Design and Implementation of Enterprise Information Based on Vpn Technology

Dianhua Wang[1], Feng Wen[1], Siping Hu[*,1,2]

[1]Hubei University of Science and Technology, Xianning 437100, China

[2]Wuhan University of Technology, Wuhan 430070, China

*E-mail: zjlg0001@126.com

*Corresponding Author

Keywords: Vpn, Data security, Scalability, Remote access

Abstract: With the advent of the information age, information technology is accelerating, and the data formats transmitted by the network are becoming more and more abundant, such as the data formats and contents of voice and video are becoming more and more abundant. Network data services cover almost all areas, sectors and regions of society as a whole. As society's demand for network continues to grow, companies are proposing new and higher data security requirements for their company's network performance, and paying more attention to network flexibility, scalability, and economics when building their own corporate networks. Practicality. Under this background, this paper mainly provides a reference value for the networking scheme of mobile communication office information through the analysis of the networked deployment of mobile information office information, combined with the characteristics of private network and VPN network. Mainly for the application of VPN remote access network and the traditional way to remotely access the network to compare the specific advantages, highlighting the advantages of using VPN for remote access to the network, the VPN is applied to enterprise office information.

1. Introduction

With the advent of the information age, information technology is accelerating, and companies are paying more attention to network flexibility, scalability, and economic utility in building their own networks. At the same time, as the company continues to develop, it may establish a branch office, and employees in the enterprise are not necessarily all working in the corporate office area. Therefore, how the branch office and these outgoing employees communicate with the corporate headquarters and work is a problem. If the traditional fiber access method is adopted, the cost is high and the implementation is difficult, and the scalability is poor afterwards. Under this background and premise, VPN virtual private network has become one of the indispensable network technologies for many companies to establish enterprise networks and realize office network informationization. In the past decade, VPN technology has developed rapidly, and it no longer uses traditional physical leased lines, which is a good way to improve network flexibility. The VPN mode combines the private network and the public network well, so that the flexibility and security of the private network are fully utilized, and the scalability, reliability, and richness of the public network resources are fully utilized. At the same time, it also reduces the investment cost of network equipment. The main purpose of this research is to use VPN technology to make use of existing network resources to provide network access to the establishment of branch offices and office workers who need remote access during the development process. And it can provide more high-quality and reliable services for the employees, and further enhance the competitiveness of the company in the market.

2. Vpn Related Technology Research

VPN is a wide area network (WAN) technology and a remote access network technology.

DOI: 10.25236/ISMHI.2019.005

Because the entire VPN network is based on the network platform provided by the public network service provider, it can also be called a virtual network. In the traditional enterprise network configuration, DDN (Digital Data Network) leased line or frame relay is used to realize interconnection between different local area networks (LANS). This communication scheme inevitably leads to higher costs for network communication and maintenance. Mobile users and remote individual users usually enter the corporate LAN through dial-up lines, which inevitably poses a security risk to users.

In order to solve these problems, a virtual private network VPN is proposed. The virtual private network VPN has the following advantages over the traditional network:

(1) Cost savings. Establishing a wide area network over a public network eliminates the large amount of human and material resources required to install and maintain WAN devices and remote access devices.

(2) The transmission data is safe and reliable. The tunneling technology used by the virtual private network and the technologies such as encryption and authentication ensure the security of the transmitted data.

(3) Full control. The virtual private network can allow users to make full use of the public network's service facilities, and also allows users to fully control their own networks, and can change the security settings and network management of their own networks. The basic VPN reference model of the virtual private network can also be established within the enterprise network.

3. Vpn Technology Design and Implementation

M company's address is located in Xinjiang, its company is large in scale, and its network coverage is wide. Its network terminal extends to Xinjiang counties, townships and towns. M company has a total of 104 branches and offices in Xinjiang, with more than 6,000 service outlets. The service area covers most of Xinjiang. At present, the services provided by the company mainly include various comprehensive information services. M has nearly 5,000 full-time employees and nearly 4,000 labor dispatchers with nearly 9,000 employees. More than 80% of all M-Community employees use computers in their daily work.

In M's network topology design, simulation software was used to simulate the company's branch offices, out-of-office employees, and the public network between the head office and them. The head office consists of the company's personnel department, technical department, administration department, sales department, logistics department, finance department and the core of the entire head office network - the data center. Because the finance department is a relatively confidential department, the finance department can access other departments in the network, but other departments cannot access the finance department at will.

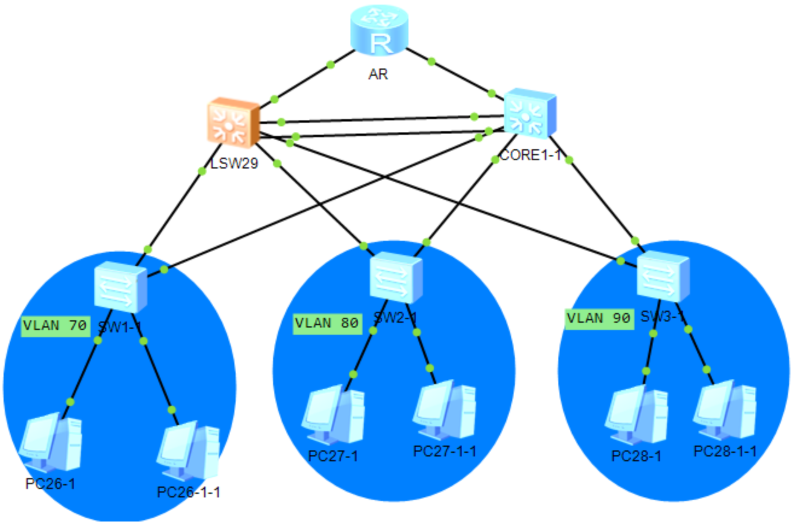


Fig.1 Network Topology

To ensure data security in the data center, firewall devices are deployed as barriers in the data center. Branch offices and office workers do not directly access the company's internal network through the public network, but access the company network through a logically established VPN tunnel. By establishing a VPN tunnel to access the company's internal network, the security of data transmission can be guaranteed. Network connectivity between the company, including branch offices and out-of-office workers, and the relative security of data transmission can be achieved without the need to deploy actual network lines.

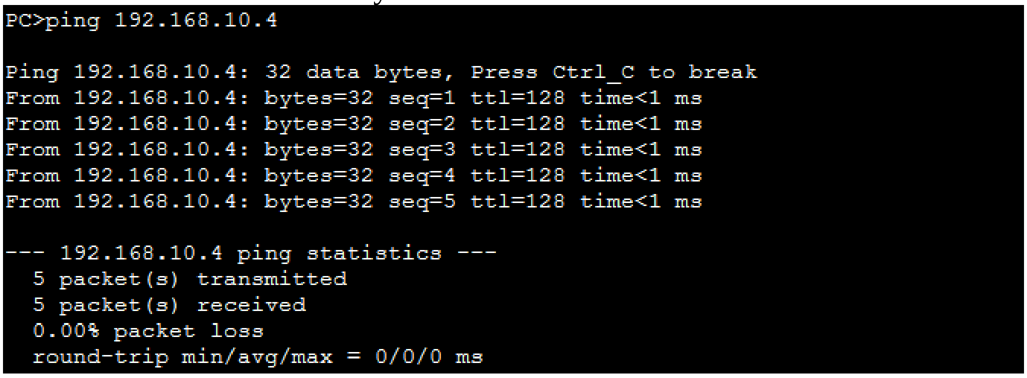
4. Network Running Test

Testing the running state of the network is an important part of the network design. After the corresponding configuration of the entire network topology, the connectivity and stability of the entire network of the company are tested as follows.

4.1 Connectivity Test between Branch Office and Head Office

The connectivity between the branch office and the head office network was tested. The results are as follows:

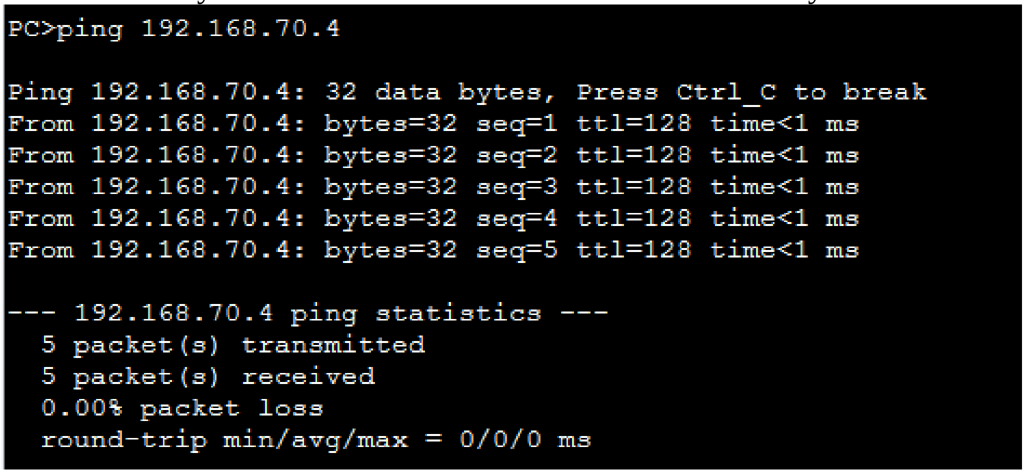
(1) Use the host of the branch network to test the ping command of a host in the data center of the head office. The host address of the branch office is 192.168.70.4, and the host address of the head office is 192.168.10.4. The test results are shown in Figure 2. It can be seen from the test results that the branch office can already have normal access to the head office network.



```
PC>ping 192.168.10.4

Ping 192.168.10.4: 32 data bytes, Press Ctrl_C to break
From 192.168.10.4: bytes=32 seq=1 ttl=128 time<1 ms
From 192.168.10.4: bytes=32 seq=2 ttl=128 time<1 ms
From 192.168.10.4: bytes=32 seq=3 ttl=128 time<1 ms
From 192.168.10.4: bytes=32 seq=4 ttl=128 time<1 ms
From 192.168.10.4: bytes=32 seq=5 ttl=128 time<1 ms

--- 192.168.10.4 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/0/0 ms
```

Fig.2 the Host of the Branch Network Pings the Test Results of the Head Office Host

(2)Using a host of the head office to test the ping command of one of the branches of the branch office, where the host address in the head office is 192.168.20.4, and the host address of the branch office is 192.168.70.4. The test results are shown in Figure 3. It can be seen from the test results that the head office can already access the subnet of the branch office normally.

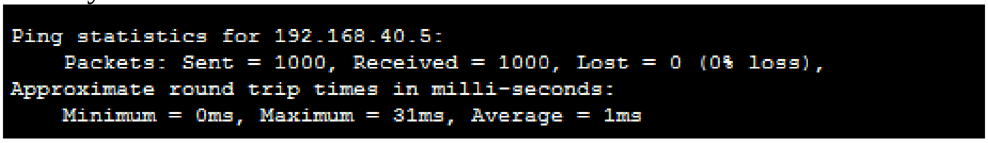


```
PC>ping 192.168.70.4

Ping 192.168.70.4: 32 data bytes, Press Ctrl_C to break
From 192.168.70.4: bytes=32 seq=1 ttl=128 time<1 ms
From 192.168.70.4: bytes=32 seq=2 ttl=128 time<1 ms
From 192.168.70.4: bytes=32 seq=3 ttl=128 time<1 ms
From 192.168.70.4: bytes=32 seq=4 ttl=128 time<1 ms
From 192.168.70.4: bytes=32 seq=5 ttl=128 time<1 ms

--- 192.168.70.4 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 0/0/0 ms
```

Fig.3 Host in the Head Office Pings the Test Results of the Branch Host

4.2 Network Stability Test

Secondly, the overall performance of the network is tested, that is, the packet loss rate of the test packet during transmission. Here, using one host in the head office to perform 1000 ping command tests on one host of the branch office, the host address in the head office is 192.168.20.4, and the host address in the branch office is 192.168. 40.5, the test results are shown in Figure 4. From the test results, the packet loss rate is almost zero during the network operation, so the M company's network runs stably.



```
Ping statistics for 192.168.40.5:
    Packets: Sent = 1000, Received = 1000, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 31ms, Average = 1ms
```

Fig.4 the Host in the Head Office Pings the Test Result of the Host of the Office Worker

This paper mainly tests the connectivity of the designed M company network and the stability of the network. The test results show that between the head office and the branch office, the head office and the out-of-office personnel can already achieve network interoperability, and due to the particularity of the finance department, all branches, out-of-town personnel and other departments cannot access the finance department. It can be concluded from the test results that the network has been successfully implemented.

5. Conclusion

This paper first analyzes the network problems and related needs of the current enterprise in the development process, and discusses the advantages of using VPN technology to build the internal network. Taking the office communication network of M company as an example, the application information system of M company office based on VPN technology is proposed. It is obviously unrealistic to apply traditional network construction forms for remote access, such as accessing optical fibers. In contrast, VPNs do not require physical network links for remote access, but only logically. The network can access the link and apply the existing network communication resources. Therefore, it is concluded that it is necessary to apply VPN to the company's network composition.

Acknowledgements

This research was supported by the Scientific Research Project of Education Department of Hubei Province under Grant B2018175.

References

[1] Gao D., Cai J.F., Foh C.H. Improving WLAN VoIP capacity through service differentiation. IEEE Transactions on Vehicular Technology, 2008, 57(1): 465-474.

[2] 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.

[3] 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.

[4] 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.

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

[6] Yuan Z., Muntean G. iVoIP: an intelligent bandwidth management scheme for VoIP in WLANs. Journal of Wireless Networks, 2014, 20(3):457-473.