Enterprise Network SDN Solution Research
Jian-feng JIANG
Suzhou Industrial Park Institute of Services Outsourcing, China, 215123

Keywords: SDN, Enterprise network, Network construction.

Abstract. With the continuous development of network technology, the traditional network of distributed control architecture reflects the shortcomings gradually. After collecting the network topology with the network devices each time, you need to run a large number of routing protocols to calculate routes, generate a routing table in order to forward data. It is need to configure a large number of agreements instead of using the network devices to run the same algorithm, and then to avoid the device loop. This topic introduces the network reconfiguration method based on the new network architecture SDN (software defined network) technology during the entire process of network design. It makes the enterprise network safe, stable and easy to maintain with the new technology.

Introduction

In traditional network architectures, data forwarding and control of network devices rely on a large number of protocols. The network administrator needs to modify a large number of network devices when an enterprise's business needs change, such as switches and routers. The network will always face congestion problems to adapt to new business needs, because the company's network bandwidth is limited. The SDN[1] technology separates the control planes of an enterprise's network control by a unified controller, and then delivers them to the data plane and forwards them by the data plane. In the face of network changes, network administrators only need to make corresponding changes at the control level, and then send them to the data layer, which not only simplifies the configuration of the network, but also improves the performance of the network to some extent.

SDN Network Architecture

SDN Three-tier Model of Network Architecture

In the entire SDN network architecture[2], there are three levels: the collaborative application layer, the control layer, and the forwarding layer. The traditional network architecture itself consists of three levels: management plane, control plane and forwarding plane. The three levels of SDN just correspond to it.

The main purpose of the collaborative application layer is to complete the user's various upper-layer applications, such as OSS, which can be responsible for business collaboration across the network. Openstack is responsible for computing, and storage collaboration in the data center.

The control layer is the core part of the whole SDN. The implementation entity of this layer is the SDN controller, which is responsible for the internal switching path of the network and the generation of border service routes. When the network status changes, the control layer will adjust the internal switching path and service routing of the network.

The forwarding layer is a basic forwarding network consisting of network devices and connecting lines between devices. The data forwarding operation of the user is performed according to the flow tables sent by the control layer. The forwarding layer itself is a system of execution units, which itself does not make any decisions under normal circumstances. The forwarding engine of its core component system works according to the instructions issued by the control layer to forward data. Another function of the forwarding layer is to upload the information and status of the network resources to maintain network stability.
SDN Three Interfaces of the Network Architecture

The core of the SDN network architecture is the SDN controller at the control layer[3-4]. It consists of three interfaces: the northbound interface (NBI), the southbound interface (SBI), and the east-west interface.

The NBI interface is similar to the management interface in the traditional network. It is an interface connected to the collaborative application layer. The main job of the interface is to provide service management such as deployment virtualization services.

The SBI interface is mainly used between the controller and the repeater. On one hand, the controller can send the flow table to the forwarding layer through the interface. On the other hand, the forwarding layer can upload a variety of information collected from the devices such as network topology information and alarm information.

The east-west interface is mainly used to interconnect with other networks, especially traditional networks. At present, this interface is not fully popularized in the SDN solution. In most operators and enterprise networks, large-scale traditional networks are still deployed.

SDN Plan Design

RG-ONC is an SDN controller based on RG-ONP of Ruijie Intelligent Open Network Platform[5]. Fully compliant with the SDN philosophy, the platform advocates openness, virtualization and intelligence. With the modular technology architecture of java OSGi, it can be upgraded online and compatible with multiple versions while satisfying scalability.

Network Architecture

The network solution is established through the SDN core switch, and the traffic is uniformly processed and managed through the SDN controller. The network topology is shown in Fig. 1.

IP Address Planning

The enterprise network uses the 200.200.200.1/30 address to connect to the external network. The internal network uses 172.16.0.0/16 space as the service network segment, and the egress gateway uses the 10.10.0.0/16 network segment. The SDN management network uses the 192.168.1.0/24 network segment. The specific IP address planning is shown in Table 1 and Table 2.
Table 1. IP address planning.

<table>
<thead>
<tr>
<th>Devices/Management</th>
<th>Interface</th>
<th>IP address</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit Gateway</td>
<td>GI0/0</td>
<td>10.10.1.1/30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GI0/1</td>
<td>200.200.200.1/30</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loopback</td>
<td>1.1.1.1/32</td>
<td></td>
</tr>
<tr>
<td>SDN core switch</td>
<td>vlan10</td>
<td>172.16.0.254/24</td>
<td>Cloud platform public</td>
</tr>
<tr>
<td></td>
<td>vlan20</td>
<td>172.16.1.254/24</td>
<td>Wired user</td>
</tr>
<tr>
<td></td>
<td>vlan30</td>
<td>172.16.2.254/24</td>
<td>Wireless user</td>
</tr>
<tr>
<td></td>
<td>vlan100</td>
<td>10.10.1.2/30</td>
<td>Interconnected</td>
</tr>
<tr>
<td>Wireless AP</td>
<td>GI0/0</td>
<td>172.16.1.253/24</td>
<td>gateway</td>
</tr>
</tbody>
</table>

Table 2. Core network IP.

<table>
<thead>
<tr>
<th>Features</th>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDN management network</td>
<td>SDN Core switch</td>
<td>GI0/1</td>
<td>192.168.1.1/24</td>
</tr>
<tr>
<td></td>
<td>SDN Access switch</td>
<td>GI0/1</td>
<td>192.168.1.3/24</td>
</tr>
<tr>
<td></td>
<td>Cloud Server</td>
<td>ETH1</td>
<td>192.168.1.4/24</td>
</tr>
<tr>
<td></td>
<td>SDN controller</td>
<td>ETH1</td>
<td>192.168.1.2/24</td>
</tr>
</tbody>
</table>

**SDN Solution Configuration and Implementation**

The collective process of SDN solution design is shown in Fig. 2.

Controller Docking

The mininet environment is built and connected to the RG-ONC controller. Then the network topology is built as Fig. 3 by the mininet image.
The specific steps include: Static IP address configuration -> Connected controller-> Establishing a simulated network topology using Mininet -> Controller web access -> Verify flow table information.

**SDN-based Network Device Interconnection**

First, ensure that the wireless device can access the IP address 1.1.1.1 through the AP520, and then send the flow table so that each PC can access the IP address 1.1.1.1 normally. The configuration file is shown in Figure 4.

```bash
RG-S2910(config)# of controller-ip 192.168.1.2 interface gigabitethernet 0/1
RG-S2910#show of
Version:openflow1.3,controller[0]:tcp:192.168.1.2 port 6653 interface gigabitethernet0/1.main is connected,aux is disable,role is master.
Current controller mode : multiple.
Current packet process mode : Lookup all flow.
Datapath id = 97209820679302
```

**SDN-based Business Access Strategy**

Configure the ARP information entry between PC1 and PC2 through the SDN controller, and send two flow tables on S2910 with a priority of 600 (higher than the arp flow table in the previous requirement). The packet from the GI0/3 and the source mac is the MAC address of the PC1 is transmitted from GI0/4, so that the packet from the GI0/4 and the source mac is the MAC address of the PC2 is transmitted from the GI0/3.

Then, two flow tables are sent in S2910 with priority 500. So that the flow from GI0/3, source ip is 172.16.2.1/32 and the destination ip is 172.16.2.2/32. It is transmitted from GI0/4. The stream from GI0/4, the source ip is 172.16.2.2/32, and the destination ip is 172.16.2.1/32 is transmitted from GI0/3.

**Wireless Network Environment**

At first, AP should be configured to work in FAT mode with the SSID as rubi-X at broadcast status. Then Set the network with the SSID ruijie-X to perform encryption authentication based on WPA2 and set the authentication password. Finally, the AP's DHCP option is enabled to assign wireless users an address in the range of 172.16.1.100-172.16.1.200 and configure ARP spoofing defense in the wireless environment to prevent ARP spoofing inside the LAN.

**Exit Gateway Strategy**

Configure the mutual access between the internal and external network users and enable the ARP defense and traffic attack. When abnormal ARP flooding occurs, limit the number of packets to avoid unnecessary impact. Do not restrict traffic with manage IP. The limit of the FTP traffic on the
external network is 5000Kbps per user, and the total ftp traffic on the internal network does not exceed 100M. Specific steps are as follows: Open the web-server service -> Enable ARP traffic attack -> Configuring a flow control policy.

Result Analysis
The result of the terminal is as shown in Fig. 5. The flow table releases the CIMP packets between the hosts and the packets are sent without packet loss.

![Figure 5. Communication test.](image)

Conclusion
After the introduction of the new technology SDN, the overall network architecture of the enterprise has changed. Compared with the original traditional network, the maintenance and update of the network becomes faster, and the task of the network administrator becomes relatively easy. Under the basic premise of satisfying customer needs, the working pressure of network equipment becomes smaller, and the forwarding efficiency of data streams is improved.

Acknowledgement
This research was financially supported by the Jiangsu philosophy and social science project (2019SJA1310). Jiangsu Province Higher Education Teaching project (2017JSJG081). School-level teaching reform project (JG-201901). Jiangsu University Student Innovation Project (201914295011Y).

References