

Implementation Analysis of Network Core Redundancy Using HSRP and VRRP Protocols for Enterprise Infrastructure Reliability Assurance

Tengku Firdaus Syah ^{a*}, Sopan Adriyanto ^b

^{a*,b} Informatics Engineering Study Program, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, East Jakarta City, Special Capital Region of Jakarta, Indonesia.

ABSTRACT

This study examines the role of redundancy protocols in enhancing the reliability of core networks within enterprise infrastructures. The research is motivated by the growing reliance of organizations on network-based services and the increasing risks of financial losses caused by downtime, which are projected to escalate alongside global traffic growth. A simulation-based approach was conducted using Cisco Packet Tracer to compare baseline networks without redundancy against implementations of Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP). The evaluation focused on key performance indicators, including failover time, uptime rate, packet loss, latency, and jitter. The results demonstrate that both protocols successfully provided automatic recovery mechanisms, achieving an average failover time of less than five seconds while maintaining stable connectivity. Further analysis revealed that HSRP excels in failover speed, whereas VRRP offers cross-vendor flexibility with consistent stability. These findings confirm that redundancy protocol selection should align with specific network requirements, yet both HSRP and VRRP have proven effective in minimizing downtime risks and ensuring service continuity in enterprise-scale environments.

ARTICLE HISTORY

Received 19 July 2025
Accepted 25 August 2025
Published 30 November 2025

KEYWORDS

HSRP; VRRP; Network Redundancy; Failover; Enterprise.

1. Introduction

In the digital era, computer networks have become the foundation of organizational and corporate operations. Nearly all business activities—ranging from internal communication to data-driven services and cloud-based applications—are highly dependent on stable and reliable infrastructures. However, vulnerabilities such as device failures, link disruptions, and anomalies in the *core network* often lead to downtime, which results in both productivity loss and substantial financial damage. The *Cisco Annual Internet Report (2023)* projects that global network traffic will triple by 2025, with the enterprise sector accounting for approximately 65% of the overall load. This forecast underscores the pivotal role of computer networks in sustaining contemporary business ecosystems. Complementing this perspective, the *Uptime Institute (2023)* reported that organizations, on average, face five to seven major network incidents annually, with 43% of failures originating from *core network* devices. The mean recovery time per incident is 3.7 hours, and financial losses are estimated between USD 150,000 and 450,000 for each hour of downtime. In Indonesia, the situation is equally concerning. A survey conducted by IDC (2023) on 100 large

enterprises revealed that 68% of organizations do not yet have an adequate redundancy strategy to maintain continuous service availability.

To address these risks, redundancy protocols are essential to ensure service continuity even when the primary device encounters a failure. Previous studies have highlighted the importance of *Hot Standby Router Protocol* (HSRP) and *Virtual Router Redundancy Protocol* (VRRP) in implementing *failover gateways* at the core layer (Puspitasari *et al.*, 2020; Cahya & R. W., 2023; Syahputra *et al.*, 2024). HSRP, a Cisco proprietary protocol, designates one router as *active* while others remain in *standby* mode, ready to take over automatically in case of device failure (Haryoyudhanto *et al.*, 2020; Fadhilah *et al.*, 2020; Firmansyah, 2023). On the other hand, VRRP is an open standard that enables cross-vendor compatibility, operating with a mechanism similar to HSRP but with distinct terminology and configurations. Several studies have shown that VRRP can minimize packet loss and maintain stable connectivity during failover events (Prasetia & Soelistyo, 2023; Machdi, 2022). Comparative research has also examined HSRP and VRRP alongside the *Gateway Load Balancing Protocol* (GLBP), which distributes workload across multiple routers simultaneously, offering better throughput and resource utilization (Claudia & Rifqi, 2021; Dharma *et al.*, 2021; Surya *et al.*, 2019; Alaika & Santoso, 2024). These findings suggest that redundancy protocol selection is strongly influenced by specific network requirements: HSRP is often preferred when fast failover is prioritized, VRRP is more suitable for heterogeneous environments requiring vendor interoperability, while GLBP is advantageous for high-bandwidth services demanding load balancing.

Practical implementations further demonstrate the adaptability of redundancy protocols across various environments. For instance, the integration of HSRP within VLAN-based architectures has been proven to maintain service stability even during device outages (Rahman & Pamungkas, 2024; Hariadi, 2021). Other studies indicate that combining VRRP and HSRP with routing protocols such as OSPF and BGP enhances efficiency while mitigating the risk of connectivity loss (Mudhoep *et al.*, 2021). Moreover, redundancy mechanisms have been extended to both small-scale networks, such as *homestead* environments (Machdi, 2022), and enterprise-scale infrastructures, including large telecommunications providers (Syafrizal *et al.*, 2023). Recent work by Silalahi *et al.* (2025) highlights that integrating HSRP and VRRP into virtualized networks significantly increases service availability while reducing downtime risks. Against this backdrop, the present study focuses on evaluating the implementation of HSRP and VRRP to establish redundancy within enterprise core networks. The analysis emphasizes failover time, configuration complexity, device compatibility, and network stability. By examining the practical performance of both protocols, this study aims to provide network architects and system designers with actionable insights in selecting the most suitable redundancy protocol to ensure resilience, stability, and service continuity in modern enterprise infrastructures.

2. Methodology

This study employs a simulation-based approach using *Cisco Packet Tracer* to model a network topology that reflects enterprise infrastructure. At the initial stage, a baseline network was designed with routers and switches configured without redundancy. The design was then extended by implementing two redundancy protocols, namely *Hot Standby Router Protocol* (HSRP) and *Virtual Router Redundancy Protocol* (VRRP), to assess their effectiveness in maintaining connectivity under failure conditions. Both protocols were configured on the core routers to test their reliability during device outages by deliberately disabling the active gateway and monitoring the failover mechanism. The evaluation focused on several performance indicators, including

failover time, network uptime before and after redundancy implementation, the number of lost packets during transition, as well as other quality of service parameters such as latency and jitter. To ensure accuracy, connectivity tests were performed through continuous *ping* commands, *traceroute* verification, and interface inspections using commands such as *ifconfig* and *show interface*. The methodology also incorporated IPv6 tunneling tests to validate routing paths between users, ensuring that both normal operation and failover scenarios could be systematically examined.

The methodological design is consistent with earlier studies that emphasized the importance of simulation-based testing in evaluating redundancy mechanisms prior to real-world deployment (Fadhilah *et al.*, 2020; Haryoyudhanto *et al.*, 2020). For instance, Claudia & Rifqi (2021) and Alaika & Santoso (2024) demonstrated how comparative simulations of HSRP, VRRP, and *Gateway Load Balancing Protocol* (GLBP) under IPv6-based routing provided valuable insights into protocol behavior. Dharma *et al.* (2021) further highlighted that measuring parameters such as throughput and packet loss is crucial for assessing the suitability of redundancy protocols for multimedia traffic. In practical applications, Firmansyah (2023) and Hariadi (2021) tested HSRP under IPv6 environments with multi-group configurations, showing that simulation results strongly correlate with real-world scenarios. Similarly, Machdi (2022) and Prasetia & Soelistyo (2023) underscored that VRRP can be effectively evaluated in both small-scale and enterprise networks using simulation to determine stability during failover events. Moreover, Mudhoep *et al.* (2021) showed that combining redundancy protocols with dynamic routing protocols such as OSPF and BGP enhances network resilience and efficiency, thereby strengthening simulation outcomes. The research also emphasizes the importance of collecting numerical data and technical observations from simulation, including failover time, uptime percentages, packet loss, latency, and jitter. Such data serve as the basis for a comparative evaluation of HSRP and VRRP. This methodological perspective aligns with Silalahi *et al.* (2025), who emphasized that documenting protocol configurations and simulation results provides empirical evidence of redundancy effectiveness. In this way, the methodology adopted in this study not only offers a structured framework for evaluating redundancy performance but also strengthens academic contributions to the discourse on reliable network design within modern enterprise infrastructures.

3. Results

The results of this study demonstrate clear differences between network performance without redundancy and with redundancy protocols such as HSRP and VRRP. In the initial scenario, the configuration relied on a single core router as the primary *gateway*, as illustrated in Figure 2. Core Network Configuration Plan (Without Redundancy). Continuous *ping* and *traceroute* tests revealed that all traffic was dependent on a single device; when the core router was deactivated, connectivity was completely lost, as no automatic recovery mechanism was available. This finding highlights that a non-redundant topology exposes the network to significant risks of service interruption.

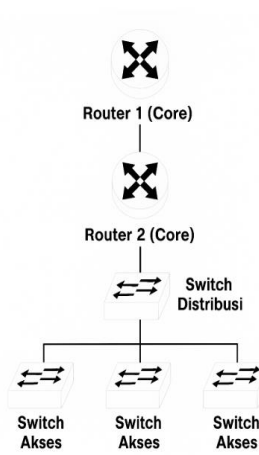


Figure 1. Topology Analysis

This diagram illustrates the hierarchical three-layer architecture adopted in the study, consisting of the core, distribution, and access layers. The core layer contained two routers acting as the central control and main traffic path. The distribution switch connected the core layer to three access switches, each linked to various end-user devices. The narrative of this figure emphasizes that the critical point of failure is located at the core layer, thus requiring redundancy mechanisms to ensure continuity.

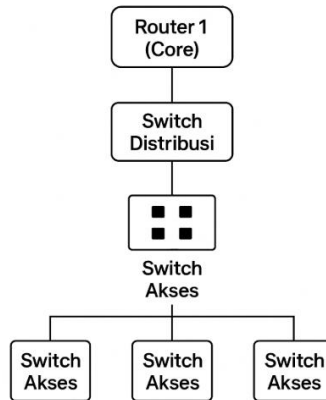


Figure 2. Core Network Configuration Plan (Without Redundancy)

The visualization depicts the initial configuration with a single core router serving as the only path to the external network. All end-user devices were configured to use this router as their default gateway. Test results showed that once the core router failed, all services stopped entirely, reaffirming the high dependency on a single device and the lack of resiliency in this setup.

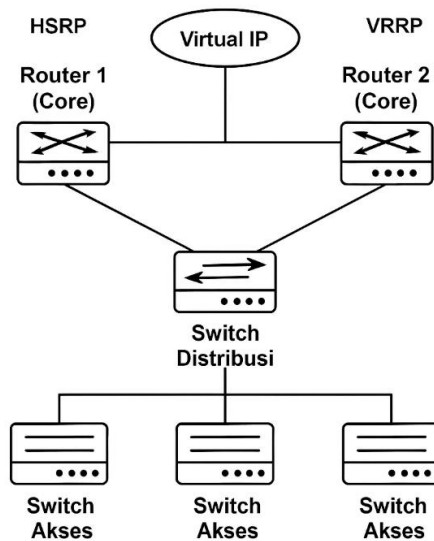


Figure 3. Configuration Plan with HSRP and VRRP

After redundancy mechanisms were introduced, two core routers were configured to share a single *virtual IP* address that all end-user devices used as their default gateway. In the HSRP configuration, one router was designated as the *active router* while the other operated in *standby* mode, ready to take over in case of failure. In the VRRP configuration, one router functioned as the *master* and the other as the *backup*. Test results revealed that when the active router was disabled, the backup router automatically assumed control within an average recovery time of less than 5 seconds. This seamless transition ensured that network services continued without noticeable disruption to users. Overall, the simulation results confirm that both HSRP and VRRP successfully provide an active backup path that significantly enhances the reliability of the core network, minimizes the risk of downtime, and ensures service continuity in enterprise infrastructure environments.

4. Discussion

The projected threefold increase in global network traffic by 2025, with the enterprise sector accounting for approximately 65% of the total load (Cisco, 2023), underscores the urgency of deploying robust redundancy mechanisms. This necessity becomes more critical considering the *Uptime Institute* (2023) reported that organizations experience an average of five to seven serious network incidents annually, with potential financial losses reaching hundreds of thousands of dollars per hour of downtime. In Indonesia, an IDC (2023) survey of 100 large enterprises revealed that 68% lacked adequate redundancy strategies, further exposing vulnerabilities to service disruption. In this context, redundancy protocols such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP) are essential to ensure continuous service availability. HSRP, a Cisco proprietary protocol, designates one router as the *active router* while others remain in *standby* mode, ready to take over in the event of failure. Multiple studies confirm that HSRP excels in failover speed and minimizes downtime, particularly in default configurations where fast failback is prioritized (Haryoyudhanto *et al.*, 2020; Fadhilah *et al.*, 2020; Cahya & R. W., 2023; Alaika & Santoso, 2024; Firmansyah, 2023). VRRP, in contrast, is an open standard protocol with similar

functionality, assigning one router as *master* and others as *backup*. Recent studies demonstrate that VRRP effectively reduces packet loss and maintains stable connectivity during failover events (Syahputra *et al.*, 2024; Prasetya & Soelistyo, 2023). Furthermore, VRRP has proven reliable in smaller-scale deployments such as homegrid networks (Machdi, 2022) and has shown significant improvements in availability when integrated with HSRP in virtualized infrastructures (Silalahi *et al.*, 2025). Meanwhile, GLBP provides a distinctive advantage by enabling load balancing across multiple routers, ensuring that all devices participate in forwarding traffic, thereby optimizing resource utilization (Claudia & Rifqi, 2021; Dharma *et al.*, 2021; Surya *et al.*, 2019). Research has shown that GLBP often outperforms in reducing packet loss and improving throughput, making it particularly suitable for bandwidth-intensive applications such as video streaming. Beyond protocol performance, some studies emphasize the importance of integrating redundancy with dynamic routing protocols like OSPF and BGP to further strengthen network resilience (Mudhoep *et al.*, 2021). In practice, HSRP has also been deployed in VLAN encapsulation and multi-group redundancy scenarios to maintain service stability (Hariadi, 2021; Rahman & Pamungkas, 2024), as well as in large-scale enterprises such as telecommunications environments to enhance server accessibility (Syafrizal *et al.*, 2023). Collectively, these findings suggest that protocol selection must be aligned with the specific requirements of the infrastructure: HSRP is well-suited for environments prioritizing rapid failover, VRRP is preferable when vendor interoperability and stable failover with minimal packet loss are essential, and GLBP offers the most efficient solution for load distribution and throughput optimization. Consequently, the present study reinforces existing literature by demonstrating that both HSRP and VRRP significantly mitigate downtime risks and ensure service continuity in enterprise-scale core network environments (Puspitasari *et al.*, 2020).

5. Conclusion

This study demonstrates that the implementation of redundancy protocols HSRP and VRRP significantly enhances the reliability of core networks by providing automatic failover mechanisms when the primary device experiences failure. The test results show that the average recovery time was less than five seconds, with a higher uptime rate compared to configurations without redundancy. In addition, packet loss, latency, and jitter were more controlled during the failover process, ensuring consistent connectivity quality. Configuration documentation on core devices highlights performance differences between the two protocols, where HSRP excels in failover speed while VRRP offers cross-vendor flexibility with consistent stability. Overall, the study concludes that the implementation of redundancy protocols not only reduces the risk of downtime and potential financial losses but also ensures service continuity within enterprise-scale network infrastructures.

References

- Alaika, I. A. A., & Santoso, B. (2024). *Analisis perbandingan QoS antara HSRP dengan GLBP pada routing EIGRP menggunakan IPv6*. Indonesia Journal of Computer Science.
- Cahaya, A. I., & Widiyari, I. R. (2023). Analisis perbandingan performansi metode HSRP dan VRRP sebagai backup link koneksi jaringan. *Progresif: Jurnal Ilmiah Komputer*, 19(1), 381. <https://doi.org/10.35889/progresif.v19i1.1180>

- Claudia, M., & Rifqi, M. (2021). Analisa perbandingan performansi Hot Standby Router Protocol (HSRP) dengan Gateway Load Balancing Protocol (GLBP) pada router spoke DMVPN. *Jurnal Media Informatika Budidarma*, 5(2), 504-512
- Dharma, I. P. G. K. Y., *et al.* (2021). Kinerja protokol network redundansi VRRP, HSRP dan GLBP pada layanan video streaming. *Jurnal Spektrum*, 8(2), pages not specified.
- Fadhilah, M. I., *et al.* (2020). Perancangan backup router dengan metode HSRP (Hot Standby Router Protocol). *Jurnal Teknokris*, 23(1), pages not specified.
- Firmansyah, M. (2023). Performa redundancy link Hot Standby Router Protocol IPv6 dengan routing EIGRP untuk IPv6. *Jurnal Sains dan Informatika*, 7(1), 58-66. <https://doi.org/10.34128/jsi.v7i1.297>
- Hariadi, F. (2021). Manual load balancing pada redundancy link menggunakan multi-group Hot Standby Router Protocol. *Jurnal Teknik Informatika dan Sistem*.
- Haryoyudhanto, H. D., *et al.* (2020). Implementasi encapsulation jaringan redundansi VLAN menggunakan metode Hot Standby Router Protocol (HSRP). *Journal of Information Technology and Computer Science*.
- Machdi, A. R. (2022). Analisa implementasi VRRP (Virtual Router Redundancy Protocol) berbasis Mikrotik pada jaringan homegrid. *Jurnal Teknik Majalah Ilmiah*.
- Mudhoep, D. I., *et al.* (2021). Kombinasi protokol routing OSPF dan BGP dengan VRRP, HSRP, dan GLBP. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 10(1), pages not specified.
- Prasetia, A. W., & Soelistyo, W. (2023). Perancangan backup-link menggunakan metode VRRP pada jaringan VLAN dalam penyediaan redundancy pada layer 3. *JUPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*.
- Puspitasari, A., *et al.* (2020). Protokol redundansi Hot Standby Router Protocol (HSRP) di PT Indonesia Power. *JIKA Universitas Muhammadiyah Tangerang*.
- Rahman, T., & Pamungkas, E. T. (2024). Optimalisasi jaringan komputer di SMK Travina Prima dengan implementasi inter VLAN, VLSM, dan HSRP. *IKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang*.
- Silalahi, E. K., *et al.* (2025). Implementasi dan analisis protokol HSRP dan VRRP dalam meningkatkan redundansi gateway pada jaringan virtual. *Jurnal Informatika dan Teknik Elektro Terapan*.
- Surya, I. G. M., *et al.* (2019). Performansi jaringan TCP/IP menggunakan metode VRRP, HSRP, dan GLBP. *Majalah Ilmiah Teknologi Elektro*.
- Syafrizal, M., *et al.* (2023). Load balancing dengan metode HSRP untuk meningkatkan akses layanan server PT Telekomunikasi Indonesia Tbk. *Jurnal Elektro & Informatika Swadharna (JEIS)*.
- Syahputra, R., *et al.* (2024). Analisis dan implementasi perbandingan protokol VRRP dan HSRP pada jaringan topologi star. *Jurnal Penelitian Rumpun Ilmu Teknik*.