ISSN: 2664-9640

Enterprise Network Design and Deployment Practice based on eNSP

Huangkun Chen, Liangxu Sun*

University of Science and Technology Liaoning, Anshan 114051, China

*Corresponding Author

Abstract

In recent years, with the frequent occurrence of network security incidents, the importance of enterprise network security has become increasingly prominent. The design of enterprise networks should not only meet the requirements of efficient communication, but also prioritize security to ensure the stable operation of the network. This article constructs a large-scale corporate park network, including the DMZ area and connected to the backbone network through dedicated lines. At the same time, with offices, it is necessary to achieve interconnectivity between the two networks. Based on dynamic routing protocol, IPSecVPN, VRRP and other technologies, combined with Huawei network equipment, the company has built a secure and efficient enterprise network architecture. The design content covers wireless network coverage, IPv6 support, traffic optimization, and redundant path selection to ensure stable communication between the company's campus network, offices, and the Internet, ultimately achieving a balance between security, flexibility, and reliability.

Keywords

IPSecVPN; eNSP; Wireless Network; Security.

1. Introduction

With the rapid development of internet technology, enterprise networks play a crucial role in modern construction[1]. An enterprise network must not only meet the daily business needs but also ensure high security, efficiency, and stability. In recent years, frequent network security incidents have highlighted the urgency of protecting user data and corporate information[2]. A secure and reliable network environment has become the foundation for the sustainable development of enterprises[3,4]. To promote the development of domestic network technologies, many companies are gradually moving away from reliance on foreign technologies such as Cisco and are instead adopting self-developed network solutions to enhance domestic technological capabilities and autonomy[5].

As network technology continues to evolve, emerging technologies such as SDN (Software-Defined Networking) and SR (Segment Routing) provide opportunities for digital transformation in enterprises[6]. Network technology not only supports internal business and data management but also drives innovation by optimizing processes and improving efficiency[7,8]. During the pandemic, the widespread adoption of remote work and online education further proved the importance of network high availability and reliability. By adopting advanced network technologies to build enterprise networks, businesses not only ensure daily operations and customer privacy but also provide a solid foundation for future business expansion and diversified development[9].

To ensure the stable, secure, and efficient operation of enterprise networks, support from multiple core technologies is essential. Key technologies include VLAN (Virtual Local Area Network), OSPFv2 (Open Shortest Path First version 2), DHCP (Dynamic Host Configuration

ISSN: 2664-9640

Protocol), ACL (Access Control List), and NAT (Network Address Translation)[10]. VLAN technology logically divides the network to enhance its security and management efficiency; the OSPFv2 protocol ensures efficient transmission of data packets through dynamic routing management; the DHCP protocol simplifies device access and network management; and ACL and NAT technologies ensure network security by preventing external threats to the internal network.

For network design and optimization, this project utilizes the Huawei eNSP (Enterprise Network Simulation Platform) simulation environment. The eNSP platform supports large-scale network simulation, enabling the modeling and testing of various configurations and performances of enterprise networks. Combined with debugging tools like Wireshark, the efficiency of network debugging and optimization can be improved, ensuring the feasibility and stability of the technical solutions. By integrating these technologies and simulation environments, enterprises can achieve efficient network management while ensuring network security, driving digital transformation, and fostering business innovation.

2. Enterprise Network Function Design

2.1. Overall Topology Design

The enterprise network topology consists of the corporate campus network, DMZ area, backbone network, and office area, with each area working together to achieve multiple core functions. The corporate campus network provides comprehensive wireless coverage, data communication between devices, and the ability to access the internet and servers, supporting efficient office operations. The DMZ area is used to implement the interconnection between the corporate campus network and external networks, while also providing important data storage and external access services to enhance network security. The backbone network connects different corporate campuses and external networks, using the OSPF/OSPFv3 protocol to achieve efficient routing and ensure communication between the corporate campus network and DMZ area. The office area is securely connected to the headquarters network via an IPSecVPN tunnel, providing employees with convenient and low-cost remote access services. The overall network design integrates multiple functions, including VLAN, VRRP, ACL, BFD, and QoS, to ensure the security, reliability, and efficiency of data transmission.

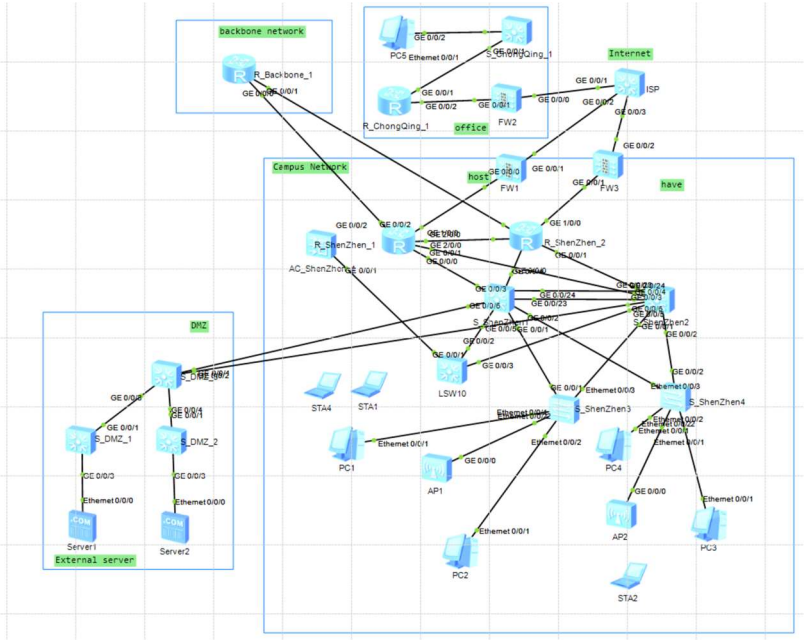

Figure 1. Overall Topology of the Enterprise Network.

ISSN: 2664-9640

2.2. Corporate Campus Network Design

The corporate campus network mainly implements the following thirteen functions: VLAN partitioning, wireless network, BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), route redistribution, VRRP (Virtual Router Redundancy Protocol), BFD (Bidirectional Forwarding Detection), port aggregation, ACL (Access Control List), prefix lists, OSPFv3 (Open Shortest Path First for IPv6), QoS (Quality of Service), and IPSecVPN.

VLAN: The interfaces connecting S_ShenZhen1, S_ShenZhen2, S_ShenZhen3, and S_ShenZhen4 are configured in trunk mode to facilitate the forwarding of traffic between different VLANs. The interfaces of the connected router are also configured in trunk mode for routing purposes. The interfaces connected to client machines are configured in access mode to facilitate external network access for the clients.

Wireless Network: On AC_ShenZhen_1, configure wireless network parameters such as SSID, wireless radio frequencies, VAP templates, etc. It also acts as a DHCP server to allocate addresses and gateways for the APs and clients to enable network communication.

BGP: BGP protocol is configured on R_ShenZhen_1 and R_ShenZhen_2 to facilitate route selection when connecting the corporate campus network and backbone network, ensuring the optimal path.

OSPF: OSPF protocol is configured on R_ShenZhen_1, R_ShenZhen_2, S_ShenZhen_1, and S_ShenZhen_2 to ensure internal communication within the corporate campus network and between the corporate campus network and DMZ.

Route Redistribution: Bidirectional route redistribution is configured between R_ShenZhen_1 and R_ShenZhen_2 to enable communication between the corporate campus network and the backbone network.

VRRP: VRRP is configured on S_ShenZhen_1 and S_ShenZhen_2 to prevent single points of failure. Once VRRP is configured, even if one of these switches goes down, business operations will continue without disruption.

BFD: BFD is configured between R_ShenZhen_1 and R_ShenZhen_2 for link detection, acting as a backup mechanism. BFD allows for millisecond-level failover, ensuring that if one device fails, the switch happens quickly without affecting business operations.

Port Aggregation: Port aggregation is configured between S_ShenZhen_1 and S_ShenZhen_2 to increase bandwidth and maintain data flow in case of a physical interface failure. This ensures the stability of the entire enterprise network.

ACL: ACL is configured on the boundary firewall of the corporate campus network to allow internal traffic to access the external network and branch office while ensuring security and not disrupting business operations.

Prefix Lists: Prefix lists are used for controlling route redistribution between R_ShenZhen_1 and R_ShenZhen_2. For example, traffic destined for the backbone network 10.3.3.0/24 will use the link between R_ShenZhen_1 and R_Backbone_1, and traffic destined for 10.3.4.0/24 will use the link between R_ShenZhen_2 and R_Backbone_1. BGP MED attributes are used to influence BGP path selection, controlling how R_ShenZhen_1 and R_ShenZhen_2 affect the BGP route selection on R_Backbone_1.

OSPFv3: To prepare for the arrival of IPv6, the corporate campus network and DMZ are first deployed with IPv6 for testing and research purposes, without connecting to the Internet. OSPFv3 is configured on the core switches in the corporate campus network and network devices in the DMZ to ensure network communication.

QoS: To prevent Internet traffic, such as video or FTP, from affecting business-critical applications, QoS is deployed on the Internet link. This prioritizes critical applications, ensuring that HTTP traffic has a bandwidth guarantee of 1M and IPSecVPN traffic has a guarantee of

ISSN: 2664-9640

512K. This is achieved through traffic management configured using MQC on the two boundary routers, R_ShenZhen_1 and R_ShenZhen_2.

IPSecVPN: Branch offices need to connect to the DMZ for resource access. Due to the high initial setup and usage costs of dedicated lines, Site-to-Site IPSecVPN is used as the solution. The VPN endpoints need to have fixed public IPs, which incur some cost, but the advantage is that both sides can actively establish the IPSecVPN connection. To simplify deployment, IPSecVPN is configured on FW1 and FW2. The VPN traffic of interest is between the branch office network 10.4.0.0/16 and the DMZ network 10.2.0.0/16.

2.3. DMZ Area Design

This area mainly implements the following four functions: VLAN, OSPF (Open Shortest Path First), OSPFv3 (Open Shortest Path First for IPv6), and DHCP (Dynamic Host Configuration Protocol).

VLAN: The interfaces between S_DMZ_3, S_DMZ_2, and S_DMZ_1 are configured in trunk mode to allow traffic between different VLANs, providing DHCP services to the corporate campus network.

OSPF: OSPF protocol runs between S_DMZ_1, S_DMZ_2, and S_DMZ_3 to ensure communication within the DMZ. Additionally, S_DMZ_3 ensures OSPF communication with the corporate campus network.

OSPFv3: OSPFv3 protocol is implemented in the DMZ to prepare the enterprise for IPv6 and support research into IPv6 applications in the enterprise network.

DHCP: S_DMZ_1 is configured as a DHCP server to provide DHCP services to hosts in the corporate campus network.

2.4. Backbone Network Design

This area mainly implements the following four functions: VLAN, OSPF (Open Shortest Path First), OSPFv3 (Open Shortest Path First for IPv6), and DHCP (Dynamic Host Configuration Protocol).

VLAN: The interfaces between S_DMZ_3, S_DMZ_2, and S_DMZ_1 are configured in trunk mode to allow traffic between different VLANs, providing DHCP services to the corporate campus network.

OSPF: OSPF protocol runs between S_DMZ_1, S_DMZ_2, and S_DMZ_3 to ensure communication within the DMZ and ensure OSPF communication with the corporate campus network through S_DMZ_3.

OSPFv3: OSPFv3 protocol is implemented in the DMZ to prepare the enterprise for IPv6 and support research into IPv6 applications in the enterprise network.

DHCP: S_DMZ_1 is configured as a DHCP server to provide DHCP services to hosts in the corporate campus network.

2.5. Office Design

The branch office mainly implements the following functions: VLAN and IPSecVPN.

VLAN is configured on S_ChongQing_1, with the appropriate gateway for PC5. Additionally, IPSecVPN is configured on FW2 to establish a connection with the corporate campus network's FW1. This allows the branch office to access the DMZ area over the public Internet.

3. Enterprise Network Function Implementation

3.1. Equipment Selection

The overall network construction equipment shown in Table 1 is all Huawei brand, including layer 2 switches, layer 3 switches, routers, firewalls, AC, AP and other models, with varying

ISSN: 2664-9640

quantities and all produced in China. Huawei is a leading technology enterprise in China, with a profound foundation and strong research and development capabilities. Its products provide reliable and advanced technical support for network construction.

Table 1. Overall Equipment

Equipment Name	Brand	Model	Quantity	Origin
Layer 2 Switch	Huawei	S3700	2	China
Layer 3 Switch	Huawei	S5700	7	China
Router	Huawei	AR3206	4	China
Firewall	Huawei	USG5500	3	China
AC	Huawei	AC6605	1	China
AP	Huawei	AP8030DN	2	China

3.2. Equipment Configuration Implementation

3.2.1. Branch Access to Headquarters (IPSecVPN)

To ensure secure communication between the branch network and headquarters, IPSecVPN tunneling technology is used. First, security proposals need to be configured and related encryption algorithms and authentication mechanisms defined. Then, peer configurations are set to ensure secure data transmission, and security policies are applied under the interface.

Key Commands:

ACL Configuration: Used to define which traffic is allowed to pass through the firewall.

acl number 3000

rule 5 permit ip source 10.2.3.0 0.0.0.255 destination 10.4.10.0 0.0.0.255

IKE Proposal Configuration: Defines the encryption algorithm, key exchange method, and other security protocols.

ike proposal 1

dh group2

integrity-algorithm aes-xcbc-96

IPSecProposal Configuration: Defines the ESP (Encapsulating Security Payload) encryption and authentication algorithms.

IPSecproposal test

esp authentication-algorithm sha1

esp encryption-algorithm aes

Apply Security Policy on Interface: Assign a security policy to the interface to ensure traffic complies with the defined security standards.

interface GigabitEthernet0/0/1

ip address 202.96.3.2 255.255.255.0

IPSecpolicy map

3.2.2. Interconnection of Backbone Network and Corporate Campus Network (BGP and OSPF Redistribution)

To achieve interconnection between the backbone network and the corporate campus network, BGP routing protocol is configured, and the redistribution of OSPF and BGP is implemented to avoid routing loops and ensure stable route selection.

Key Commands:

BGP Configuration: Configure the BGP routing protocol, define neighbor relationships, and add the local network to the BGP routing table.

ISSN: 2664-9640

```
bgp 65200
  router-id 3.3.3.3
  peer 172.16.1.1 as-number 65100
  network 10.3.3.0 255.255.255.0
  peer 172.16.1.1 enable
```

OSPF and BGP Redistribution Configuration: Control the exchange of routing information between BGP and OSPF via routing policies to avoid loops.

```
import-route ospf 1 route-policy O2B
import-route bgp route-policy B2O
```

Route Optimization (BGP Route Priority Adjustment)

When networking, especially in an environment with BGP and OSPF redistribution, it is important to ensure data flows through the desired path. By adjusting BGP's route priority (e.g., Local Preference) and route cost (e.g., MED), as well as configuring routing policies, the routing path can be optimized.

Key Commands:

Local Preference Adjustment: Increase the priority of specific routes to ensure they are the preferred routes.

```
route-policy 3 permit node 10
if-match ip-prefix 3
apply local-preference 1000
```

MED (Multi-Exit Discriminator) Adjustment: Control the priority of exit points for routing.

```
route-policy MED permit node 10
if-match ip-prefix 101
apply cost 100
```

3.2.3. Wireless Network Configuration

When deploying a wireless network within the corporate campus network, configure WLAN security settings, create SSID (Service Set Identifier), and configure the VAP (Virtual Access Point) template to support wireless client connections.

Key Commands:

Wireless Network Security Configuration: Define WPA2-PSK security protocol and password to ensure the security of the wireless network.

```
security-profile name wlan-net
security wpa-wpa2 psk pass-phrase 123456789 aes
```

SSID and VAP Configuration: Create SSID and assign VLAN to ensure wireless coverage in different areas.

```
ssid wlan-net
vap-profile name wlan-net
service-vlan vlan-id 200
```

AP (Access Point) Configuration: Configure multiple access points and associate them with the corresponding wireless network group.

```
ap-group name ap-group1
ap-id 0 type-id 40 ap-mac 00e0-fc5e-4f50 ap-sn 210235448310C715B530
```

3.2.4. Corporate Campus Network Interconnection Configuration (OSPF Configuration)

Configure the OSPF protocol between corporate campus network devices to achieve efficient internal routing and add security by configuring OSPF authentication.

ISSN: 2664-9640

Key Commands:

OSPF Configuration: Enable OSPF protocol on routers and declare the related networks.

ospf 1 router-id 1.1.1.1

network 10.1.51.2 0.0.0.0

OSPF Authentication: Set an authentication mechanism for OSPF links to ensure the security of routing information.

ospf authentication-mode md5 1 cipher 123456

3.2.5. DHCP Configuration

Configure DHCP service pools and assign IP addresses for different VLANs. Also, configure DHCP relay to forward DHCP requests to the central DHCP server.

Key Commands:

DHCP Pool Configuration: Configure IP pools for different VLANs and set gateway, DNS, etc.

ip pool vlan01

gateway-list 10.1.1.254

network 10.1.1.0 mask 255.255.255.0

dns-list 10.2.100.100

DHCP Relay Configuration: Configure VLAN interface to forward DHCP requests.

interface Vlanif1

dhcp relay server-ip 10.2.1.2

3.2.6. Traffic Control Configuration (QoS)

Use QoS to classify and control network traffic, ensuring priority for critical business traffic. For example, configure bandwidth control policies for IPSecVPN and HTTP traffic.

Key Commands:

ACL Traffic Classification: Create ACL rules and apply them to traffic classification.

acl number 3200

rule 1 permit tcp source-port eq www

Traffic Behavior Configuration: Define bandwidth control policies for traffic, such as setting a 512kbps traffic limit for IPSectraffic.

traffic behavior ipsecvpn

car cir 512 cbs 96256 pbs 160256 green pass yellow pass red discard

3.2.7. Link Detection Configuration (NQA and BFD)

To ensure the stability of the link, configure link detection mechanisms (such as ICMP probing and BFD sessions) to monitor the network link health in real-time.

Key Commands:

NQA Configuration: Use ICMP probes to detect link status.

nqa test-instance admin icmp

test-type icmp

destination-address ipv4 202.96.1.1

BFD Configuration: Use BFD sessions to achieve fast link failover.

bfd 1 bind peer-ip 10.1.55.2 source-ip 10.1.55.1 auto

3.2.8. Corporate Campus Network Redundancy Configuration (VRRP and BFD Integration)

Configure VRRP (Virtual Router Redundancy Protocol) and integrate it with BFD technology to achieve fast link switching and ensure high availability for the corporate campus network.

ISSN: 2664-9640

Key Commands:

VRRP Configuration: Set the VRRP virtual IP address, priority, and preempt mode to ensure the high availability of redundant routing.

vrrp vrid 1 virtual-ip 10.1.1.254

vrrp vrid 1 priority 120

vrrp vrid 1 preempt-mode timer delay 5

4. Enterprise Network Testing

To ensure the stability and reliability of the entire enterprise network, comprehensive testing of the connectivity between the corporate campus network, external network, backbone network, and DMZ area was conducted. The results are as follows:

4.1. Network Connectivity Testing

The connectivity testing between the corporate campus network and the external network, backbone network, and DMZ area shows that the network configuration and device operation are stable and meet the design requirements. As an example, one of the connectivity tests is shown in Figure 2.

Corporate campus Network and External Network Connectivity Test:

The test results indicate that the corporate campus network can establish normal two-way communication with the external network, showing that the corporate campus network's exit configuration is correct, and the network devices are operating stably, effectively supporting external access needs.

Corporate campus Network and Backbone Network Connectivity Test:

Communication between the corporate campus network and backbone network is smooth and uninterrupted. The test results show that the routers and related configurations have been correctly set, and the data forwarding performance of each node is good. As the core of the enterprise network, the efficient connectivity of the backbone network ensures stable communication between the data center, branch offices, and the external network.

Corporate campus Network and DMZ Area Connectivity Test:

Communication between the corporate campus network and DMZ area is completely normal. The test shows that the firewall rules, routing policies, and ACL configurations in the DMZ area are accurate, and data exchange meets design requirements, ensuring the secure operation of the enterprise network.

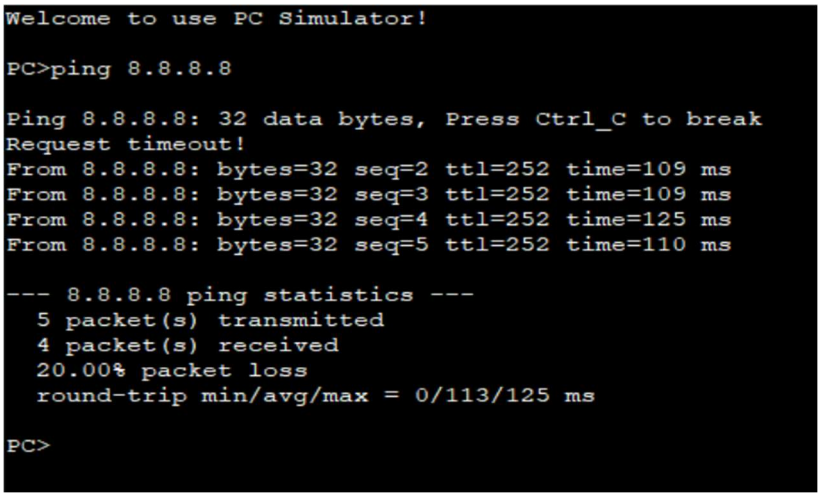

Figure 2. Ping Test from Corporate Campus Network to External Network

ISSN: 2664-9640

4.2. Corporate Campus Network Redundancy Testing

As shown in Figure 3, the corporate campus network redundancy feature has been successfully implemented. Through the redundancy configuration, the corporate campus network can automatically switch in the event of device or link failure, ensuring the continuity and high availability of network services.

The redundancy design includes backups for key network devices and links. During the test, single-point failure scenarios were simulated, and the system was able to quickly switch to the backup path when a device or link failed, ensuring that network communication was not interrupted. Specifically, the corporate campus network achieves automatic switching of redundant routes and links using VRRP (Virtual Router Redundancy Protocol) and link aggregation technologies.

The test results show that the redundancy mechanism operates stably and can achieve millisecond-level recovery in the event of a failure, minimizing the risk of business disruption. This redundancy design provides strong support for the high availability and business continuity of the enterprise network.

```
<S_ShenZhen_1>display vrrp brief
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Master       Vlanif1                  Normal   10.1.1.254
1     Master       Vlanif2                  Normal   10.1.2.254
1     Backup       Vlanif3                  Normal   10.1.3.254
1     Backup       Vlanif4                  Normal   10.1.4.254
1     Master       Vlanif100                Normal   10.1.100.254
1     Backup       Vlanif200                Normal   10.1.200.254
------------------------------------------------------------------
Total:6     Master:3     Backup:3     Non-active:0
<S_ShenZhen_1>
```

Figure 3. Corporate Campus Network Redundancy Test

4.3. Corporate Campus Network Wireless Signal Coverage

The wireless network signal coverage test results of the corporate campus network are shown in Figure 4. From the figure, it is visually evident that the entire corporate campus network has achieved comprehensive coverage, with no significant signal dead zones, and can meet the wireless connectivity needs in all areas of the corporate campus.

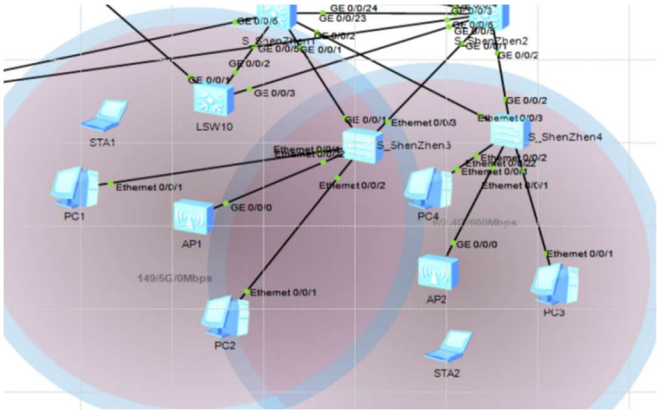

Figure 4. Corporate Campus Network Wireless Signal Coverage

Through various tests, it can be confirmed that the connectivity between the different modules of the entire enterprise network is good, laying a solid foundation for the normal operation of the enterprise network. These tests also verify the rationality of the network architecture

ISSN: 2664-9640

design and the effectiveness of its implementation. In the future, network performance and security will continue to be optimized to further improve the network's reliability and risk resistance.

5. Conclusion

In the current environment of frequent network security incidents, the importance of enterprise network security is increasingly prominent. It not only needs to meet the needs of efficient communication, but also ensure the stable operation of business. To achieve this goal, a network architecture that meets the company's needs has been designed, including the overall planning of the company's campus network, backbone network, DMZ area, and offices. Network design focuses on security and reliability, taking into account the convenience of employees' work and data security. By combining core technologies such as VLAN, OSPFv2, DHCP, ACL, NAT, etc., it ensures the efficient operation and security of the network.

By dividing VLANs, isolation between devices and data traffic has been achieved, improving network security and management convenience; The OSPFv2 protocol is used for dynamic routing to ensure efficient routing of data packets; DHCP automatically assigns IP addresses, simplifying management; ACL technology is used to filter unnecessary data streams, further enhancing security; NAT technology solves the problem of insufficient IP addresses and enhances network security protection. Through careful planning and design, an efficient, stable, and secure network architecture has been constructed to meet the company's interconnection needs between different regions while ensuring optimal network performance.

In terms of network planning, emphasis was placed on feasibility analysis at the technical, economic, and social levels, confirming the feasibility of the project and verifying the rationality of the network architecture design through simulation using the Huawei eNSP platform. Through device selection and configuration optimization, combined with measures such as traffic control, link detection, and wireless network coverage, good connectivity between regions has been ensured, laying a solid foundation for the normal operation of enterprise networks. At the same time, redundant deployment and fault recovery schemes have been optimized, improving the network's fault tolerance and emergency response capabilities.

The entire design scheme demonstrates advantages in security, stability, and performance, providing an efficient, reliable, and secure network infrastructure for enterprise digital transformation, ensuring the smooth operation of the company's business, and providing solid support for future network optimization and expansion.

Acknowledgments

The authors gratefully acknowledge the financial support from college student innovation and entrepreneurship project of University of Science and Technology Liaoning in 2025.

References

[1] Zhang Pei, Liu Wuteng. Design of ACL Configuration Simulation Experiment Based on eNSP[J]. Integrated Circuit Applications, 2024, 41(07): 20-21. DOI: 10.19339/j.issn.1674-2583.2024.07.008.

[2] Zhang Lin, Zeng Yan. Design and Implementation of IPv6 over IPv4 Tunnel Experiment Based on eNSP Simulation Platform[J]. Computer Programming Skills & Maintenance, 2024, (03): 34-36. DOI: 10.16184/j.cnki.comprg.2024.03.035.

[3] Wang Ge. Typical Applications and Implementations of Access Control Lists Based on ENSP[J]. Information Recording Materials, 2023, 24(09): 142-145. DOI: 10.16009/j.cnki.cn13-1295/tq.2023.09.026.

ISSN: 2664-9640

[4] Ren Hongxia, Lin Xiwen, Liu Xuefeng, et al. Design and Implementation of VLAN and OSPF Comprehensive Experiment Based on eNSP[J]. Computer Programming Skills & Maintenance, 2023, (05):167-169.DOI:10.16184/j.cnki.comprg.2023.05.031.

[5] Chen Zhanchi, Wang Xiaopin. Design and Simulation of End-to-End IPSec VPN Experiment Based on eNSP[J]. Modern Information Technology, 2022, 6(24): 69-71. DOI: 10.19850/j.cnki.2096-4706. 2022.24.017.

[6] Liu Zejun, Liu Ying, Li Zhuohang, et al. Design and Implementation of Network Topology Structure for Small and Medium-sized Enterprises[J]. Software, 2022, 43(02): 30-37+48.

[7] Wang Hao, Zhang Shaofang, Liu Yanfeng. Design and Simulation of Typical ACL Experiments Based on eNSP[J]. Computer Programming Skills & Maintenance,2024,(02):117-120.DOI:10.16184/ j.cnki. comprg.2024.02.028.

[8] Meng Xiangcheng. Design and Simulation of Enterprise Campus Network Based on Virtual Three-Layer Architecture[J]. Scientific and Technological Innovation, 2022, (22): 67-71.

[9] Xing Huifen, Che Hui. Design and Implementation of Network Security Access Control Based on ACL and Firewall[J]. Journal of Qujing Normal University, 2022, 41(03): 67-74.

[10] Guo Wenpu, Chen Tianhao, Yang Bailong. Design of Networking Experiment for Small and Medium-sized Enterprises Based on eNSP[J]. Laboratory Research and Exploration, 2022, 41(02): 125-129+296. DOI: 10.19927/j.cnki.syyt.2022.02.027.