Smart Systems and Green Energy (2020) Vol. 2: 11-19
Clausius Scientific Press, Canada

DOI: 10.23977/ssge.2020.020102
ISSN 2523-904X

Application Discussion of SDN Technology in Multi-data Center

Zhenyu Zhai[1, a, *], Qiang Li[2]

[1]*State Grid International Development Co., Ltd, China*

[2]*Information Systems Integration Branch, NARI Technology Co., Ltd, China*

[a]zhaizhenyu@stategrid.com.cn

*Corresponding author: zhaizhenyu@stategrid.com.cn

Keywords: software defined network, VXLAN, distributed cloud data center

Abstract: Single-point cloud data center solutions are no longer able to meet customer needs, and only from the entire data center cluster structure to start to solve the interoperability among various data centers, unified management and scheduling issues in order to solve the overall group IT System utilization, management efficiency and business experience problems. The Distributed Cloud Data Center (DC) is born to address the architectural challenges of this overall data.

1. Introduction

With the rapid development of ultra wideband network, the emergence of SDN (software defined network separated from data forwarding and control), as well as the development of various technologies involved in cloud computing in the past decade, is promoting a new round of changes in data center.How to seize the opportunity, lead the change, make full use of the advantages of the established system, introduce a new architecture that meets the needs of the industry, avoid the problems of large investment, long cycle, high energy consumption, low resource utilization, and system isolation caused by the intensive construction of traditional data centers and the operation mode with slow business response ability are challenges for all enterprises.

Different stages of traditional data center construction have different technical and cognitive characteristics.In the course of more than 20 years of development, some enterprises have built more than 85 data centers of different sizes based on different stages of technical capabilities and business needs, with more than 5,000 servers of different specifications, supporting more than 4,000 applications and more than a dozen different structure the database.Diversified and heterogeneous it data center not only supports the business and development of enterprises in different stages, but also brings huge management, upgrading, maintenance and operation costs, and delays the subsequent rapid development.Enterprises have to invest huge human resources to maintain the existing large-scale data center and its business, while carefully exploring new architecture. Facing these challenges, distributed cloud data center becomes an inevitable trend.

The core idea of distributed cloud data center is: physical distribution and logical unity.It can integrate the data centers of enterprises distributed around the world, so that it can provide services

like a large server.The main solution is the integration of multiple data centers to improve the overall IT efficiency of the enterprise. De-localization, data center definability, and automation are the main features of this stage.

Logical unification has two meanings: Unified management, scheduling, operation and maintenance support of all data centers and their resources, as well as decentralized and domain based management, which involves providing a unified operation and maintenance management support platform for distributed cloud data centers;When the distributed cloud data center wants to provide external services, it needs to provide a unified service presentation interface and a unified support process, which involves providing a unified service platform for the distributed cloud data center.

2. The overall architecture of distributed cloud data center

The distributed cloud data center is no longer limited to solving the efficiency and user experience of a single data center, but regards multiple data centers as an organic whole.Around the design of cross data center management, resource scheduling and disaster recovery. It includes the cloud operating system to realize the cloud resource migration across the data center, the operation and maintenance management system for the unified resource management and scheduling of multiple data centers, the ultra wideband network of the second tier and the ability to define the data center by software.

The overall architecture design of the distributed cloud data center is shown in Figure 1.

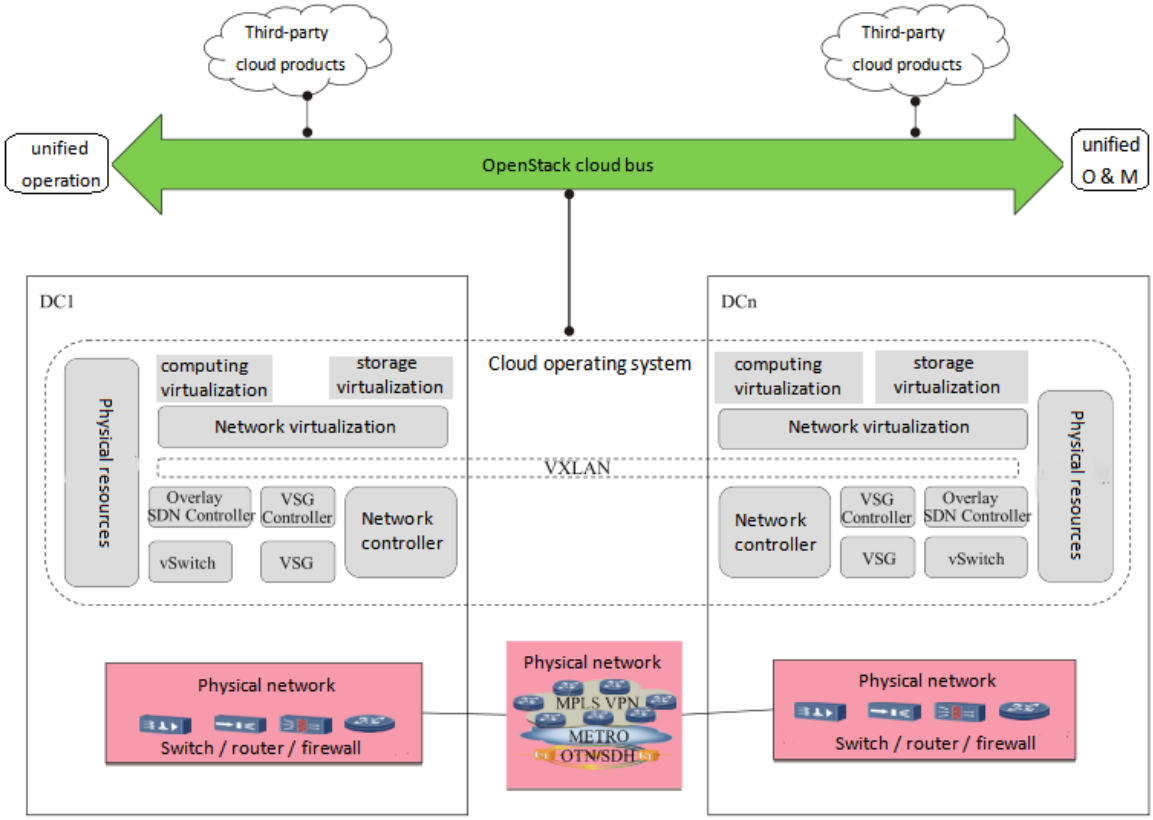

Figure 1 Overall architecture of distributed cloud data center

The distributed cloud data center architecture is not only suitable for large data centers, but also for branches and second-line data centers.On the basis of providing high performance and high

security, through the whole machine pre installation and pre configuration, Data center construction cycle is shortened to hour level; The branch can be unattended and managed by the group through openstack standard interface.

3. Data deployment strategy of distributed cloud data center

The distributed cloud data center optimizes data deployment through the following strategies, user access location awareness and global scheduling of resources to ensure the user's business experience, and supports multi-level business disaster recovery scheme to ensure business continuity, providing users with SLA (service level agreement, service level agreement, hereinafter referred to as SLA) guaranteed cloud services.

3.1 Hot data nearby calculation and centralized storage of cold data

Because the bandwidth between data centers is usually 10-1000 times more convergent than that in data centers,

Therefore, for online class data (hot data) that need to be frequently accessed by computing nodes,

In principle, the computing cluster and the storage cluster as the hot data carrier should be deployed nearby to achieve better performance, otherwise the performance of online applications may be greatly reduced.

For the cold data that offline class seldom accesses, such as enterprise backup data, business and operation log data, call list and statistics data, etc.

Data storage and calculation can be decoupled remotely. Data can be stored as centralized as possible to realize large-scale centralized deployment, so as to give full play to the scale economic advantages brought by the technology of storage thin allocation, compression, and weight removal brought by the super large-scale storage resource pool in the data center.

After centralized deployment, it provides excellent conditions for big data analysis and mining data value.

The distributed cloud data center deploys data according to the data's heat and cold, attribute strategy, which can realize the optimization of data access performance and storage cost, and maximize the use of data value

3.2 Business flexibility

Cloud computing data center network is large in scale and complex in networking. In network design, in order to ensure the reliability and flexibility of the network, it is necessary to design redundant links, protect links and deploy corresponding protection mechanisms.VRRP (virtual route redundancy protocol), double link uplink, SPT (shortest path tree) and other technologies are widely used in the existing data center networking, which have the problems of low network utilization, easy to appear fault, and can only realize local protection.

Proximity access: The delay of cloud service affects the user's business experience. The distributed cloud data center follows the principle of nearby access, minimizing the transit delay and bandwidth consumption from the access point to the data center. The general principle is to ensure that the delay is less than 50ms. And all online processing data of "business application" and "it application", including system image, application image, business configuration, user signing, user private data and media data, are distributed in the data center closest to the user by default.

Uniform resource request routing: The computing, storage, and network resources in each data center logically belong to the same "data center resource pool" or "logical resource pool". All data

centers in the same "logical resource pool" can accept resource requests from local portal or global portal, and support intelligent routing of resource requests to the data center, so as to ensure that the most appropriate data center is selected according to the preset policy to provide the required virtual machine / physical resource services.

3.3 Continuity of business

Business continuity in data center:The distributed cloud data center provides the following business continuity mechanisms within the data center: cross physical machine ft (fault tolerance) to keep the image synchronization of the host and the standby machine in real-time operation state, so as to achieve zero interrupt business continuity guarantee, but the operation state synchronization has a large demand for network bandwidth; cross physical machine ha (high Availability (high availability) is based on shared storage. After the host goes down, the standby starts and takes over the external services of the host in the backup node according to the heartbeat mechanism.

Business continuity across data centers:If the transmission distance of multiple data centers belonging to the same city is less than 300km and there is special optical fiber bandwidth to ensure the transmission delay between data centers is less than 5ms, then the data center can classify the multiple data centers into the same "multi activity disaster recovery pool", and realize the real-time I / O (input / output) synchronization between data centers in this unified "multi activity disaster recovery pool", Thus, after a station fails, the mutual aid station in the pool can take over immediately; for the data center between cities of more than 300km, if the required bandwidth and delay during synchronization can meet the requirements of specific services, it can also be deployed in different places.

For the data centers in different cities, the transmission distance is usually more than 300km, and the bandwidth and transmission delay are not guaranteed stably. Therefore, the distributed cloud data center adopts the "asynchronous disaster recovery" mode by default, that is, to maintain a certain period of data synchronization between specific applications deployed in different data centers. Although the synchronization does not guarantee real-time consistency, it ensures that disaster recovery sites are in occurrence Consistency data of snapshot points in the latest cycle before failure; when one of the data centers fails, the takeover application of its disaster recovery data center can continue to provide services at the latest snapshot point to ensure business continuity.

4. The challenge of traditional network technology in the era of cloud computing

With more and more data center services running on virtual machines, the dynamic and elastic deployment, migration, start and stop characteristics of virtual machines bring great challenges to the traditional static business based network architecture.

In order to support the characteristics of virtual machine live migrate, it is necessary to ensure that the IP address and MAC address of virtual machine remain unchanged before and after migration. At present, virtual machines in data center can only realize live migration in the same IP subnet. Generally, the virtual machines of the same IP subnet are configured in a VLAN (virtual local area network, hereinafter referred to as VLAN), while a VLAN can only be in a two-layer network, that is, the current virtual machines can only be migrated in real time in the two-layer network, and can not support the migration of arbitrary locations.

STP (spanning tree protocol) is used in the second layer network to solve the loop problem, which will block some links and cause some ports to be idle and waste.

Currently, VLAN is used in the second layer network to divide the network into multiple broadcast domains, while vlanid is only 12bit, representing 4094 VLANs. In the multi tenant

scenario, each tenant wants to be logically isolated from other tenants, and the applications of each tenant also want to be isolated from each other, so the number of VLANs in the cloud data center is likely to exceed 4094.

The server connected to the switch contains multiple virtual machines, each of which has its own MAC address. When the number of virtual machines is large, the MAC address table of the switch will overflow, resulting in the loss of data frames or a large number of broadcast frames, seriously affecting the performance of the network.

To solve the above problems, we will introduce the technical solutions of vxlan (virtual extensible local area network, hereinafter referred to as vxlan) and SDN (software defined network, hereinafter referred to as SDN).

4.1 VXLAN

VXLAN is a technology that encapsulates two layer packets with three layer protocol. It can expand two layer network in three layer range. It is applied in the data center, so that virtual machines can be migrated within the scope of three-layer network connected with each other, without changing the IP address and MAC address, so as to ensure the continuity of business. Vxlan adopts 24bit network identification, which enables users to create 16m isolated virtual networks, breaking the limit of 4K isolated networks represented by VLAN, which makes large-scale multi tenant cloud environment have sufficient virtual network zoning resources.

In the deployment of cloud computing data center, each customer's application needs to be logically isolated. The existing VLAN segmentation technology is difficult to meet the multi tenant and scale expansion. The original VLAN technology has the following bottlenecks:

VLAN cannot provide enough segments (more than 4096).

The VLAN network is bound to the physical network structure, which limits the mobility or flexibility of the virtual machine required by the distributed cloud data center.

A large number of VLAN configuration interfaces bring high load to STP (spanning tree protocol).

Customer benefits of vxlan: Virtual machine can migrate in real time across three-tier network without reconfiguration of physical network and business interruption; Abandon STP protocol and make full use of link;It can create 16m isolated virtual subnets to fully meet the needs of multi tenant data center;The access switch only learns the MAC address of the physical server and does not need to learn the MAC of each virtual machine, which greatly saves the exchange performance of MAC table space improvement.

The data plane of vxlan depends on the multicast function of the physical switch, which maps the broadcast in vxlan to multicast, while the physical switch for IGMP (Internet group management protocol, Internet Group management protocol (hereinafter referred to as IGMP) has limited support for the number of multicast groups. Although it can use the method of adding multiple vxlans to the same multicast group to alleviate the problem of insufficient specifications of the switching group, there are problems such as network performance degradation. In addition, Wan usually does not support multicast forwarding, and can not directly realize the expansion of vxlan between different data centers. Instead, SDN controller and vxlan need to cooperate to map multicast to unicast to other data centers.

4.2 SDN

The core goal of SDN is to separate the control surface of network equipment from the data surface through network technology, so as to realize the flexible control of network traffic and provide a good platform for the innovation of core network and application. The ability of SDN is

open and programmable. The core technology of SDN is the flexibility of hardware and software. SDN can upgrade all kinds of bearer protocols online without updating hardware. Through innovative technology, it realizes protocol independent forwarding architecture, which can change the basic bearer protocol on demand without upgrading the router hardware and achieve the maximum flexibility of data plane; realizes the separation of forwarding and control, centralization of control and reduces the operation and maintenance cost of IP network; high performance, distributed routing computing ability supports large-scale SDN network; customized, multi-dimensional routing The algorithm can meet the traffic path selection requirements of different applications and maximize network utilization.

SDN distributed architecture: SDN is to concentrate the function of control plane on the controller. Through the centralized controller to manage and configure various network devices with standardized interface, more possibilities are provided for the design, management and use of network resources, so as to promote the innovation and development of network more easily. From the perspective of virtualized data center, the centralized control surface of SDN can master the topology information of data center network, MAC / IP / location attribute of virtual machine, realize ARP learning function through centralized controller, and avoid a large number of ARP (address resolution Protocol, address resolution protocol, hereinafter referred to as ARP) message impact on server performance; in addition, SDN controller provides open API (application programming interface, hereinafter referred to as API) interface, which can realize flexible programmable ability and provide an open platform for network virtualization, automation, various network services and new business development.

In the distributed data center scenario, the network is divided into the network within the data center and the network between the data centers. The overall architecture of SDN is shown in the figure below.

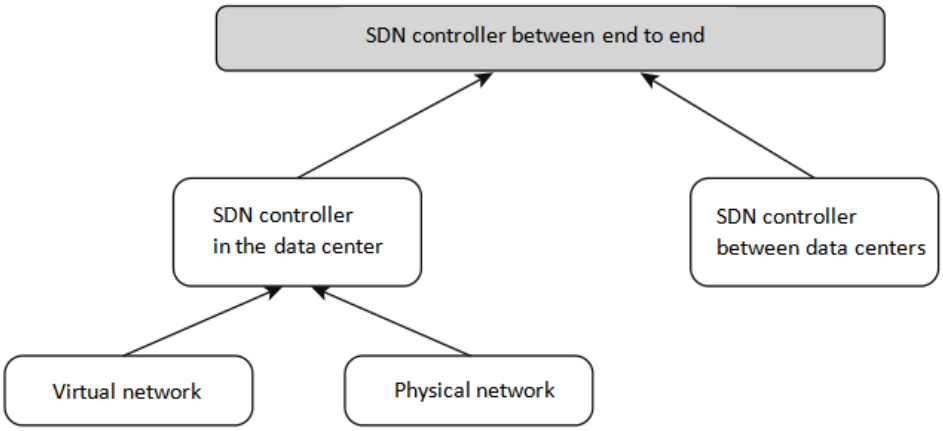

Figure. 2 SDN overall architecture

The end-to-end SDN controller supports the deployment and distribution of network automation services, SLA control of network services, and interconnection of heterogeneous data centers. Through the collaborative control and management of it (information technology industry) and CT (communication technology industry), it can realize the E2E (end to) within and between data centers End, end-to-end) automatic business deployment; through online software configuration, it can flexibly support all kinds of data center technical solutions without upgrading equipment and hardware, and avoid data center operators' worries about technical route selection and subsequent smooth evolution; data center interconnection gateway defined by software can support those built

in different historical periods and adopt no Seamless interconnection with the data center of the technical solution.

Vxlan distributed gateway: When the centralized vxlan L3 (Level 3, three-layer, hereinafter referred to as L3) gateway scheme is adopted, the traffic between different vxlans and the traffic of vxlan accessing the external network are all processed by the centralized spine node (ridge node), as shown in Figure 4, the gateway pressure is large, and the consumption of network bandwidth resources is increased. As shown in Figure 5, in the distributed vxlan L3 gateway scheme, each leaf (leaf node) device can act as a vxlan L3 gateway, forwarding the traffic of the local site in three layers, which greatly alleviates the pressure of the gateway.

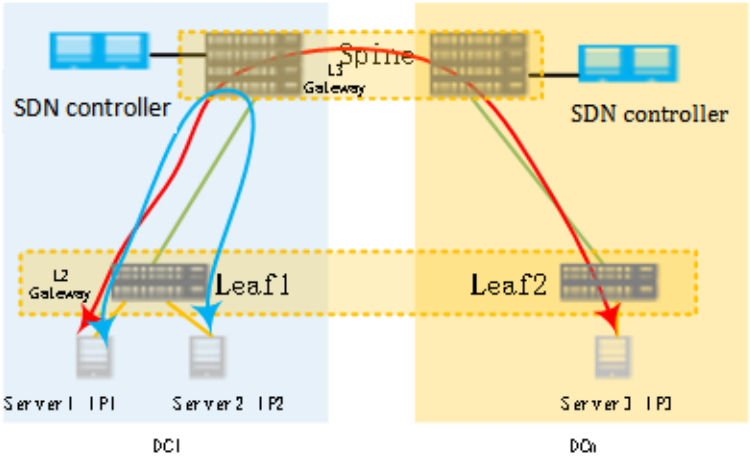

Figure. 3 Vxlan centralized gateway diagram

The traditional centralized three-layer gateway sets the gateway of the server at the convergence or spine node. As shown in Figure 4, all messages across the subnet must be forwarded by the spine node. If the three-layer gateway is deployed centrally, there are the following problems:

The forwarding path is not optimized: the traffic of the local data center across the subnet needs to be forwarded through the centralized three-layer gateway.

The bottleneck of ARP and VNI (vxlan network identifier, vxlan network identifier, hereinafter referred to as VNI) table item specification: since the centralized three-layer gateway is adopted, ARP and VNI table items of terminal tenants forwarded through the three-layer gateway need to be generated on the three-layer gateway, while the specifications of ARP and VNI table items on the three-layer gateway are limited, which is not conducive to the network expansion of data center.

The above problems can be solved by configuring vxlan distributed gateway. Vxlan distributed gateway refers to taking leaf node as vxlan tunnel end point vtep (vxlan tunnel end point, hereinafter referred to as vtep) under the typical "spine leaf" network structure. Each leaf node can be used as vxlan three-layer gateway. Spine node does not sense vxlan tunnel, but only as vxlan message transmission node. As shown in Figure 5, Server1 IP1 and server2 IP2 are not in the same network segment, but they are all hung under the leaf1 node. When Server1 and server2 communicate, the traffic only needs to be forwarded in the leaf1 node, and no longer needs to pass through the spine node.

Vxlan distributed gateway is composed of leaf and spine. Combined with figure 5, the functions of leaf node and spine node in vxlan distributed gateway scenario are introduced:

Spine: The spine node focuses on high-speed IP forwarding and emphasizes the high-speed forwarding capability of the device.

Leaf: As a layer 2 access device in vxlan network, it interfaces with physical server or VM

(virtual machine, hereinafter referred to as VM) to solve the problem of terminal tenants accessing vxlan virtual network.As a three-layer gateway device in vxlan network, VPN (virtual private network, hereinafter referred to as VPN) instance needs to be bound. The establishment of vxlan tunnel depends on the establishment of VPN neighbors. The three-layer gateway encapsulates / de encapsulates vxlan messages to realize the communication between terminal tenants across subnets and the access of external networks.

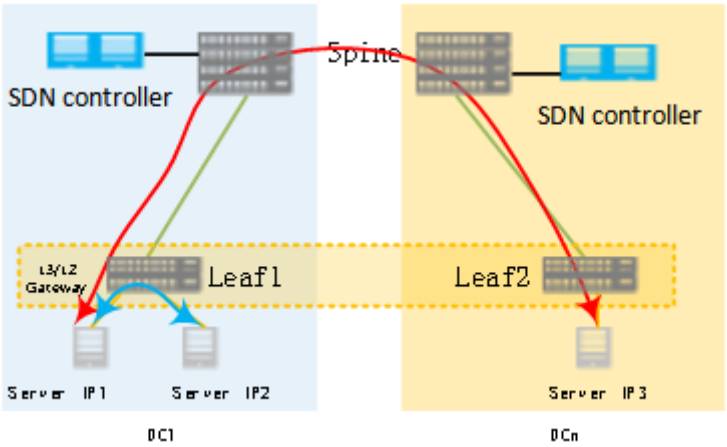

Figure. 4 Vxlan distributed gateway diagram

Vxlan distributed gateway has the following characteristics: The same leaf node can be used as the vxlan two-layer gateway and three-layer gateway at the same time, so the deployment is flexible.The leaf node only needs to learn the ARP and VNI table entries of its own servers, instead of learning the ARP and VNI table entries of all servers like the centralized three-tier gateway. It solves the bottleneck problem of ARP and VNI table entries brought by the centralized three-tier gateway, and has strong capacity of network scale expansion.

If there are servers with the same subnet in different leaf nodes, the three-layer gateway should be configured on the leaf node, and the same IP address and MAC address of the gateway should be configured to realize that the terminal tenant only perceives one three-layer gateway. When the terminal tenant or server moves, there is no need to change the three-tier gateway configuration of the server, which reduces the maintenance workload.

5. Conclusion

Network virtualization is the last step to realize the complete virtualization of IT resources. Network virtualization can meet the needs of dynamic business, and has the ability of intelligent elastic expansion. It can automatically link network configuration management with the deployment and distribution process of upper virtual machine and business application, build the large-scale two-tier network within and across the data center, and simplify application deployment and elastic resource scheduling. Based on the traditional data center network switching equipment, network virtualization has realized the evolution and transformation from the traditional data center network architecture to the software defined network (SDN) target architecture characterized by "network function service", "network equipment pipeline" and "network control software", so as to perfectly cope with and solve the large-scale cloud virtualization environment , multi tenant, flexible virtual network delivery challenges.

References

[1] Huiling Zhao, Baohua Lei, Feng Wang. SDN core technology analysis and practical guide. Publishing House of Electronic Industry, China Telecom, September 2013.

[2] Baohua Lei, Shaoyang Rao, Jie Zhang, etc. Cloud computing decoding (version 2) [M]. Publishing House of Electronic Industry, China Telecom, 2012.

[3] Huiling Zhao, Xi Wang, Fan Shi. Software network: a network revolution about to start [J]. China Telecom, 2013 (6): 53-55.

[4] Dezhong Cai, Bojian Wang. The solution of edge network virtualization for operators [EB/OL]. Cisco Perspective, 2012

[5] Wenmao Liu. Research on network security of enterprise data center defined by software [J]. Science of Telecom, 2014, 30 (11): 140-144.

[6] Mengmeng Wang, Jianwei Liu, Jie Chen, etc Software Defined Network: security model, mechanism and research progress [J]. Journal of software, 2016, 27 (4): 969-992.

[7] Liwen He, Zhi Li, Xiangdong Chen, etc Security services defined by software in cloud environment [J]. Journal of Nanjing University of Posts and Telecommunications (NATURAL SCIENCE EDITION), 2014, 34 (4): 1-6.

[8] Yanfeng Shao, Zhe Jia. Research on network security technology of software definition [J]. Radio Engineering, 2016, 46 (4): 13-17.

[9] Wenmao Liu, Xiaofeng Qiu, Pengcheng Chen, etc. SDN oriented software definition security architecture [J]. Computer science and exploration, 2015, 9 (1): 63-70.

[10] Yu Jin, Hua Zhu. Discussion on security protection strategy of cloud resource pool for operators [J]. Computer knowledge and technology, 2015, 11 (7X).

[11] Laifu Wang, Huamin Jin, Jun Shen.Research on Key Technologies of virtualization security protection [J]. Science of Telecom, 2014 (S2): 107-110.

[12] Ahmad I, Namal S, Ylianttila M, et al. Security in Software Defined Networks: A Survey [J]. IEEE Communications Surveys & Tutorials, 2015, 17 (4): 2317-2346.

[13] Shin S, Porras P, Yegneswaran V, et al. FRESCO: Modular Composable Security Services for Software-Defined Networks. [J]. Proceedings of Network & Distributed Security Symposium, 2013.

[14] Baoshe Qi. Design and implementation of vxlan system for data center [D]. Nanjing University, 2017.

[15] Zhixin Zhang, Zhiming Wu, Wenhua Xu. Research on Key Technologies of overlay network for VDC [J]. Science of Telecom, 2014, 30 (5): 138-144.

[16] Basta A, Hoffmann K, Hoffmann K, et al. Applying NFV and SDN to LTE mobile core gateways, the functions placement problem [C] // The Workshop on All Things Cellular: Operations. ACM, 2014: 33-38.

[17] Big Switch Networks. Revolution: Transforming the network with Open SDN. Open Networking Summit 2013. SANTA CLARA, April 15-17, 2013.

[18] Xiaofeng Qiu, Liang Zhao, Teng Gao. VSA and SDS: Research on two kinds of SDN network security architecture [J]. Minicomputer system, 2013, 34 (10): 2298-2303.

[19] Chen L, Qiu M, Xiong J. An SDN-Based Fabric for Flexible Data-Center Networks [C] // IEEE, International Conference on Cyber Security and Cloud Computing. IEEE, 2015:121-126.