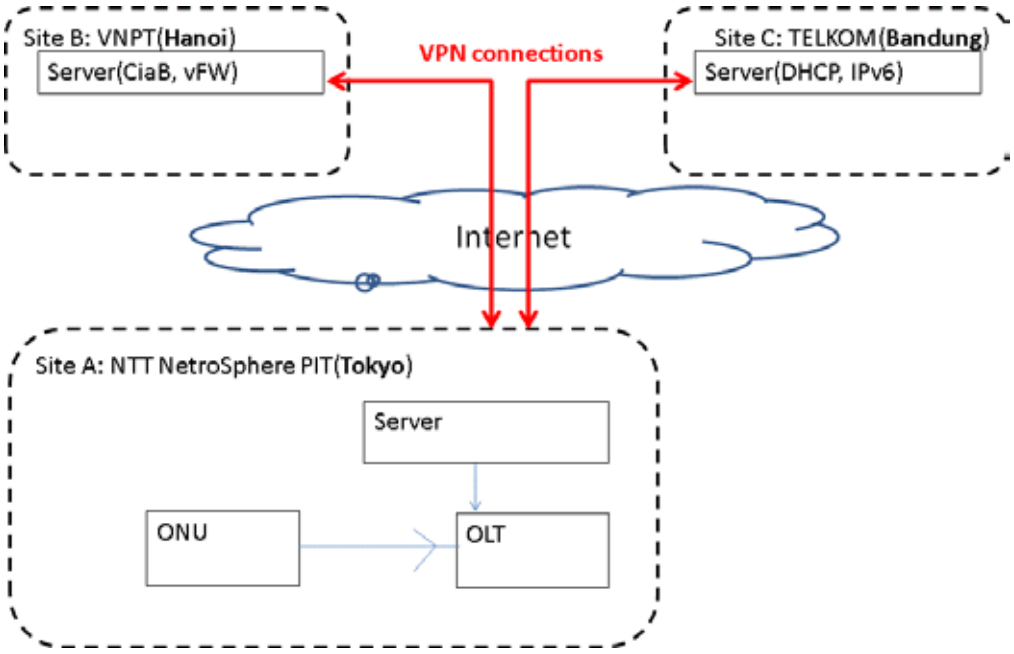

Figure 2: Environment of Joint PoC

Each use case is designed as following:

Ø Simple line opening operation for zero-touch provisioning

The purpose of the simple line opening operation for zero-touch provisioning experiment is to verify operational cost savings through near automated service activation. The network function addition following line opening is also to verify the effective use of resources and the ease of service changes during operation.

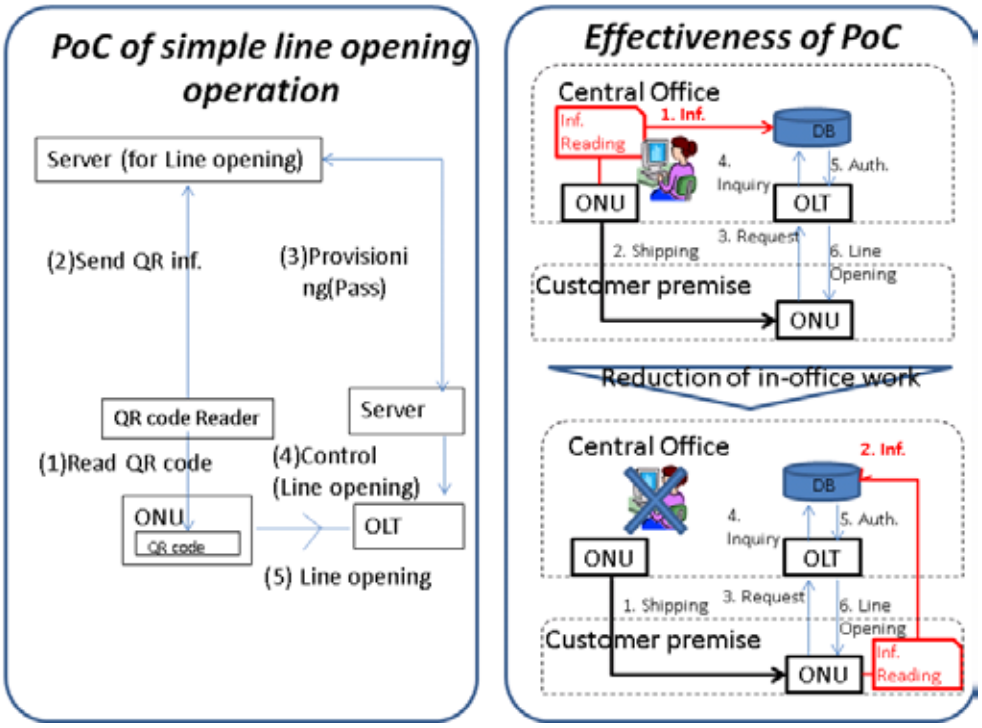

Figure 3: Simple line opening operation for zero-touch provisioning

Ø DHCPv6:

The purpose of the DHCPv6 experiment is to see how the process of obtaining IPv6 on a network configuration using virtual OLT. The function and performance are observed during the trial process and compared with the existing non virtual OLT. The trial process also showed that the service activated almost automatically (line opening, IPv6 address assignment, and Internet access through NAT64) just by scanning the QR code.

Ø vFW on CiaB:

The purpose of vFW on CiaB is to build and verify the feasibility of Fiber to the Home (FTTH) and vFW zero-touch provisioning system. An APAC sized infrastructure testbed (among NTT, VNPT and TELKOM: CiaB, OLT, ONU, Broadband Network Gateway (BNG)...) has been built and a centralized zero-touch control software (Time-based One-time Password algorithm (TOTP) Server) has been developed in the PoC to test the level of automation in multi-services provisioning system.

8. Technologies

Pluggable module-type OLT

WP3 uses technology, which is an access virtualization platform using disaggregated OLT architecture based on SEBA concept [4], as the key architecture to support the flexible access network virtualization. The architecture is shown in Fig. 5. The architecture based on virtualization is composed of hardware and service functions made into software mounted on servers as general purpose hardware at first. This architecture decomposes not only software but also hardware, other than functions that can be realized by general-purpose hardware, is separated to form external modules. The external module is added to a general-purpose hardware to provide a system corresponding to various needs. As one of this architecture, the pluggable module-type OLT that is added to general purpose hardware, an Ethernet-switch (SW) or a server, has been developed by NTT.

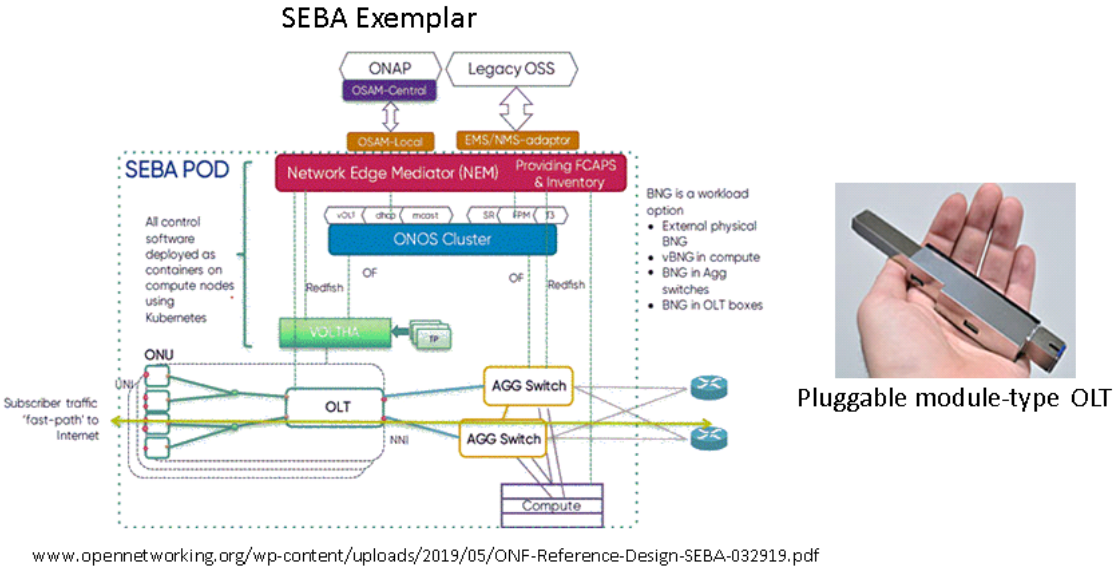

Figure 4: Overview of pluggable module-type OLT

DHCPv6

Technologically, because the prototype virtual access (OLT & Optical Network Termination (ONT)) uses a solution from NTT and is connected via VPN with the TELKOM Lab, so for this experiment, TELKOM is focused on the needs of the current development of how to implement IPv6 in solutions with this access virtualization. Indeed there are some things that cannot be

done, especially related to the experiments on the ONT side, what has just been trialed is the transparent configuration in the OLT-ONT to pass the message needs DHCPv6. In the future, TELKOM will try to make an OLT-ONT virtual prototype, making it possible to test various configurations that are close to the current OLT operations.

CORD: The virtualization technologies for future network

R-CORD which is residential CORD virtualizes legacy FTTH system of telephone company (Telco)'s central office to replace closed and proprietary hardware with software running on commodity servers, switches, and access devices. It allows network operators to benefit from providing new virtualized services (vFW, load balancing, intrusion detection system/intrusion prevention system (IDS/IPS)...) to residential customers, the economies of scale (infrastructure constructed from a few commodity building blocks) and agility (the ability to rapidly deploy and elastically scale services) that commodity cloud providers enjoy today. The main R-CORD's components: OpenStack and Docker are cloud controller for controlling every aspect of virtual machine (vm) s and container's life cycle; ONOS which is SDN controller for controlling every aspects of network infrastructure. The eXtensible cloud Operating System (XOS)-Virtual Network Function (VNF) Manager (VNFM) is the framework used to assemble and control services. XOS controls the cloud infrastructure (provided by OpenStack and Docker) and the network infrastructure (provided by ONOS) to provide a unified control of the CORD's cluster.

9. Details of Joint PoC

In this section, we describe the details of joint PoC which realizes three scenarios shown in Section 7.

9.1. Simple Line Opening Operation for Zero-Touch Provisioning

This section describes the details of the configuration that implements the simple line opening operation for zero-touch provisioning.

9.1.1. System Design and Functional Architecture

The system consists of followings:

- Ø QR code[1] reader
  - n QR code read function and QR code transfer function
- Ø Authentication server
  - n Authentication function and line opening operation function
- Ø Optical access system
  - n ONU, pluggable module-type OLT, SW

9.1.2. Sequence Flow

The sequence flow of simple line opening operation for zero-touch provisioning is shown in Fig. 5. As shown in the figure, the sequence proceeds. The QR code is read and its information is sent to the authentication server. When the server receives it via pre-trusted line for a specific user, the server instructs the optical access system to open the line of ONU corresponding to the code. After opened, traffic from the client is passed to the server.

The DHCPv6 function for ONU 3, the DHCPv6 function for ONU 4, and the Network Address and protocol Translation from IPv6 clients to Internet Protocol version 4 (IPv4) servers (NAT64) function as the vFW function equivalents were added sequentially on the TELKOM router in order to confirm the operation of network functions addition after the line was opened.

---

[1] "QR code" is a registered trademark of DENSO WAVE inc..

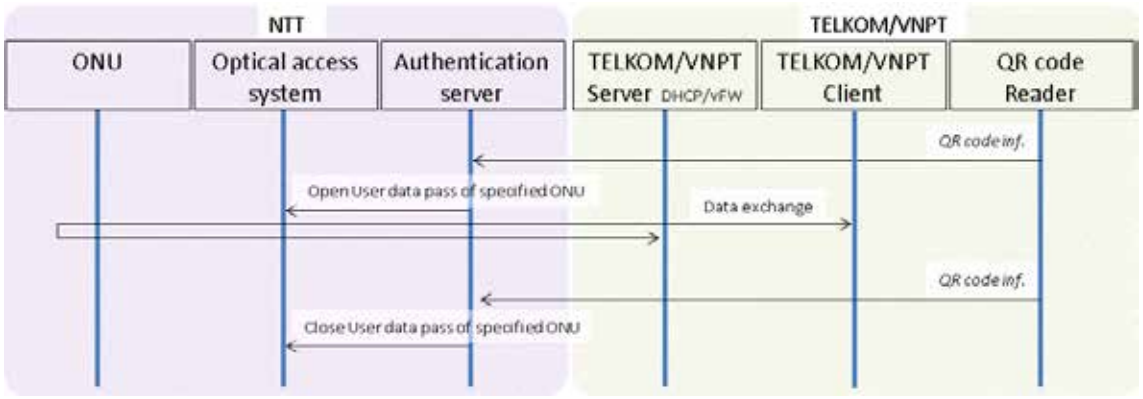

Figure 5: Sequence Flow

9.1.3. Implementation

9.1.3.1. Physical Configurations

An optical access system was installed at NetroSphere PIT of NTT in Tokyo, Japan, and clients were installed at an office of TELKOM in Bandung, Indonesia and at an office of VNPT in Hanoi, Vietnam, respectively.

9.1.3.2. Logical Configurations

Logically, TELKOM/VNPT clients and NTT ONUs are placed close together. The authentication server and QR code information source can be located on any server port of the NTT/TELKOM/VNPT router. In the performance test, the QR code information sources were placed in the office of TELKOM and the authentication server was placed in NetroSphere PIT of NTT.

9.1.3.3. Hardware Specification

The main hardware is listed in Table 1.

Table 1: Hardware Specifications

Hardware	Note
Authentication server	A Windows 7 PC
ONU	Components of optical access network, prototype
Pluggable module-type OLT	A component of optical access network, prototype
SW	A component of optical access network, plugged by a pluggable module-type OLT,

Router	NTT/TELKOM/VNPT sites
TELKOM Client/Server	Raspberry Pi Linux 9.1 Stretch

9.1.3.4. Functions

9.1.3.4.1. QR code Read Function and QR code Transfer Function

A QR code read function reads a QR code. A QR code transfer function transfers information of the QR code to an authentication server. QR codes indicate HTTP requests that include authentication server address as a destination, the target ONU information and flag of open/close. Fig. 6 shows the QR codes used in this experiment.

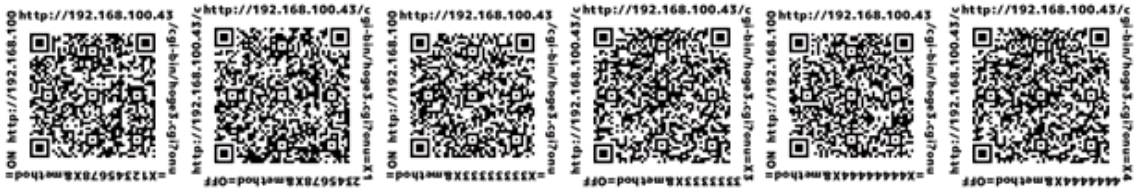

Figure 6: QR Code

9.1.3.4.2. Authentication Function and Line Opening Operation Function

An authentication function and a line opening operation function are composed of an Apache server which receives a HTTP request generated from QR code information and a CGI program which starts a script for open/close the line of a specific ONU according to the QR code information. The program cyclically monitors the presence of HTTP requests to the server. When it detects and authenticates the request, it instructs the OLT to open the line of ONU corresponding according to the code.

9.1.4. Evaluation

9.1.4.1. Evaluation Items and Methods

The usefulness was evaluated by following items and methods.

- Ø Scenario evaluation
  - n Effect of simple line opening operation for zero-touch provisioning

A qualitative evaluation was made from the viewpoints of the amount of work required at the time of new line opening/line relocation and the

reliability of authentication.

- Technology evaluation

The behavior was evaluated by the following method.

- Functional capability test
  - Verified the functionality is working properly.
  - Captured packets at the network layer, analyze the captured data, and verify that HTTP requests and controls are communicating correctly.
  - Confirmed that only the corresponding ONU is open/close.
  - Confirmed that ONUs other than the corresponding ONU are not affected.
  - Verified that network functions are added and removed without interruption to others.

- Performance test
  - Verified the dependence of opening time on the number of ONUs.
  - Verified the dependency of the time of network function addition after line opening on the number of network functions.

9.1.4.2. Evaluation Results

- Scenario evaluation
  - Effect of simple line opening operation for zero-touch provisioning

The evaluation results are shown in Table 2. From left to right, the table shows maintenance worker, notification of authentication and ONU information via the target line for authentication, and notification of ONU information via pre-trusted line for specific user. Each was compared and verified. As shown in the table, the last one is superior to others. That is, the following effects can be expected.

- Reduce latency and improve user experience with fast remote control of customers.
- Management and operation costs can be reduced by services, and human resources can be applied to other valuable activities.

Table 2: Comparison of line opening operation

	maintenance worker	Notification of authentication and ONU information via target line for authentication	Notification of ONU information via pre-trusted line for specific user
Amount of work in new line opening/line relocation	No Good	Good	Good
reliability of authentication	Good	No Good	Good

Ø Technical evaluation

n Function capability test

Table 3 shows the results of the functional capability test. Functions are verified as shown in the table.

Table 3 Test results of simple line opening operation for zero-touch provisioning

No	test items	test results
1	QR code: Are QR codes read properly?	OK.
2	QR code: Does an HTTP requests for a QR codes arrive at authentication server?	OK
3	Authentication server: Does the displayed web page correspond to a QR code?	OK
4	Authentication server: Is the proper ONU's script started according to QR code?	OK
5	Authentication server: Is an instruction sent to the optical access system?	OK
6	Optical access system: Is only the ONU specified in the authentication server's instructions open/close?	OK
7	Open/Close: Does traffic from the client not reach the server or the Internet before opening or after closing?	OK

8	Open/Close: Does traffic from the client reach the server or the Internet after opening and before closing?	OK
9	Open/Close: Is there no change in traffic from the client under the ONU that is not the target of the operation?	OK
10	Configuration: Can the simple line opening operation function be placed on either of NTT and TELKOM/VNPT?	OK
11	Addition of network function following line opening: Is it possible to add and to remove respective DHCPv6 functions and NAT64 function without restarting routers nor affect other functions?	OK

- Performance test

In the performance test, assuming the simultaneous operation of up to 32 ONUs, the dependence of the opening time on the number of ONUs was measured. The time increases as the number of ONU increases.

The dependence of the time of network function addition after line opening on the number of network functions was also measured. The time increases as the number of functions increases.

9.2. DHCPv6

9.2.1. System Design and Functional Architecture

For DHCPv6 trial needs via virtual access, DHCPv6 servers and clients are prepared on the TELKOM side, the connection is using VPN. Every communication between client-server & client-client must go through virtual access (OLT-ONT) in the NetroSphere PIT of NTT. The general configuration is as follows:

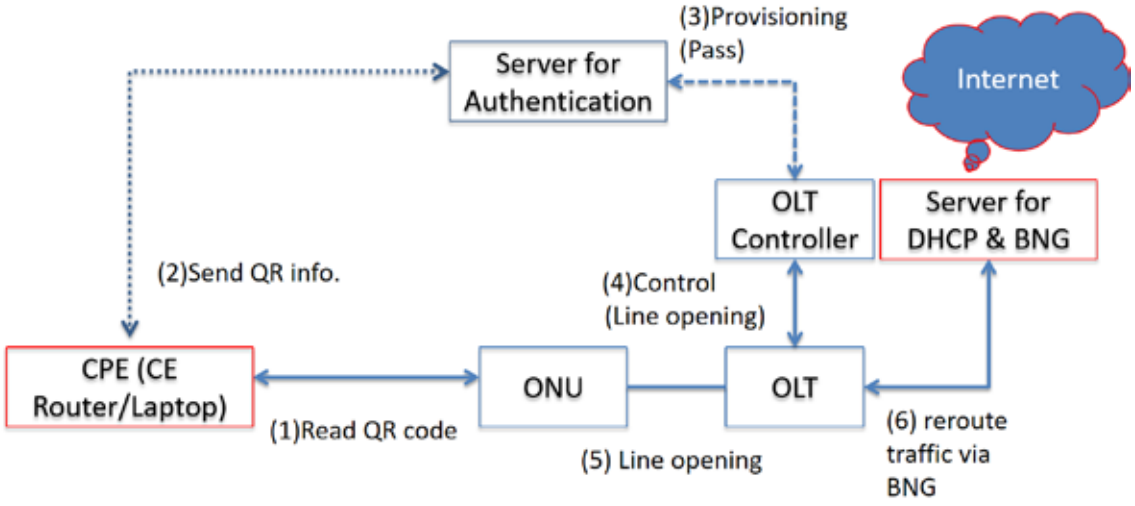

Figure 7:

Subject to monitor:

- Function test for Customer Premises Equipment (CPE)/Client from TELKOM connected to NTT running same use case, NTT share QR Code, initiate service from TELKOM CPE, after success open profiling, continue with process get IPv6 address and open to the Internet.
- Monitor function test for DHCPv6 success/not success.
- Monitor function test for Point-to-Point Protocol over Ethernet (PPPoE) on BNG success/not success
- Monitor delay process get IPv6 address compare between using vOLT & existing OLT.
- Monitor service test for the Internet connection

9.2.2. Sequence Flow

For sequence flow, the experiment starts from the PC Client via Virtual

Access DHCPv6 Server and BNG to the application/the Internet, the details are as in the following chart

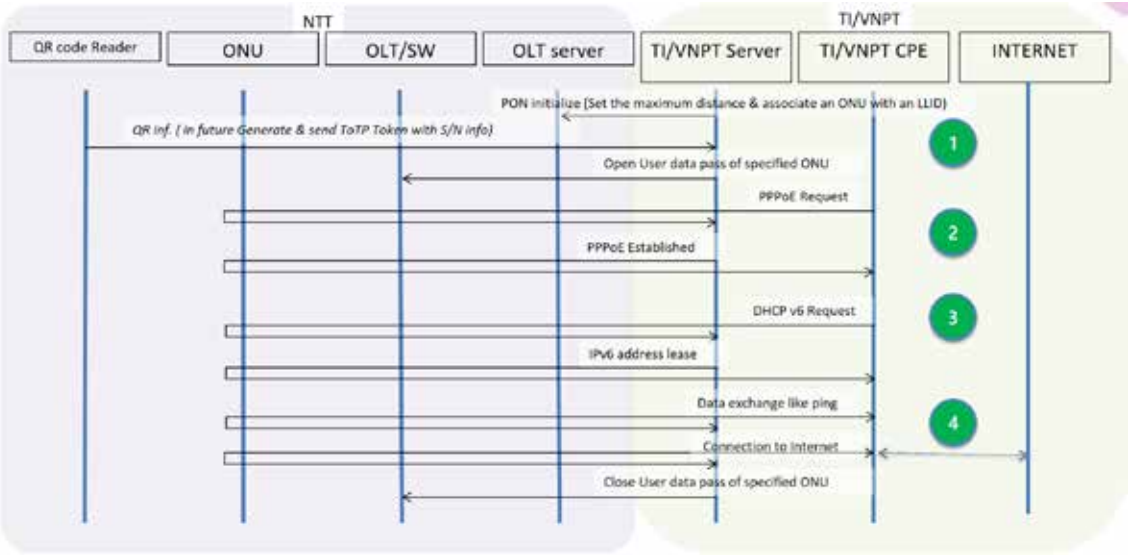

Figure 8:

An attempt to get/release IPv6 from DHCPv6 was carried out after the open profile process was successful at the PON level between OLT and ONT and PPPoE already success establish. Observations made are in terms of function and performance.

9.2.3. Implementation

9.2.3.1. Physical Configurations

Physical configuration in each lab in TELKOM, VNPT & NTT and the relationship between the three labs that use VPN

9.2.3.2. Hardware Specification

The specifications of the devices used in TELKOM are as follows:

- Router for VPN connection & NAT64: Juniper
- Server for TOTP, DHCPv6 & PPPoE/BNG: DELL
- Router/Access Point: Mikrotik hAP Series
- Client for connection test: Raspberry Pi (Linux), Windows 10, iPad Pro, Smartphone SAMSUNG C9 PRO
- Existing Access: OLT Huawei MT5600 & ONT Huawei HG8245H

9.2.3.3. Function

The function that will be observed on this trial is how that prototype virtual access with pluggable module-type OLT when serving existing broadband access, in this trial we running use case open profile & IP over Ethernet (IPoE) using IPv6. Due to limited resources and time, the use case that was tested was still very simple, namely that on the access node side it was quite transparent to see that it could function-fully skip and see its performance compared to the current one. In the future, this virtual access function needs to be made as a testbed facility on our lab so that it can be thoroughly explored in preparation for its implementation.

9.2.4. Evaluations

9.2.4.1. Evaluation Items and Methods

The parameters that will be observed for this experiment are as follows:

Table 4: Test results of DHCPv6

Test	Expected	Result
Test Connection, case initiate service from TELKOM CPE	Success open profiling, PPPoE established, get IPv6 address, and connect the Internet. [need observe response time, delay process & monitor stability of connection]	OK. Trial success open profiling, PPPoE established, until get IPv6 address and test ping to public address. Observations of connection stability during trials are generally quite stable as long as the VPN connection can be kept operating normally.
Test Function for DHCPv6 with both clients from TELKOM using pluggable module-type OLT and ONU located at NTT (Virtual Access: VA)	Success open profiling, PPPoE established, get IPv6 address, ping test between, connect the Internet. [measure DHCPv6 response & delay process on node	OK. Trial success open profiling, PPPoE established, until get IPv6 address and test ping to public address and between client. Observations of

	access]	connection stability during trials are generally quite stable as long as the VPN connection can be kept operating normally.
Test Function for DHCPv6 with both clients from TELKOM using commercially-available OLT and ONU located at TELKOM (Fixed Access: FA)	Success PPPoE established, success get IPv6 address, ping test between, connect the Internet. [measure DHCPv6 response & delay process on node access]	OK. Trial success PPPoE established until get IPv6 address and test ping to public address and between client. Observations of connection stability during trials are generally quite stable with any simulation on Optical Distribution Network (ODN) side to prefer like real network FTTH.

For the existing OLT conditions in the TELKOM Lab, the mechanism of using Dynamic Bandwidth Assignment (DBA) greatly influences the process delay. To use an access virtualization solution that hasn't been explored in relation to this DBA, it should conceptually improve this DBA mechanism to support services that require low delay. Overall the results when compared to their performance related to response time and delay are still relatively the same, with notes on the existing OLT side that are conditioned on not much traffic load. The analysis is likely to be significant differences for the use of different DBA mechanisms and the distribution of distributed clouds.

9.2.4.2. Evaluation Results

- Scenario evaluation
  - Feasibility verification of PoC concept

To prove conceptually how to implement IPv6 in access virtualization, an experiment was carried out to see its function and performance. The function

is how the client side of the ONT can get an IPv6 address from DHCPv6 which in this case is simulated in a centralized cloud/server. The next step is the function of the connection using IPv6 can communicate with several scenarios, namely client-server, client-client & client-the Internet. Due to limited time and resources available, then in this initial stage only experiments can be carried out for transparent configuration on the OLT side. The ONU is for the ONT only as a Single Family Unit (SFU)/bridge, whereas to make the ONU function as a Home Gateway (HGW) it has not been done, considering that the functions are already represented. Another thing to consider is that, with the concept of virtualization in access nodes and Network Termination Equipment (NTE), both OLT and ONT will use simple generic white boxes with simple capability, the main capabilities will be placed on the server/cloud.

- Effects of PoC

In accordance with the initial conditions that exist, which is only possible to see the function and performance that follows it. In accordance with the objectives of this PoC, it has been able to meet its objectives, only for the detailed requirements of the characteristics of access virtualization, the relationship between the separation of generic hardware OLT/ONT with functions that are placed virtually in the cloud and the possibility for proposals using other DBA mechanisms cannot be done at the stage of this. The next plan for TELKOM is to make prototypes and testbeds for virtual access solutions based on the knowledge and experience gained during discussions and trials in the ATII WP3 container with NTT and VNPT.

- Technical evaluation
  - Functional capability test

In connection functions performed at this PoC are as follows:

1. Successful open profile connections are carried out in accordance with the agreed flow message concept.
2. The connection to DHCPv6 was successfully carried out and both clients used during this trial were successful in getting the IPv6 address as specified.
3. Test the connection function successfully done, both from client-server, client-client or from client to the Internet.

4. The connection mechanism for IPv6 during the trial uses the NAT64 concept, because the availability of public IP is only IPv4. The function can already represent because the connection is successful using either IPv4 or IPv6.

- Performance test

For the performance observed in this experiment are response time and delay. Response time is related to process flow to get an IPv6 address from DHCPv6, while delay is the process of communication between client-server, client-client and client to the Internet using IPv6 addresses. These two results are then compared between those using access virtualization in the NetroSphere PIT of NTT by using existing access in TELKOM. At the time of trial and calculation the results must pay attention to the difference in connection between the two. When the round trip time over the Internet is extracted, the average response time is around 150 ms.

The process delay (i.e. process time between OLT and ONT) for VA & FA at traffic load of 1 to 10% is also evaluated. Results are relatively the same on all conditions. It was found that there is a significant increase in the process delay when the traffic load in FA becomes 90%. Experiments for full traffic load on VA have not been carried out due to the limitations of environment trials. In theoretical analysis, because the VA concept uses a modular concept, it is possible to get a smaller process delay when implementing different DBA mechanisms for different customer needs. In the future, this will be an incentive to immediately prepare a VA testbed so that more complex experiments can be carried out.

9.3. vFW on CiaB

9.3.1. System Design and Functional Architecture

At the VNPT side, a CiaB server is implemented as a cluster of three libvirt based vagrant's vms: corddev, head1, and compute1. The compute1 node works as a commodity server hosting both containers based and vm based VNFs. The container based VNFs are hosted as Linux namespace whose network can be configured by veth-pair. The vm based VNFs are hosted on libvirt. This node also has an OpenvSwitch (OVS) to do the overlay switching (switching among vnfs) for traffic flowing inside the node.

The head1 node is the controller node with OpenStack, Docker, lxc, ONOS…to control every CiaB cluster's component. The OpenStack is used to control the libvirt's vm life cycle, the Docker is used to control the container life cycle, the lxc is used to control the Linux container's life cycle and ONOS is used to control the openvswich. Besides hosting the CORD components' controller, head1 also hosts the XOS which is the overall controller for CORD system. Via api, XOS can control all other components controllers: OpenStack, Docker, lxc, ONOS to manage the service life cycle (it is equivalent to VNFM in Network Functions Virtualisation (NFV) references).

We have developed and implemented a web-based TOTP server to do the network auto-provisioning tasks. The TOTP server can manage users, traffic flows, NTT interface, Token for the following auto-provisioning process. TOTP server generates the pair (customer, QR code) and controls the CORD system to open the Internet line, spin up VNF and route the customer traffic though VNF to the Internet. At the NTT side, there is an authentication server to control OLT to open the Internet line, the OLT and ONU for the FTTH system.

The control and data flow in the system is described as following: The installation worker uses the FreeOTP app on his mobile phone to capture the QR code on ONT to get the token and send it back to TOTP server to check whether the token belongs to a customer. If it is right, the ToTP server will send a rest api command to XOS server to request it to spin up vFW VNF, then TOTP server will send the rest api command to the ONOS controller on the head node for adding flows to OVS to route customer traffic through the vFW. Finally, the TOTP server sends the command to NTT's authentication server to ask it opening the Internet line. After finishing the provisioning

process, Test client PC can connect to the Internet via: Router -> Voen -> ATTT -> Router -> VPN -> Router -> ONU1 -> OLT -> Router -> VPN -> Router -> ATTT-Router -> voen -> Router -> em3 -> virbr4 -> fabric port2 -> eth0.222 (vsg vm 222) -> eth1 -> eth0 -> eth0.500 -> head node -> em1 -> the Internet.

The current CORD's traffic flow does not meet our PoC requirements. Specifically, we need the traffic from Client PC after flowing through NTT system to enter CiaB server at port em3 to compute1's OVS and flow through vFW to go out of em1 port for the Internet. But, current CORD assumes there is only one port for traffic both entering CiaB server and exiting to the Internet. Furthermore, the CORD system assumes test client staying on the head1 so the traffic flow is from head1 to compute1's OVS -> vFW -> head1 -> the Internet. We have re-designed the network by creating a new Linux bridge virbr4 and add the pair port to virbr4 to connect directly to compute1, the outgoing traffic is kept unchanged as traditional CORD.

9.3.2. Sequence Flow

When the installation worker finishes his fiber optic work, he can open the FreeOTP app on his mobile phone and capture the ONT's QR code (1) and check the time based generated Token on TOTP website (2, 3). If the token is valid, TOTP server will spin up a vm on compute1 node for vFW (5') and add flow to OVS to route customer's traffic through that vFW (5) then send the command to NTT's authentication server to open the Internet for this customer (6). When the control process finishes, the Test client PC can connect to the Internet. Furthermore, the customer can remotely access to vFW to allow/deny traffic to go to any specific destination.

9.3.3. Implementation

9.3.3.1. Physical Configurations

- CiaB server: CPU (Intel(R) Xeon(R) CPU E5-2640 v4 @ 2.40GHz 20 cores, 40 threads) Ram (64 GB), Storage (212 GB), Operating system: Ubuntu 16.04.6 LTS;
- Voen switch: CPU (Intel(R) Xeon(R) CPU E3-1220 v3 @ 3.10GHz, 4 cores), RAM (8 GB), Storage (110 GB), Operating system: Ubuntu 18.04.3 LTS;
- Client PC: CPU (Intel(R) Core(TM) i3 CPU 530 @ 2.93GHz, 4 cores),

RAM: 2GB, Storage: 291 GB, Operating system: Ubuntu 16.04.1 LTS

9.3.3.2. CORD Implementation

CORD's backbone network structure is shown as follows. There are 4 main networks used to connect among Head1, RD5 (CiaB server), Compute1 and Corddev. Network virbr1 (virtual interface virbr1's IP address 192.168.121.1) is used to connect between Head1's eth0 and Compute1's eth0 for control traffic. This network includes 2 virtual interfaces: vnet0 which is the virtual pair of Head1's eth0 and vnet6 which is the virtual pair of compute1's eth0. Network virbr2 is used to connect between Head1's eth1 and Corddev's eth1. This network includes 2 virtual interfaces: vnet1 which is the virtual pair of Head1's eth1 and vnet5 which is the virtual pair of corddev's eth1. Network virbr3 (IP address 10.1.0.x) is used to connect between Head1's eth2 and Compute1's eth1 for management traffic. This network includes 2 virtual interfaces: vnet2 which is the virtual pair of Head1's eth2 and vnet7 which is the virtual pair of compute1's eth1. Network leaf1 is used to connect between Head1's eth3 and Compute1's eth2 for data traffic. This network includes 2 virtual interfaces: vnet3 which is the virtual pair of Head1's eth3 and vnet8 which is the virtual pair of compute1's eth2.

Beside the Ethernet and vnet ports used to connect the back bone network, CORD also has many other ports and virtual switches to connect many kinds of its components. All virtual and physical ports of CORD are presented as follows.

A CORD's tenant network structure is presented as follows. A test client sends from port VLAN eth0.222.111 the traffic tagged by 2 VLANs: 222 and 111. The packets flow to OVS's port 2 and switched to its port 3. From here the packets enter port vsg vm's eth0 and following VLAN classification to go to port eth0.222 and eth0.222.111 of vsg vm and enter eth1 of Docker vsg.222.111. The packets after entering this container will be proceed by firewall and then sourced NAT by iptables to the IP address of 10.7.1.3 and push out to port eth0.500 to go out of the Docker container. Then, the packets are entered OVS and popped the labeled then send out to Head1 then to the Internet.

CORD has four main types of virtual network connections to connect many components inside this cluster. First, the tap device is used to connect a virtual machine port with host. Usually, the interface pair (ethX-vnetX) of

tap device has the same mac address's lower octet. We have seen many tap devices in CORD's backbone network structure. Secondly, veth-pair is used to connect the OVS port with the host. Usually, the interface pair (qvbXXX-qvoXXX) has the same mac address. Thirdly, Linux bridge is a logical bridge created in Linux to connect many components' interfaces together. For example, the Linux qbrXXX connects two interfaces: vnet0 and qvbXXX for vm01 to connect to the OVS br-int. OVS is a multilayer software switch used to connect and control traffic in many components of CORD.

Beside many above network elements, CORD also has many components: OpenStack (ceilometer, glance, juju, keystone, mongodb, nagios, neutron-api, nova-cloud-controller, openstack-dashboard, percona-cluster, rabbitmq-server), Docker container for XOS (rcord_xos_gui, rcord_xos_ws, rcord_xos_chameleon, rcord_xos_tosca, rcord_xos_ui, rcord_xos_core, rcord_addressmanager-sysnchronizer, rcord_openstack_synchronizer, rcord_volt_synchronizer, rcord_vsg_synchronizer, rcord_onos_synchronizer, rcord_fabric_synchronizer, rcord_vrouter_synchronizer, rcord_vtn_synchronizer, rcord_xos_db, rcord_xos_redis, rcord_registrator, rcord_consul) and Docker container is also for SDN ONOS (onosfabric_xos-onos, onoscord_xos-onos)

9.3.3.3. Traffic flow implementation for CORD

The current CORD flow traffic is not satisfied with our implementation demand because our testbed not only controls traffic flow inside CORD but also the traffic flowing from NTT side. We have revised the traffic flow design of CORD for TELKOM to be able to control the traffic from NTT. When the data traffic enters CiaB through em3 we route it to the virtual bridge virbr4 which is created by us to manage the specialized flow and the virbr4 also includes the port vnet6 and as in the core network structure, vnet6 is connected to eth0 of compute1. We include compute1's eth0 to OVS so that OVS can control all the traffic from compute1's eth0. When the traffic enter OVS, we have set the flow to map that traffic out to port 3 to vsg vm then to eth1 of vFW container; from here, packets are controlled by firewall then source NAT to IP address 10.7.1.4 of port eth0 then push them out through the port vsg vm's eth0.500 to flow back to OVS which has been setup by us to route these packets out port 2 to head1 then to virtual switch virbr1 and to the Internet via port em1.

9.3.3.4. TOTP server implementation

TOTP server is a web-based software self-developed by VNPT to do the FTTH and Middlebox auto-provisioning. The software has the following interfaces and functions:

Manage user: List Users, Delete Users, Insert Users, Show QR code

The Insert Users feature let the software admin insert a user including name and phone number then the software will generate a secret for the user and store in its database. The Delete Users feature let the software admin delete a specific user based on his phone number. The List User feature let the admin list all the current users in the system, the Show QR code feature let the admin show the QR code of the user.

Manage flows: List Flows, Add Flow, Delete a Flow

The Add Flow feature lets the admin add a flow to the OVS to control customer traffic flowing through vFW. The Delete a Flow feature deletes a flow from OVS. The list flow feature lists all the flows of the OVS.

Manage NTT interface: Start ONU, Stop ONU

The Start ONU feature lets the admin send the commands to NTT's authentication server to open the Internet line; The Stop ONU feature lets the admin send the command to NTT's authentication server to close the Internet line.

Manage Token: Check Token

The Check Token feature lets the installation worker add the customer's information (phone number, token) to check if the token is right belong to customer, the software will spin up vFW, control OVS to forward customer traffic via vFW and send the command to NTT's authentication server to open the line to the Internet. The algorithm of Check Token is presented as follows:

The auto-provisioning process with TOTP Server

After the VNPT's worker finishes setting up the optical fiber, he can open FreeOTP software in his mobile phone, capture the QR code attached on ONT, and enters the generated token to TOTP Server. The TOTP Server will: (1) spin up the vFW, (2) add flows to OVS for routing customer's traffic through vFW then (3) send commands to NTT's authentication server to open the Internet line for customer. Fig. 9 shows this auto-provisioning

process.

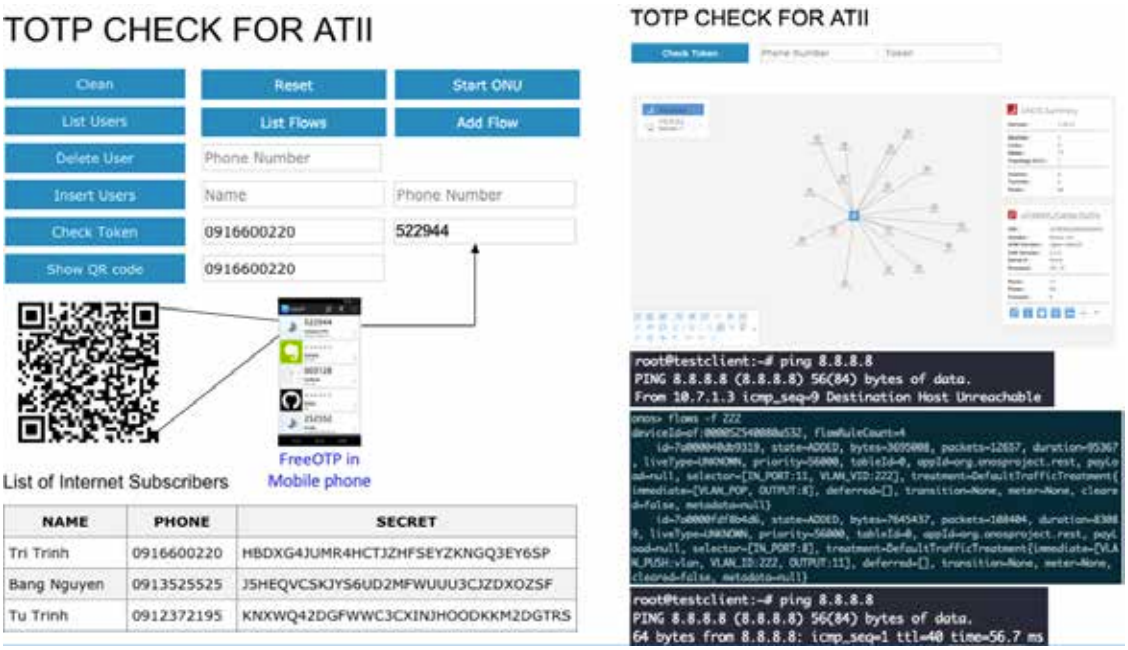

Figure 9: The Overall auto-provisioning process with TOTP Server

9.3.4. Evaluations

9.3.4.1. Evaluation Results

- Technical evaluation
  - Functional capability test

Table 5: TOTP Server functional capability test

No	Category	Test items	Results
1	Manage user	List Users	OK
2		Delete Users	OK
3		Insert Users	OK
4		Show QR code	OK
5	Manage flows	List Flows	OK
6		Add Flow	OK
7		Delete a Flow	OK
8	Manage NTT interface	Start ONU	OK
9		Stop ONU	OK
10	Manage Token	Check token	OK

Table 6: FTTH and Middlebox auto-provisioning process test

Step	Actions	TOTP Functions	Results
1	FTTH system administrator adds new customer information (name, mobile number) to the system.	Insert Users	OK
2	FTTH system administrator get the QR code of the newly added user (the system will generate a secret string from the customer's mobile number and generate the QR code based on this secret string) and paste it on the customer's ONT	Show QR Code	OK
3	When the customer side's installation worker finishes installing optical fiber, he can open FreeOTP app. from his mobile phone, capture the QR code on ONT and get the timebased token (FreeOTP app will generate a token from the information of QR code and the time)	FreeOTP function of mobile phone	OK
4	The worker opens the TOTP server website to enter that time based token for the TOTP server to check the validity of token then executing the Internet line opening and setting up vFW for that the Internet line if the token is validated. This process comprises the following steps:	Check Token	OK
4.1	Check whether the Token is valid: System will generate a token based on time and secret of the customer and compare this token with the token submit by the customer side's installation worker.	Check Token	OK
4.2	Add flows to OVS to route the traffic through vFW	Add Flow	OK
4.3	Send the command to NTT's authentication server to open the line for the Internet	Start ONU	OK
4.4	Customer's traffic flows to the Internet via		OK

	vFW		

- Performance test

End to end performance test

As expected, the Internet traffic has to flow through so many hops so the performance of the system is not so good. We realize that, to make the traffic auto-provisioning for both FTTH and vFW practical, many solutions need to propose to improve the switching performance of vFW based on VNF and decrease the hop need for customer traffic flow to the Internet. In WP4, we have proposed OVSPP (OVS+Soft Patch Panel (SPP)) for integrating Data Plane Development Kit (DPDK)-SPP on OVS to improve the switching performance inside CORD and we also deploy DPDK on vFW VNF for improving switching performance of vFW.

Time to execute each function

The time to execute each partial function of the whole system: compare TOTP Token (right token), compare TOTP token (wrong token), add flow to OVS for routing traffic via vFW, send control frame to NTT for opening the Internet port are presented. The processing time is very low comparing to the end to end system delay time. So, we conclude that, most of delay time for end to end traffic from customer to the Internet via CORD system is the transmission time, but not the processing time.

10. Considerations

10.1. Simple line opening operation for zero-touch provisioning

- Scenario evaluation

  Simple line opening operation for zero-touch provisioning eliminates the need for off-site operations by operators and dramatically reduces the opening time, especially in the case of ONU relocations by customers. Also, service activation following simple line opening operation for zero-touch provisioning dramatically reduces the amount of time it takes customers to add services by themselves.

- Technical evaluation

  - Functional capability test

    It was confirmed that simple line opening operation for zero-touch provisioning using QR code was operating and addition of network functions following to simple line opening operation normally, and the basic operation was confirmed.

  - Performance test

    The time required for line opening of all the 32 ONUs to start up is several ten seconds, which is considered to be practical.

    The time in which the addition of 3 functions can be confirmed is about 2 minutes, and when 3 functions per user are simultaneously processed by 32 users, the time becomes 1 hour, so that speedup is desired.

10.2. DHCPv6

Specifically from the PoC conducted with TELKOM, VNPT & NTT on ATII WP3, it has been able to demonstrate the functioning of access virtualization with the agreed use case. For TELKOM according to the selected use case, it can show functionally that IPv6 can be implemented on a virtualization-based access node. The results in terms of performance response time and delay have not shown significant improvement. Things that need to be followed up are related to ease of operation, automation and modular systems to facilitate the

development of new services and new solutions needed in the future. Because of limited time and resources cannot be done at this stage of the POC, if possible it can become an advanced program for WP3 ATII collaboration next.

10.3. vFW on CiaB

VNPT has developed the TOTP Server and worked with NTT as well as TELKOM to build the APAC sized FTTH and vFW auto-provisioning testbed. All functional tests of the software and system are OK and work as expected. But, the end to end performance test of the system is not as good. Besides the many hops, the reason for the poor performance is in the software switch is capability inside CORD and vFW. We have realized the switching performance of software switch in CORD and FW and have proposed to integrate DPDK-SPP in CORD and vFW to improve its performance. This proposal has been implemented in ATII WP4

11. Conclusion and Future Work

ATII WP3 has successfully completed three-parties joint PoC on access virtualization via international testbed. ATII WP3, as a team, has obtained some insightful results through this activity, while all of TELKOM, VNPT and NTT have also gained some insights according to their specific interests. Especially, the basic concept of zero-touch provisioning has been proved to be technically feasible. This result implies that access virtualization technologies would be one of the key factors to evolve future network architecture and functionalities.

It should be noted, on the other hand, that the joint PoC have been done by applying state-of-the-art technologies which are still in the R&D phase, therefore it is not enough mature for actual commercial services. Performance improvement and operational considerations have to be studied as future works. Further extensive efforts are obviously required to realize actual commercial services based on our joint PoC considering customers' demands and technological maturity.

Acknowledgment

ATII WP3 is grateful to former ATII Board members, Ms. Yukari Tsuji and Mr. Arief Mustain, current ATII Board members, Mr. Okazaki and Mr. Hernady, and a VNPT director, Mr. Nguyen Viet Bang for continuous encouragement and their comments that enriched our activity, as well as to ATII secretariat for their support on the conclusion of the joint experiment agreement and arrangement of meeting events.

References

[1]http://www.ansl.ntt.co.jp/img/fasa/ATII_WP3_WP_v1.pdf

[2]https://indonesiadrc.id/page/what-is-research

[3]http://www.vnpt.vn/en/News/NewsEvents/View/tabid/219/newsid/47544/admin/1/seo/APAC-telecom-carriers-common-requirements-on-access-network-virtualization/Default.aspx

[4]www.opennetworking.org/wp-content/uploads/2019/05/ONF-Reference-Design-SEBA-032919.pdf