Simulation cycle for network scenario based on AD-Campus solution

Zhang Wenhua
Faculty of Information Science and Technology, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia
p113956@siswa.ukm.edu.my

Wan Muhd Hazwan Azamuddin
Faculty of Information Science and Technology, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia
p101964@siswa.ukm.edu.my

Azana Hafizah Mohd Aman
Faculty of Information Science and Technology, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia
azana@ukm.edu.my

Hasimi Sallehudin
Faculty of Information Science and Technology, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor, Malaysia
hasimi@ukm.edu.my

Zhang Yanke
Technical Service Department
H3C Malaysia
50470 Menara Q Sentral, Kuala Lumpur, Malaysia
zhangyanke@h3c.com

Abstract*— A software-defined-networking (SDN)-based controller (SeerEngine-Campus) provides service intelligence. This controller sets up connections, enforces service levels, and automates operations in order to provide full policy management. When the H3C Application-Driven Campus (AD-Campus) solution SD-WAN architecture is used, it gives users secure network access through a variety of transport technologies. EVPN and VXLAN work together to make campus networks that can manage multiple LANs over SDWAN that are highly scalable, efficient, and flexible. Network operators can set up much bigger networks than they could with traditional Ethernet-based Layer 2 architectures by deploying common sets of policies and services across campuses. EVPN-VXLAN separates network infrastructure from services and applications specific to each department or customer. This idea of network virtualization makes it possible to keep traffic separate and to add services to any part of the network without having to use expensive methods like plumbing VLANs. To demonstrate this simulation concept, an experiment was set up with several procedures, beginning with setting up the experiment topology, configuring the devices, and obtaining the experiment results. From the AD-Campus Solution, three areas must be deployed: the underlying physical cable, development services on SeerEngine Campus, and finally the protocol for Service Deployment and Verification (EIA). This experiment gave us a typical network scenario and a modern way to implement a network architecture for connecting network access securely across multiple transport technologies using AD-Campus solutions.

Keywords*— AD-Campus, H3C, Experiment, EIA, EVPN, SDN-WAN, SeerEngine, OpenFlow, VXLAN, Spine-Leaf-Access.

I. INTRODUCTION

The H3C Application-Driven Campus (AD-Campus) solution applies Software-Defined Wide Area Network (SD-WAN) architecture delivering secure connectivity network access over multiple transport technologies [1]. The service intelligence is delivered with a software-defined-networking (SDN)-based controller (SeerEngine-Campus) that sets up connectivity and enforces service levels and automates operations to provide overall policy management [2].

The AD-Campus services combine with VXLAN-EVPN to provide much more capabilities over a mainly IP-based underlay [3]. Ethernet VPN (EVPN) is an overlay solution for connecting dispersed groups, such as campus offices, it uses both L2 (MAC addresses) and L3 (IP addresses) connectivity to provide a logical separation between consumers using shared network resources. Virtual extensible LAN (VXLAN) defines a tunnelling scheme to overlay the L2 network on top of the L3 network.

EVPN and VXLAN work together to create highly scalable, efficient, and agile campus networks and improve quality of services (QoS)[4]. Common sets of policies and services across campuses deployed allow network operators to deploy much larger networks than are otherwise available with traditional Layer 2 Ethernet-based architectures[5]. EVPN-VXLAN decouples the network infrastructure from the services and applications germane to each department or each customer. This concept of network virtualization provides native traffic isolation and the ability to extend services to any part of the network without introducing costly operational methods such as plumbing VLANs.

Fig. 1. Network diagram of EVPN distributed VXLAN IP gateway.

Figure 1 depicts a network diagram from a VXLAN experiment in which PC_A and PC_B remain in separate VXLANs and appear as two distinct hosts. Switch S6850A (leaf) and S6850B (leaf) are used as distributed EVPN VXLAN gateway devices. Switch S6850C (spine) as the route reflector (RR) to reflect EVPN routes to PCs with the RR has established peer relations. This greatly shortens the network complexity and the number of networks signalling message.

In this scenario, PCs IP address was manually assigned, OSPF needs to configure in the leaf to enable the IP address reachable by endpoints. Besides this, some briefing knowledge has been learned such as debugging BGP packets in the leaf, displaying BGP neighbours and tunnels, reading the leaf table and displaying RD messages, mac-address, and routing-tabling vpn-instance with commands.

From Figure 2, this experiment starts with underlay cabling using an L3 switch by applying various switching technologies such as spline, leaf, and access. After finishing the cabling phase, SeerEngine Campus has been setup for development of DHCP Server, AAA Server, and applications to incorporate devices. Each device is set up with its own specific services. Lastly, evaluation of protocols that have been tested, such as 802.1X, MAC Portal and Mac Authentication.

2022 International Conference on Cyber Resilience (ICCR) | 978-1-6654-6122-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCR56254.2022.9995812

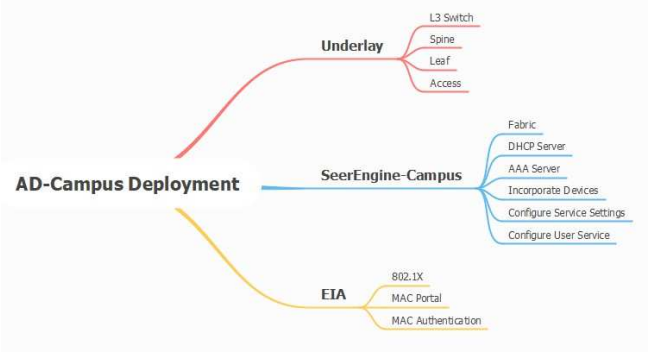

Fig. 2. The progress of AD-Campus deployment

According to the literature that exists in the smart campus domain, only a few experiments have been conducted on AD-Campus consequently. This experiment aims to achieve several objectives, such as:

1. Identify parameter setting for AD-Campus experiment by using H3C technology.

2. Develop Seer Engine Campus by applying various services on campus solution.

3. Dissecting the issues faced during the deployment and configuration steps, providing the solutions, how to fix and how to avoid them in future real word deployment.

II. Related Works

The AD Campus solution was proposed many years ago to overcome issues with SD-WAN technology. Some of the issues have been solved by applying data-driven and evidence-based solutions but lack implementation by using machine learning[6]. This plan for technology applies to future technology [7] but it needs to be used in a different way. Some researchers go for simulation testing [8] before applying directly to an experiment or testbed method.

Some parameters need to be setup in order to make sure the AD Campus solution becomes successful. Research has found that to make sure to get a good result for an experiment, good parameters need to be chosen [9]. Implementation VXLAN for EVPN will improve throughput and latency [10] for AD-Campus solution.

III. Methodology

This study uses a combination of online training and hands-on experiments. Before the starts, EVPN experiment was advanced to understand the underlying logic of the underlay, which is very beneficial to the configuration and deployment of the subsequent underlay. The tool using H3C Cloud Lab software, many learning materials also can be freely found in h3c official website [11].

List of the key commands in the experiment

Command	***describe***
l2vpn enable	Enable l2 vpn
service-instance instance-id	Create and enter ethernet service instance view
tunnel {tunnel-number [flooding-proxy] | all}	Configure vxlan and tunnel association
vsi vsi-name	Create and enter vsi view
vxlan vxlan-id	Create and enter vxlan view
Xconnect vsi vsi-name [access-mode {ethernet | vlan}] [track track-entry-number&<1-3>]	Used to associate AC with vsi
encapsulation	Configure packet matching rules for ethernet instance
evpn encapsulation	Create and enter evpn instance view
l3-vni	VXLAN ID used to configure l3 vpn
advertise l2vpn evpn	To allow external advertisement of bgp evpn routes
display vxlan tunnel [vxlan-id vxlan-id]	Display tunnel associated with the specified vxlan
display l2vpn mac-address [vsi vsi-name] [dynamic] [count]	Display vsi mac address table

By manual configuration, VLAN 4094 need to configured because: VLAN 4094 is managing IP address in switch, was reversed by the controller. The vlan 4094 is created also used for the DHCP relay source address. SWAP the management IP when the IP address was obtained by the managed device (vlan 1 using the temporary IP address).

IV. Simulation Cycle

The simulation cycles involve three areas: the underlying physical cable, development services on SeerEngine Campus, and finally the protocol for Service Deployment and Verification.

A. Underlay Configuration

In AD-Campus architecture deployment scop, underlay includes spine, leaf, and access [12-14]. The underlay configuration is the basic setup before the controller manages the devices, mainly configuring the physical connection between/among the devices, then auto or manually adding the configured devices into the campus network.

1) Experiment Topology

In this section will describe and highlight the main steps, and commands for the underlay devices configuration.

In this experiment, we applied the typical networking scheme [15] spine-leaf access of the AD-Campus solution. The spine devices need to support VXLAN, mainly act as RR to route forwarding over all different leaf devices and play a border role in communication with various types of servers. Leaf devices also need to support VXLAN for user authentication and route forwarding. Access devices connect to endpoints and support multi-level cascading.

The figure below shows the typical networking scheme: spine-leaf-access.

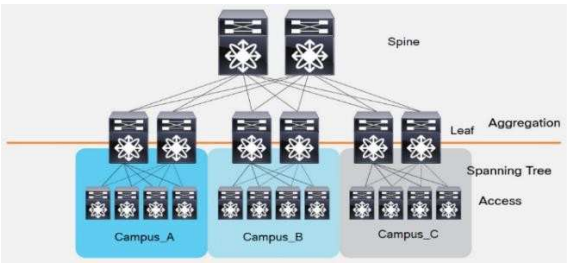

Fig. 3. Spine-leaf-access scheme

The single fabric network topology was applied, one spine, one leaf and one access device were configured in this experiment.

Figure 4 shows the underlay networking topology applied.

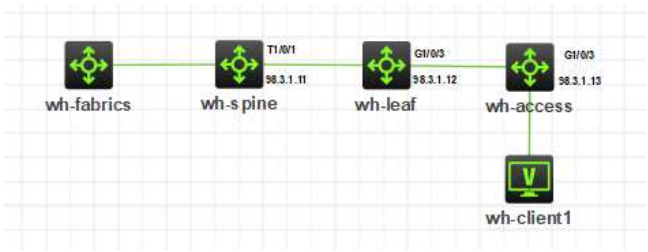

Fig. 4. Underlay Network Topology

The underlay network configuration can be done manually or automatically. We manually configured the devices in this experiment for better practise. Recommended EVPN experiment to become acquainted with the principle and develop an understanding of the configuration procedures. A few more elements should be emphasised to secure the devices' connection.

The spine, leaf, and access are all switches, assigned with different usage. To connect the device and make them reachable, some extra elements need to focus on:

- VLAN 4094: There are two types of layer network access Layer 2 (l2) and Layer 3 (l3). The device management segment and campus controller network do not belong to the same vlan and need to be forwarded at l3. VLAN 4094 as the Management IP address, managing switch address.
- Underlay Link: The link between spine and leaf, to connect them accessible.
- Downlink Interface: The link interface connected from leaf device to the access device is called the downlink interface, configured for user authentication.
- Uplink Interface: The link between the access device and leaf device, to permit all VLANs by command: port trun permit vlan all.

2) Devices Configuration.

a) Spine Configuration

The spine device plays an important role acting as BGP and RR, the device needs to support vxlan to synchronize information among VTEPs, and to connect the external network to the overlay network.

b) Leaf Settings

The leaf device plays L3 distributed gateway and authentication endpoint role in this network scheme, also act as RR client, need to support vxlan to implements evpn and nas device.

c) Access Settings

Access devices connect to the endpoint, it's an optional option, in this experiment we applied a spine-leaf-access scheme, need to configure it to isolation per port per vlan. After multiple rounds of the configuration of spine and leaf, much more familiar with the command behaviours, in this configuration does not face too many issues.

B. Controller Deployment

SeerEngine-Campus or Controller is the key feature of the AD-Campus solution, it provides the graphical user interface (GUI) for engineers to deploy and configure with visible maintenance. The overlay configuration is related to user services, such as isolation domain, layer 2 network domain, private network, and other services.

1) Pre-requirement

To enter this stage, a virtual machine (VM) needs to be created. The hardware device requirement can be find in H3C guidance document, here I will skip the introduction of the installation steps and focus on the controller deployment.

2) Campus Network deployment

a) Fabric

Fabric can be considered a network of devices that are connected in the same geographic domain, such as a university campus, or technology park campus. In this scenario, a single fabric was implantation. The AS number was BGP configured in underlay.

b) Parameters

A few more submenus hidden in this category need to set up DHCP, AAA, and Parameters, the setup rules, and parameters are as follow.

- DHCP Server: Setting up vDHCP server as the pre-requirement for the BYOD security group configuration, the DHCP server generates reservation entries to use the role-based IP address pool with the controller.
- AAA Server: AAA server supports H3C and third-party authentication; after configuring an EIA V9 server, the system sets it as the default EIA server. A third-party authentication server is used for Web Portal authentication and only need to configure the IP address of the third party server on the SeerEngine-Campus controller and make sure they can reach each other.
- Parameters: For the service IP address configuration.

c) Configure Service Settings

This configuration provides service for network access, the settings include isolation domain, private network, layer 2 network domain, and security group. The configuration steps show below:

- Isolation domain: The system contains a default isolation domain named **isolate_domain1**. Use the default isolation domain in a single-isolation domain scenario.
- Private Network + Layer 2 network domain
- Security Group: Configure the security group parameters, add the Layer 2 network domain configured.

d) Devices

The controller does not assign the address to the loopback interface automatically in the Single Leaf scenario, the USER needs to manually add the VTEP IP address to the fabric setup page in order to support the fabric interconnect service.

The VETP IP address was assigned during the underlay configuration.

The SNMP write and read, Netconf username and password are configured in underlay.

Repeat the above steps for leaf and access devices incorporated, please take note of the management IP and VTEPs IP address. After the devices add up, the page shows below displayed the Active devices' information. The IP address pool for vlan 1 and vlan 4094 are also found here.

After the device onboarding, navigate to the general device group and on the right side to set up the policy template. The policy includes AAA, 802.1X, MAC/MAC portal authentication, web portal authentication, and user-defined.

3) Configure User Service

From the above steps, we have configured underlay devices, add the device into the network, setup the parameters and services for the devices, and in this section, will provide the services for user onboard.

The user onboard, need to configure the access user with access services and parameters, user access to the network by network devices, so also need to configure the endpoint devices. The remaining steps and screenshots are as follows:

a) Access Service – Access policy needs to configure in this service, to enter a name for the access policy and use the default service group.

b) Access User - The user account, password and services need to setup. In the next chapter service verification, will use the accounts setup-ed here to verify.

c) Access Parameters - User Endpoint Settings

This chapter provides step by steps on the controller deployment, generally divided into three parts: The first is VM installation. Secondly, port 8443 cluster parameter setup, application deployment and upgrade, and the last is campus network deployment and user service configuration.

V. Experiment Result

The service provided in this chapter is user authentication-related configurations, such as user management, access policies, and access services. The service-related configurations are implemented through the EIA authentication server, which controls whether users can access the network.

A. Service Scope

Some basic configurations need to add include 802.1x, mac authentication, and mac portal, then assign the policy templates to respective groups.

1) 802.1X

From the submenu Access Parameters enter Certificate, and click Import Build-in Certificates, after configuration, the third-party client can use 802.1x service for the certification.

2) MAC Portal

The BYOD was created in chapter 3 configuration service settings - security group steps, was used for the mac portal authentication.

3) MAC Authentication

The MAC authentication scenario is mainly for users who do not have a client device and use the terminal MAC address to trigger online authentication. The mac address is mandatory for this authentication method.

This chapter provides three ways to do the authentication, the services configured will provide the services for the next part verification purpose.

B. Service Verification

The solution supports authentication through 802.1X, MAC, Web/Portal, and VPN.

In the previous part, we configured the authentication service, and we will verify whether those configuration methods are effective or not in the following sections. The related configurations are implemented through the EIA authentication server.

1) 802.1X Verification

To create a new virtual machine, name it as Client Server, with the details matching the relevant settings. Login to virtual machine and open iNode, key in the account info and password to login, if success means the connection is reachable.

Fig. 5. 802.1x

In the AD-Campus system, also can check the login status in Monitor-Monitor List-User.

Fig. 6. Monitor list user

2) MAC Portal Verification

The initial method to verify this configuration authentication is to login to the VM device, open the browser, and enter any IP address. The webpage will directly guide you to the login page, enter the account username and password configured in the BYOD group, if the web show success means the authentication method works.

The second method, to verify the authentication by verifying vsi 3 and subnet IP address configured in layer 2 network domain, BYOD group.

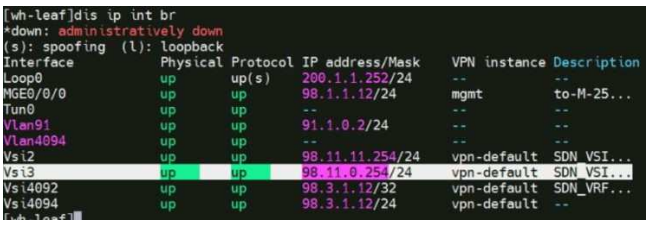

Fig. 7. Vsi verification

The subnet IP address configured in the BYOD group, layer 2 network domain mapping to the vsi 3 interface. The mac portal will obtain the IP address from BYOD setup.

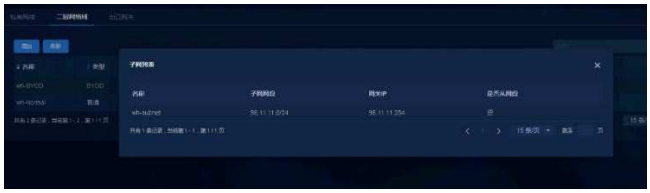

Fig. 8. BYOD

3) MAC Authentication Verification

VM created and add the VM details info into the campus system, if the VM can log in, means connecting successfully.

Fig. 9. MAC address

In the service authentication verification, three different authentication methods are performed against the authentication setup from the previous section. Successful authentication indicates that the experiment has been carried out, from initial configuration to user online, all successfully completed.

VI. Conclusion

Through this training and experiment, the author obtained a typical network scenario and a modern network architecture implementation for securely connecting network access over multiple transport technologies using AD-Campus solutions.

For AD-Campus, from the conceptual understanding at the beginning to the completion of own step-by-step deployment, there is anxiety when encountering setbacks, joy after fixing the issues, all kinds of emotions, beyond words.

There are still some limitations in this paper, such as the experimental data limitation, ad-campus advantages comparison in addressing the traditional network issue, and the comparison before and after the implementation of ad-campus, which will be further explored in future studies.

Acknowledgment

The authors hereby express their gratitude to H3C Malaysia for providing training, resources, devices, equipment, and knowledge transfer for this study. They also would like to acknowledge the support of the Network Communication Lab Technology (NCT) Research Groups, FTSM, and UKM in providing facilities for this research. This article is supported under the Fundamental Research Grant Scheme FRGS/1/2019/ICT03/UKM/02/1.

References

[1] P. Segec, M. Moravcik, J. Uratmova, J. Papan, and O. Yeremenko, "SD-WAN- A rchitecture, functions and benefits," ICETA 2020 - 18th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc., pp. 593–599, 2020, doi: 10.1109/ICETA51985.2020.9379257.

[2] Enlighten Designs_Products & Technology. (2022, August 25). Products & Technology- H3C Application-Driven Campus Solution- H3C.http://www.h3c.com/en/d_201808/1103997_294550_0.htm

[3] G. Salazar-Chacón, E. Naranjo, and L. Marrone, "Open networking programmability for VXLAN data centre infrastructures: Ansible and cumulus linux feasibility study," RISTI - Rev. Iber. Sist. e Tecnol. Inf., vol. 2020, no. E32, pp. 469–482, 2020.

[4] W. M. H. Azamuddin, R. Hassan, A. H. Mohd Aman, M. K. Hasan, and A. S. Al-Khaleefa, "Quality of service (Qos) management for local area network (LAN) using traffic policy technique to secure congestion," Computers, vol. 9, no. 2, 2020, doi: 10.3390/computers9020039.

[5] D. Pucci and G. Casoni, "Monitoring an EVPN-VxLAN fabric with BGP Monitoring Protocol," 2020.

[6] U. Jayawickrama, M. Sedky, and O. Ettahali, "A smart campus design: data-driven and evidence-based decision support solution design," no. May, pp. 22–25, 2018, [Online]. Available: http://www.staffs.ac.uk/.

[7] W. M. H. Ahmad Azamuddin, A. H. Mohd Aman, R. Hassan, and taj al-deen Abdali, Named Data Networking Mobility: A Survey. Springer Nature Switzerland AG, 2022.

[8] T. W. Ching, A. H. M. Aman, W. M. H. Azamuddin, and Z. S. Attarbashi, "Performance Evaluation of AODV Routing Protocol in MANET using NS-3 Simulator," 2021 3rd Int. Cyber Resil. Conf. CRC 2021, 2021, doi: 10.1109/CRC50527.2021.9392519.

[9] T. W. Ching, A. H. M. Aman, W. M. H. Azamuddin, H. Sallehuddin, and Z. S. Attarbashi, "Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery," 2021 3rd Int. Cyber Resil. Conf. CRC 2021, pp. 0–5, 2021, doi: 10.1109/CRC50527.2021.9392475.

[10] A. H. M. Aman, A. H. A. Hashim, and H. A. M. Ramli, "Throughput and handover latency evaluation for multicast proxy mobile IPV6," Bull. Electr. Eng. Informatics, vol. 6, no. 4, pp. 311–316, 2017, doi: 10.11591/eei.v6i4.850.

[11] Enlighten Designs_Support. (2021, December 31). H3C Cloud Lab. https://www.h3c.com/en/d_201811/1129464_294551_0.htm.

[12] Sultan, M., Imbuido, D., Patel, K., MacDonald, J., & Ratnam, K. (2020, October). Designing knowledge plane to optimize leaf and spine data center. In 2020 IEEE 13th International Conference on Cloud Computing (CLOUD) (pp. 13-15). IEEE.

[13] Okuyucu, A. F., Karataş, C., Levi, A., Gürbüz, Ö., Kırca, A., & Oruk, T. (2019). Performance of Load Balancing Algorithms for SDN Controlled Data Center Networks with Leaf-Spine Topology.

[14] Hou, D. (2020, November). Discussion on the Construction of Wireless Campus Network Based on SDN Architecture. In International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (pp. 163-170). Springer, Cham.

[15] Njah, Y., Pham, C., & Cheriet, M. (2020). Service and resource aware flow management scheme for an SDN-based smart digital campus environment. IEEE Access, 8, 119635-119653.