International Journal of Technology and Engineering Studies
volume 5 issue 3 pp. 80-89 doi: https://dx.doi.org/10.20469/ijtes.5.10002-3

Software Defined Network, The Design, Technique, and Internet of Things Defined in Campus Network

Aumnat Tongkaw*
Faculty of Science and Technology,
Songkhla Rajabhat University, Songkhla, Thailand

Abstract: In the current research, Software Defined Network (SDN) is implemented and tested on campus networks to build a framework for easier and manageable, more extensive networks. SKRU deployed ONC software from Ruijie for network administration. The current study also defines the Internet of Things (IoT) devices among faculty, including IoT for Smart farm from agriculture faculty. In an SDN architecture, the ability to configure, manage, secure, and optimize network resources via software affords many benefits to enterprises. This article is contextualized from the concept of the IoT, its security, the interoperability of VLANs, and software-defined networks. By taking into account existing architectures and technologies, intelligent infrastructure is proposed to support all processes. Based on the implementation and evaluation of SDN, valuable insights and research directions are discussed.

Keywords: *SDN, campus network, IoT, smart university*

Received: 31 March 2019; ***Accepted:*** 17 May 2019; ***Published:*** 21 June 2019

I. INTRODUCTION

Today, IoT devices have a role to be used in many everyday situations. Whether scientific instruments office equipment Safety detector equipment or even various medical instruments. In large networks, when an IoT device connects to a Wi-Fi system, it will make authentication difficult because IoT devices cannot use web authentication. User authentication requires a MAC address to allow access to that device. Nevertheless, because there are many IoT devices in an extensive network system, entering the MAC Address into the system to authentication or even allowing users to search for Mac Address from IoT devices is very difficult [1]. Because some devices do not tell how to display the MAC Address in the manual or datasheet. These devices are deployed explicitly in an application context to participate in creating a smart environment ranging from networks, wide ranges of IoT application are stipulating paradigms to connect physical objects some of the application scenarios are health automation, first automation, first responder monitoring, and safety systems smart university and buildings, car park control and management and Industrial control and monitoring system, IoT application is shown in Fig. 1.

IoT is connected to the architecture which is divided into three layers: 1) physical layer, consists of a physical object and sensing devices; 2) Network layer: responsible for transmitting data from physical objects to the gateway of the network and application layer: deals with application/services of the user demand [2, 3].

II. IOT IN CAMPUS

A campus is traditionally the land on which a college or university and related institutional buildings are situated. Usually, a college campus includes faculty, laboratories, residence halls, student centers or lecture halls, and park-like settings. A modern campus is a collection of buildings and grounds that considerable area.

Campus network access poses significant risks to campus network security and to the protection, integrity, and reliability of data, including instructional, research,

*Correspondence concerning this article should be addressed to Aumnat Tongkaw, Faculty of Science and Technology, Songkhla Rajabhat University, Songkhla, Thailand. E-mail: aumnat.to@skru.ac.th

financial, personal, operational, and other sensitive data, that are maintained on or served from university information systems. These radio transmissions can be intercepted by radio receiving devices and the data captured by individuals without university authorization. University-owned, leasing, or operated wireless devices connected to university network infrastructure must be carefully installed and administered to manage these security risks.

The purpose of the wireless policy is to explicate how wireless devices will be installed and operated to protect the integrity, reliability, service quality, and security of the entire SKRU network, and to ensure as ubiquitous wireless coverage as possible in public campus spaces for all members of the SKRU community.

The pain point occurred, for intranet security, some university preferentially use manual or dynamic authentication modes. For example, At SKRU, we use 802.1x authentication and web authentication, to control mobile and/or terminate access to the network. According to current technologies of mainstream manufacturers, defects single point of failure of the authentication server, authentication performance, dependency on an authentication client, and reliability issues. These decrease the users services performance. Computer centers, then, try to eliminate these problems and free from the other defects.

There are two types of authentication failure. First, authentication client failure because of the limitations. For example, there are a lot of dumb terminals in SKRU, such as the automated book return machine, agricultural machine. The client cannot install software, and web authentication and auto authentication are unavailable. Second, authentication server faults due to the abnormal of improper operations of routine maintenance. Besides, a conventional auto authentication admission solution causes risks of patient information leakage.

From the above pain point, it comes up with the IP and MAC binding solution. However, it causes other problems. First, low information collection efficiency, a network administrator may need to manually collect the MAC address of each access terminal and learn each particular device information connected access switch. However, when the device changes, it will cause the information disorder and required the network administrator to maintenance. Second, troublesome configurations, human errors, for example, the manually configuring of network administrator a similar character such as eight and B is in a similar handwritten MAC address. Third, limited use of entry resources, terminals that purchased in the same batch may have similar MAC address segments, and manual static configuration is error-prone. When an access switch has much static configuration, and IP+MAC bindings need to be changed, it quickly happens that entries of relevant users are not deleted, or entries of irrelevant users are deleted. When the inpatient wards are decorated, and the offices are adjusted in the middle- and late-stage, the IP+MAC binding entries of access switches need to be re-configured. If devices are migrated across gateways, IP addresses need to be re-allocated. Finally, complex IP address management, Using conventional Excel and other methods to manage IP addresses, is cumbersome, inefficient, and poor in visualization. IP addresses are often randomly used in the network, resulting in network IP address conflicts. In addition, after a device is scrapped, the IP address is usually abandoned, and the IP address recycles the rate is low.

SKRU resolves those problems of IP address by using the multi-VLAN over IPSec VPN, the VLAN design, and implementation of multi-application between two campuses of Songkhla Rajabhat University. This research shows three benefits of Multi-VLAN design [4]. First, it is a cost-effective way to deploy multiple types of applications, second, it increases protection and security, and third, it can also reduce the network administrators management of maintaining and managing the network as a whole, even if the two campuses are far away and maintain data transmission efficiency [5, 6].

Since SKRU has limited network administrators, network management needs to be very effective. Also, considering network security is essential Causing the introduction of various technologies More advanced applications such as rapid development and deployment of cloud computing, cloud storage, big data analysis and AI to help For example, to consider network security in SKRU, network administrators must be able to access dumb terminals, PC terminals and any other self-service machines, or self-service printers. Furthermore, the network administrator needs to maintain IP address, allocation status of devices, and manage conflict IP address.

Network management needs clarity, so visualization is therefore necessary in the SDN software to be able to see the topology of the entire network and various devices attached. In addition, various settings if linked from visualization is easier and faster for management.

III. SDN SECURITY CONSIDERATION

SDN security is weak, as the previous paper noted. For example, the vulnerable from attacking SDN layers.

A. *Potential risks on SDN data plane layer and SDN controller southbound interface*

Southbound interface controls network communication between the SDN data plane and SDN controller layers. Several protocols can be used for this communication purposefor example, OpenFlow, OVSDB, NETCONF, PCEP, SNMP, and BGP.

Although OpenFlow is the widely used protocol in the SDN world. There are several security vulnerabilities in OpenFlow, which lead to potential risks from the attacker. An attacker can introduce attacks like DoS on OpenFlow switch, which uses a packet injection technique. This attack technique could affect the services and networking applications which are based on these services. This kind of DoS attack may lead to disruption of the SDN network system [5, 7].

Furthermore, if no encryption applies to API traffic flow to/from Southbound interface and the OpenFlow switch, an attacker can spoof, eavesdrop, probe, manipulate API message flow as well as create a new flow that allows loop-hole or forward the traffic to a malicious person in order to sniff network traffic or redirect the network traffic flow to the rogue controller instead. Therefore, this represents a high-security risk to the SDN environment against MTM (Man in the Middle).

B. *Potential risks on the SDN controller northbound interface and SDN application layer*

Northbound interface uses API (Application Programming Interface) to control network connectivity between the SDN controller and SDN application layers. Several APIs such as Java API, Python API, RESTful, and OSGi are being used to serve this purpose. By using different APIs may cause difficulty to secure against malicious network application. An insecure programming practice and access controls can create a loop-hole in the API that can be a potential risk to malicious injection attacks like Code and Flow rule injections. The result of such injections can lead to a modification of northbound interface service components, insert or delete flow rule as well as data leakage. This causes serious poor performance as well as response time to the overall SDN system [8].

C. *SDN layer (application)*

The SDN layer covers upper levels of network information, including topology, state, and statistics. This network information allows developers to create various network applications, for instance, network automation, configuration, monitoring, troubleshooting, management, policies, and security.

After an attacker gaining control of the SDN controller, the attacker can create their network back-door and policy, which allows him to take control of the SDN system includes all its network devices.

Let us look at one of the popular SD-WAN software in the SDN market, Cisco Meraki SD-WAN cloud software. Meraki SD-WAN software has its features allowing the administrator to manage network and security, for example, wireless setting, DHCP, VPN, firewall, traffic shaping, threat protection, content filtering, access control, and more.

Imagine, if an attacker has wholly gained control of the SDN controller on both lower (Southbound interface) and upper (Northbound interface) levels, he can reconfigure an existing Meraki SD-WAN policy such as network access control from sign-on with RADIUS option to directly access or no authentication requirement option. This can be a high-security threat to the system.

D. *Objective*

Campus networks require the agility to dynamically adapt and evolve with the ever-changing needs of business applications. They also need centralized manageability and strong integration capabilities with every other piece of enterprise IT. To this end, IDC has seen SDN emerge into medium to large enterprise campus networks to address 3rd Platform network challenges as each enterprise experiences its digital transformation.

IV. IMPLEMENTATION PILOT

RG-ONP, RG Open Networking Platform, is a new-generation future-oriented network platform launched by Ruijie. This network is following the SDN concept. The platform consists of the network infrastructure, for example, layer, control layer, and network application layer, and supports the open device, control, and application layers. Based on these open APIs, users can extend network applications, and integrates computing, storage, and network, fully reflecting the openness, flexibility, extensibility, and usability of the ONP.

RG-Open Networking Controller (ONC) is a network controller software, developed based on OpenDaylight on RG-ONP. It adopts the microservice system architecture, combines the modularization of OSGI and the Feature mechanism of the Apache Karaf framework, and implements dynamic online installation and uninstallation of applications. Based on OpenDaylight, the RG-ONC strengthens is the management on the controller itself, adds essential network services and support to multiple protocols, adds services such as device management, topology management, user management, online upgrade, cluster management, and log advertisement, and opens

various southbound and northbound APIs.

Network devices can receive SDN controller information and configuration in conventional modes, including SNMP, NETCONF, and command lines, as well as in the OpenFlow mode in the SDN architecture, to communicate with the controller. Based on the C/S architecture, a switch is an OpenFlow client, and a controller is an OpenFlow server [9]. The essence of this protocol is a primitive flow table. Similar to the ACL, the first flow table determines the action (such as switching, routing, discarding, modifying, and sending to the control plane) of a flow based on the wildcard entry. On a conventional service switch, control and forwarding are determined by itself. In the architecture with control and forwarding separated, the controller plays an important role. Taking MAC address learning as an example, a conventional service switch determines whether to learn the source MAC address of a packet based on the switch configuration. On a service switch with control and forwarding separated, a packet is received through the device ingress and transferred to the controller, and then the controller determines whether to learn the MAC address of the packet and notifies the device [10].

SKRU deployed ONC software from Ruijie for network administration. The primary view of the ONC of Ruijie show as below:

A. Topology view

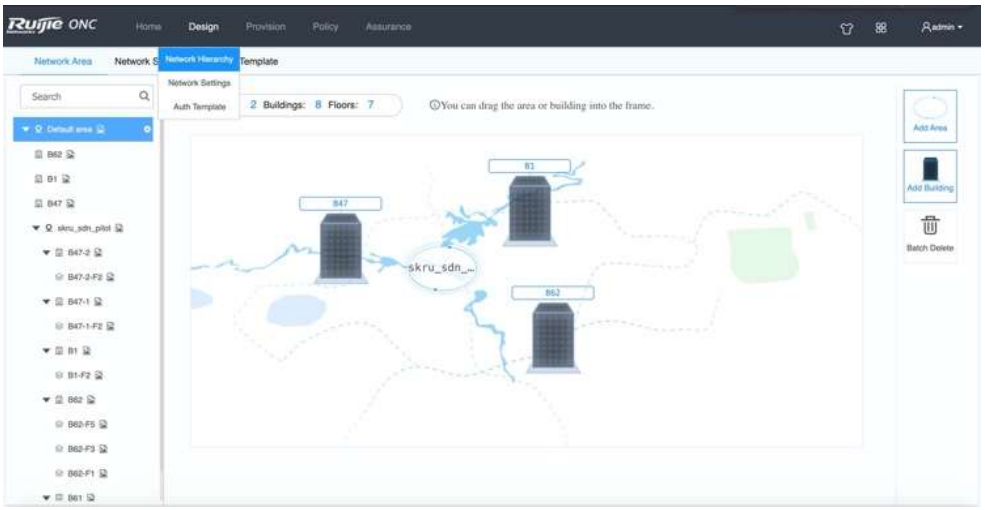

Fig. 1. Topology view

B. Real-time User Checking with Path: Policy -> Endpoint Policy

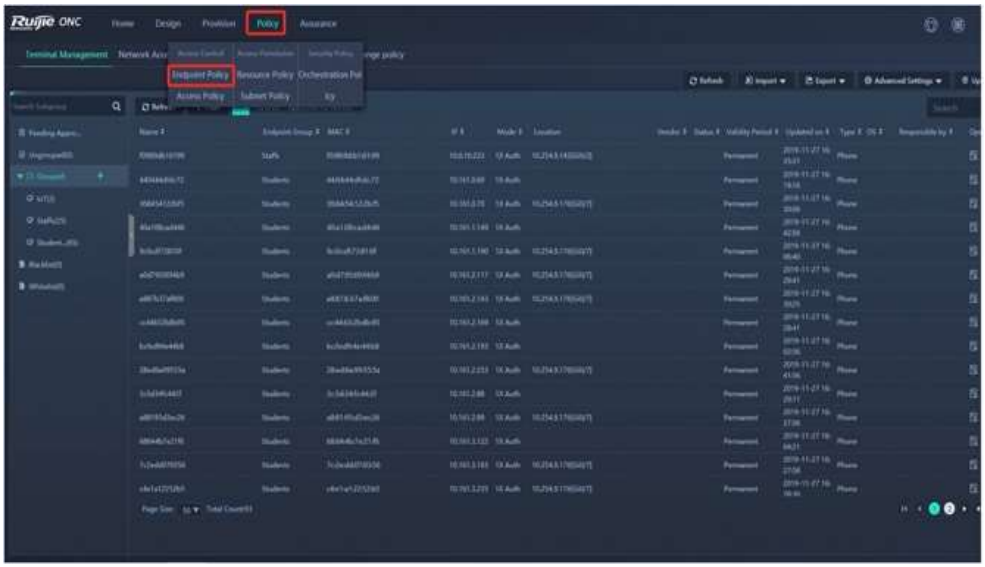

Fig. 2. Endpoint policy

C. *Network Status Checking Path: Assurance -> Network Health*

It contains health score, which show total devices, this score comes from CPU Errors (percent of CPU Threshold) MAC Errors (percent of MAC Threshold) Memory Errors (percent of Memory Threshold) Link Errors (percent of Port Threshold) ARP Errors (percent of ARP Threshold) and Frame Errors (Monitor status), see Figure below.

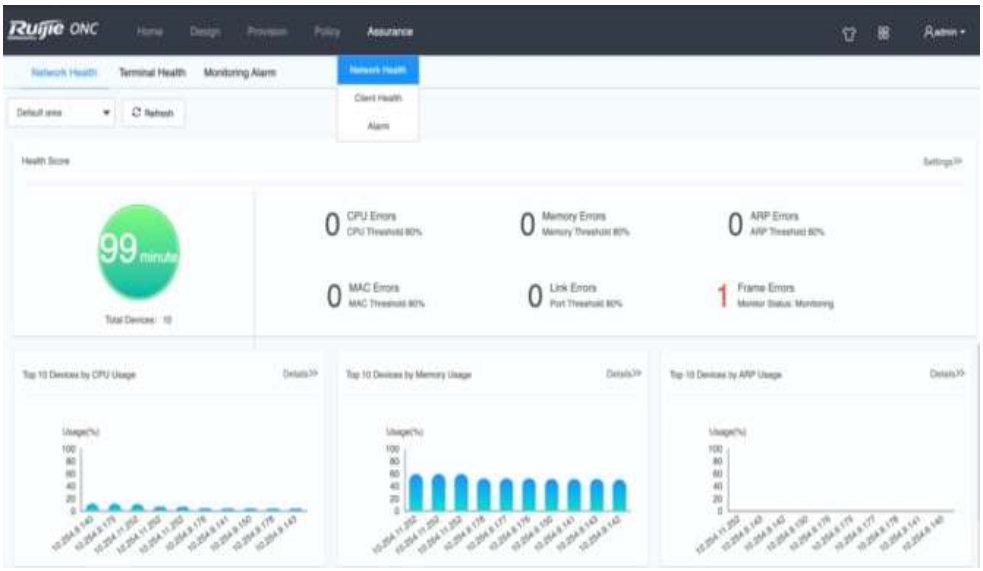

Fig. 3. Network health

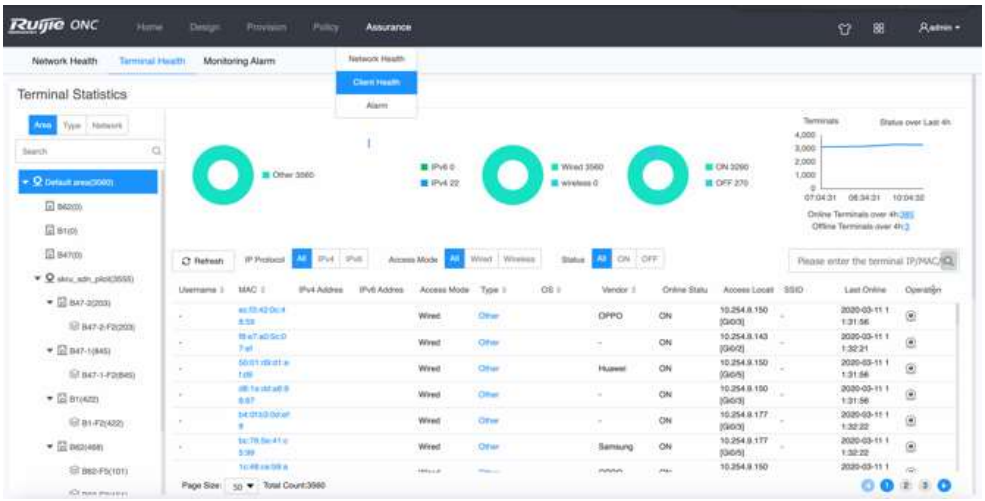

Fig. 4. Client health

At SKRU, ONC's overall implementation and deployment process is as follows:

1) Upgrade device version: The implementation pilot start with upgrade device version of the existing devices. Then, we configure all devices related the protocols of switch and add some devices on the ONC. The new area called "skru_sdn_pilot", showing in Fig. 1 at the center of topology view. Fig. 5 shows the configuration of creating the new area "skru_sdn_pilot".

Fig. 5. Creating the new area skru_sdn_pilot

Then, add each sub areas for example, the Fig. 6 is the case of configuring B62 by selecting parent area as skru_sdn_pilot. Next, add new buildings for corresponding area, add floor to building (B62-F5). This sub areas follow the multi-vlan design from the previous research [4].

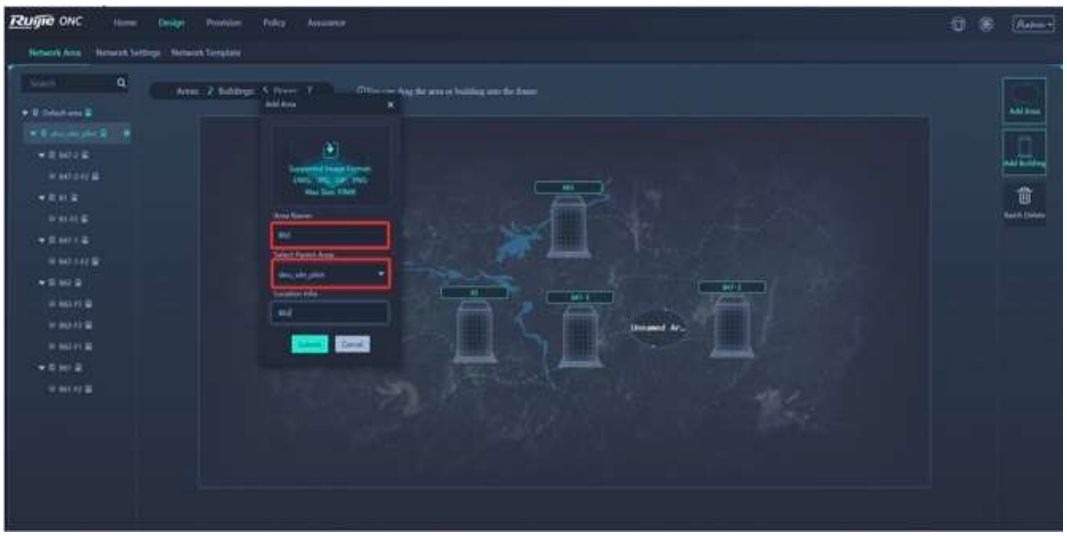

Fig. 6. Configuration of creating sub area B62

We need to connect the switch to the ONC controller, which requires the SNMP protocol. The configuration on switch included : core N18K configuration, Aggregation switch configuration, and Access switch configuration.

Next, the configuration is implemented on devices by using SSH protocol and NETCONF protocol. Finally, configure OpenFlow protocol.

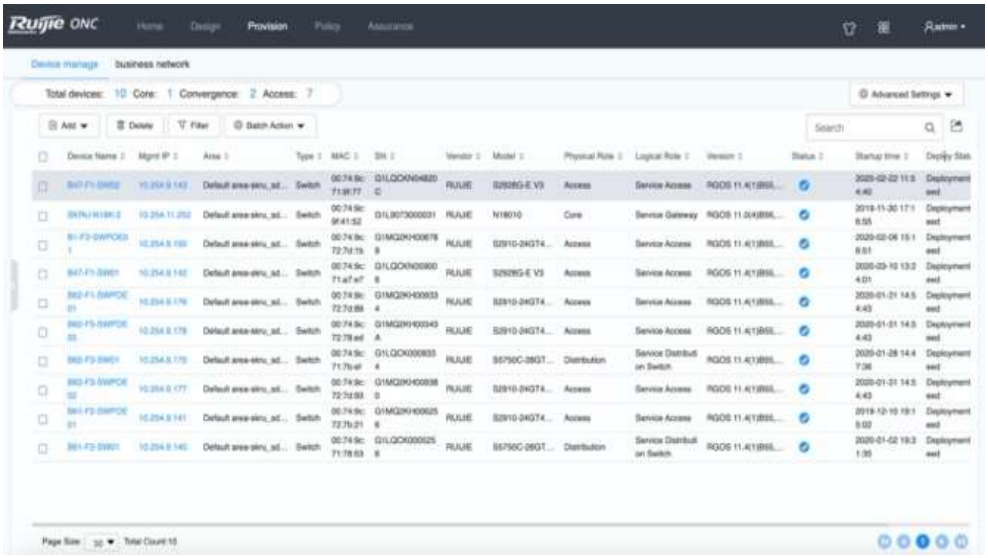

Fig. 7. Device manager

Fig. 7 shows the device manager of ONC, which contains device name, mgmt IP, area, type of device, MAC address of the device, serial number, vendor, model, physical role, logical role, version, status, start-up time, deploy status and action that admin would like to manage [1].

- Create a supervlan service network: We need to create a supervlan service network to provide all the services that the device required. The step will include: create supervlan network template, create an IP address pool create a virtual network, add business subnet, and delivery configuration (deployment).
- Create supervlan network template: The Next step is to create a flat network template on the SDN controllersupervlan by using path DesignNetwork TemplateFlat Network Template (SuperVLAN), see Fig. 8.

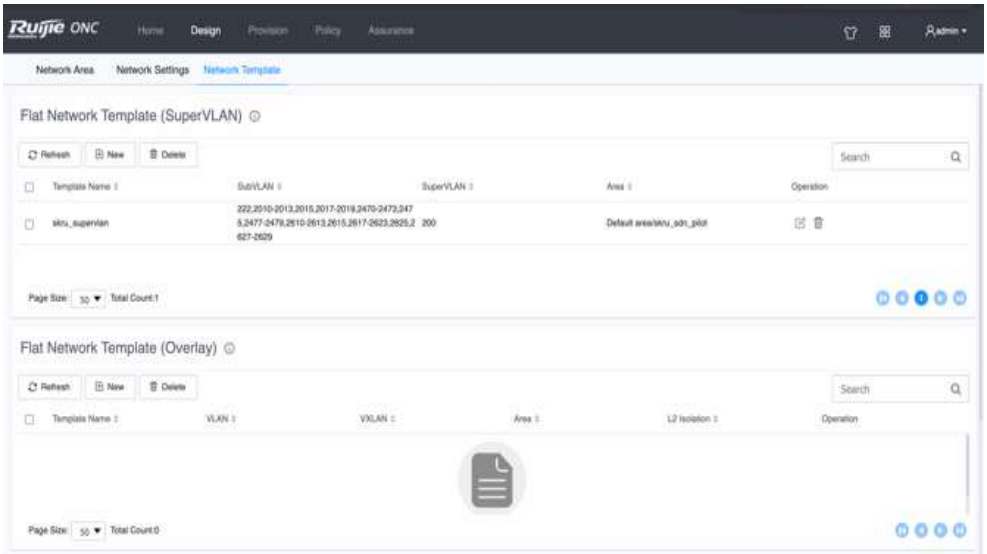

Fig. 8. Create superVLAN network templat

- Creating an IP address pool: Then, we create an IP address pool on the SDN controller corresponding to the service subnet.
- Creating a virtual network: Create a virtual network on the SDN controller, associate the area where the supervlan network template is configured, add a business network, select the supervlan network template, configure the VLAN id, and click the associated supervlan and subvlan (See Fig. 9). Add a virtual network, fill in the virtual network name, and associated area.

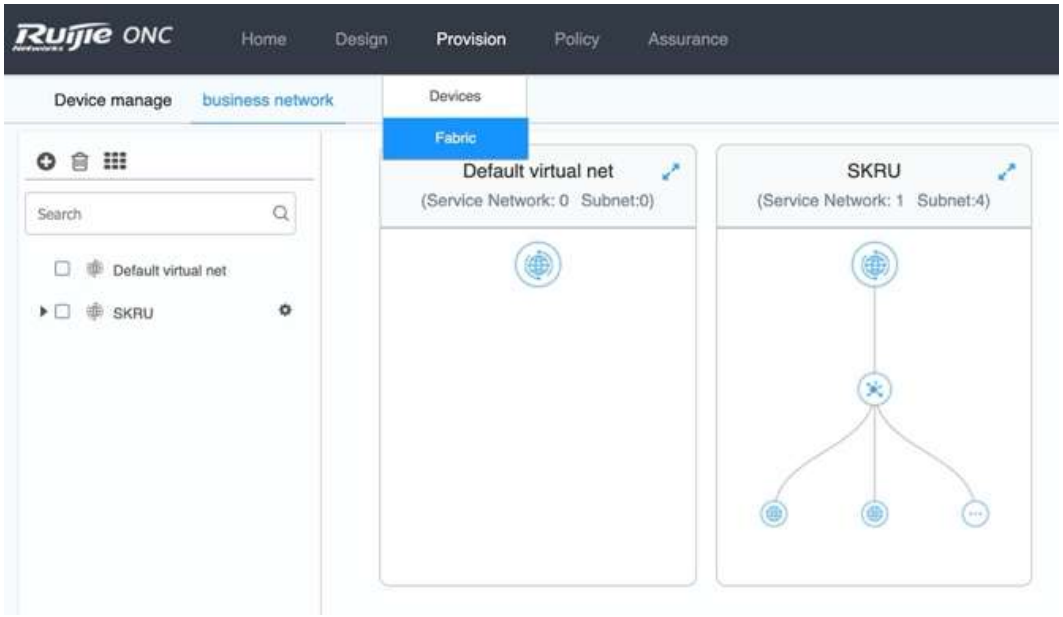

Fig. 9. Create Virtual Network

- Add business subnet: At the service, network to add a service network subnet, fill in the name, network segment, and gateway information. Then, we can configure the corresponding DHCP dynamic address pool information as required. The configuration shows in Fig. 10 and Fig. 11 below.

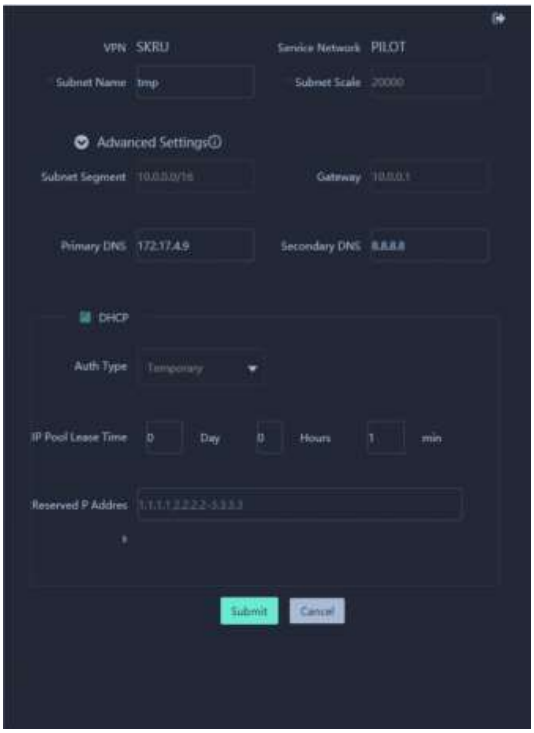

Fig. 10. Configure the corresponding DHCP

- Delivery configuration: After the configuration subnet, the service network and service subnet will be deployed to the service gateway device in the associated area of the service network.

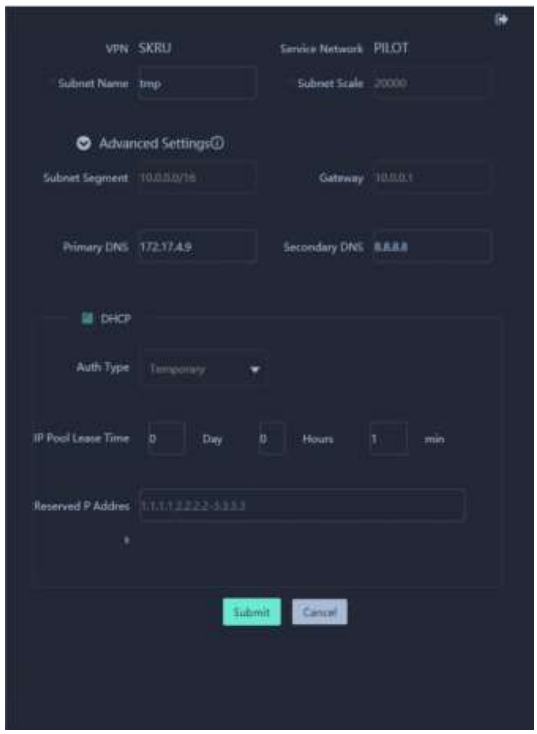

Fig. 11. Create virtual network

2) IP address management: The terminal group name must be the same as the user group name on the SAM (case sensitive), see Fig. 12.

Other configurations may require such as enable the policy migration function, enable loop detection for alarm and monitoring, enable IoT terminal access control, authentication-free. Moreover, the administrator can choose policies and scopes according to actual business requirements.

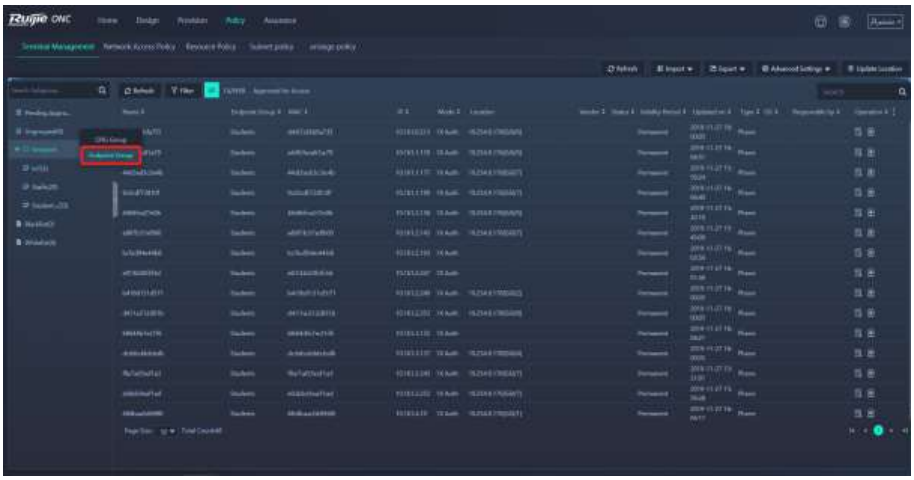

Fig. 12. Endpoint group

3) Business subnet isolate strategy: The Administrator can set subnet policy by selecting the grid corresponding to the two subnets to be isolated, click the icon, and choose whether they can access each other. See Fig. 13.

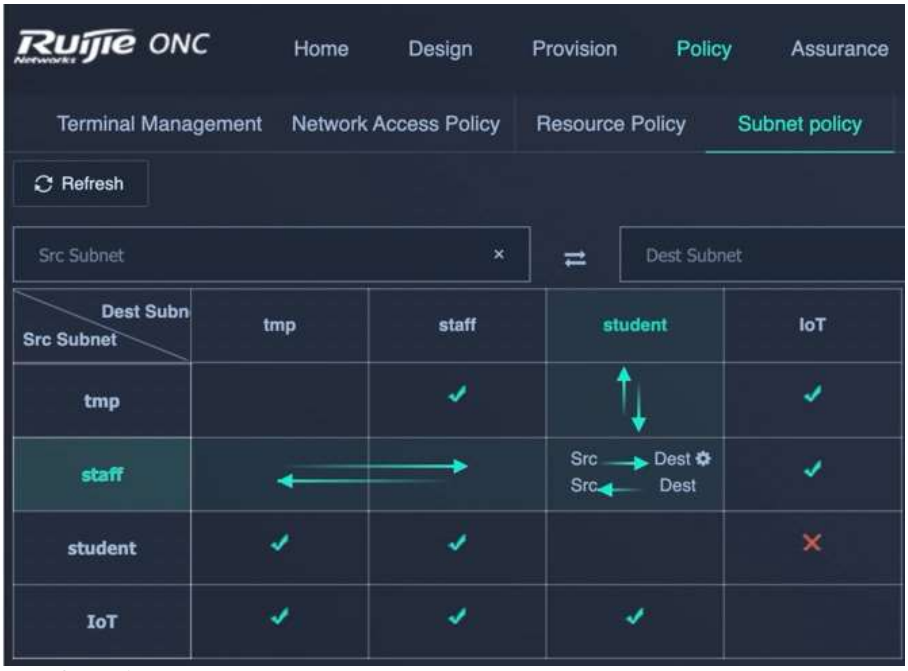

Fig. 13. Subnet policy configuration

V. CONCLUSION AND RECOMMENDATIONS

This paper explained the contextualized from the concept of the SDN configuration for the IoT, its security, the interoperability of VLANs, and software-defined networks that call ONC of Ruijie. By taking into account existing architectures and technologies, intelligent infrastructure is proposed to support all processes. The guiding line is used for the administrator in terms of deployment and consideration of SDN security and management on the campus. For future work, SKRU will include the artificial intelligence technique to classify the type of IoT devices and the automatic management of each group of devices.

Declaration of Conflicting Interests

No competing interests, financial and non-financial, are present in this work.

REFERENCES

[1] A. El-Mougy, M. Ibnkahla, and L. Hegazy, "Software-defined wireless network architectures for the internet-of-things," in *40th Local Computer Networks Conference Workshops (LCN Workshops),* Florida, FL, 2015.

[2] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network (sdn) based internet of things (iot): A road ahead," in *Proceedings of the International Conference on Future Networks and Distributed Systems,* Cambridge, UK, 2017.

[3] O. A. Osahenvemwen and O. F. Odiase, "Effective management of handover process in mobile communication network," *Journal of Advances in Technology and Engineering Studies*, vol. 2, no. 6, pp. 176–182, 2016. doi: https://doi.org/10.20474/jater-2.6.1

[4] S. Tongkaw and A. Tongkaw, "Multi-VlanDesign over IPSec VPN for campus network," in *Conference on Wireless Sensors (ICWiSe),* Langkawi, Malaysia, 2018, pp. 1–8.

[5] T. A. Assegie and P. S. Nair, "A review on software defined network security risks and challenges," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, p. 3168, dec 2019. doi: https://doi.org/10.12928/telkomnika.v17i6.13119

[6] L. A. Alindayo and J. C. Maglasang, "Wireless sensor network development: Targeting and control system for semi-ballistic vehicle for rapid and precise search and rescue applications," *Journal of Advances in Technology and Engineering Studies*, vol. 4, no. 4, pp. 149–161, 2018. doi: https://doi.org/10.20474/jater-4.4.2

[7] A. A. Mohsin, "A comprehensive comparison and classification of routing attacks in wireless sensor networks," *Journal of Advances in Technology and Engineering Studies*, vol. 3, no. 1, pp. 27–36, 2017. doi: https://doi.org/10.20474/jater-3.1.5

[8] Y.-C. Wang and H. Hua, "An adaptive broadcast and multicast traffic cutting framework to improve ethernet efficiency by SDN," *Journal of Information and Engineering*, pp. 1–9, 2019.

[9] F. A. Shuhaimi, M. Jose, and A. V. Singh, "Software defined network as solution to overcome security challenges in IoT," in *5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* Noida, India, 2016.

[10] P. Mishra, D. Puthal, M. Tiwary, and S. P. Mohanty, "Software defined IoT systems: Properties, state of the art, and future research," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 64–71, 2019. doi: https://doi.org/10.1109/mwc.001.1900083