Design and Implementation of VPN Related Protocols

Siping Hu, Shejie Lu, Feng Wen*

Hubei University of Science and Technology, Xianning 437100, China

Keywords: VPN, Network Topology, Reliability, Quality Assurance

Abstract: This paper designs the carrier's backbone network topology, which provides accessibility and quality assurance for various traffic in the network, such as multicast data streams used for live broadcast, voice streams used by IP phones, and common data streams. In order to achieve secure, fast and reliable communication across customers, MPLS VPN technology is used to build a secure tunnel, and to transfer private network routes between sites to connect different sites of the same enterprise. At the same time, the VRRP technology is used to back up the gateway when the user accesses, providing reliability assurance.

1. Introduction

As the core network, the backbone network has always been crucial in the network. China has four backbone networks. The “China Public Computer Internet“ operated by telecommunications originally belonged to the Ministry of Posts and Telecommunications, and the Ministry of Posts and Telecommunications was rescinded and then operated by China Telecom. Mobile has a special "China Mobile Internet", China Unicom also has "China Unicom Computer Internet", and Netcom has "China Netcom Public Internet". Each operator has its own backbone network, providing network foundation for all localized LANs and customers. service.

The backbone network is generally a network structure formed by interconnection of many routers, providing different paths to the same target network segment. When some links are faulty or congested, other links are available for selection, and there is considerable redundancy. Sex. In addition, the backbone network provides some secure VPN connections. For the site, the backbone network is equivalent to a network cloud. The customer does not need to know how the backbone network implements data transmission securely, but only passes the data to the backbone network. The PE device, the other site can receive data from another PE of the backbone network. The transmission of these data over the network is relatively secure.

The design of the backbone network is generally flat, in order to simplify its design and increase stability. The so-called flat network means that the network outlets at all levels are directly connected to the data center. Only the data center is the central node, and the rest are end nodes. Each end node is configured with reasonable bandwidth and QoS as needed. The backbone network needs to ensure the smooth and sTable routing and data transmission, unlike enterprise networks that require many routing control strategies.

As more and more information is transmitted in the network, it is getting faster and faster, and the backbone network is under increasing pressure. A variety of technical challenges coexist. Space backbone network applications are huge and have many users. They pose challenges to high-capacity high-speed data transmission, different priority service quality, integrated network management, and system security. If there is a problem with a backbone network, the customers served by the company that runs the backbone network will be affected more or less, and may even cause disruption of business data and cause incalculable losses.

2. IGP comparison and selection

The Internet is a collection of autonomous systems (ASs). Each AS is operated and managed by a different organization. A set of its own routing protocols and management policies are used within the AS. The routing protocols used within the AS become IGP (Interior Gateway Protocol).

Currently, the widely used IGP routing protocols include OSPF, IS-IS, and RIP. They have their own features and application scenarios. The following sections describe and compare them.

2.1 Open Shortest Path First

OSPF (Open Shortest Path First) was born in the 1980s and uses the SPF (Shortest Path First) algorithm, which is a link state routing protocol. In OSPF, a set of networks or routers grouped together according to certain OSPF routing rules is called an area. OSPF can classify a network into multiple types of areas, such as stubs, NSSAs, non-complete sub-zones, backbones, and common areas. When the topology of a certain area changes, the nodes in other areas only need to modify the routes in their routing Table without re-calculating the SPF. The multi-zone design reduces the LSDB (Link State Database) of the OSPF router and simplifies the routing calculation process. Each area will synchronize the LSDB, the synchronization process is reliable, and each LSU (link status update) must have a corresponding LSACK (link status corresponding) response.

OSPF technology can support large-scale networks, support interface authentication, and multicast protocol packets. Authentication is based on interface authentication, zone-based authentication, and authentication for V-link. Note that the authentication is performed as long as the authentication user name and password are the same. The authentication information is carried in the OSPF packet header. Each OSPF packet carries the packet header. There is no authentication type field.

Each network node draws its own shortest path tree according to its own LSDB. Therefore, loops are not possible in the area. However, loops may occur between the areas due to network planning and other reasons. This requires higher requirements for engineers. OSPF classifies networks into four types: Broadcast, P2P (point-to-point), P2MP (point-to-multipoint), and NBMA (non-broadcast multi-access). Different physical networks have different default network types. The working modes of the four network types and the way of describing the topology are different, providing a good working method for adapting to various networks. As the current network scale continues to increase, OSPF uses the incremental SPF algorithm to introduce an "intelligent timer", which uses BFD (bidirectional forwarding detection) technology and interface penalty (dampening) technology to optimize OSPF to shorten the relay. Route interruption, device failure, etc. cause the route convergence time generated by the recalculation of the metropolitan area network network, reduce the impact on network delay and jitter sensitive services, reduce the impact of equipment faults on services, improve network availability, and satisfy network-to-multiple Business bearer support.

2.2 Intermediate System-to-Intermediate System

The OSPF protocol is too complex and greatly limits the number of supported routers and the number of routes. IS-IS (Intermediate System - Intermediate System) routing protocol is simpler than OSPF, so more and more enterprises adopt ISIS protocol as the network. In the IGP agreement.

The IS-IS routing protocol also uses the SPF algorithm, which is also a link-state routing protocol, but has some fast convergence mechanisms, such as i-SPF (incremental SPF) calculation. After the network system is started, only one full SPF is performed. It is calculated that all subsequent nodes change only i-SPF calculation. If the network on the node changes, only the PRC (local route calculation) calculation is performed. The i-SPF calculation is faster than the full SPF calculation compared to the PRC calculation. In addition to this, there is a simplified SPF calculation. The topology of the entire network needs to be recorded, and the SPT tree generated by each SPF calculation is saved. IS-IS has an intelligent timer mechanism and is divided into an LSP (Link State Packet) intelligent timer and an SPF intelligent timer. The LSP intelligent timer specifies that the LSP spread in the network should be within a certain range. If the LSP spreads too frequently, the diffusion is restricted to reduce the CPU usage. The SPF intelligent timer can prevent the SPF calculation from being too frequent while ensuring that the network performs SPF calculation as soon as possible to reduce unnecessary resource consumption. By default, an LSP is flooded periodically. Even if a new LSP is received, it will not flood quickly. However, the fast flooding mechanism of the LSP stipulates that when an intermediate system receives an LSP, it should immediately spread out. Then perform the SPF calculation.

ISIS works at the data link layer, and most of the attacks in the current network are based on the IP layer and above, so it is more secure than OSPF. In addition, ISIS has a special authentication method that greatly guarantees the legitimacy of ISIS-related messages received. Different from OSPF, its area division is simpler. Only the level-1 area and the level-2 area make the configuration and operation tasks of engineers easier. IS-IS uses TLV (type, length, value) structure to carry information, so it is more scalable, supports non-IP networks, and is easy to transition to IPv6. Originally developed based on the OSI seven-layer system model, although the current IS-IS is mainly used to support IP networks, the structural ideas have not changed, and the current network is a five-layer model of TCP/IP, so engineers familiar with IS-IS a bit less. Because of these characteristics of IS-IS, IS-IS is mostly used in carrier backbone networks.

3. Network topology design

Fig.1 shows the topology of the backbone network. There are 8 routers in the network. R5 and R6 are PEs (edge devices) of the backbone network, which are used to provide VPN connections between sites. R1, R4, R7, and R8 are used to connect to the NAT route of the site, and send the data sent by the site to the public network. R2 and R3 are used to connect the backbone network to the Internet.

The IGP protocol running on the backbone network is the IS-IS routing protocol. The IS-IS protocol belongs to the link layer protocol, and its security is higher than other protocols. The TLV structure makes it more scalable. If you need to carry other types of routes or new authentication information, just develop a new TLV.

The backbone network runs the BGP routing protocol, which is used for route delivery between ASs. Run MP-BGP routing protocol between R5 and R6 to deliver VPN-IPv4 routes so that the two sites can access each other.

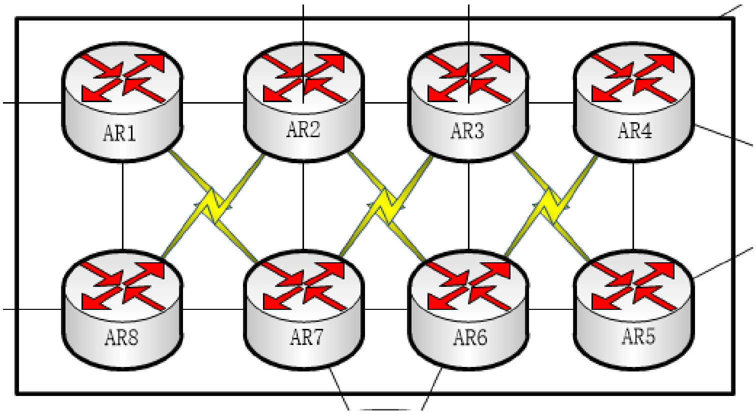
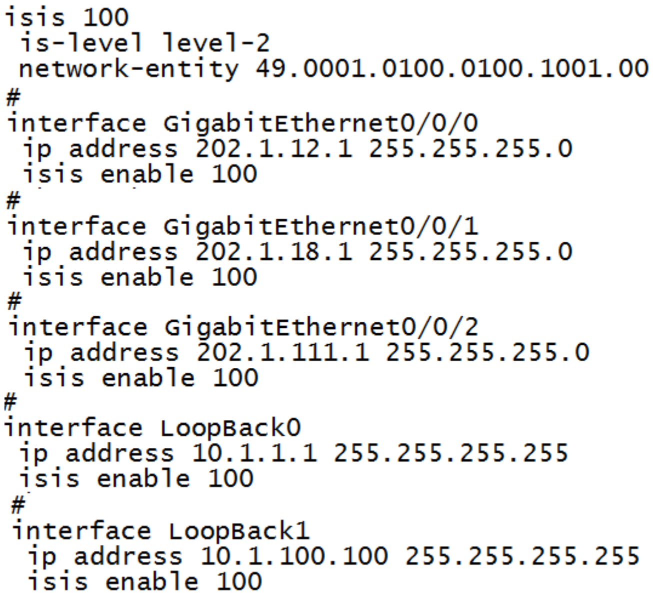


Fig.1 backbone network topology

3.1 Backbone Network IGP Configuration

The configuration process ensures the connectivity of the backbone network. ISIS is configured on the loopback0 interface to establish a sTable BGP neighbor. The ISIS is configured on the loopback1 interface for the Anycast RP. The physical interface is configured to ensure the basic network connectivity of the backbone network. The configuration of R1 is shown in Fig.2. The IS-IS process configuration process of other routers is similar.

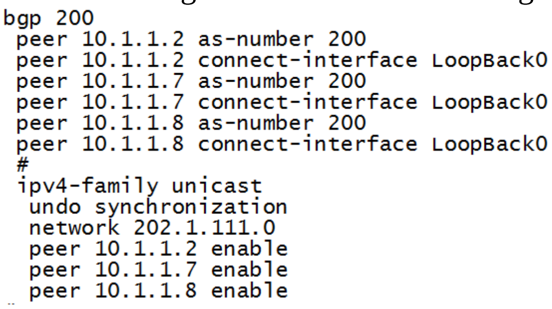


```
isis 100
 is-level level-2
 network-entity 49.0001.0100.0100.1001.00
#
interface GigabitEthernet0/0/0
 ip address 202.1.12.1 255.255.255.0
 isis enable 100
#
interface GigabitEthernet0/0/1
 ip address 202.1.18.1 255.255.255.0
 isis enable 100
#
interface GigabitEthernet0/0/2
 ip address 202.1.111.1 255.255.255.0
 isis enable 100
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.255
 isis enable 100
#
interface LoopBack1
 ip address 10.1.100.100 255.255.255.255
 isis enable 100
```

Fig.2 IS-IS configuration of R1

3.2 Backbone network BGP configuration

The BGP configuration process is to establish a neighbor relationship with a loopback interface. Can make neighbor relationships more sTable. Even if the physical interface is down, as long as the loopback route is reachable, TCP interaction can be performed to establish a neighbor. Note that the original IP address of the configured packet is the loopback IP address. Otherwise, the peer neighbor will not recognize the Hello packet sent from the non-locally configured neighbor. The related configuration on R1 is shown in Fig.3. The other router configuration process is similar.



```
bgp 200
 peer 10.1.1.2 as-number 200
 peer 10.1.1.2 connect-interface LoopBack0
 peer 10.1.1.7 as-number 200
 peer 10.1.1.7 connect-interface LoopBack0
 peer 10.1.1.8 as-number 200
 peer 10.1.1.8 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  network 202.1.111.0
  peer 10.1.1.2 enable
  peer 10.1.1.7 enable
  peer 10.1.1.8 enable
```

Fig. 3 R1 BGP configuration

4. Conclusion

In order to solve the problem of secure mutual visits between company sites, this paper adopts MPLS-VPN technology. Ordinary inter-site mutual access uses NAT address translation. The destination address of this access can only be a public network address. To achieve mutual access, you must access the server through the public network indirectly. For security requirements, after using MPLS-VPN technology, The VPN-IPv4 routes can be transmitted between the sites. The sites have their own private network routes. The backbone network is also responsible for transferring the data directly sent by the private network. The data is directly transmitted through the LSP tunnel in the backbone network, achieving efficient and secure data. purpose. The test results also prove that the access between the company sites 2-1 and 2-2 is passed through the VPN tunnel after being encapsulated by MPLS.

Acknowledgements

This research was supported by key scientific research projects of Doctor Initial Funding of Hubei University of Science and Technology (No. 2016-19XB003, BK1419), the Scientific

Research Project of Education Department of Hubei Province under Grant B2018179 and B2017181 and B2018175, NSFC-Big Data Science Center Project of Guangdong , U1611262, Research and Development Fund of Hubei University of Science and Technology (2018-19GZ01).

References

[1] Rami Akeela, Behnam Dezfouli. Software-defined Radios: Architecture, state-of-the-art, and challenges. Computer Communications, 2018,128(9): 106-125.

[2] Haixia Peng,Dazhou Li,Khadige Abboud et.Performance Analysis of IEEE 802.11p DCF for Multiplatooning Communications With Autonomous Vehicles,IEEE Transactions on Vehicular Technology, 2017,66(3): 2485-2498.

[3] Azadeh Faridi,Boris Bellalta,Alessandro Checco.Analysis of Dynamic Channel Bonding in Dense Networks of WLANs,IEEE Transactions on Mobile Computing, 2017,16(8): 2118-2131.

[4] Seyhan Ucar,Sinem Coleri Ergen,Oznur Ozkasap.Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination, IEEE Transactions on Vehicular Technology, 2016,65(8): 2621-2636.

[5] Ather S., Imdad U. Effect of transmission opportunity and frame aggregation on VoIP capacity over IEEE 802.11n WLANs. 8th International Conference on Signal Processing and Communication Systems, 2014:1-7.

[6] Jinyeong U., Jongsuk A., Kangwoo L. Evaluation of the effects of a grouping algorithm on IEEE 802.15.4 networks with hidden nodes.Journal of Communications and Networks, 2014,16(1):81-91.

[7] Um J.Y., Ahn J.S., Lee K.W. Evaluation of the effects of a grouping algorithm on IEEE 802.15.4 networks with hidden nodes, Journal of Communications And Networks, 2014, 16(1): 81-91.

[8] Minho K., Choi C.H. Hidden-node detection in IEEE 802.11n wireless LANs. IEEE Transactions on Vehicular Technology, 2013, 62(6): 2724-2734.