Research on Network Isolate Method in Cloud Environment

Lai Xinming¹, Wang Haitao², Zhao Jing², Zhang Fan², Zhao Chao², Wu Gang²,*

¹Aisino Corporation, Beijing, China
²China National Institute of Standardization, Beijing, China
*Corresponding author
Email: wugang@cnis.ac.cn

Abstract. This paper proposes a network isolation method for large-scale cloud environments. The method run an Envoy-based endpoint program to proxy all network traffic on a physical node. And by configuring a route discovery registration center to uniformly maintain the network meta information of all virtual machines, the virtual machine uses the native VLAN technology to divide the user's subnet to ensure the communication performance of the subnet nodes and the virtual machine network maintained by the route discovery center. Meta information improves the speed of virtual machine ARP addressing and improves cross-node network request performance. Envoy's network proxy technology is used in conjunction with the route discovery center to broadcast the subnet broadcast communication of all virtual machines to the route discovery center, which improves the accuracy of the broadcast and greatly improves the utilization efficiency of the public network bandwidth.

1. Introduction
Cloud computing is an Internet-based computing resource delivery model. Virtualized software and hardware resources are virtualized resources of different sizes and packaged into commodities for circulation through the Internet. In this way, resources are provided to users on demand, enabling software and hardware to make maximum use of resources. Because of the characteristics of virtualization, convenient delivery and high resource utilization, cloud computing has the advantages of low cost, rapid deployment and flexible expansion. Cloud computing user boundaries can be divided into public clouds, private clouds, hybrid clouds, and so on.

With the continuous development and improvement of cloud computing technology and the convenience and expansibility of the use of cloud resources, more and more enterprises have started to build their own private clouds to replace traditional physical clusters as the operating environment for business applications. Regardless an enterprise uses a private cloud service from a cloud computing provider or builds a private cloud environment within the enterprise, the enterprise usually only builds and maintains a cloud data center for use by all molecular companies and departments in the enterprise. Therefore, the resources used by each user need to be isolated, especially network isolation, to ensure data security. Because the virtual computing resources rented by each user are usually scattered on different physical resources, it is impossible to use a physical isolation method for any user. Therefore, VLAN technology is usually used to achieve network isolation between virtual machines. Then the VLAN-based technology standard reserves only 12 bits for VLAN user division. Therefore, VLAN technology can be used to divide up to 4096 subnets for users in a cloud data center. This is sufficient
if it is used in a small business. If it is in a large enterprise, especially for cloud computing providers, it is not enough.

Although Generic Routing Encapsulation (GRE) and Virtual Extensible LAN\(^{[1]}\) (VXLAN) technologies solve the problem of the number of subnet divisions in a large-scale cloud data center environment, their performance is not small, and there is no better solution in the industry. In a large-scale cloud environment, there are a large number of users, and its performance is a very important factor. Therefore, a solution to improve the network isolation performance of a large-scale cloud environment has important economic significance.

2. Related Work
At present, in the industry, both GRE and VXLAN upgrade technologies are proposed as extensions to address the shortcomings of this VLAN technology. The principle of GRE is to run a tunnel program on a physical machine to perform packet encapsulation and unpacking operations. When a virtual machine needs to communicate across physical machines, it encapsulates a GRE header for the original IP data packet and then routes it to the destination through the physical machine network. The tunnel program is unpacked when the physical machine is used. The GRE header has 24 data bits for subnet division, which is sufficient to meet the subnet division requirements in all environments. However, the disadvantage of GRE technology is that tunnels need to be established between two networks. When there are a large number of networks, a large number of tunnels will consume a lot of physical machine routing performance. In addition, GRE technology does not support multicast. When a virtual machine needs to perform broadcast requests such as ARP, the GRE Tunnel tunnel will send request packets to all networks with tunnel connections, which will consume a lot of public network bandwidth and consume network performance.

VXLAN technology also runs a VTEP endpoint program on each physical machine to packetize and unpack data packets, providing 24-bit subnetting quantization. Different from GRE, VXLAN does not need to establish a connection between two networks, and when the virtual machine needs to broadcast, it only needs VTEP to interact with each other based on the IGP protocol. Therefore, the deficiency of GRE technology is solved. However, VXLAN technology still needs to use VTEP to perform packet unpacking operations, which has lost the communication performance of all physical nodes to a certain extent, and the virtual machine based on VXLAN technology needs to communicate with VTEP first during ARP broadcast. In order to truly address the MAC address of the target virtual machine, the number of routes increases, which also reduces the addressing performance. The problems of current network isolation methods for large-scale cloud environments are summarized as follows:

1) VLAN with a maximum of 4096 IDs, which is not practical in large-scale cloud environments.
2) GRE and VXLAN packet decapsulating endpoint programs will lose network request performance.
3) GRE cannot perform multicast, and all subnet broadcasts will occupy a lot of public bandwidth.
4) VXLAN communication across physical nodes has to go through multiple routing and addressing, loss of performance.

3. Methodology
Aiming at the problem of user subnet division and isolation in a large-scale cloud environment, and the performance loss problem in the current solution, this proposal based on Envoy network proxy technology and include a routing endpoint program and a route discovery registry.

3.1. Overview of Logical Architecture
The virtual machine still uses the native VLAN ID. Among the virtual machines in the same physical machine, the same VLAN ID belongs to the same user, but the same VLAN in different physical machines does not necessarily belong to the same user.
Run a route discovery center (RDC) record all of the mapping relationship of VLAN and user information, RDC use quintuple data structure storage the mate information of virtual machine in the cloud environment to make sure the high availability of RDC. The quintuple format as "<vip, gip, mac, vlanid, userid>", vip is the IP address of the virtual machine, gip is the gateway to the virtual machine, mac is the MAC address of the virtual machine, vlanid is the VLAN ID number of the virtual machine, and userid is the user id number of the virtual machine, RDC will build an index based on the userid and VIP of the 5-tuple table to improve access performance.

The overall logical architecture diagram is shown in Fig.1. Physical machine A contains two subnets, VLAN1 and VLAN2, which belong to two users. Each virtual machine on each subnet is registered to RDC through EEP. Physical machine B contains three subnets: VLAN1, VLAN2, and VLAN3, which belong to three users. VLAN1 in physical machine B and VLAN1 in physical machine A belong to the same user and need to be confirmed by RDC.

3.2. Modules

3.2.1. Envoy End Point Program This program listens to all network card traffic on the physical machine and proxy the physical machine traffic based on the Envoy network proxy technology. Responsible for registering the virtual machine network meta information with RDC when the local virtual machine is created and started. When virtual machine is destroyed, the virtual machine network meta information in RDC is cancelled. At the same time proxy all local virtual machine requests and broadcast communications. The ARP request performance of the local virtual machine is enhanced by obtaining the MAC address of the target IP address from the RDC, and the bandwidth utilization efficiency of the public physical network is improved by proxy the broadcast communication of the local virtual machine to the RDC.

3.2.2. Route Discovery Register Center The route discovery register center based on the MySQL database, the network meta information of all virtual machines is saved to realize the function of route discovery and registration. By storing the network meta information of all virtual machines in the form of a five-tuple, the userid field and the vip field are quickly established to enhance query performance. The RDC is responsible for receiving and saving the virtual machine registration information sent by the external EEP, and receiving broadcast requests from the external EEP. It broadcasts the user network according to the VLAN information, gateway information, and user information of the virtual
machine network information table, ensuring VLAN subnet broadcasts. Routing performance and network efficiency

4. Conclusion
Both cloud computing service providers and private clouds built by large enterprises need to provide cloud services to a large number of users. In order to ensure user data security, different users must be isolated at the network layer. The method proposed in this paper is applied to the network isolation of large-scale cloud data center environments, which can improve the communication performance and ARP addressing performance of virtual nodes in the cloud environment, and can greatly improve the broadcast communication performance in the same VLAN, and public Bandwidth utilization efficiency of the network.

The key points of this paper are:
1. Based on Envoy network proxy technology, it reuses the native VLAN subnet division specifications, solves the problem of packet unpacking of GRE and VXLAN, and improves the network routing performance of physical nodes.
2. Design a route discovery and registration center to centrally maintain the mapping relationship between VLAN subnets and users on the physical machine to solve the problem of insufficient number of VLAN subnets. At the same time, the RDC saves the network meta information of all virtual machines, which improves the virtual machine's network praise.
3. Through the route discovery registration center, the broadcast information of the virtual machine is uniformly proxy to make the broadcast target more accurate and improve the utilization efficiency of the public network bandwidth.

Acknowledgment
This paper is supported by grants from National Key R&D Program of China (522016Z-4973) and China National Institute of Standardization (522018Y-5941, 522018Y-5948).

References
[1] Mahalingam M, Dutt D, Duda K, et al. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks[J]. 2014.
[2] A scalable, commodity data center network architecture[J]. Mohammad Al-Fares, Alexander Loukissas, Amin Vahdat. ACM SIGCOMM Computer Communication Review . 2008 (4).
[3] vnss:a network security sandbox for virtual computing environment. Gao Xiaopeng, Wang Sumei, Chen Xianqin. Youth Conference Information Computing and Telecommunications . 2010
[4] Zitan Chen, Alexander Barg. "The repair problem under connectivity constraints: Explicit MSR codes for the rack-aware model of distributed storage", Communication Control and Computing (Allerton) 2018 56th Annual Allerton Conference on, pp. 710-714, 2018.
[5] S. Sahraei, M. Gastpar, Increasing availability in distributed storage systems via clustering, 2017.
[6] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, S. Vishwanath, "Locality and availability in distributed storage", IEEE Transactions on Information Theory, vol. 62, no. 8, pp. 4481-4493, 2016.