# Application of Redundant Backup Technology in Network Security

**Shuwen Deng[1], Siping Hu*, [1], Dianhua Wang[1], Limin Liu[2]**

[1]Hubei University of Science and Technology, Xianning, 430070, China

[2]Luxi Town Central Primary School of Jiayu County, Xianning, 430070, China

*E-mail: zjlg0001@126.com

**Keywords:** redundant backup, virtual local area network, security authentication, fault tolerance

**Abstract:** This paper mainly introduces the implementation of bank network design and system construction. In the era of rapid network development, the network is becoming more and more important in daily life, especially in some large facilities and institutions, the network has become a necessary means to maintain its development. Because the bank is a large financial institution, its design needs are relatively high, not only to be safe, efficient, convenient, but also to consider fault tolerance and data integrity. In terms of bank demand, the performance planning and implementation of various aspects of the banking network are described point by point. This paper also introduces the overall structure of the bank design, implementation plan and test results.

## 1. Introduction

With the rapid development of society, banks play an indispensable role in everyone's life. Therefore, bank network construction plays a very important role. Security is extremely important for banks for banks. At the same time, it is necessary to establish reliable connections between other branches to ensure data integrity. The connectivity and security of the entire bank are determined. The foundation for the stable development of banks today. This design is the concept and implementation of these two developments.

The continuous updating of information technology has made the e-commerce process faster and faster. The emergence of new business technologies based on the network platform has fundamentally changed the traditional banking management system and management system, and gradually developed and established information. A new model for automated office and scientific management. With the change of payment and transaction brought by information technology system, the banking industry has developed non-cash electronic trading methods such as online banking and e-banking, forming a new type of financial transaction mode characterized by network, rapidization and currency digitization. Expanding the bank's business, this electronic trading method is integrated into every aspect of today's society and has greatly changed people's lives.

As the financial industry's reliance on network technology continues to deepen, regulators have also imposed stricter requirements on network security in related industries. However, in order to comply with the development trend of the industry, the entire banking industry has invested in building its own network system to meet the production and office needs of daily business. However, due to the huge economic interests of the financial industry, the criminals have targeted banks in a row, new information attacks have emerged in an endless stream, and the network security system is imperfect, resulting in security vulnerabilities and hidden dangers. Bank networks are often highly threatened. Accidents will not only cause direct economic losses to customers and banks, but will also bring losses to national interests. Therefore, higher and stricter standards must be imposed on the security level and security measures of the banking information network system.

## 2. Network technology

Virtual Local Area Network Technology

VLAN is a Layer 2 technology of OSI. It is the redistribution of network and network resources.

  DOI: 10.25236/systca.18.009

They are connected to the switch ports defined by the administrator. By creating VLANs, you can specify switch ports to serve different subnets, creating smaller broadcast domains in Layer 2 switched networks, providing inter-network segment security, and splitting large networks into small networks to address broadcast and multicast. The problem of taking up too much bandwidth.

The VLAN can logically segment the connected Layer 2 port according to the requirements of the switching network, such as function, location, department, network protocol or application policy, and is not restricted by the physical location of the user. The same VLAN can communicate between a single switch or different switches.

Therefore, VLAN technology is used on Layer 2 and Layer 3 switching devices. By controlling each port and resources that can be accessed through the port, network administrators can build a secure and reliable network platform.

Advantages of dividing VLANs:

1) Control broadcast: A VLAN is a logical broadcast domain. By creating a VLAN, the broadcast is isolated, the broadcast range is narrowed, and broadcast storms can be controlled.

2) Security: All ports and users can be controlled by creating a broadcast domain using VLANs. It can also create VLANs based on the network resources that users need to access and configure the switch to notify network management workstations without authorized access to network resources. If you need to communicate between VLANs, you can implement these restrictions on the router to ensure communication security. You can also limit hardware addresses, protocols, and applications. This improves the overall performance and security of the switching network.

3) Flexibility and scalability: With VLAN technology, different users in different locations and different networks can be divided into logical network segments according to department functions and object functions, achieving the same flexible and convenient effect as the local LAN. On the one hand, the flexible combination mechanism of the network segment and the mechanism provided by the VLAN reduces the workload of the administrator, and on the other hand, reduces the network maintenance cost of moving or changing the geographical location of the workstation.

### 3. Bank network overall architecture

As shown in Figure 1, the devices in the core area use two CISCO 3560 Layer 3 switches. The main function is redundant backup. The two devices back up each other. If one of the devices fails, the other one can take over. It becomes the primary forwarding device. The traffic trend is that the traffic of the access zone and the outbound zone of the device 1 is left, and the traffic of the outreach zone and the office zone of the device 2 is left, and the two devices back up each other. Two 3A servers are configured on the two core switches to authenticate users accessing the core and other devices.

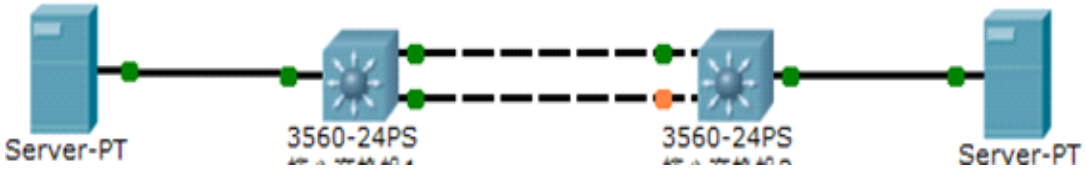


Figure 1 core area topology

The branch aggregation layer uses two 2811 routers. The line is one branch office area partition 1 traffic, the other is office area 2 traffic, and the two devices back up each other. The branch access zone equipment also uses the 2811 router, which is the flow control and forwarding of the two partitions of the branch office area.

The two access switches are configured with trunk mode through EtherChannel technology to form VLAN port aggregation, so that VLANs on different switches can access each other. The two switches use trunk mode to effectively improve data forwarding and share server pressure. This mode can effectively reduce the equipment failure rate.

The outreach area consists of two 3560 Layer 3 switches and two 2811 routers. The following two PCs access the other internal devices as simulation tests, and realize the secure controlled

interconnection of the outer zone and the branch core zone through the ACL access control list. When the service is provided externally, the outreach service area is configured with NAT and ACL configuration, which can prevent the disclosure of important information such as its own internal IP to the external connection terminal.

The production switch uses two 3560 Layer 3 switches. In the experiment, the ACL access control list is used to achieve security isolation between the production area and the core area. The production switch independently plans vlan33 for access to the production server. Ethernet technology is used for trunking between the two production switches to ensure that VLANs on different switches can communicate with each other. The production area uses a static routing protocol to implement interworking with the core switch. The floating static route is used to set up different priorities to implement link redundancy and form a backup mechanism. The two production switches are respectively connected to the host and standby of the production server.

The office aggregation switch uses a 3560 Layer 3 switch, and the access layer switch uses two 2950 switches. The two switches at the aggregation layer function to isolate and forward data by two different devices. In the experiment, each department was simulated with a PC. The office area uses the ACL access control list to implement security isolation between the office area terminal and other area network segments. Other departments only allow internal access within the office area and mutual access with the office terminals of the head office and branch offices. A static routing protocol is implemented between the branch core switch and the office area to implement interworking.

Bank regional network architecture

This section mainly introduces the role of each department in each region, as well as the IP allocation and which VLAN it belongs to.

Branch line access area: Two branch line routers access the branch branch through the office line and connect to the core switch through the LAN link. Its purpose is to connect other branches to achieve data synchronization.

Outreach area: The component is the outreach aggregation layer and the access layer, which is used to provide outbound services, including service access of the supervision department, intermediate agent service, and key customers, and access to the core area of the branch through the firewall.

The VLAN of the production area is set up on the Layer 3 switch. The traffic in the production area is important. The EtherChannel is used. This switch enables HSRP to implement redundant backup. The SVI is enabled on both devices. The aggregation switch 1 is the root bridge of VLAN 30 and the aggregation switch 2 is the root bridge of VLAN 40.

## 4. Bank Area Connectivity Test

### 4.1 Office Area Connection Test

The network administrators in the office area manage and maintain the network equipment of the branch every day. Therefore, each time the equipment is inspected, it is a daily task. In this process, it is allowed to log in to each LAN device for inspection and maintenance. Therefore, the 3A authentication method is adopted here, and the login process must be verified by the server before being authorized to log in. Here, I test the object of the technical department of the office area, through the AAA authentication method, access the encrypted aggregation switch 4 to see if verification is needed.

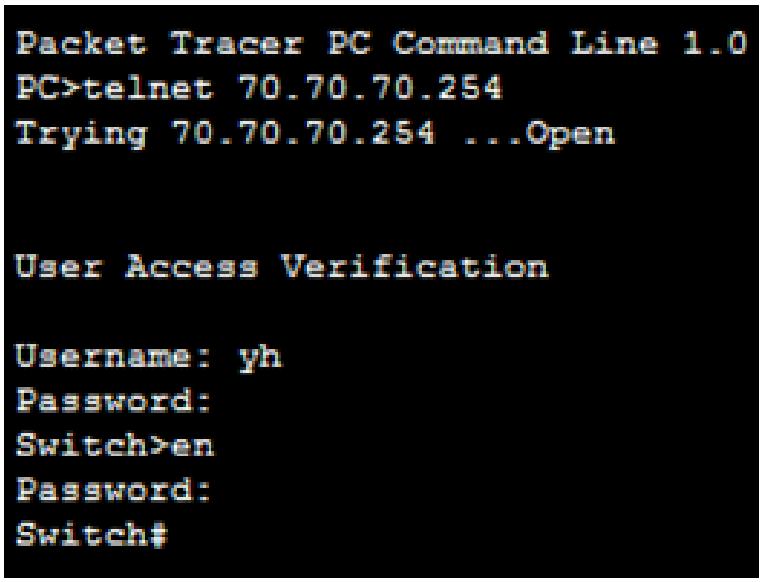


Figure 2 Office area test chart

Test results: as shown in Figure 2. It can be seen that the PC2 in the office area has successfully accessed the aggregation router in the production area and the 3A authentication is enabled and effective. This indicates that the connectivity between the PCs in the office area and the local area is normal, and the 3A authentication configuration is successful.

### 4.2 Branch Access Zone Connection Test

This part tests the connectivity between the branch access area and the Bank's production area. The purpose is for business needs. Some devices in the two regions require data exchange, and the two regional network devices can access each other. In the experimental test, the branch server 1 and the branch server 2 of the branch can ping the PC1 of the branch production area and the PC1 of the office area respectively, which proves that the data communication between the two departments is normal. The test results are shown in Figure 3.

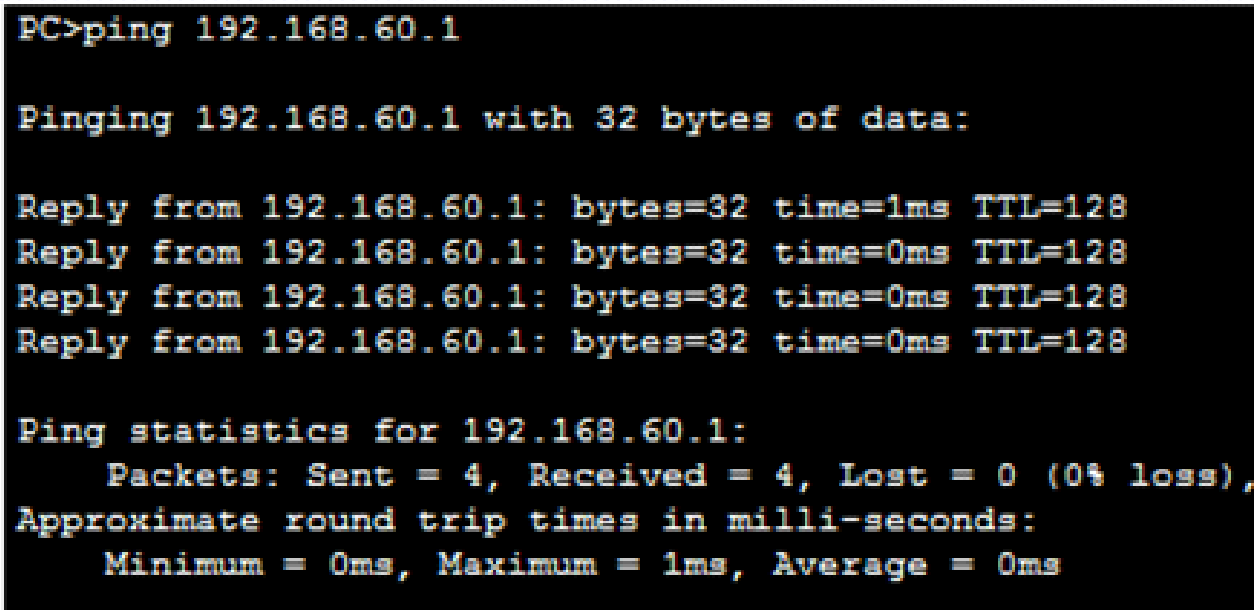


Figure 3 Branch access zone PC2 test chart

As shown in the test results in Figure 3, the branch access area and the office area implement network interworking. Combine the test content of all the above diagrams to open, ACL configuration. OSPF configuration, VLAN division, and trunking are effective. This design implements the entire network interworking and configuration takes effect. The result reflects that the overall communication of the bank network is normal, and this solution can be initially

determined to be used in real life.

## 5. Conclusion

This article is aimed at the simplified design of some small and medium-sized banks in China. In the real situation, the network will be more complicated. This design is a reference to some of the topographical maps of bank planning on the Internet, as well as the matching of certain departments of the bank, as well as the role of various parts and the allocation of network resources. In the future development, bank network security issues will become more important, with the continuous updating of technology and the superior performance of the equipment will make the banking network diversified. Because the development of technology will make future vicious attacks more and more diverse, it is essential to design a feasible, reliable, and manageable solution.

## Acknowledgements

This research was supported by Doctor Initial Funding of Hubei University of Science and Technology (No. 2016-19XB003 and KY12050 and 2016-XZ-016), the Scientific Research Project of Education Department of Hubei Province under Grant B2018179 and B2017181 and B2018175, the National Natural Science Foundation of China (No.51479155).

## References

[1] Malati H., Pavan K., Vasudev K.R., et al. Experiences with a centralized scheduling approach for performance management of IEEE 802.11 wireless LANs, IEEE/ACM Transactions on Networking, 2013, 21(2):648-662.

[2] Zhao J., Qiao C.M., Raghuram S.S., et al. Improve efficiency and reliability in single-hop WSNs with transmit-only nodes, IEEE Transactions on Parallel and Distributed Systems, 2013, 24(3):520-534.

[3] Lei L. J., Zhou X., Chen L., et al. Modelling and analysing medium access delay for differentiated services in IEEE 802.11s wireless mesh networks, IET Networks, 2012, 1(2):91-99.

[4] Chen L., Leneutre J. A game theoretic frame-work of distributed power and rate control in IEEE 802.11 WLANs, IEEE Journal on Selected Areas in Communications, 2008, 26(7): 1128-1237.

[5] Hyoil K., Kang G. Admission and eviction control of cognitive radio users at Wi-Fi 2.0 hotspots, IEEE Transactions on Mobile Computing, 2012,11(11):1666-1677.