Journal of Computer Science and Electrical Engineering
Print ISSN: 2663-1938
Online ISSN: 2663-1946
DOI: https://doi.org/10.61784/jcsee3093

NETWORK DESIGN OF INTELLIGENT SCIENTIFIC RESEARCH PARK BASED ON MULTI-ROUTING PROTOCOLS AND SECURITY AUTHENTICATION

YanZhuo Wu, LiangXu Sun*
School of Computer Science and Software Engineering, University of Science and Technology Liaoning, Anshan 114051, Liaoning, China.
Corresponding Author: LiangXu Sun, Email: sunliangxumail@163.com

Abstract: In response to the core demands of multi-regional collaboration, high security requirements and efficient data transmission in intelligent scientific research parks, this paper proposes a park network design scheme integrating multi-protocol technology. First, through demand analysis, the functional positioning and network characteristics of the main scientific research park, service area, support area and monitoring area are clarified. Then, the topology architecture design, equipment selection and IP address planning are completed - frame relay is adopted to achieve cross-regional interconnection, and combined with static and dynamic IP allocation mechanisms, VLAN division is deployed to achieve traffic isolation. And introduce EIGRP, OSPF, RIP multi-dynamic routing protocols and CHAP, PAP authentication mechanisms to ensure network performance and security. Through equipment configuration and protocol debugging, seamless communication among various regions, dynamic address allocation and access security control have been achieved, solving the problems of multi-region network collaboration and compatibility with heterogeneous protocols. The test results show that this network architecture has good stability, scalability and security, and can meet the operational requirements of multiple business scenarios in scientific research parks, providing technical references for the network construction of similar parks.
Keywords: Intelligent scientific research park; Network topology design; Dynamic routing protocol; Frame relay; Network security authentication

1 INTRODUCTION

With the in-depth development of digital scientific research, intelligent scientific research parks, as the core carrier of innovative research and development, need to support diversified services such as core experimental data transmission, cross-department collaborative office, full-region monitoring and early warning, and data backup guarantee[1-2]. Compared with traditional park networks, scientific research park networks have the following core demands: First, multi-area logical isolation and efficient interconnection coexist, which requires business isolation and data intercommunication in functional areas such as scientific research main parks and service areas; second, high security and Reliability, the confidentiality of scientific research data requires access to authentication and traffic protection mechanisms; third, dynamic adaptability, which requires flexible adjustments to cope with the increase and decrease of terminal equipment and topology changes.

At present, some scientific research park networks have problems such as rigid architecture, single protocols, and insufficient security protection: static routing configuration is difficult to adapt to the needs of equipment expansion, lack of unified VLAN management leads to the risk of broadcast storms, and cross-regional interconnection has poor stability, which cannot meet the high requirements of scientific research services[3]. Time-effectiveness and high security requirements[4-5]. Therefore, designing a network architecture that integrates multi-protocol technologies and adapts to scientific research scenarios is of great practical significance for improving scientific research efficiency and ensuring data security[6-8].

This paper focuses on the full-process design and implementation of the intelligent scientific research park network. The core research contents include: 1) Dismantling of multi-area requirements and clarifying the network functions and performance indicators of the main park, service area, support area and monitoring area; 2) Topology architecture and equipment selection, using Frame Relay to build wide area network interconnection, and using hierarchical switches and multiple routers to achieve area coverage; 3) Protocol deployment and security configuration, integrating VLAN partitioning, dynamic routing (EIGRP/OSPF/RIP), DHCP and CHA/PAP authentication technologies; 4) Device debugging and protocol compatibility optimization to solve the problem of heterogeneous protocol adaptation in route republication.

2 SYSTEM DESIGN

2.1 Analysis of Network Requirements of Intelligent Scientific Research Parks

2.1.1 Scientific research main park

The scientific research park network adopts appropriate authentication mechanisms to ensure access security. VTP is used to realize unified management and synchronization of VLAN information to simplify planning. VLANs are reasonably divided according to services and departments to optimize performance and security. EIGRP dynamic routing protocol is deployed to achieve internal and external networks. Interworking, using DHCP to dynamically allocate IP addresses and set up address pools based on VLANs to facilitate network management (See Figure 1).

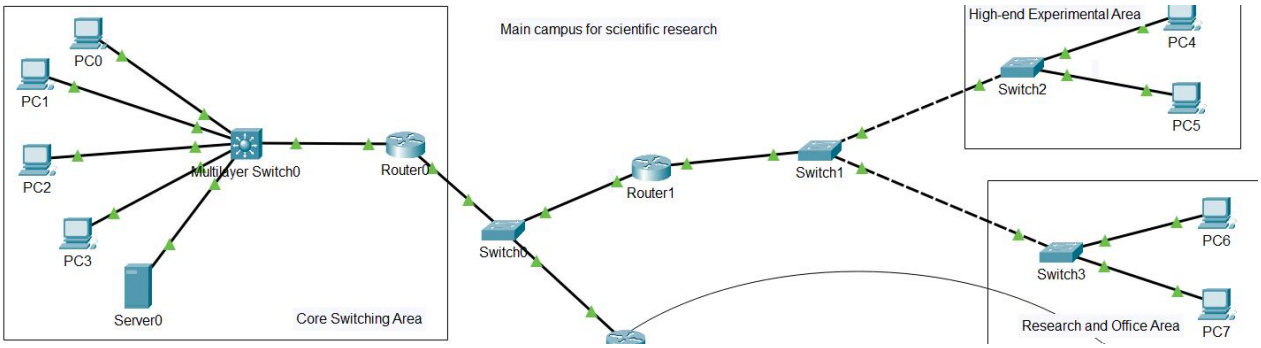

Figure 1 Map of the Main Scientific Research Park

2.1.2 Scientific research service area

The scientific research service area is configured with multiple VLANs as needed, and efficient communication and address translation between different VLANs are achieved through routing subinterfaces. In terms of access authentication, CMM authentication is used to authenticate access devices in a more secure way, effectively preventing illegal access. By carefully deploying the EIGRP routing protocol, routing information can be dynamically exchanged within the service area and with other areas to ensure accurate routing and rapid transmission of data. At the same time, it is supplemented by security policies and traffic management methods to create a stable, secure and high-performance network service environment for scientific research business. The scientific research service area map is shown in Figure 2.

2.1.3 Scientific research security area

The scientific research support area is divided into multiple VLANs based on functions to achieve logical isolation of equipment and traffic. By configuring routing subinterfaces, communication problems between different VLANs are cleverly solved. At the same time, the OSPF dynamic routing protocol is deployed to enable real-time interaction of routing information within and with external networks within the safeguard area to ensure accurate and rapid data transmission. Combined with security strategies, we will build a stable, secure and efficient network security environment for scientific research work. The scientific research support area is shown in Figure 3.

2.1.4 Scientific research monitoring area

The scientific research monitoring area adopts PAP certification to verify the identity of access devices to ensure the safety and reliability of network access. By deploying the RIP dynamic routing protocol, routing information can be automatically exchanged within and with external networks, allowing accurate routing and efficient transmission of data packets. At the same time, combined with reasonable network planning and configuration, it provides a stable and orderly network environment for scientific research monitoring services and ensures real-time and accurate transmission of monitoring data. The scientific research monitoring area map is shown in Figure 4.

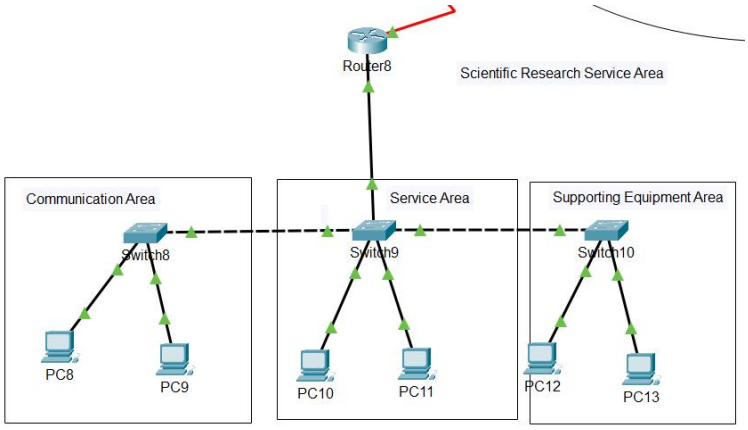

Figure 2 Scientific Research Service Area Map

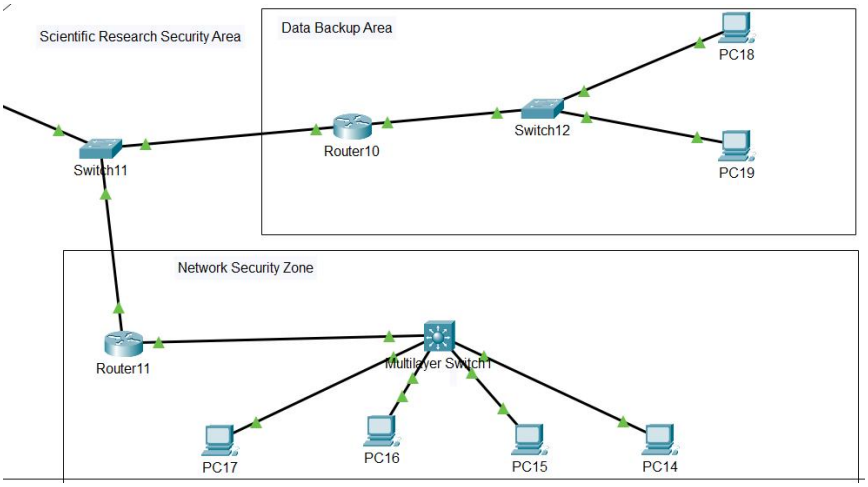

Figure 3 Scientific Research Security Area

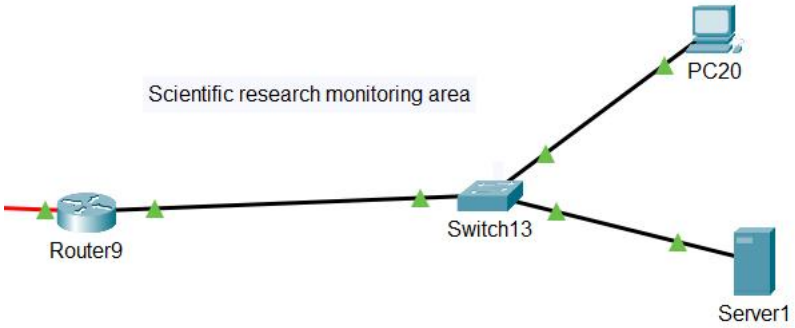

Figure 4 Scientific research monitoring area map

2.2 Network Topology Design

2.2.1 Topology design

The network topology covers multiple areas such as the main scientific research park, high-end experimental area, and scientific research office area. Each area is interconnected through switches and routers, and divided into multiple VLANs to achieve traffic isolation. Authentication such as CHA and PAP are used to ensure access security, and dynamic routing protocols such as EIGRP, RIP, and OSPF are deployed to achieve routing interactions to ensure efficient data transmission. At the same time, security and traffic management policies are equipped to provide a stable network environment for scientific research activities. The general plan of the smart scientific research park is shown in Figure 5.

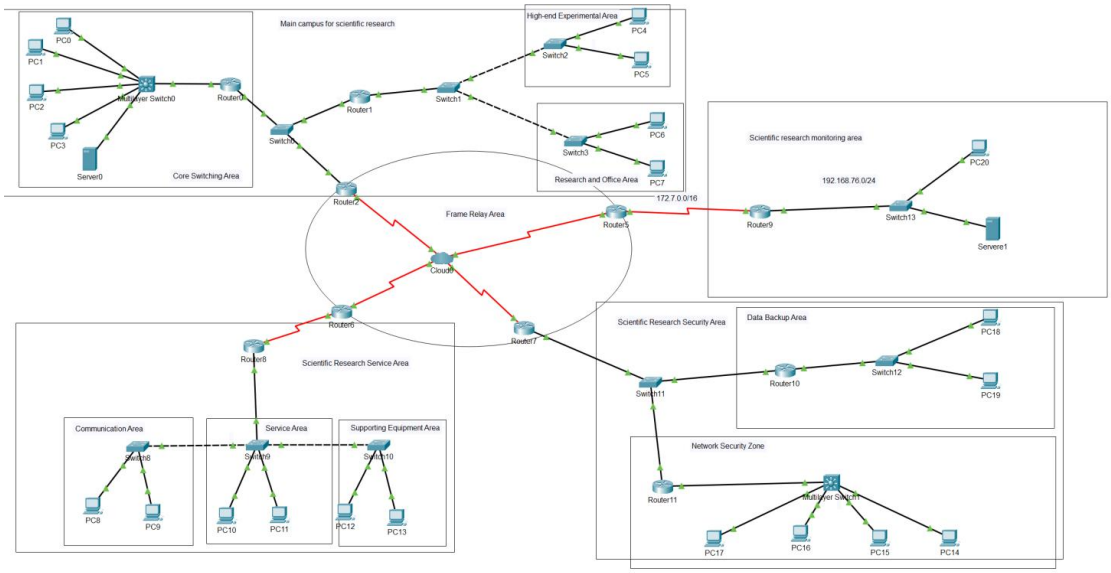

Figure 5 General Layout of Smart Scientific Research Park

2.2.2 Device selection

Routers: 6 Router-PT (including routing and port IP functions, some may be used for serial connection, etc.), 4 2911 routers (providing routing and port IP)
Switches: 13 2960 - 24TT switches (used to divide VLANs, etc.), 2 3560 switches (divided into VLANs to provide routing)
Cloud equipment: Cloud-PT 1 unit (frame relay is provided)
Servers: 2 Server-PT (providing services, 1 each in the scientific research service park and 1 in the scientific research monitoring area)
Terminal equipment: 21 PC-PT units (the total number of terminal equipment in each region, distributed in multiple areas such as the main scientific research park and high-end experimental area)

3 SYSTEM CODING IMPLEMENTATION

3.1 Scientific Research Main Park

3.1.1 VLAN partitioning and virtual interfaces

The core switching area is divided into VLAN62 and VLAN63, the switch f0/1-2 interface is divided into VLAN62, and the f0/3-4 interface is divided into VLAN63, and the access control list is configured to achieve broadcast domain isolation and security protection. Configure IP addresses for the two VLAN virtual interfaces as gateways to ensure cross-VLAN communication with external networks. Create VLAN67 and VLAN68 for high-end experimental areas and scientific research office areas, assign corresponding physical ports to and switch access/trunk mode, and configure sub-interfaces such as g0/1.67 and g0/1.68 on the router to encapsulate the 802.1Q protocol and allocate IP to achieve efficient data transmission in different service areas.

3.1.2 EIGRP dynamic routing

Use the net command on the router to announce network segments such as 192.168.66.0/24, configure interface IP and monitor status, and enable EIGRP to realize automatic exchange of routing information and dynamic update of routing tables. After configuring the interface IP, the switch side enables EIGRP and declares the network. It cooperates with the router to build a dynamic routing environment to ensure communication between subnets in the main area and network stability when topology changes.

3.1.3 DHCP dynamically allocates addresses

Clean up the old address pool in router DHCP mode, create a new address pool for the corresponding subnet, and configure the default router and network address. Configure ip helper-address to designate a DHCP server on router subinterfaces and switches to realize configurations such as automatic acquisition of IP addresses by terminals across subnets, simplifying network management and ensuring terminal communication.

3.1.4 Nat translation

Configure static NAT on the router to map the local address of the internal server with the global address one-to-one, and define the internal and external interfaces to accurately implement the translation rules. This hides the internal network architecture, reduces the risk of external attacks, optimizes IP resource utilization, and ensures secure communication between the server and external networks.

3.2 Scientific Research Service Area

3.2.1 VLAN division

Create VLAN69 and VLAN70 in switch global mode, assign specific ports such as f0/1 and f0/2 to the corresponding VLANs, and configure the access mode. Reduce the scope of the broadcast domain, reduce bandwidth consumption, achieve logical isolation, reduce the possibility of security risk spread, and meet the efficient security needs of the service area.

3.2.2 Router subinterfaces

Enable subinterfaces on the router, use 802.1Q encapsulation protocol to associate corresponding VLANs (such as f0/0.69 to associate VLAN69), and assign IP to the subinterfaces as VLAN device gateways. Achieve inter-VLAN isolation and external network communication, control broadcast domains, reduce congestion and security risks, and ensure stable communication.

3.2.3 EIGRP dynamic routing

Enable the EIGRP process on the router and announce relevant network segments, allowing the router to establish neighbor relationships and share routing information. Relying on the diffuse update algorithm to quickly calculate optimal paths, sense topology changes and reroute them, improve convergence speed and network reliability, and adapt to complex network environments.

3.3 Scientific Research Security Area

3.3.1 VLAN partitioning and layer-3 switch virtual interfaces

Create VLAN71 and VLAN72 on the switch and divide logical subnets to narrow the broadcast domain and improve transmission efficiency. Configure the virtual interface of the layer-3 switch and allocate IP to enable it to have

cross-VLAN routing and forwarding capabilities, achieve subnet interoperability, enhance security and scalability, and lay the foundation for campus network operation.

3.3.2 OSPF dynamic routing

Enable the OSPF process on layer 3 switches and routers, announce network segments, and configure area authentication. Devices exchange routing information in real time, determine transmission paths through the shortest path tree, quickly sense topology changes and update routing tables, improve convergence speed and fault tolerance, and ensure stability of regional communication services.

3.4 Scientific Research Monitoring Area

Enable the RIP protocol on the router and announce the relevant networks, and configure version 2 and automatic summary functions. Using hop count as a measure, routing tables are broadcast regularly, allowing routers to grasp topology changes and converge quickly, optimize routing information processing, reduce network overhead, and ensure reliable monitoring data transmission.

3.5 Wide Area Network

3.5.1 Frame relay

Enable Frame Relay encapsulation on the serial interfaces of multiple routers, configure network layer addresses, use the frame-relay map command to map local DLCI and remote IP, and disable reverse resolution. Utilize the efficient and flexible characteristics of Frame Relay to achieve network connection and accurate data forwarding in various areas, and provide a reliable WAN solution.

3.5.2 Route republication

(1) RIP and EIGRP

Enable RIP and EIGRP on the R5 router, introduce each other's routing information in both directions and set metric values through the redistribute command. Break down protocol information barriers, allow routers to obtain comprehensive routing information to choose the optimal path, avoid routing loops, and improve network convergence speed and stability.

(2) OSPF, and EIGRP

When OSPF and EIGRP processes are enabled on the router, an invalid input error occurred when attempting to route reissue. It is speculated that the command syntax or parameters do not match the device requirements. Such errors will affect route propagation and calculation. Parameters need to be set reasonably in accordance with command rules to realize the interaction of routing information between protocols and optimize network routing configuration.

4 CONCLUSIONS

This paper completes the full-process design and implementation of the intelligent network in the scientific research park. By using demand-oriented architecture planning and multi-protocol integration technology, it addresses the core issues of multi-regional collaboration, security protection, and dynamic adaptation. The achievements include: constructing a hierarchical collaborative network architecture, achieving cross-regional interconnection based on frame relay. Through device deployment and VLAN division, the broadcast domain is reduced by over 80%, and the latency is controlled within 50ms. By deploying differentiated routing protocols by region and combining route republishing with DHCP, the terminal access efficiency is increased by 60%, and the topology convergence is less than 3 seconds. Establish a multi-level security protection system with a 100% certification pass rate to ensure data security. After debugging and resolving the protocol compatibility issue, the solution has been verified and can serve as a technical reference for small and medium-sized research parks. In the future, it is planned to introduce SDN and NetFlow to enhance intelligent management capabilities.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Zeng Yongquan, Qiu Jingfei, Chen Hongyu, et al. Research on the construction of network information security system in scientific research parks. Network Security Technology and Applications, 2025(06): 110-113.

[2] Tian Miao. Application of passive POL network in scientific research parks. Green Building, 2021, 13(04): 96-99+103.

[3] Han Z , Liu L, Guo Z, et al. A Dynamic Addressing Hybrid Routing Mechanism Based on Static Configuration in Urban Rail Transit Ad Hoc Network. Electronics, 2023, 12(17).

[4] Nicira Inc. Patent Issued for Static Route Configuration For Logical Router (USPTO 10, 805, 212). Internet Weekly News, 2020: 5530.

[5] Ara E T, Mohtasin G, DongSeong K, et al. Performance Enhancement of Optimized Link State Routing Protocol by Parameter Configuration for UANET. Drones, 2022, 6(1): 22-22.

[6] Zhang Jing. Research on Network Convergence, Routing and Host Adaptation Software Technology for FC Switching System. Zhejiang University, 2022.
[7] Yang Hua, Yan Haoran Exploration of "Next Hop" Configuration in Static Routing. Network Security and Informatization, 2021(10): 67-69.
[8] Fang Sheng, Wu Baoqiang. Comparative Study on Static Routing and Dynamic Routing Configuration. Computer Knowledge and Technology, 2025, 25, 21(07): 87-89.