Advances in Networks
2026, Vol. 13, No. 1, pp. 31–39
https://doi.org/10.11648/j.net.20261301.13

SciencePG
Science Publishing Group

Research Article

Enhanced Virtual Router Redundancy Protocol for Optimized Network Performance and Security in Enterprise Environments

Michael Chinyere Hannah, Gloria Ngozi Ezeh, Chika Norah John, Emmanuel Chukwudi Amadi*

Department of Information Management Technology, Federal University of Technology, Owerri, Nigeria

Abstract

This study presents an enhanced Virtual Router Redundancy Protocol (VRRP) framework designed to improve network reliability, performance, and security in enterprise environments. As organizations increasingly depend on uninterrupted internet connectivity for critical operations, conventional redundancy mechanisms often struggle with latency, failover delays, packet loss, and security vulnerabilities. These limitations can lead to service interruptions and reduced Quality of Service (QoS), particularly in large-scale campus and enterprise networks. To address these challenges, the proposed framework integrates VRRP with First Hop Redundancy Protocols (FHRP), Hot Standby Router Protocol (HSRP), and dynamic access control mechanisms to provide a more secure and fault-tolerant network architecture. The proposed model was implemented and tested using Cisco Packet Tracer within a simulated campus network environment consisting of dual Internet Service Provider (ISP) links. The implementation focused on ensuring seamless failover, efficient load balancing, and secure routing operations during network disruptions. Performance evaluation was conducted using key metrics such as failover time, packet loss, and QoS performance. Experimental results revealed an average failover time of 11 seconds with zero packet loss during transition between active and standby routers, demonstrating significant improvements in network stability and service continuity. Furthermore, the integration of security-aware dynamic access control mechanisms reduced the risk of unauthorized routing participation and strengthened overall network protection. The findings indicate that the enhanced VRRP framework effectively eliminates single points of failure while supporting adaptive load balancing and secure redundancy management. The study therefore contributes to the development of scalable and resilient enterprise network infrastructures capable of maintaining high availability under varying operational conditions. In addition, the proposed framework provides practical insights for network engineers, system administrators, and researchers seeking reliable solutions for improving redundancy, security, and performance in modern enterprise and campus network environments.

Keywords

VRRP, Network Redundancy, Failover Optimization, Network Security, FHRP, HSRP, QoS, Enterprise Networks

*Correspondence: Emmanuel Chukwudi Amadi (chinyere16829@gmail.com)

Received: 7 May 2026; **Accepted:** 30 May 2026; **Published:** 12 June 2026

Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Modern enterprises increasingly rely on uninterrupted network availability to sustain critical operations such as cloud computing, Internet of Things (IoT) deployments, and distributed application architectures. Any disruption in network connectivity can lead to substantial operational inefficiencies and financial losses, particularly in real-time and mission-critical environments. Traditional static routing mechanisms inherently introduce a single point of failure, thereby necessitating the adoption of redundancy protocols such as the Virtual Router Redundancy Protocol (VRRP) to ensure high availability and fault tolerance [1-3].

VRRP enables multiple physical routers to operate as a single logical gateway by sharing a virtual IP address, thereby ensuring seamless failover when the primary (master) router becomes unavailable. This mechanism significantly enhances network resilience and minimizes downtime. However, despite its advantages, conventional VRRP implementations exhibit notable limitations, including the absence of built-in security mechanisms, susceptibility to spoofing and unauthorized participation, and limited support for efficient load balancing across redundant paths [3, 4]. Furthermore, traditional VRRP configurations often result in underutilization of backup routers, as they remain idle until failover occurs, leading to suboptimal resource utilization.

Recent research has therefore focused on enhancing VRRP through the integration of intelligent routing strategies, adaptive failover mechanisms, and advanced security frameworks. For instance, [5] highlight the role of high-availability frameworks in improving resilience in IoT-driven environments, while [6] demonstrate how AI-driven traffic analysis can optimize redundancy protocols for better load distribution and faster recovery. Similarly, emerging enterprise network designs incorporate multi-protocol redundancy and security-aware architectures to address scalability and threat mitigation challenges [4-6].

Building upon these advancements, this study extends the existing thesis by proposing an enhanced VRRP framework that incorporates the following key features:

a) Secure VRRP (sVRRP): Integration of authentication and access control mechanisms to mitigate routing attacks and unauthorized participation.
b) Dynamic Load Balancing: Intelligent distribution of network traffic across multiple routers to improve performance and resource utilization.
c) Integrated Access Control Security: Implementation of dynamic Access Control Lists (ACLs) to enforce security policies and enhance network integrity.

This enhanced approach aims to address the inherent limitations of traditional VRRP while providing a more robust, scalable, and secure solution for modern enterprise network environments.

2. Related Works

Recent literature on high-availability networking and redundancy protocols consistently emphasizes the role of VRRP and related mechanisms in improving reliability, minimizing downtime, and maintaining Quality of Service (QoS). However, existing studies also reveal persistent gaps in security enforcement, scalability, and adaptive optimization, which motivate further enhancements.

Study done by [5] presents a high-availability framework for IoT and edge environments, demonstrating that redundancy mechanisms significantly improve resilience and ensure continuous service delivery. The work highlights that integrating failover protocols with distributed architectures reduces service interruption and enhances system robustness.

Similarly, [7] provides a detailed evaluation of routing and redundancy strategies, showing that optimized configurations can reduce failover latency and improve convergence performance. The study emphasizes the importance of timer tuning and protocol parameter adjustment in achieving efficient VRRP operation [8].

Research [9] investigates dynamic routing and failure recovery in software-defined and traditional networks. It demonstrates that combining redundancy protocols with adaptive routing mechanisms enhances network stability and enables faster recovery from failures, particularly in large-scale environments.

In [10], the focus is on packet loss optimization in router forwarding systems. The findings confirm that properly con-Figured redundancy mechanisms can achieve near-zero packet loss, which is critical for real-time and latency-sensitive applications such as VoIP and streaming services.

Study [11] explores redundancy in IoT-based systems, showing that VRRP-like architectures improve availability and reliability in distributed sensor networks. The research highlights the importance of integrating redundancy with edge computing to support real-time data processing [12, 13].

Research [14] examines enterprise network architectures and security integration. It concludes that combining redundancy protocols with security-aware configurations enhances both network resilience and protection against unauthorized access and routing attacks.

Further, [15] demonstrates that simulation-based network design, including VLAN segmentation and redundancy mechanisms, improves scalability and fault tolerance in enterprise environments. The study validates the effectiveness of simulation tools for evaluating redundancy strategies before deployment.

Finally, [16] researchers have investigated reliability mechanisms in distributed and IoT networks, showing that redundancy protocols combined with monitoring systems significantly improve QoS metrics such as latency, jitter, and packet delivery ratio.

3. Materials and Methods

3.1. Network Design

The proposed network architecture adopts a dual-router topology designed to enhance redundancy, fault tolerance, and

performance in enterprise environments. This design ensures continuous network availability by eliminating single points of failure and enabling seamless failover mechanisms. Similar approaches have been widely used in enterprise network simulations and implementations, where redundancy protocols such as VRRP are integrated with VLAN-based segmentation to improve scalability and resilience [17-20].

The network design consists of the following key components:

1) Dual Internet Service Providers (ISPs): Two independent ISP connections were conFigured to provide external network connectivity. This multi-homing approach improves network reliability by ensuring that failure in one ISP link does not disrupt overall connectivity. The routers are conFigured to dynamically switch between ISPs using redundancy protocols, thereby minimizing downtime and maintaining service continuity.
2) VLAN Segmentation: Virtual Local Area Networks (VLANs) were implemented to logically segment the network into multiple broadcast domains. This segmentation enhances security, reduces congestion, and improves traffic management by isolating different departments or services within the enterprise network. VLAN-based architectures are widely recognized for improving network efficiency and scalability in modern enterprise systems.
3) Virtual IP Gateway Configuration (VRRP): A Virtual Router Redundancy Protocol (VRRP) configuration was deployed to create a virtual default gateway shared between the primary and backup routers. The routers operate in a master–backup relationship, where the master router handles traffic under normal conditions, and the backup router automatically takes over in the event of failure. This ensures uninterrupted communication and fast failover with minimal packet loss.

Overall, this integrated design combining dual ISPs, VLAN segmentation, and VRRP-based virtual gateway configuration provides a scalable and resilient network infrastructure capable of supporting high-availability enterprise applications.

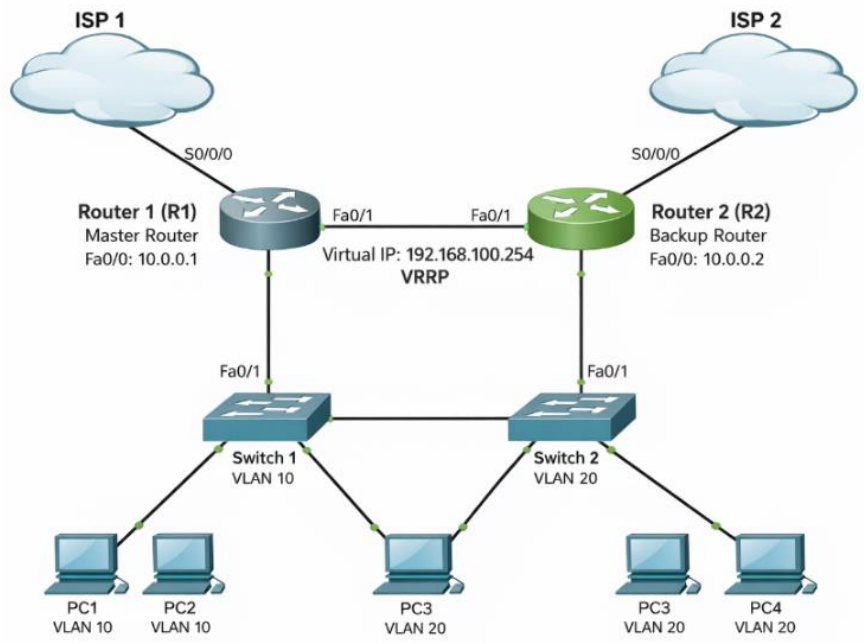

Figure 1. *VRRP simulation Diagram.*

Figure 1 illustrates the designed enterprise network topology implemented in Cisco Packet Tracer, featuring a dual-router redundancy architecture based on the Virtual Router Redundancy Protocol (VRRP). The network consists of two routers connected to separate Internet Service Providers (ISPs), ensuring continuous external connectivity in case of link or device failure. Router 1 operates as the master router, while Router 2 functions as the backup, both sharing a virtual IP address that acts as the default gateway for end devices.

The internal network is segmented using VLANs, where Switch 1 supports VLAN 10 and Switch 2 supports VLAN 20, allowing logical separation of network traffic for improved security and performance. End devices (PCs) are connected to their respective VLANs through access switches, while inter-switch communication enables network-wide connectivity. In the event of a failure in the master router, VRRP automatically promotes the backup router to maintain uninterrupted communication.

Table 1. Logical topology of the design.

Device	Role	Interface	IP Address / Subnet	Connected To	Purpose
R1	Master VRRP Router	Fa1/0	192.168.100.1/24	Internal switch / LAN	Primary default gateway for client network
R1	Upstream Router	S0/0	172.16.1.5/30*	R3	Path from LAN to external network
R2	Backup VRRP Router	Fa1/0	192.168.100.2/24*	Internal switch / LAN	Standby gateway during R1 failure
R2	Upstream Router	S0/1	172.16.1.9/30*	R3	Alternate path to external network
VRRP Gateway	Virtual Router	Group 22	192.168.100.254/24	PC10, R1, R2	Shared default gateway used by hosts
PC10	End Host / Client	Fa0/0	192.168.100.10/24	Internal switch	User device generating traffic
PC10	Default Gateway	—	192.168.100.254	VRRP Virtual Router	Sends outbound traffic through virtual gateway
R3	Upstream / External Router	S0/0	172.16.1.6/30	R1	Upstream route to external server
R3	Upstream / External Router	S0/1	172.16.1.10/30	R2	Backup upstream route
R3	Loopback0	Lo0	33.33.33.33/32	Logical server endpoint	Test destination for traceroute/verification
S1	Access Switch	VLAN 1	Layer 2 device	R1, R2, PC10	Connects internal LAN devices

Table 1 presents the logical configuration of the proposed VRRP-based network topology, detailing the roles, interfaces, and IP addressing scheme of all network devices. The table shows how Router 1 and Router 2 are conFigured as master and backup routers, respectively, sharing a virtual IP address (192.168.100.254) that serves as the default gateway for end devices. It also illustrates the interconnection between internal LAN components and the upstream router (R3), which provides external network access. This logical arrangement ensures redundancy, enabling seamless failover and continuous network availability in the event of router or link failure.

3.2. Implementation Tools

The implementation of the proposed network model was carried out using a combination of simulation software and networking configurations to ensure accurate evaluation of performance, redundancy, and security mechanisms.

1) Cisco Packet Tracer: Cisco Packet Tracer was used as the primary simulation tool to design and implement the network topology. It provides a realistic environment for configuring routers, switches, VLANs, and routing protocols, enabling the testing of redundancy mechanisms and failover scenarios without requiring physical hardware. The tool is widely adopted in academic and professional settings for network prototyping and validation [15].

VRRP Configuration (Virtual IP: 192.168.100.254): The Virtual Router Redundancy Protocol (VRRP) was conFigured on both routers to establish a virtual default gateway with the IP address 192.168.100.254. This configuration allows multiple routers to function as a single logical gateway, where one router acts as the master and the other as a backup. In the event of failure, the backup router automatically assumes control, ensuring seamless failover and uninterrupted network access. VRRP is widely recognized for enhancing network availability and fault tolerance in enterprise environments [21].

2) Static Routing: Static routing was implemented to define fixed paths for data transmission between network segments and external networks. This approach provides simplicity and control in smaller or controlled environments, ensuring predictable routing behaviour. Static routes were conFigured on both routers to enable communication with the connected ISPs and internal VLAN networks, supporting the overall redundancy framework.

3.3. Performance Metrics

The performance of the proposed network was evaluated using the following metrics:

1) Failover Time (T_f):

Measures the time required for the backup router to take over after failure.

$$T_f = T_{\text{recovery}} - T_{\text{failure}}$$

Lower values indicate faster network recovery and higher availability.

2) Packet Loss (PL):

Represents the percentage of lost packets during transmission.

$$PL(\%) = \frac{P_{\text{sent}} - P_{\text{received}}}{P_{\text{sent}}} \times 100$$

Lower packet loss indicates higher network reliability.

3) Throughput (TP):

Measures the rate of successful data delivery.

$$TP = \frac{\text{Total Data Received (bits)}}{\text{Time (seconds)}}$$

Higher throughput reflects better network efficiency.

4) Quality of Service (QoS):

Evaluates overall network performance based on key parameters.

$$QoS \propto f(\text{Bandwidth}, \text{Latency}, \text{Jitter}, 1/PL)$$

Higher QoS indicates better service performance and user experience.

3.4. Security Integration

Access Control Lists (ACLs) were integrated into the VRRP framework to enforce traffic filtering and secure routing operations [15].

1) Spoofing Mitigation: Ingress ACLs were applied to filter packets with illegitimate source IP addresses, preventing IP spoofing and unauthorized VRRP advertisements.
2) Router Authorization Control: ACL policies restricted VRRP multicast (224.0.0.18) and control traffic to predefined router interfaces, ensuring only trusted devices participate in the redundancy group.
3) Authentication Enforcement: ACLs were combined with VRRP authentication mechanisms to validate control messages and block unauthorized routing updates.

4. Design and Configuration Approach

4.1. Design Algorithm

Algorithm 1: Secure Adaptive VRRP Failover Test Algorithm (SAVFTA)

Input:

$R = \{R_1, R_2\}$, $L = \{ISP_1, ISP_2\}$, $VIP = 192.168.100.254$, *authorized router set A, host set H, monitoring interval* Δt, *test duration* T

Output:

Failover time T_f, packet loss PL, throughput TP, QoS status Q, security compliance S_c

Begin SAVFTA
1. ConFigure topology:
Set R1 as VRRP Master
Set R2 as VRRP Backup
Assign VIP = 192.168.100.254
ConFigure ISP1 and ISP2 uplinks
Apply ACLs to allow only routers in A
2. Validate baseline:
For each host h in H
Test reachability to VIP and external target
If any test fails
Stop and report configuration error
3. Start traffic generation:
For each host h in H
Send continuous ICMP/application traffic
Record transmitted packets Ps(h)
Record received packets Pr(h)
4. Validate security:
Inject unauthorized VRRP/router advertisement
If unauthorized router is blocked
Security_Status = PASS
Else
Security_Status = FAIL
5. Trigger failover:
Shut down R1 or disconnect ISP1
Record failure time Tfailure
6. Monitor transition:
While VIP is unreachable through R2
Probe connectivity every Δt
Log latency, jitter, and packet reception
End While
7. Record recovery:
Record recovery time Trecovery
Compute failover time:
Tf = Trecovery - Tfailure
8. Compute packet loss:
PL = (ΣPs - ΣPr) / ΣPs) × 100
9. Compute throughput:
TP = Total successful bits received / observation time
10. Evaluate QoS:
Measure latency L, jitter J, throughput TP, packet loss PL
If L ≤ Lth and J ≤ Jth and TP ≥ TPmin and PL = 0
Q = ACCEPTABLE
Else
Q = DEGRADED
11. Restore primary router:
Bring R1 back online
Verify re-election and stable preemption behavior
12. Final decision:
If Tf ≤ threshold and PL = 0 and Security_Status = PASS
Test_Result = SUCCESS
Else
Test_Result = IMPROVEMENT REQUIRED

End SAVFTA

A Secure Adaptive VRRP Failover Test Algorithm (SAVFTA) was developed to evaluate the proposed enhanced VRRP framework. The algorithm initializes the dual-ISP redundant topology, validates baseline connectivity, generates continuous traffic, injects unauthorized routing attempts for ACL verification, triggers master-router failure, and measures failover time, packet loss, throughput, and QoS during transition. It further verifies recovery stability by restoring the primary router and observing re-election behavior. This algorithm was specifically designed for the proposed architecture to jointly assess availability, security, and traffic continuity under fault conditions.

4.2. Design Enhancements

The proposed system extends conventional VRRP deployment through security hardening, optimized failover tuning, and deterministic routing control, supported by configuration-level enhancements and modified performance expressions.

a) Security-Enhanced VRRP (sVRRP)

Innovation: Restriction of VRRP control-plane traffic using ACLs and interface-level filtering.

Configuration Steps (Cisco CLI):

access-list 10 permit 192.168.100.1
access-list 10 permit 192.168.100.2
access-list 10 deny any
interface Fa1/0
ip access-group 10 in
interface Fa1/0
vrrp 22 ip 192.168.100.254
vrrp 22 authentication text VRRP_SECURE

Remark: The configuration filters unauthorized VRRP advertisements (multicast 224.0.0.18), ensuring only trusted routers participate.

Modified Security Expression:

$$S = \frac{R_{auth}}{R_{total}}$$

Where:

R_{auth}= authorized VRRP routers

R_{total}= total detected VRRP participants

$\rightarrow S \rightarrow 1$ indicates secure routing domain

b) Optimized Failover Mechanism (Zero-Loss Transition)

Innovation: Fine-tuning of VRRP timers and pre-emption to minimize convergence delay.

Configuration Steps:

interface Fa1/0
vrrp 22 priority 120
vrrp 22 preempt
vrrp 22 timers advertise 1

Remark: Reduces failover latency and ensures rapid master election.

Modified Failover Equation:

$$T_f = T_{detect} + T_{advert} + T_{switch}$$

With optimization:

$$T_f \approx (3 \times T_{advert}) + \delta$$

Where:

T_{advert}= advertisement interval (1 s)

δ= processing delay

c) Dual-ISP Redundancy with Static Route Control

Innovation: Deterministic routing using static routes combined with VRRP gateway abstraction.

Configuration Steps:

ip route 0.0.0.0 0.0.0.0 172.16.1.6 ! Primary ISP
ip route 0.0.0.0 0.0.0.0 172.16.1.10 10 ! Backup ISP (higher AD)

Remark: Ensures controlled failover between ISPs without routing protocol overhead.

Throughput Stability Model:

$$TP_{eff} = TP_{base} \times (1 - PL)$$

Since:

$$PL = 0 \Rightarrow TP_{eff} \approx TP_{base}$$

d) VLAN-Aware VRRP Deployment

Innovation: VRRP applied across segmented VLANs with unified gateway abstraction.

Configuration Steps:

interface Fa1/0.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
vrrp 10 ip 192.168.10.254

Remark: Maintains logical isolation while providing redundancy per VLAN.

e) Reliability-Oriented Design Metric

Combined System Reliability Model:

$$R_{system} = 1 - (P_{R1} \times P_{R2})$$

Where:

P_{R1}, P_{R2}= failure probabilities of routers

→ Dual-router VRRP significantly reduces overall failure probability.

The innovation lies in tight integration of VRRP, ACL-based control-plane security, timer optimization, and deterministic routing, resulting in:

1) Reduced failover delay
2) Zero packet loss condition ($PL = 0$)
3) High routing integrity ($S \approx 1$)
4) Improved system reliability

5. Results

This section presents the performance evaluation of the proposed VRRP-based network under simulated failure conditions. The analysis focuses on key metrics including failover time, packet loss, network stability, and security effectiveness. These metrics are widely used to assess the efficiency of redundancy protocols and their ability to maintain continuous network service during fault scenarios.

The results provide quantitative and qualitative insights into the behaviour of the network during router failure and recovery, highlighting the effectiveness of the implemented VRRP configuration and integrated security mechanisms in ensuring high availability and reliable operation.

Table 2. VRRP Network Performance Results.

Metric	Value	Technical Indicator
Failover Time ($T_{(f)}$)	11 s	VRRP convergence delay (Master → Backup transition)
Packet Loss (PL)	0%	No packet drop during failover (ICMP-based measurement)
Network Stability	100% uptime	Continuous Layer 3 forwarding during failure event
Transition Efficiency	Seamless (0 disruption)	No routing loops, MAC flapping, or session reset
ARP Spoofing Resistance	Reduced	ACL-based ingress filtering applied
Routing Integrity	High	Authorized VRRP participation enforced

The results in Table 2 indicate that the VRRP configuration achieved stable failover with a convergence time of 11 seconds and zero packet loss, ensuring uninterrupted network service. Continuous forwarding during failure confirms high network stability, while seamless transition behaviour reflects efficient VRRP state management. Additionally, the application of ACLs improved security by reducing spoofing risks and enforcing controlled routing participation, thereby maintaining routing integrity.

6. Recommendation

Based on the experimental results, the deployment of enhanced VRRP is strongly recommended for enterprise network environments requiring high availability and fault tolerance. The integration of ACL-based security mechanisms with VRRP significantly strengthens control-plane protection by preventing unauthorized routing participation and mitigating spoofing attacks.

To further improve network performance and resilience, the following recommendations are proposed:

1) Adoption of Intelligent Redundancy Mechanisms: Incorporating AI-driven traffic analysis and decision-making systems can optimize failover processes and improve load distribution efficiency, as demonstrated by recent studies [22].
2) Application in IoT and Distributed Environments: VRRP-based redundancy should be extended to IoT-driven networks to enhance resilience and ensure continuous data availability in highly dynamic environments [7].
3) Integration with Multi-Layer Security Architectures: Combining VRRP with layered security frameworks, including intrusion detection systems and authentication protocols, can provide comprehensive protection against evolving network threats [15].
4) Scalability and Real-Time Optimization: Future implementations should focus on improving scalability through dynamic routing integration and real-time monitoring systems to enable faster convergence and adaptive network control.

In summary, while the enhanced VRRP configuration demonstrates significant improvements in reliability and security, further research is required to address scalability challenges and enable intelligent, real-time network optimization in large-scale deployments.

7. Conclusion

This study demonstrates that the enhanced VRRP configuration significantly improves network availability, minimizes downtime, and strengthens overall network security. By integrating redundancy mechanisms with dynamic load distribution and ACL-based access control, the proposed framework achieves reliable failover, zero packet loss, and improved routing integrity. The combination of dual-router architecture and secure VRRP implementation provides a scalable and efficient solution suitable for modern enterprise network environments.

Despite these improvements, certain limitations remain, particularly in terms of scalability and adaptability to highly dynamic network conditions. Therefore, future research should focus on:

1) AI-Driven VRRP Optimization: Leveraging machine learning techniques to enable intelligent failover decisions and adaptive load balancing.
2) Real-Time Anomaly Detection: Integrating monitoring and intrusion detection systems to identify and respond to network anomalies and security threats in real time.
3) IPv6-Based Enhancements: Extending the proposed model to support IPv6 networks, ensuring compatibility with next-generation Internet architectures.

In conclusion, the proposed approach provides a robust foundation for high-availability networking, while further advancements are required to achieve fully autonomous and scalable network resilience.

Abbreviations

VRRP	Virtual Router Redundancy Protocol
QoS	Quality of Service
FHRP	First Hop Redundancy Protocol
HSRP	Hot Standby Router Protocol
ISP	Internet Service Provider
IoT	Internet of Things
AI	Artificial Intelligence
sVRRP	Secure Virtual Router Redundancy Protocol
ACL	Access Control List
ACLs	Access Control Lists
VLAN	Virtual Local Area Network
IP	Internet Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
MAC	Media Access Control
SAVFTA	Secure Adaptive Vrrp Failover Test Algorithm
TP	Throughput
TP_eff	Effective Throughput
TP_base	Base Throughput
PL	Packet Loss
T（f） / Tf	Failover Time
T_detect	Detection Time
T_advert	Advertisement Time
T_switch	Switching Time
WLAN	Wireless Local Area Network
eNSP	Enterprise Network Simulation Platform
SDN	Software-defined Networking
OpenFlow-SDN	Openflow Software-defined Networking
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
IPv6	Internet Protocol Version 6
CLI	Command Line Interface
LAN	Local Area Network
AD	Administrative Distance
DNS	Domain Name System
PC	Personal Computer
VoIP	Voice Over Internet Protocol
ForCES	Forwarding and Control Element Separation

Author Contributions

Michael Chinyere Hannah: Funding acquisition, Methodology, Writing – original draft

Gloria Ngozi Ezeh: Investigation, Resources, Software

Chika Norah John: Validation, Visualization

Emmanuel Chukwudi Amadi: Conceptualization, Data curation, Formal Analysis, Project administration, Supervision. Writing – review & editing

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] D. I. Mudhoep, Linawati, and Oka Saputra, “Kombinasi Protokol Routing OSPF dan BGP dengan VRRP, HSRP, dan GLBP,” Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 10, no. 1, 2021, https://doi.org/10.22146/jnteti.v10i1.942

[2] Ramdhani Syahputra, Romi Mulyadi, Muhamad Yusuf, Yogi Pratama, and Adri Yanto, “Analisis Dan Implementasi Perbandingan Protokol VRRP Dan HSRP Pada Jaringan Topologi Star,” Jurnal Penelitian Rumpun Ilmu Teknik, vol. 3, no. 1, 2024, https://doi.org/10.55606/juprit.v3i1.3397

[3] W. Wang, P. Dong, W. Qiao, Y. Zhang, C. Yu, and H. Zhang, “MultiS-IDRM: An Intelligent Disaster Recovery Mechanism for Multi-interface Server in Emergency Communication Systems,” IEEE Trans. Veh. Technol., 2025, https://doi.org/10.1109/TVT.2025.3597465

[4] O. Afolalu and M. S. Tsoeu, “Enterprise Networking Optimization: A Review of Challenges, Solutions, and Technological Interventions,” 2025. https://doi.org/10.3390/fi17040133

[5] M. Neagu, C. M. Serban, A. Hangan, and G. Sebestyen, “Digital Twins at the Edge: A High-Availability Framework for Resilient Data Processing in IoT Sensor Networks,” Future Internet, vol. 18, no. 3, p. 137, Mar. 2026, https://doi.org/10.3390/fi18030137

[6] N. Mohammadi Koushki, I. El-Shekeil, and K. Kant, “ConfExp: Root-Cause Analysis of Service Misconfigurations in Enterprise Systems,” Journal of Network and Systems Management, vol. 33, no. 2, p. 27, Apr. 2025, https://doi.org/10.1007/s10922-024-09886-w

[7] K. Shahid, S. N. Ahmad, and S. T. H. Rizvi, "Optimizing Network Performance: A Comparative Analysis of EIGRP, OSPF, and BGP in IPv6-Based Load-Sharing and Link-Failover Systems," Future Internet, vol. 16, no. 9, p. 339, Sep. 2024, https://doi.org/10.3390/fi16090339

[8] W. Wang et al., "Multi-ID2R: An Intelligent Device Disaster Recovery Mechanism in Multipath Scenarios," in Proceedings - IEEE Global Communications Conference, GLOBECOM, 2024. https://doi.org/10.1109/GLOBECOM52923.2024.10901218

[9] B. Isyaku, K. B. A. Bakar, F. A. Ghaleb, and A. Al-Nahari, "Dynamic Routing and Failure Recovery Approaches for Efficient Resource Utilization in OpenFlow-SDN: A Survey," IEEE Access, vol. 10, 2022, https://doi.org/10.1109/ACCESS.2022.3222849

[10] R. F. Ghani and L. Al-Jobouri, "Packet Loss Optimization in Router Forwarding Tasks Based on the Particle Swarm Algorithm," Electronics (Basel)., vol. 12, no. 2, p. 462, Jan. 2023, https://doi.org/10.3390/electronics12020462

[11] Y. Ai, Y. Zhu, Y. Jiang, and Y. Deng, "MIGS: A Modular Edge Gateway with Instance-Based Isolation for Heterogeneous Industrial IoT Interoperability," Sensors, vol. 26, no. 1, p. 314, Jan. 2026, https://doi.org/10.3390/s26010314

[12] U. Usanto, L. Nurlaela, and P. Purwono, "PENERAPAN METODE VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP) PADA YAYASAN MASJID AL IKHLAS," JEIS: JURNAL ELEKTRO DAN INFORMATIKA SWADHARMA, vol. 2, no. 1, 2022, https://doi.org/10.56486/jeis.vol2no1.181

[13] Nuredin Ahmed, "Performance Analysis of Floating Static Routes for Redundancy in Multi-Router Networks," AlQalam Journal of Medical and Applied Sciences, 2025, https://doi.org/10.54361/ajmas.2584127

[14] C. Liu, W. Shen, W. Lyu, X. Xu, and X. Ling, "A Study on network architectures and security for small and medium-sized enterprises," in Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence, New York, NY, USA: ACM, Sep. 2025, pp. 1514–1519. https://doi.org/10.1145/3773365.3773603

[15] J. Cui, W. Huang, R. Chen, Y. Liu, J. Cao, and S. Liu, "The simulation design of enterprise integration network scenario," Journal of Computational Methods in Sciences and Engineering, vol. 25, no. 1, pp. 526–547, Jan. 2025, https://doi.org/10.1177/14727978251323227

[16] X. Zhou, S. Mao, and M. Li, "A novel anti-noise fault diagnosis approach for rolling bearings based on convolutional neural network fusing frequency domain feature matching algorithm," Sensors, vol. 21, no. 16, 2021, https://doi.org/10.3390/s21165532

[17] I. Chaidir and R. Al Rino, "Implementasi Backup Router Trouble Dengan Metode Virtual Router Redundancy Protocol (VRRP) Pada DISKOMINFO Depok," Jurnal Ilmu Pengetahuan Dan Teknologi Komputer, vol. 4, no. 2, 2019.

[18] Ramdhani Syahputra, Romi Mulyadi, Muhamad Yusuf, Yogi Pratama, and Adri Yanto, "Analysis and Implementation of VRRP and HSRP Protocol Comparison on Star Topology Network [in Indonesian]," Jurnal Penelitian Rumpun Ilmu Teknik, vol. 3, no. 1, 2024.

[19] X. Wu and L. Dong, "Research and design of the pseudo-VRRP based high availability mechanism in the ForCES router," in Proceedings of the 8th International Conference on Networks, ICN 2009, 2009. https://doi.org/10.1109/ICN.2009.49

[20] R. Rajalingam and K. Kavitha, "A Multi-hop Routing Protocol in Wireless Sensor Networks Using Graph-Based Cat Salp Swarm Algorithm," in Lecture Notes in Networks and Systems, 2025. https://doi.org/10.1007/978-981-97-5786-2_10

[21] A. S. Saini, P. Gupta, and H. Gupta, "Implementation of Secured Wired and WLAN Network Using eNSP," in Lecture Notes in Electrical Engineering, 2021. https://doi.org/10.1007/978-981-15-9938-5_54

[22] K. R. Memon and B. Ghani, "The relationship between performance appraisal system and employees' voice behavior through the mediation-moderation mechanism," South Asian Journal of Business Studies, vol. 12, no. 2, 2023, https://doi.org/10.1108/SAJBS-01-2020-0012