Alqalam Journal of Medical and Applied Sciences. 2025;8(4):2967-2973
https://doi.org/10.54361/ajmas.2584128

Original article

Design and Implementation of a Virtual University Network Using the Hot Standby Router Protocol

Abdulsalam Ramah[1]*, Nuredin Ahmed [2]

[1]*Libyan Academy for Graduate Studies, Janzour, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
Corresponding Email. *absiramah@gmail.com*

Abstract
With the increasing reliance on campus networks to support educational activities, the need for solutions that ensure the availability and continuity of operation has become critical. Traditional networks face the challenge of service outages when the primary virtual gateway fails, resulting in user connectivity disruptions and impacting operational reliability. Hot Standby Routing Protocol (HSRP), a first-generation hopping routing protocol, provides an effective mechanism to mitigate these failures by establishing a shared virtual gateway across multiple routers. This study aimed to design and implement a virtual campus network using HSRP and test its performance in a Cisco Packet Tracer environment. A model was built with two primary routers, four switches, and multiple endpoints, with Preemption and Interface Tracking enabled to ensure seamless transitions during failures. The model was tested in a Packet Tracer environment using various scenarios, including primary router failure, backup router failure, network interface failure, and link failure. Performance was evaluated based on convergence time, latency, packet loss, and throughput. The results showed that HSRP automatically restores service within a few seconds with minimal packet loss and a temporary spike in latency. The results confirm the effectiveness of the protocol in enhancing reliability, noting that the study is limited by simulation and a small dataset.
Keywords. Hot Standby Router Protocol, Gateway Redundancy, High Availability, Campus Network.

Introduction

In modern campus environments, continuous network connectivity is essential to support both academic and administrative activities. Learning management systems, online educational platforms, administrative services, and digital communication tools all depend on uninterrupted network access. As a result, any network outage can significantly disrupt educational processes and institutional operations. This study aims to mitigate the impact of network outages on campus networks through the design and implementation of a high-availability system based on the Hot Standby Router Protocol (HSRP), which provides an effective mechanism for maintaining service continuity in the event of router failure (1). Many campus networks traditionally rely on a static virtual gateway to route traffic between internal and external networks. This approach represents a critical point of failure: if the primary router becomes unavailable, network services may be partially or completely disrupted unless redundancy mechanisms such as HSRP are deployed. Such outages directly affect network availability and can interrupt essential academic and administrative functions.

HSRP is one of the earliest First Hop Redundancy Protocols (FHRPs) developed by Cisco to enhance the availability of gateway services in IP networks. The protocol operates by assigning a shared virtual IP address and virtual MAC address to a group of routers, allowing them to appear as a single default gateway to end devices. When the active router fails, a standby router immediately assumes the forwarding role, ensuring that users experience minimal or no noticeable disruption in connectivity (4). To achieve this level of resilience, HSRP employs several technical mechanisms, including router priority values ranging from 0 to 255 (with a default value of 100), Hello and Hold timers for status monitoring, and the use of predefined virtual MAC addresses. In addition, HSRP supports advanced features such as Preemption, which allows a higher-priority router to reclaim the active role once it recovers, and Interface Tracking, which dynamically adjusts router priority when critical interfaces fail. The protocol also supports Multigroup HSRP (MHSRP) to enable load sharing and improved performance in local area networks (5)(6)(7). When compared with other FHRP solutions, such as Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP), HSRP demonstrates distinct operational characteristics. VRRP, as a vendor-independent standard, provides similar gateway redundancy but relies on a different master election process and virtual MAC addressing scheme. GLBP extends redundancy by enabling traffic load distribution across multiple active routers, offering improved resource utilization in suitable environments. These differences highlight the flexibility available to network designers when selecting redundancy solutions that align with specific network requirements (8).

Related work has demonstrated the effectiveness of redundancy protocols, particularly HSRP, in reducing recovery time, packet loss, and service disruption during network failures. Several studies have shown that HSRP can outperform VRRP in metrics such as failover time and packet loss, especially during peak network usage (9)(10)(11)(12). Other research emphasizes the importance of multiple paths, backup links, and

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

integration with dynamic routing protocols such as OSPF to further enhance network resilience and availability (12)(14).

Despite these contributions, relatively few studies have examined advanced HSRP features—such as preemption and interface tracking—within realistic campus network scenarios, particularly in simulated learning environments. This gap underscores the need for practical, scenario-based evaluations. Accordingly, this study focuses on designing and testing a campus network model using Packet Tracer to assess the effectiveness of HSRP under various failure conditions. In light of this research gap, this study focuses on the design and implementation of a virtual campus network using Packet Tracer to evaluate the effectiveness of HSRP under multiple failure conditions. The work aims to assess how HSRP contributes to maintaining connectivity following router failures, to analyze its performance in terms of recovery time, packet loss, and service availability, and to demonstrate its advantages over traditional static gateway configurations commonly deployed in educational institutions. By conducting scenario-based testing that incorporates advanced HSRP mechanisms, this study provides a practical and systematic evaluation of HSRP suitability for modern campus network environments.

Methodology

This paper focuses on an experimental methodology aimed at analyzing the effectiveness of the Hot Standby Redundancy Router Protocol (HSRP) in enhancing the reliability of higher education networks. The methodology is structured in five phases, as illustrated in (Figure 1).

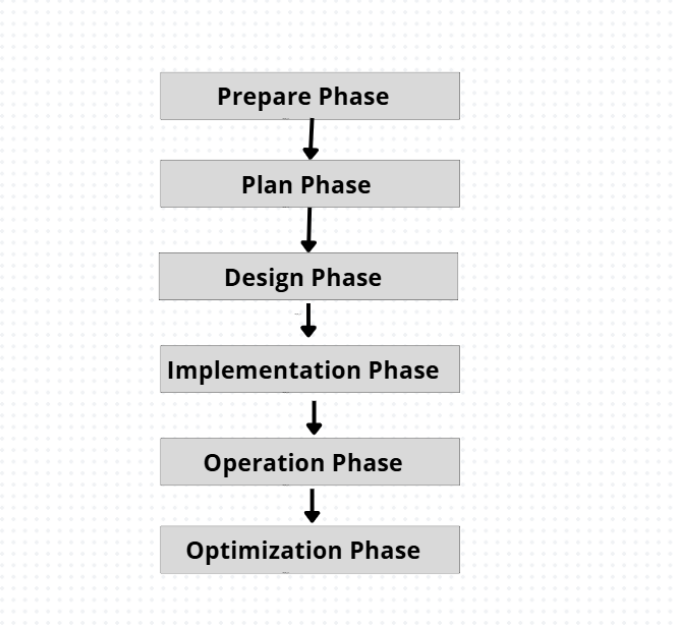

Figure 1. System Design Flowchart

Prepare Phase

During the preparation phase of campus network design, there are several sub-stages or activities that can be considered. These activities involve identifying the specific needs of different departments or student groups, such as data transfer rates, application requirements, security considerations, and scalability. Furthermore, this stage has developed a campus design plan that creates a detailed outline of the timeline, milestones, resource allocation, and responsibilities for each phase of the next design and implementation process.

Plan Phase

The planning phase has several sub-stages or activities that can be considered. One of them is gathering network requirements. This activity involves understanding the expected network capacity, desired performance, security requirements, and scalability. It also considers network topology design. It is also related to IP addressing and subnetting, and quality of service (QoS). Furthermore, it is related to the redundancy and high availability. Finally, it deals with the network management design, which means the development of the network monitoring, configuration, and troubleshooting of the campus network.

Design Phase

The design phase focuses on the logical structure of the campus network, emphasizing the architecture and addressing system while ensuring that the selection of network devices aligns with the specific requirements and objectives of the institution. Security considerations are integrated into a comprehensive framework that incorporates the Hot Standby Router Protocol (HSRP) to guarantee automatic redundancy and service continuity in the event of a primary router failure, thereby enabling seamless transition to the backup router

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

without interruption. The configuration includes router prioritization, the activation of Preemption to allow the primary router to reclaim its role once it recovers, and the use of Interface Tracking to monitor the status of external links and dynamically adjust priority in case of failure. This design approach is particularly suitable for campus environments that demand stable and reliable connectivity, as HSRP minimizes latency and packet loss during failures and enhances overall network performance under dynamic operating conditions.

Implementation Phase

The implementation phase includes preparing the university network infrastructure, starting with device installation, cable connections, and ensuring proper electrical and environmental conditions. This is followed by logical configuration, which includes IP address allocation, VLAN configuration, and applying the HSRP protocol to the distribution routers to ensure automatic redundancy. Device priorities are configured, and Preemption and Interface Tracking are enabled to guarantee seamless transitions in case of failures, thus ensuring service continuity and stable connectivity across the university campus.

Operation Phase

The operational phase of campus network design includes network monitoring and management to ensure service continuity and reliability. This phase involves implementing network monitoring tools, such as the Simple Network Management Protocol (SNMP), to continuously track network performance, availability, and security, with a focus on the effectiveness of the HSRP protocol in mitigating the impact of outages and improving response times. Capacity planning is also included through monitoring network resource usage and forecasting future needs. Furthermore, data traffic trends are analyzed, and performance reports are generated to evaluate availability and security indicators, ensuring uninterrupted support for academic and administrative operations.

Optimization Phase

The optimization phase of campus network design includes performance assessment of the current campus performance to detect required improvement. Evaluate factors such as network latency, throughput, packet loss, and application performance. It includes traffic analysis and capacity planning based on the traffic analysis and future growth. Where routing protocol optimization evaluates the efficiency and stability of routing protocols used in the campus network. These routing performance metrics such as convergence time, load balancing, and route summarization. Furthermore, network device firmware and software updates impact on campus performance. Therefore, scheduled software and platform updates should be considered.

Implementation And Results

The proposed design was implemented using the HSRP protocol on distribution routers in the campus network to evaluate its effectiveness in handling failures and achieving automatic redundancy. The system was tested under simulated primary route failure conditions, and successful control transfer to the backup router was verified. Commands such as `show standby` and `ping` were used from user devices to verify connectivity continuity.

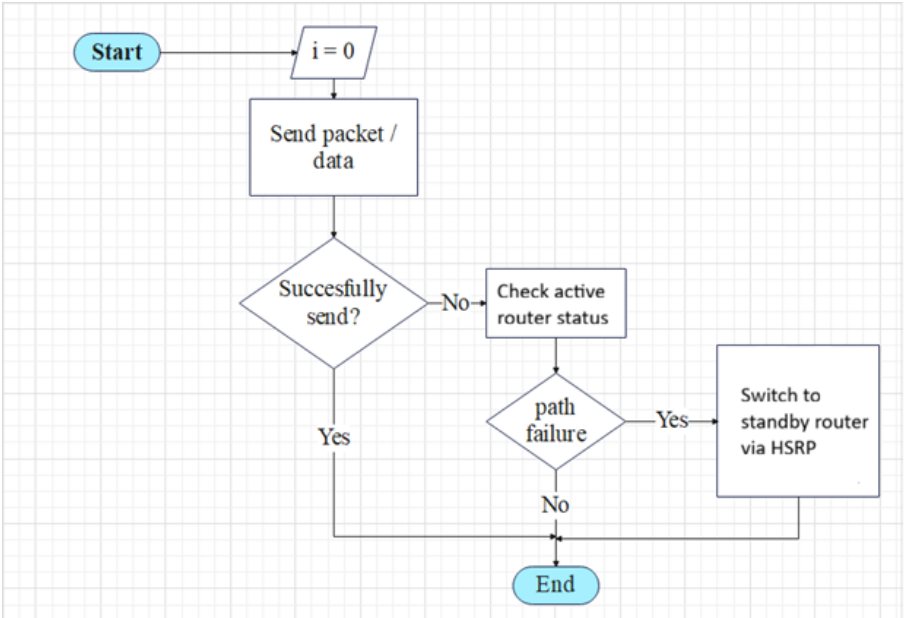

Figure 2. Transmission path and backup path flow diagram in a campus network using HSRP Topology Configuration and Setup

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

Figure 3 illustrates the configuration of servers, computers, routers, and switches within the campus network. This diagram provides a comprehensive visual representation of the network architecture, including the distribution of devices across multiple subnets and the communication paths that ensure efficient data transmission and continuous connectivity between the various components.

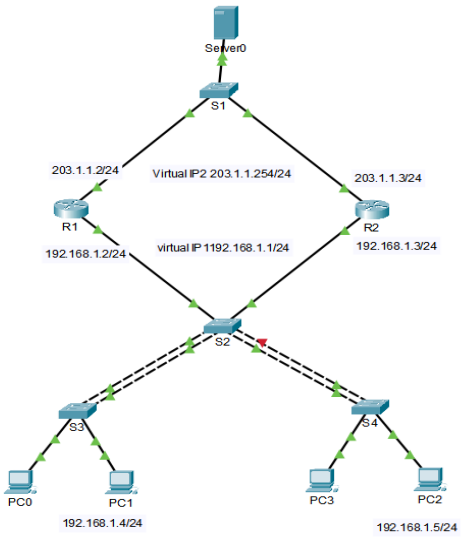

Figure 3. Proposed HSRP-based network topology for a university campus

HSRP Configuration

In the proposed campus network topology, HSRP was configured on routers R1 and R2 to create a shared virtual gateway. The default IP addresses were assigned as follows: 203.1.1.254/24 for the external network and 192.168.1.1/24 for the internal network. Router R1 was designated as the active router by prioritizing IP addresses 203.1.1.2/24 and 192.168.1.2/24 on its interfaces. Router R2 was configured as the backup router, using IP addresses 203.1.1.3/24 and 192.168.1.3/24. The HSRP configuration ensures that data traffic is automatically rerouted to the backup router in case the active router fails, without manual intervention, thus guaranteeing seamless connectivity.

Testing Procedures

After configuring the network and enabling HSRP on routers R1 and R2, a series of test scenarios were conducted to assess the system's capacity to manage connectivity disruptions. The HSRP configuration was established with a Group ID of 10, applied to both the internal and external network segments. Router R1 was assigned a priority value of 120 to function as the active router, while Router R2 was configured with a priority of 100 to operate in standby mode. The default welcome timer of three seconds was used to transmit periodic HSRP messages, and the default wait timer of ten seconds was maintained to detect the failure of the active router. Preemption was enabled on both routers with a five-second delay to ensure that each device completed its configuration before assuming the active role. Interface tracking was applied to critical interfaces so that a reduction in priority would occur automatically in the event of an interface failure, thereby allowing the more reliable router to assume control.

A shared virtual gateway was configured using the IP address 203.1.1.254/24 for the external network and 192.168.1.1/24 for the internal network. All terminal devices depended on this virtual gateway to maintain network access

Fault Scenarios

To assess the resilience of the HSRP configuration, several fault scenarios were executed to evaluate the protocol's response to different types of failures. When the primary router (R1) was powered down or disconnected, HSRP immediately transferred control to the standby router (R2), allowing all terminals to maintain uninterrupted connectivity. In the case of a backup router (R2) failure, the network continued to operate normally under the active router, demonstrating that service availability was preserved until the standby device was restored. Simulated interface failures were introduced by administratively disabling critical interfaces on either router. The interface-tracking mechanism automatically reduced the priority of the affected router, enabling a smooth transition of the active role to the more reliable device. Similarly, intentional disconnection of the physical link between either router and the network triggered an automatic rerouting of traffic through the remaining operational router, ensuring overall network stability. Throughout all scenarios, terminal commands such as "show standby" and "ping" were used to observe the status of the virtual gateway and confirm continuous service availability. The results demonstrated that the HSRP configuration—supported by appropriate group identifiers, priority settings, timer values, and preemption delays—provided effective failover performance and sustained connectivity across the campus network.

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

https://doi.org/10.54361/ajmas.2584128

Results

This section presents the results obtained after implementing, responding to, and activating the network using the HSRP protocol within the Packet Tracer environment. The system's ability to ensure operational continuity was tested under three different types of network failures: complete router R1 shutdown, interface R1 shutdown, and physical cable disconnection from R1. All tests involved sending 10,000 packet pings from a terminal (PC0) to the virtual gateway 192.168.1.1, to measure latency, loss, and throughput before, during, and after each failure. Router R1 was configured as the active router using addresses 203.1.1.2/24 for the external network and 192.168.1.2/24 for the internal network, while R2 was configured as a backup router using addresses 203.1.1.3/24 and 192.168.1.3/24. A shared virtual gateway was allocated using addresses 203.1.1.254/24 and 192.168.1.1/24, allowing endpoints to access the network.

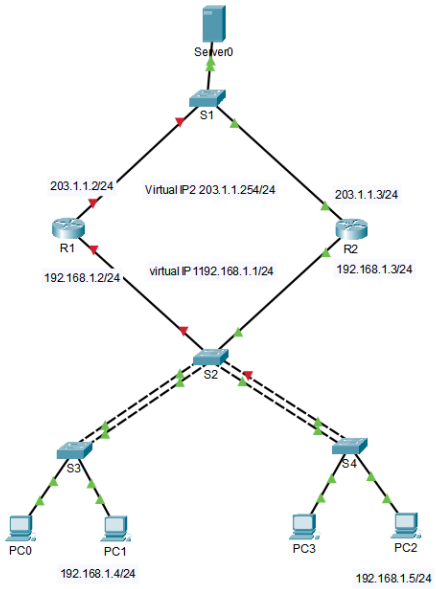

Figure 4. The automatic switching process is explained when the R1 router fails

Scenario 1: Router R1 Completely Disabled

In the first test, Router R1 was manually powered off. The result was a very limited packet loss of only two packets, after which control immediately transferred to Router R2 as the active router. The trial package showed that the impact of disabling the router was very limited, as the switch to R2 was automatically completed within fractions of a second, thanks to the HSRP settings. The performance drop during the failure was temporary, and the system returned to normal upon restarting R1.

Table 1. Network Performance Before, During, and After Router (R1) Disabled

SN.	Meter	Before failure	During failure	After conversion
1	Number of packets sent	10000	10000	10000
2	Number of packets received	10000	9998	9999
3	Number of packets lost	0	2	1
4	Loss percentage (%)	0%	0.02%	0.01%
5	Average response time (ms)	1ms>	9ms	1ms>
6	Transmission rate (kbps)	130	118	130

Scenario Two: Disabling Interface R1 (Interface Shutdown)

In this scenario, the command was executed on Router R1 to administratively disable the interface g0/0 using the shutdown instruction. This type of failure typically produces a shorter failover duration, as the Hot Standby Router Protocol (HSRP) detects the interface-down condition directly through Layer 2 signaling. This test showed a more stable result than the first scenario, with the network losing only one packet during the switch to R2 and only one packet when R1 returned to service. This high level of responsiveness is attributed to HSRP's ability to detect interface failures directly across Layer 2, unlike router downtime, which takes slightly longer to detect.

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

Table 2. Network performance when the interface is disabled

SN.	Meter	Before failure	During failure	After conversion
1	Number of packets sent	10000	10000	10000
2	Number of packets received	10000	9999	9999
3	Number of packets lost	0	1	1
4	Loss percentage (%)	0%	0.01%	0.01%
5	Average response time (ms)	1ms>	5ms	1ms>
6	Transmission rate (kbps)	130	122	130

Scenario 3: Physical Cable Disconnection from R1

Cable disconnection represents one of the most realistic failure scenarios in a campus environment, reflecting the potential for human error or a physical break in the medium. The results of this scenario are almost identical to the router failure scenario, where the network lost only two packets out of 10,000. This behavior is expected because disconnecting the cable results in an immediate loss of connectivity, allowing HSRP to switch to the backup router at high speed.

Table 3. Network performance during physical cable disconnection

SN.	Meter	Before failure	During failure	After conversion
1	Number of packets sent	10000	10000	10000
2	Number of packets received	10000	9998	10000
3	Number of packets lost	0	2	0
4	Loss percentage (%)	0%	0.02%	0%
5	Average response time (ms)	1ms>	8ms	1ms>
6	Transmission rate (kbps)	130	118	130

Discussion

The practical results confirm that the HSRP protocol is a highly effective mechanism for ensuring operational continuity in university networks. Its ability to switch seamlessly between routers with negligible packet loss, not exceeding 0.02%, makes it suitable for environments that demand high stability such as smart classrooms, registration systems, and sensitive academic services. The experiments revealed several consistent characteristics that enhance the effectiveness of HSRP in educational settings. Failure times were extremely low, with packet loss limited to one or two packets in the worst-case scenario, indicating an almost instantaneous response. Once Router R1 was restored, it resumed its role as the active router and network performance returned to its original level without manual intervention, demonstrating the stability of the recovery phase. Slight variations were observed between failure types, with router shutdown producing slightly higher loss compared to interface or cable disconnection, which corresponds to the nature of Layer 2 and Layer 3 failure detection. The accuracy of the measurements is reinforced by the use of 10,000 ICMP packets per test, providing statistical credibility to the evaluation process.

Despite these promising results, several methodological limitations must be acknowledged. All tests were conducted within the Cisco Packet Tracer simulation environment, which does not fully reflect the performance of real networks in terms of processing time, protocol behavior, or hardware response during sudden failures. Although a relatively large test sample was used, the scope remains limited compared to real-world campus traffic involving multiple simultaneous flows and diverse user loads. Furthermore, the study focused only on three types of failures—router shutdown, interface failure, and cable disconnection—while real networks may experience more complex issues such as routing table collapse or CPU congestion. The simulation environment itself also imposes constraints, including limited tuning options and the absence of physical influences such as cable quality or device performance. Future research should therefore complement these findings by conducting experiments with physical routers or within professional laboratory environments to enhance the reliability and generalizability of the results.

Conclusion

This study demonstrates how to enhance network resilience in educational institutions using the High-Speed Routing Protocol (HSRP). It proves its effectiveness in various scenarios and the protocol's ability to maintain quality of service without manual intervention. The primary router automatically returns to its active role, and the experiment showed stable operational characteristics at performance levels close to its original state. The study provides network administrators with reliable options to ensure business continuity in the event of network outages. These results underscore the importance of network continuity in maintaining administrative and academic processes. The knowledge gained from this study will be valuable

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*

in future discussions on improving data security procedures in educational environments. Network resilience methods must be continuously improved and adapted to technological advancements.

Conflict of interest. Nil

References

1. Chandra VN, Kumar K. QoS improvement in AOMDV through backup and stable path routing. In: Proceedings of the 2015 International Conference on Communication Systems and Network Technologies (CSNT). IEEE; 2015. doi:10.1109/CSNT.2015.128.
2. Cisco Systems, Inc. Understanding the features and functions of the Hot Standby Router Protocol (HSRP). Cisco Technical Documentation. 2023 [cited 2025 Dec 29]. Available from: https://www.cisco.com
3. Rahman Mohamed HA. A proposed model for IT disaster recovery plan. Int J Mod Educ Comput Sci. 2014;6(4):57-67. doi:10.5815/ijmecs.2014.04.08.
4. Patel A. Comparing top redundant switching protocols: HSRP, VRRP, and GLBP. NetSecCloud. 2024 [cited 2025 Dec 29]. Available from: https://netseccloud.com/comparing-top-redundant-switching-protocols-hsrp-vrrp-and-glbp
5. NetworkLessons.com. . HSRP (Hot Standby Router Protocol): configuration, timers, and interface tracking. 2024 [cited 2025 Dec 29]. Available from: https://networklessons.com/ip-services/hsrp-hot-standby-routing-protocol
6. Simanjuntak IUV, Haidi J, Heryanto, Silalahi LM. Simulation and performance analysis of network backup systems using Hot Standby Router Protocol (HSRP) method on real-time networks. Int J Electron Telecommun. 2023;69(4). doi:10.24425/ijet.2023.147698.
7. Yahya MS, Bongsu RHR. UNISZA campus network: backup using HSRP and OSPF in Packet Tracer. Malays J Comput Appl Math. 2024;7(2):1-15. doi:10.37231/myjcam.2024.7.2.124.
8. Odom W. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Cisco Press; 2015.
9. GeeksforGeeks. HSRP vs VRRP vs GLBP protocols. 2025 [cited 2025 Dec 29]. Available from: https://www.geeksforgeeks.org/computer-networks/hsrp-vs-vrrp-vs-glbp-protocols/
10. Mansour M, Ghneimat A, Alasem R, Jarray F. Performance analysis and functionality comparison of first hop redundancy protocols. J Ubiquitous Syst Pervasive Netw. 2021;15(1):49-58.
11. Mahmud M. Performance evaluation of bidirectional forwarding detection (BFD) over the Virtual Router Redundancy Protocol (VRRP). ResearchGate. 2024 [cited 2025 Dec 29]. Available from: https://www.researchgate.net/publication/385977931
12. IT-Solutions Center. Redundancy concepts and the differences between HSRP, VRRP, and GLBP. 2024 [cited 2025 Dec 29]. Available from: https://it-solutions.center
13. Firmansyah MWR, Rachman P. Analisis perbandingan kinerja jaringan Cisco Virtual Router Redundancy Protocol (VRRP) dan Cisco Hot Standby Router Protocol (HSRP). Repository Universitas Bina Sarana Informatika. 2018:764-769.
14. Sengupta S, Annervaz KM. Multi-site data distribution for disaster recovery—a planning framework. Future Gener Comput Syst. 2014;41:53-64. doi:10.1016/j.future.2014.07.007.

Received*: 25-10-2025 -* ***Accepted****: 22-12-2025 -* ***Published****: 29-12-2025*