I J C R M
International Journal of Contemporary Research In Multidisciplinary

*Research Article*

# Design and Simulation of a Secure and Redundant Enterprise Network Architecture Using Cisco Packet Tracer

**Ayuba Isah Malami [1*], Amit Jain [2], Ronak Duggar [3]**
[1] Master's Student (M.Tech CSE), School of Computer Science and Engineering, Geeta University, Panipat, Haryana, India
[2] Professor, School of Computer Science and Engineering, Geeta University, Panipat, Haryana, India
[3] Assistant Professor, School of Computer Science and Engineering, Geeta University, Panipat, Haryana, India

**Corresponding Author:** *Ayuba Isah Malami

**DOI:** https://doi.org/10.5281/zenodo.19728918

## Abstract

Modern enterprises are heavily dependent on secure and dependable networks; however, challenges such as network failures, less-than-optimal routing, and a lack of security prevail. This research introduces the design and simulation of a redundant enterprise network based on collapsed core network topologies interlinking headquarters, branch offices and a central server. Virtual LANs (VLANs) and Access Control Lists (ACLs) are integrated for better segmentation and security, OSPF is used for efficient routing, and HSRP is used for gateway redundancy. A structured Variable Length Subnet Masking or VLSM scheme is implemented to better use the IP address. Simulation in Cisco Packet Tracer shows that we have successfully proposed inter-VLAN communication, access control and failover functions. The proposed model provides a cost-efficient model for building resilient enterprise networks.

## Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 03-04-2026
- **Accepted:** 17-04-2026
- **Published:** 24-04-2026
- **IJCRM:**5(2); 2026: 816-821

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

## How to Cite this Article

Malami A I, Jain A, Duggar R. Design and Simulation of a Secure and Redundant Enterprise Network Architecture Using Cisco Packet Tracer. Int J Contemp Res Multidiscip. 2026;5(2):816-821.

**Access this Article Online**

www.multiarticlesjournal.com

**KEYWORDS:** Cisco Packet Tracer Simulation, OSPF (Open Shortest Path First), HSRP (Hot Standby Router Protocol), VLANs (Virtual Local Area Networks), Network Security, Enterprise Network Architecture.

## 1. INTRODUCTION

Enterprise networks are an indispensable part of modern organisation operations, allowing for easy communication, high-data-sharing methods, and multi-site coordination of operations. Nevertheless, traditional network design architectures often present many vulnerabilities, including single points of failure, poor routing and inadequate security, all of which result in operational inefficiencies and high levels of risk. To overcome these limitations, hierarchical network models with advanced technologies are increasingly adopted, which help to achieve scalability, better performance, and fault tolerance. Virtual LANs (VLANs) are used to ensure segregation of the traffic logically, whereas Access Control Lists (or ACLs) are used to create strict security policies. Reliability is further fortified by using redundancy protocols like Hot Standby Router Protocol (HSRP), and routing efficiency is increased in the form of the Open Shortest Path First (OSPF) algorithm. Moreover, simulation tools such as Cisco Packet Tracer support the analysis of complex network architectures over possible deployments, and so they become an essential tool in the design of resilient enterprise networks.

### 1.1 Research Contribution

This paper describes a scalable enterprise network architecture aimed at supporting multi-site organisations, incorporating the use of VLANs to support segmentation, ACLs to support the secure trafficking of traffic, the use of OSPF to support dynamic routes and the use of HSRP to support gateway redundancy. The Cisco Packet Tracer simulations are used to test and implement the framework and to test it with different operational and failure conditions. In general, the study shows that hierarchical design, redundancy, and routing optimisation help to increase the scalability, reliability, and efficiency of enterprise networks.

## 2. LITERATURE REVIEW

Enterprise network research reveals the need for scalability, reliability, and security within the distributed organisation. Stallings (2022) stresses the hierarchical models for efficient management, but he mentions limited redundancy. VLAN-based segmentation results in an improvement to traffic isolation and department security, but has poor multi-site validation (Tanenbaum & Wetherall, 2011). OSPF dynamic routing improves the efficiency and convergence, but redundancy integration is not well explored (Moy, 2020). Access control and traffic filtering using ACL policies is a robust approach, but simulation of large-scale enterprise simulations is not widely available (Simanjuntak et al. 2023). Redundancy protocols are good for helping to increase availability and failover performance, there are integration limitations with security architectures (Cisco Systems, 2023). More contemporary methods like Software-Defined Networking (SDN) offer centralised programmability and scalability, but there are deployment complexities and security issues (Kreutz et al., 2015).

### 2.1 Comparative Analysis of Studies

**Table 1:** Enterprise Architecture and Security Studies

| Study | Methodology | Results | Gaps |
|---|---|---|---|
| **Stallings, 2022** | Enterprise architecture models | Improved scalability and network management | Lack of focus on redundancy mechanisms |
| **Tanenbaum & Wetherall, 2011** | VLAN-based network segmentation | Increased traffic isolation & security | Multi-site validation is weak |
| **Moy, 2020** | OSPF dynamic routing protocol | Increased routing efficiency and convergence | Increased integration of redundancy is limited |
| **Simanjuntak et al., 2023** | ACL-based network security policy | Enhanced access control and traffic filtering | Lack of large-scale enterprise simulation |
| **Cisco Systems, 2023** | Redundancy and failover protocols | More downtime and higher availability | Less integration with security architectures |
| **Kreutz et al., 2015** | SDN architecture for scalable networks | Enhanced centralized control and scalability | Security concerns in SDN |
| **Oppenheimer, 2011** | Network design best practices | Reliable enterprise infrastructure models | Limited validation using Simulation |

This table above identifies six studies that together shed light upon substantial advancements in enterprise networking specifically relating to scalability, segmentation, routing, security, redundancy and software-defined networking (SDN). While there is much to gain insight into in any contribution, the overwhelming focus is indeed on discrete technology components rather than on the synthesis of integrated frameworks. This lack of methods highlights the need for the current investigation, which proposes a simulation-based enterprise network model that encompasses VLANs, ACLs, OSPF and HSRP to achieve a network model that is secure, scalable and resilient across multiple sites. The architecture of enterprise networks has been a matter of intensive academic research, mainly driven by the need to achieve better scalability, reliability, and balanced management of traffic in distributed organizational setups. Traditional enterprise network designs are based on systematic organizational principles and hierarchy models to support the work of large-scale infrastructures and ensure effective communication of data (Stallings, 2022; Oppenheimer, 2011).

## 3. PROPOSED METHODOLOGY

This paper presents a safe and scalable enterprise network architecture that captures a multi-site organization, including a headquarters, two branch offices, and a centralized server facility. The model is hierarchical but collapsed in nature,

which is simulated by the Cisco Packet Tracer to test its behaviour in terms of performance, security, and fault tolerance before being deployed in the real world.

Some of the important technologies used are VLANs to segment based on department, Access Control Lists (ACLs) based on inter-segment security and Open Shortest Path First (OSPF) used as a dynamic routing mechanism. Redundancy of the gateway is done through Hot Standby Router Protocol (HSRP), and Variable Length Subnet Masking (VLSM) allows efficient allocation of IP addresses. As a combination, the model incorporates segmentation, routing, security and redundancy to provide a robust infrastructure for the enterprise network.

### 3.1 Research Design

This research tests the suggested enterprise network structure concerning the performance, security and reliability using an experimental design based on simulation. The use of simulation is a popular methodological tool in network research, which allows studying complex network setups with controlled parameters, reducing expenses and risks of a real-life implementation.

The study builds a multi-enterprise network that constitutes three locations that each have several branch offices and a central hub of servers through which the headquarters, along with the two subordinate offices, are also hosted.

### 3.2 Network Topology

The proposed enterprise network consists of a headquarters, 2 branch offices, and centralized servers that are interconnected by a simulated Wide Area Network (WAN). The Virtual Local Area Networks (VLANs) are used to realise departmental segmentation, Access Control Lists (ACLs) control security between departmental segments, Open Shortest Path First (OSPF) routing helps realise dynamic routing, and Hot Standby Router Protocol (HSRP) serves as a gateway redundancy application.

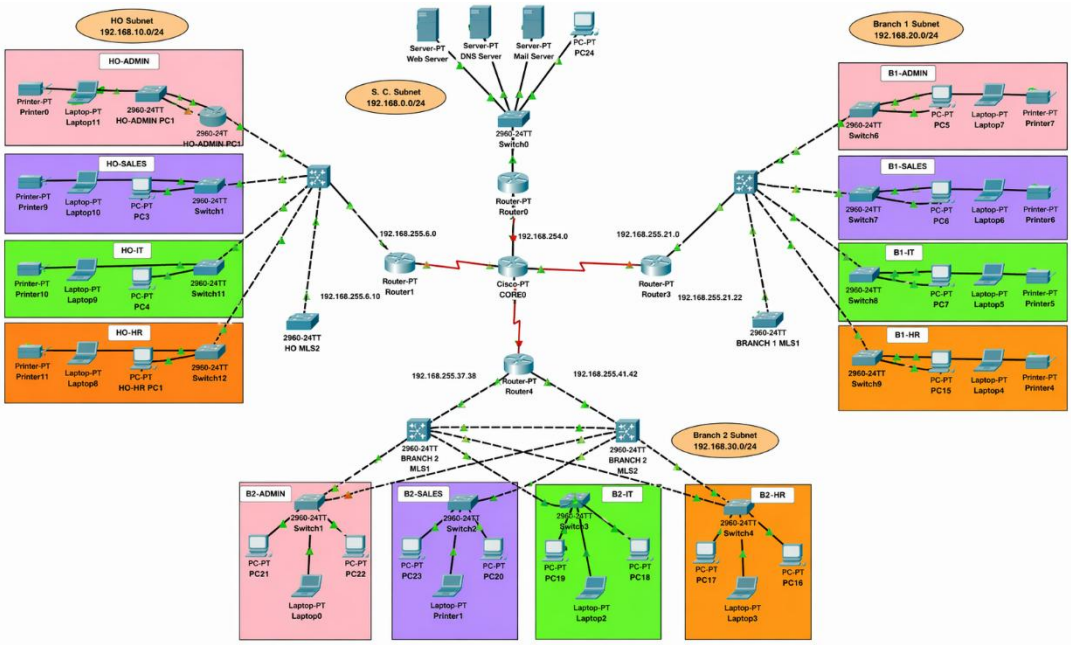
### 3.3 Simulation Environment and Tools

In this study, Cisco Packet Tracer was used to represent the model of a multi-site enterprise network consisting of a headquarters, two branch offices, and centralised server resources (Cisco, 2025; Odom, 2020). The resultant network configuration included VLAN segmentation, access control lists (ACLs), OSPF routing, HSRP failover mechanisms and variable-length subnet masking (VLSM) planning to evaluate network segmentation, routing effectiveness, access control and high availability (Odom, 2020; Moy, 1998; Li et al., 1998).

### 3.4 Parameters of Network Configuration

The simulated enterprise network was designed to produce efficient routing, strong security and reliable performance at different sites. Variable Length Subnet Masking (VLSM) was used to optimize the allocation of the IP addresses. Total VLANs are used to divide the traffic routes, and access control lists (ACLs) are used to implement security policies. Open Shortest Path First (OSPF) to enable the dynamic routing process and Hot Standby Router Protocol (HSRP) to allow redundant gateways. The modelling, along with the testing platform of Cisco Packet Tracer, was used to validate the scalability and resilience of the architecture (Odom, 2020; Moy, 1998; Li et al., 1998; Cisco, 2025).

**Fig. 1:** Network Topology Simulated in Cisco Packet Tracer



### 3.5 Data Analysis Approach

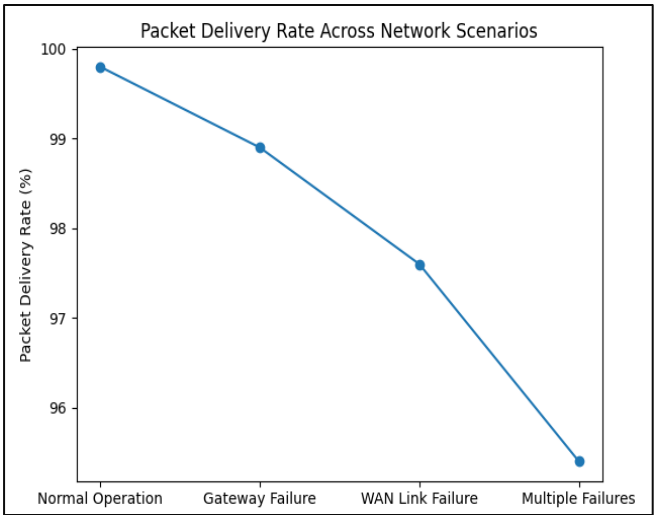
An approach to data analysis has been used, which comprised the use of simulation in Cisco Packet Tracer to evaluate the performance and fault tolerance aspects of the proposed enterprise network. Key performance indicators, such as packet-delivery rate, latency, routing convergence, and failover recovery, under nominal and faulty conditions, and the corresponding measurements using comparative tables and figures were extracted to assess reliability, scalability, and resilience.

**Table 2:** Structure of Simulation Data Analysis

| Scenario | Packet Deliver Rate (%) | Average Latency (ms) | Routing Convergence Time(s) | Failover Recovery Time(s) |
|---|---|---|---|---|
| Normal Network Operation | 99.8 | 5 | 1.2 | - |
| Gateway Failover | 98.9 | 7 | 1.5 | 3 |
| WAN Link Failure | 97.6 | 9 | 2.1 | - |
| Multiple Failure Scenario | 95.4 | 12 | 2.8 | 4 |

This analysis was aimed at demonstrating that the proposed network architecture can ensure reliable communication and fast recovery during failures. The findings provide evidence to support the effectiveness of the developed enterprise network model.

**Fig. 2:** Packet Delivery Rate Across Network Scenarios




## 4. RESULTS

This section presents the simulation results obtained from Cisco Packet Tracer to evaluate the proposed enterprise network in terms of reliability, routing efficiency, and fault tolerance. The findings showed high packet delivery, low latency, fast recovery during gateway failure through HSRP, and successful route recalculation during WAN link failure through OSPF.

Overall, the results confirm that the use of hierarchical design, dynamic routing, redundancy, and security controls improved the reliability, availability, and stability of the enterprise network.

### 4.1 Performance Evaluation Metrics

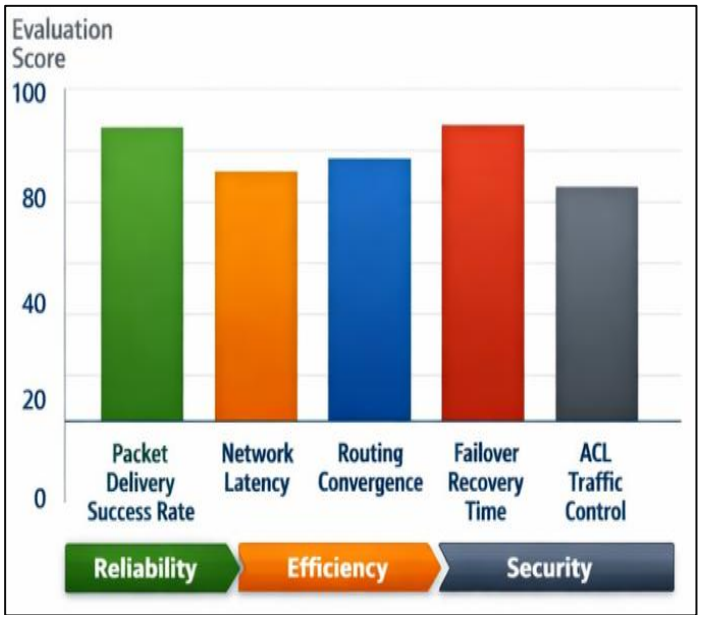
The performance of the proposed enterprise network was performed by simulation, including in terms of packet delivery success, network latency, routing convergence, gateway failover recovery, and ACL traffic control. These measurements provided a detailed basis for communication efficiency assessment, routing performance assessment, security enforcement assessment and fault tolerance assessment under simulated operational conditions.

**Table 3:** Performance Evaluation Metrics

| Metric | Description |
|---|---|
| Packet Delivery Success Rate | Measures successful data transmission |
| Network Latency | Time taken for data communication |
| Routing Convergence | Stability and adaptability of routing paths |
| Failover Recovery Time | Gateway redundancy recovery performance (HSRP) |
| ACLs Traffic Control | Effectiveness of enforcing security policies |

The metrics form a detailed set of measures to assess the reliability and performance of the proposed enterprise network architecture in a variety of operational conditions.

**Fig. 3:** Evaluation Scores of Network Performance Metrics



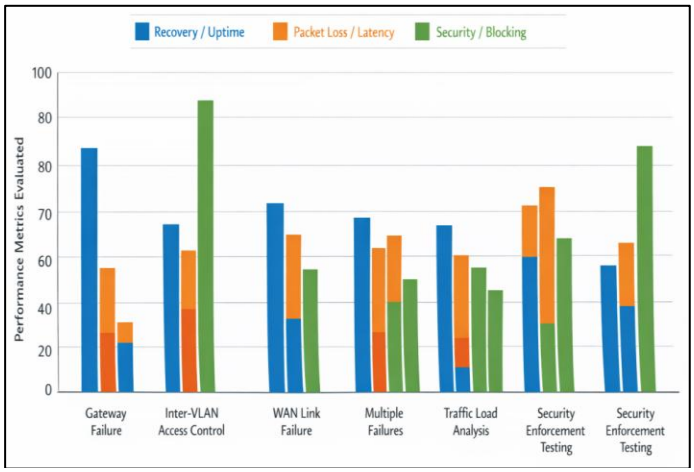
### 4.2 Experimental Scenarios

**Table 4:** Summary of Enterprise Network Architecture and Security Studies

| Scenario | Description | Performance Metrics Evaluated |
|---|---|---|
| Gateway Failure | Test HSRP redundancy | Failover recovery, packet delivery, uptime |
| Inter-VLAN Access Control | Enforce ACL rules | Block unauthorised traffic, allow legitimate traffic |
| WAN Link Failure | Simulate branch link failure | Routing reconvergence, packet loss, and latency |
| Multiple Failures | Combined gateway & WAN failures | Resilience, downtime, and delivery reliability |
| Traffic Load Analysis | Variable traffic patterns | Throughput, latency, congestion |
| Security Enforcement Testing | Simulated attacks (e.g., ARP spoofing | Routing security, Layer 2 protection (DAI) |

The table shows a synthesis of scenarios to be used to appraise the reliability, performance and security of the enterprise network under a variety of operational and failure conditions.

**Fig. 4:** Bar Graph Experimental Scenarios in Enterprise Network




## 5. DISCUSSION

The results of the simulation show that the proposed enterprise network architecture allows reliable and efficient communication to be provided across a multi-site environment. Under regular conditions, the network had a great packet delivery and low latency, meaning that it was operating effectively for traffic segmentation and routing efficiency (Stallings, 2022; Tanenbaum and Wetherall, 2011).

In failure situations, the network remained connected with minimal interruption because of the implementation of the Hot Standby Router Protocol (HSRP) and Open Shortest Path First (OSPF), which allowed quick recovery (Moy, 2020). Although there was some performance degradation under multiple failure conditions, the net connectivity didn't break down, and the network continued functioning. Overall, the results support the assertion that the inclusion of routing, redundancy and access control mechanisms provides significant contributions to the enterprise network reliability and security.

## 6. RESEARCH CONTRIBUTION

This study proposes the network architecture of a scalable enterprise network that incorporates VLAN segmentation, using an ACL as a security measure, using Open Shortest Path First (OSPF) as a routing protocol, and using the Hot Standby Router Protocol as redundancy. The model is implemented and tested with Cisco Packet Tracer and shows enhanced network reliability, performance, and fault tolerance.

The conceptualization, design, implementation and analysis of the study were done by the primary author. The second author (Amit Jain) gave guidance and validation, and the third author (Ronak Duggar) was of vital importance for the technical support and research insights.

## 7. CONCLUSION

This paper describes a simulation-based enterprise network architecture that can aid efficient and dependable communication in a multi-site organizational setting. The suggested architecture combines the hierarchical network design concepts with the segmentation of traffic by using VLANs, secure access control deployed using ACL policies, dynamic routing based on the Open Shortest Path First (OSPF) protocol, and gateway redundancy based on the Hot Standby Router Protocol (HSRP). All these technologies combined improve the efficiency of the network, reinforce the security enforcement, and enhance the operational reliability in the enterprise infrastructures (Tanenbaum and Wetherall, 2011).

The proposed enterprise network architecture was modelled and tested in Cisco Packet Tracer using normal and failure conditions. Simulation results suggested high packet delivery rates, low latency and fast recovery from the failure of gateways and links, thus proving the effectiveness of dynamic routing and redundancy schemes. Overall, the study shows that the combination of network segmentation, routing, and redundancy protocols can provide a practical, scalable, secure and resilient solution for enterprise networks.

## 8. FUTURE WORK

The next generation of research will help to improve the proposed enterprise network architecture by incorporating more sophisticated security, such as an Intrusion Detection system and intruder prevention systems, that will enhance threat detection and network security. Software-defined networking could also be considered to provide the opportunity of centralised network management, superior traffic control and scalability.

Also, for the future, one can look into the option of cloud-based infrastructure coupled with (IaaS) Infrastructure as a Service that can be used for hybrid enterprise scenarios. The use of the proposed architecture in real-world networks, as opposed to simulation use, as only seen in Cisco Packet Tracer, would also

be used to test the network's performance, reliability and scalability when used in a real-world setting.

## REFERENCES


1. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A survey on enabling technologies, protocols and applications. IEEE Commun Surv Tutor. 2015;17(4):2347–2376. doi:10.1109/COMST.2015.2444095.
2. Chatzoglou P, Chatzoudes D, Fragidis L, Symeonidis S. Factors affecting the adoption of advanced networking technologies in enterprise environments. J Netw Comput Appl. 2021;178:102982. doi:10.1016/j.jnca.2021.102982.
3. Cisco. Cisco Packet Tracer Download and Installation Instructions [Internet]. 2025. Available from: https://www.netacad.com/
4. Cisco Networking Academy. Cisco Packet Tracer Networking Simulation Tool [Internet]. 2023. Available from: https://www.netacad.com
5. Cisco Systems. Enterprise Network Redundancy and Failover Technologies [Internet]. 2023. Available from: https://www.cisco.com
6. Feamster N, Rexford J, Zegura E. The road to SDN. ACM Queue. 2014;11(12):20–40. doi:10.1145/2559899.
7. Huitema C. Routing in the Internet. 2nd ed. Upper Saddle River (NJ): Prentice Hall; 2000.
8. Javid M. Network simulation using Cisco Packet Tracer. Int J Comput Netw Inf Secur. 2014;6(2):45–50. doi:10.5815/ijcnis.2014.02.07.
9. Kreutz D, Ramos F, Verissimo P, Rothenberg C, Azodolmolky S, Uhlig S. Software-defined networking: A comprehensive survey. Proc IEEE. 2015;103(1):14–76. doi:10.1109/JPROC.2014.2371999.
10. Kumar R, Singh A. Secure enterprise network architecture using layered security approaches. Int J Netw Secur. 2021;23(3):512–520.
11. Moy J. OSPF: Anatomy of an Internet Routing Protocol. Reading (MA): Addison-Wesley; 2020.
12. Odom W. CCNA 200-301 Official Cert Guide. Vol. 1. Indianapolis (IN): Cisco Press; 2020. Available from: https://www.ciscopress.com/
13. Oppenheimer P. Top-Down Network Design. 3rd ed. Indianapolis (IN): Cisco Press; 2011.
14. Simanjuntak M, Sihombing O, Siregar B. Enterprise network design and performance evaluation using network simulation tools. Int J Comput Netw Commun. 2023;15(2):45–58. doi:10.5121/ijcnc.2023.15204.
15. Stallings W. Data and Computer Communications. 11th ed. Harlow: Pearson Education; 2022.
16. Tanenbaum AS, Wetherall DJ. Computer Networks. 5th ed. Upper Saddle River (NJ): Pearson; 2011.
17. Zhang Y, Wang L, Chen X. Performance optimisation techniques for enterprise network infrastructures. J Netw Syst Manag. 2022;30(2):1–18. doi:10.1007/s10922-021-09624-3.




**About the Corresponding Author**

**Ayuba Isah Malami** is a Master's student (M.Tech in Computer Science and Engineering) at the School of Computer Science & Engineering, Geeta University, Panipat, Haryana, India. His academic interests include computer networks, Internet of Things (IoT), network security, and emerging communication technologies. He is actively engaged in research focused on enterprise networking solutions and simulation-based performance analysis.