VOL. 19, NO. 22, NOVEMBER 2024 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

REDUNDANCY PROTOCOLS PERFORMANCE ANALYSIS IN BUSINESS NETWORKS

Avula Divya Reddy, Namineni Sowmya and Ravikumar C. V.
School of Electronics Engineering, Vellore Institute of Technology, Vellore, India
E-Mail: divyaanivs@gmail.com

ABSTRACT

The network's ability to recover from failures is a crucial factor to think about while building the network's design. Service providers, operators, and manufacturers of networking hardware have all committed to meeting or exceeding an availability objective of 99.9999% ("6 nine" availability), which means that a network can experience interruption for no more than 360 seconds each year. Therefore, it is necessary to have two or more gateways connected in a network so that the remaining gateways can take over in the event of a gateway failure. Availability is usually considered the primary goal while constructing a network. Many researchers, however, are still trying to master and create more resilient networks that can withstand significant failovers and high traffic loads. However, there are still many questions that need to be resolved in terms of funding and actual implementation. Because of their central role in the network's connectivity, routers are of paramount importance. If the gateway router goes down, the entire network is rendered inaccessible. The current investigation looks into several aspects of redundancy protocols and proposes multiple perfect solutions that are practical and realistic. The purpose of this research is to compare the effectiveness of the first-hop redundancy protocol enabled Gateway Load Balancing Protocol (FHRP-GLBP) with that of the Hot Standby Router Protocol (HSRP), the Virtual Router Redundancy Protocol (VRRP), and concerning the Quality of Service (QoS) parameters (latency, packet loss, Roundtrip time).

Keywords: gateway, VRRP, HSRP, FHRP-GLBP, latency, packet loss, and roundtrip time.

Manuscript Received 17 October 2024; Revised 28 November 2024; Published 31 December 2024

1. INTRODUCTION

The consequences of industrial network failure could be disastrous. While data outages are concerning for any firm, short gaps in connectivity may expose industrial organizations to severe productivity loss or raise serious safety concerns [1]. In practice, unplanned downtime costs industrial organizations around the world $65 billion per year, and with pandemic pressures continuing to disrupt supply and demand chains, even little network interruptions can have significant effects [2]. The result requires substantial network redundancy is vital for industrial enterprises to achieve long-term success. However, not all redundancy strategies are made equal. It is a matter of when, not if, networks will experience unforeseen disruption [3]. Cyberattacks, power outages, or weather occurrences that disrupt connectivity could all be blamed. Companies have an uphill battle to get systems back up and running and production back on track without strong layer two redundancy [4-5].

Redundancy in the Network

To ensure that data continues to flow in the event of an interruption, networks often employ redundancy or the practice of setting up multiple traffic channels as displayed in Figure 1. One interpretation is that adding more redundancy boosts dependability. As a bonus, it may be used to manage a network of sites from a single interface. If a piece of hardware fails, another can take over without disruption. Increasing the network's complexity can make it more robust in the face of disruptions. However, dependability can also be jeopardized by complexity. Higher levels of complexity increase the chance of human mistakes and the possibility that a software defect will lead to a novel failure mode [6-7]. As a result, network architects need to find a happy medium between redundancy and complexity.

Redundancy in a network can be implemented in one of two primary ways. The first is called fault tolerance, which uses a technique called full hardware redundancy, wherein a fully functional copy of the system hardware always operates in parallel with the primary system [8]. If one fails, the other will kick in at once, so there will be no interruption in service. High availability is the second form of network redundancy [9-10]. Instead of duplicating every piece of hardware, a group of servers works as a single unit with this design. Each server keeps an eye on the others and has failover capabilities if one goes down [11]. If one is wondering what sets one option apart from another, it is necessary to consider this:

While fault-tolerant systems have nearly no downtime, they are very costly to construct, and high-availability infrastructure is less costly overall but may have some minor effects on service during outages [12-13].

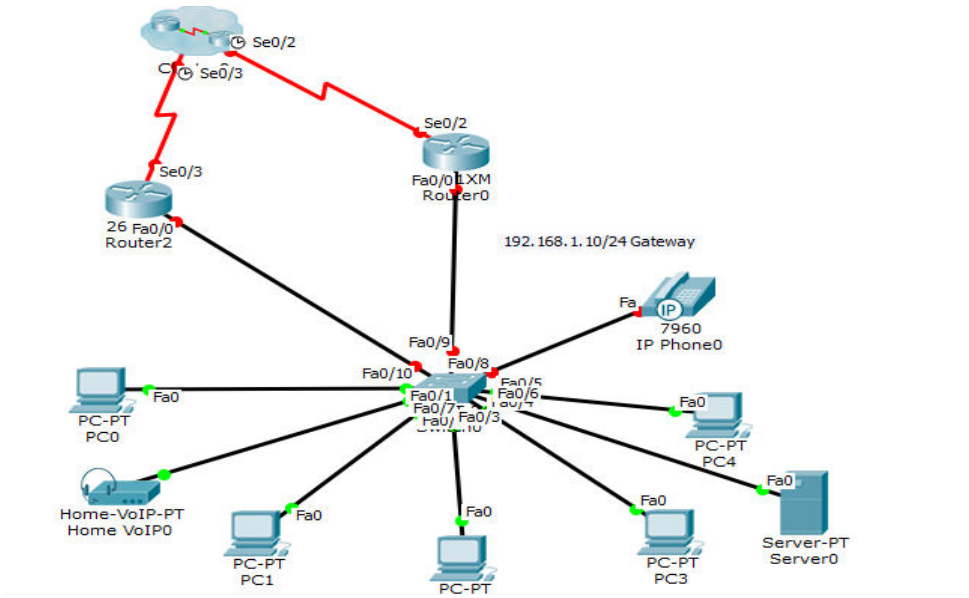

Figure-1. Typical Redundant Network.

The main contribution of the manuscript is highlighted as follows:

- Implementation of first-hop redundancy protocol (FHRP) for business networks;
- Comparison of Hot Standby Router Protocol (HSRP), the Virtual Router Redundancy Protocol (VRRP), and the Gateway Load Balancing Protocol (GLBP);
- Analysis of the packet loss of redundancy protocols with an increasing number of nodes;
- Examination of the trade-off between Roundtrip time, Packet loss, and latency;
- Recommendation of appropriate protocol for corporate networks based on the targeted performance metric.

The remaining sections of this work will be structured as follows. In section 2, we discuss the network scenario. In Section 3, we provide the performance metric. In Section 4, we provide our findings, and in Section 5, we compare and discuss the obtained findings concluding the paper.

2. NETWORK SCENARIO

Cisco Packet Tracer is a multi-platform graphical simulator that replicates the behavior of contemporary computer networks and allows users to design their network topologies. The software provides a simulated command line interface for virtually configuring Cisco routers and switches [14]. Packet Tracer's user interface is entirely drag-and-drop based, so users can freely rearrange their virtual network nodes. Users of Packet Tracer can mimic network topologies by rearranging virtual routers, switches, and other nodes. A 'cable' item represents a real-world wire that can be used to link two electronic gadgets together. Packet Tracer provides fundamental routing with RIP, OSPF, EIGRP, and BGP, as well as a wide variety of simulated Application Layer protocols [15-27]. Border Gateway Protocol support was added to Packet Tracer in version 6. Packet Tracer can be used for more than just simulating computer networks. With version 6.0, Packet Tracer has added multi-user capability, allowing multiple users to collaborate on a single network simulation simultaneously using different topologies. Additionally, Packet Tracer enables educators to design custom assignments for their classes. According to Cisco Systems, Packet Tracer is a valuable tool for testing new network configurations.

During the planning phase, a random waypoint model is used to build a model of the network:

- In the second stage, assigning logical addresses to the public and private networks;
- The third step is to configure the FHRP-enabled GLBP (FHRP-GLBP) protocol and run simulations of potential network configurations.
- In the fourth place, we have a comparison of the results of various assessments of the performance metrics;
- The last stage is composed of the analysis and interpretation of the results.

Considering the Constant Bit Rate (CBR) as a deployment application, there are accessible existing networks available [17-18]. The CBR applications are

connected by 15 and 40 nodes, of which 7 are routers, 2 are switches, and 6 are wired nodes. For 40 nodes, 10 are routers, 3 are switches, and 27 are wired nodes. Beyond OSPF, the other considered routing protocols are FHRP, VRRP, and GLBP. After finishing the test, the graphs in the simulator were considered. The required performance metrics are thus obtained, including Roundtrip time, Packet loss, and latency. The proposed Network scenario with private and public networks with multiple nodes is shown in Figure-2 and Figure-3 for variable nodes and routers. The increase in the number of nodes is displayed in Figure-4.

For the sake of argument, let us say that the administrator is entirely ignorant of the FHRP-GLBP. Without FHRP-GLBP, the administrator can make use of the following choices. It is recommended that any changes are not performed to the present configuration of the host and instead reconfigure all hosts to use the backup router if the primary gateway router fails. Set up some hosts to use the new gateway router by configuring them. If the currently active gateway router crashes, it is necessary to reconfigure the hosts to utilize the new gateway router instead of the currently active gateway router. Similarly, if the newly installed gateway router becomes inoperable, it is necessary to change the configuration of the hosts so that they utilize the previously installed gateway router instead. Every one of the choices mentioned above necessitates human intervention in the event of a power failure. Power outages are challenging to foresee [19]. The administrator must keep constant vigil over the network to identify malfunctions. When there is a service disruption, the administrator is responsible for configuring all hosts to utilize the backup default gateway router. After the outage, the administrator is responsible for resetting all hosts to use the initial configuration. These choices can be helpful in a local area network. However, some options will not function properly in a vast network. For the sake of this example, assume that a local subnet of a network with a medium-sized footprint has 5555 hosts. The administrator must configure and then reconfigure each of these hosts whenever there is a service disruption. This complex and time-consuming task is not something that any administrator would enjoy doing. In addition, because the adjustment is made on the host system, the user will not be able to access the host system while the administrator adjusts. This activity is made straightforward by an FHRP protocol. The administrator must make the following adjustments to configure an FHRP protocol.

- Establish a fictitious Internet Protocol (IP) address on the primary gateway router;
- Give the backup gateway router the same virtual IP address delivered to the primary gateway. Make sure an FHRP-GLBP protocol is set up on both routers so that they can react to the virtual IP address;
- Make sure that every host is set up to utilize the virtual IP address as the IP address of the gateway router. The administrator does not need to constantly monitor the gateway router after configuring an FHRP-GLBP protocol. This situation frees up the administrator's time. The FHRP-GLBP protocol, once set up, will automatically replace the gateway router that is currently down with the gateway router that is currently available. For instance, if the primary gateway router becomes inoperable, the traffic will be redirected to the backup router. The traffic will be immediately redirected to the primary router if either the backup router or the primary router goes down and then comes back online again.

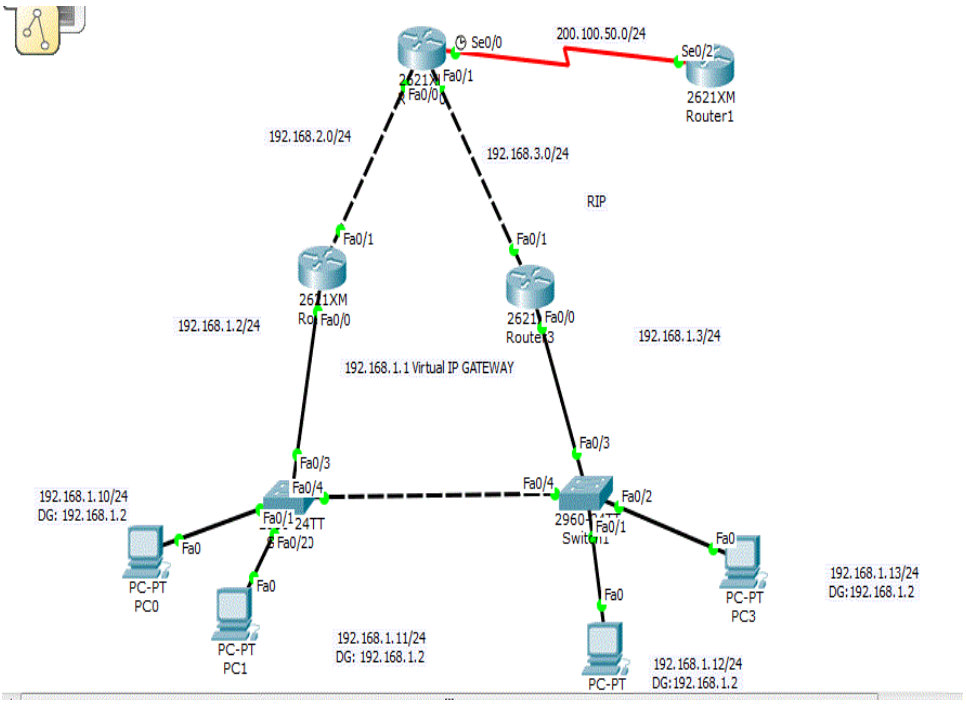

Figure-2. Network scenario with private and public networks.

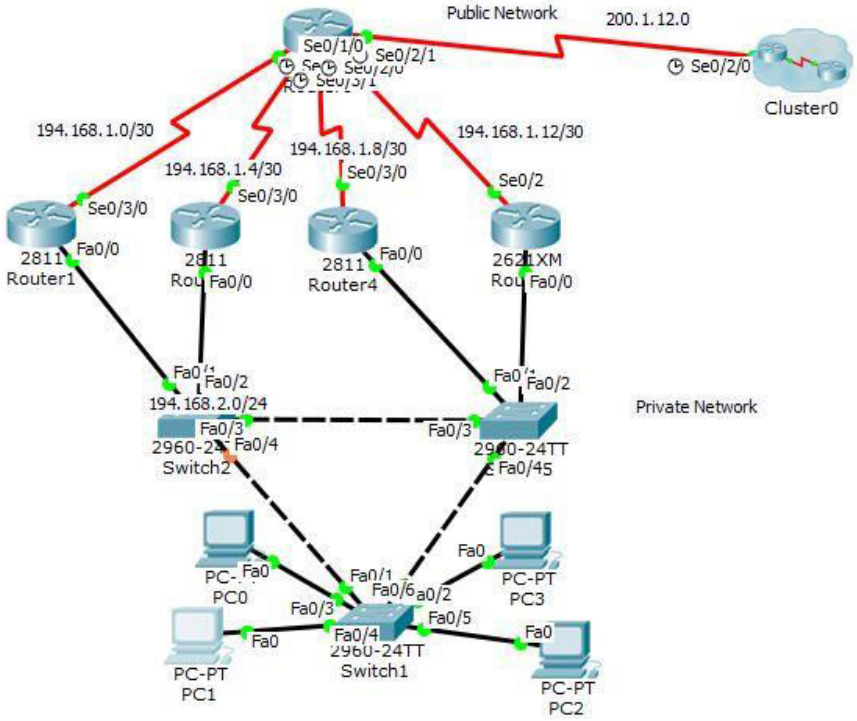

Figure-3. Network scenario by enabling FHRP-GLBP / HSRP / VRRP in Business Network.

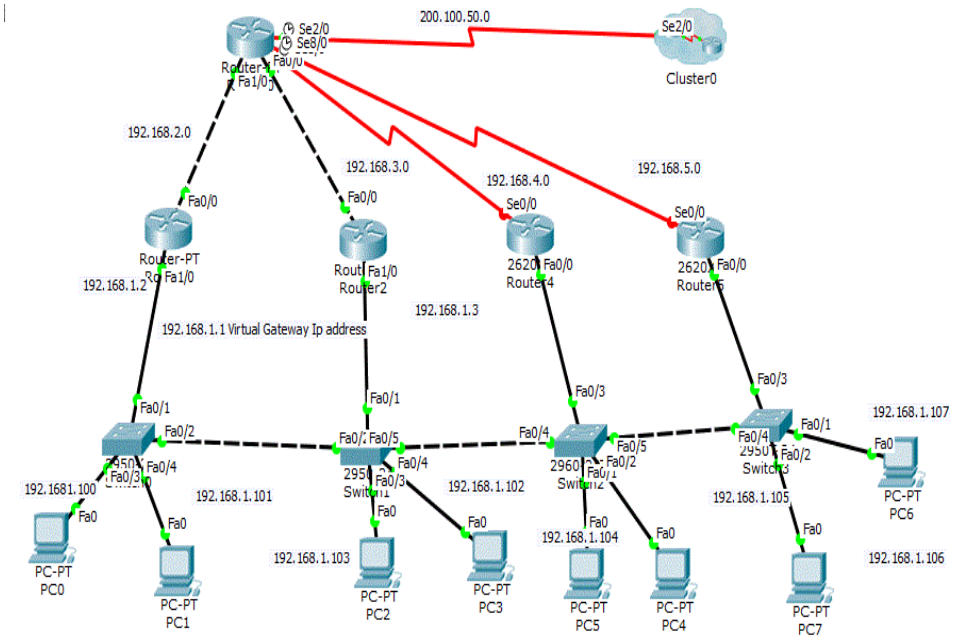

Figure-4. Network Topology with FHRP-GLBP / HSRP / VRRP and increase in number the private business interface

3. PERFORMANCE PARAMETERS

Latency: The latency of a network connection describes how long it takes for a data packet to transit between two points in the network.

As close to zero latency as possible is the ideal situation. The amount of time it takes for a data packet to go to its destination and back is the round-trip time (RTT), which can be used to quantify network latency. Page loads, media playback, and program functionality can all be negatively impacted by excessive network latency. An increase in latency, no matter how slight, can have a devastating effect on user experience in some applications. Geolocation issues are a significant contributor to latency problems. Internet Protocol (IP) networks that span great distances require more time for data to travel between nodes, which might cause problems for some applications. It makes sense to place the computer that is processing the data as close to the source of the data as feasible, a notion known as edge computing, in any case where the latency between sensing and responding needs to be highly minimal; for example, some actions in autonomous driving.

It is not always possible to assess latency between different applications. Latency can be assessed with a stopwatch in some situations, but more advanced tools or understanding of computer instructions and programs are required in others. Traceroute, My traceroute (MTR), and Ping are just a few tools available to network administrators for this purpose. When a user is unsure whether or not the host machine, they are trying to connect to be active, they can use ping commands to find out. Latency can be measured by having a network administrator issue an Internet Control Message Protocol (ICMP) echo request to a selected network interface and then waiting for a response. A traceroute command can also be used to determine how long a delay is between two points. To record the delay between hosts along an IP network, traceroute creates a graphical representation of the path that packets traverse. MTR combines features of Ping and Traceroute to determine the total transit time and the delay between devices along the way.

Average Jitter: A Jitter in a network, also known as packet delay variation (PDV), causes a stuttering-like effect in the signal quality during data transmission. Packets may arrive at their destination out of sequence or not if the transmission is routed differently for each packet (called packet loss). Packet jitter, like latency, is quantified in milliseconds. Delays are inevitable even though technology can fix the problem and reorder the packets. To give an example of the impact, consider what happens to a user's video or voice call when there is much jitter: stuttering, choppy video or audio, or even dropped calls.

4. RESULTS AND DISCUSSIONS

Figure-2 shows the topology we created without using HSRP, and Figure-5 displays the ping results. As displayed in Figure-6 and Figure-7, when the default gateway is disrupted in the system topology, the bundle suffers more because it cannot automatically assign another course. With reference to the network in Figure-3, a topology is built using HSRP and Figure-8 shows the result of doing a ping against an ISP.

```
Packet Tracer PC Command Line 1.0
PC>ping 200.1.2.2 -n 10

Pinging 200.1.2.2 with 32 bytes of data:

Reply from 200.1.2.2: bytes=32 time=0ms TTL=254
Request timed out.
Reply from 200.1.2.2: bytes=32 time=4ms TTL=254
Reply from 200.1.2.2: bytes=32 time=0ms TTL=254
Reply from 200.1.2.2: bytes=32 time=0ms TTL=254
Reply from 200.1.2.2: bytes=32 time=1ms TTL=254
Reply from 200.1.2.2: bytes=32 time=0ms TTL=254
Reply from 200.1.2.2: bytes=32 time=4ms TTL=254
Reply from 200.1.2.2: bytes=32 time=0ms TTL=254
Reply from 200.1.2.2: bytes=32 time=0ms TTL=254

Ping statistics for 200.1.2.2:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

Figure-5. Transmission of data between public and private networks.

```
Ping statistics for 200.1.2.2:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

PC>ping 200.1.2.2 -n 16

Pinging 200.1.2.2 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.
```

Figure-6. Transmitted Packets are discarded in public and private networks.

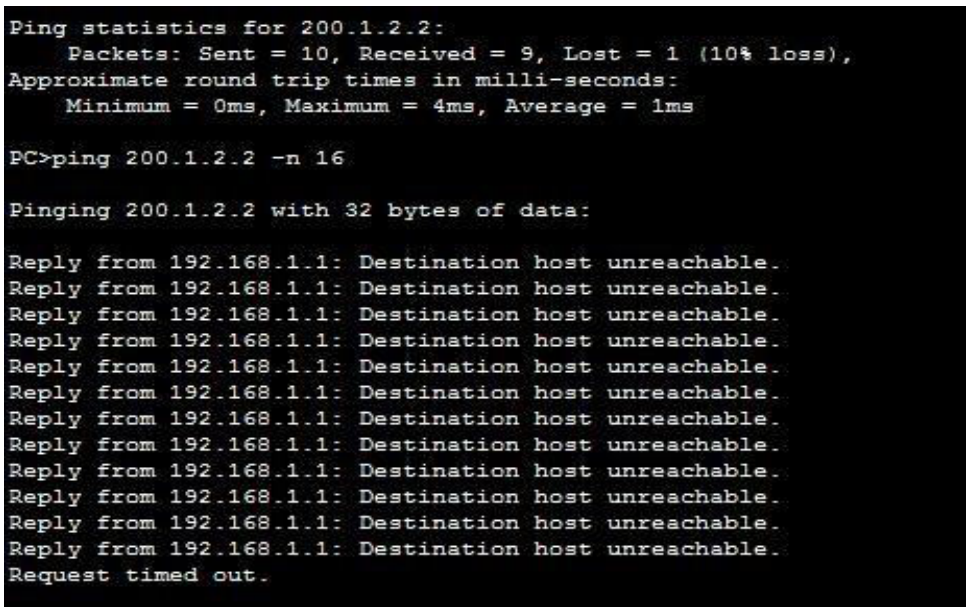

Figure-7. Packets loss without enabling HSRP.

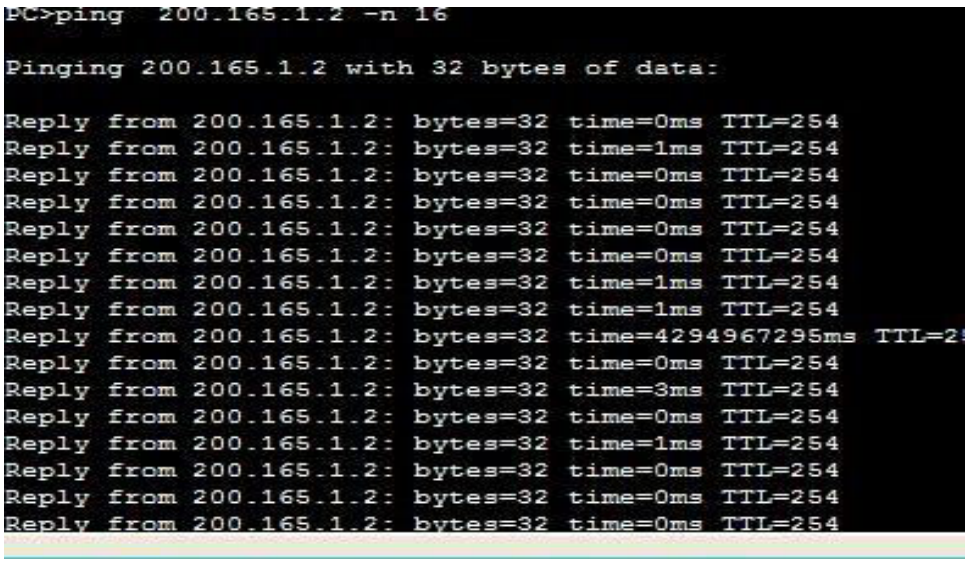

Figure-8. Transmission of packets by enabling HSRP.

```
PC>ping  200.165.1.2 -n 16

Pinging 200.165.1.2 with 32 bytes of data:

Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=1ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=1ms TTL=254
Reply from 200.165.1.2: bytes=32 time=1ms TTL=254
Reply from 200.165.1.2: bytes=32 time=4294967295ms TTL=2
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=3ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=1ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
Reply from 200.165.1.2: bytes=32 time=0ms TTL=254
```

Figure-9. Communication in the business network with FHRP-GLBP when a link fails.

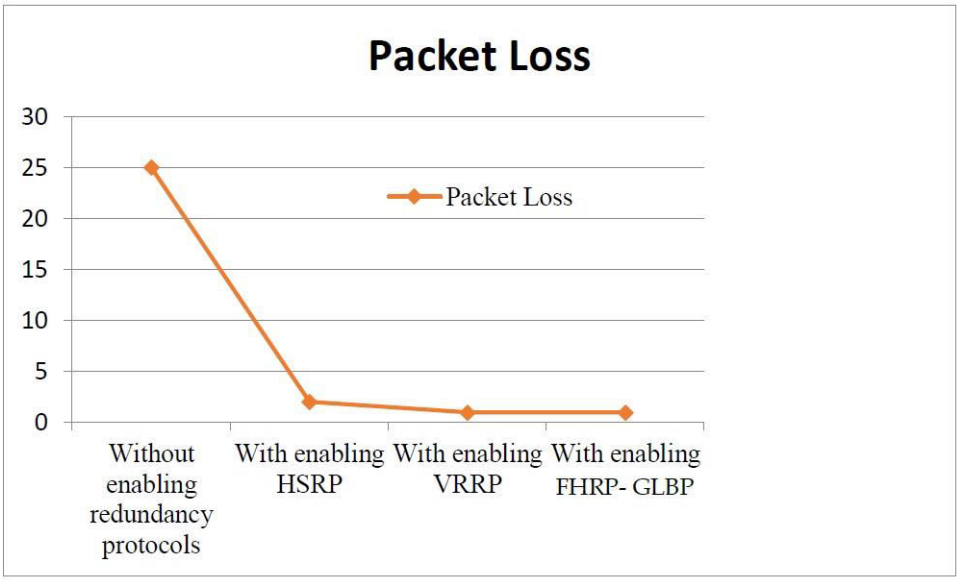

Figure-10. Packet loss of all Redundancy Protocols.

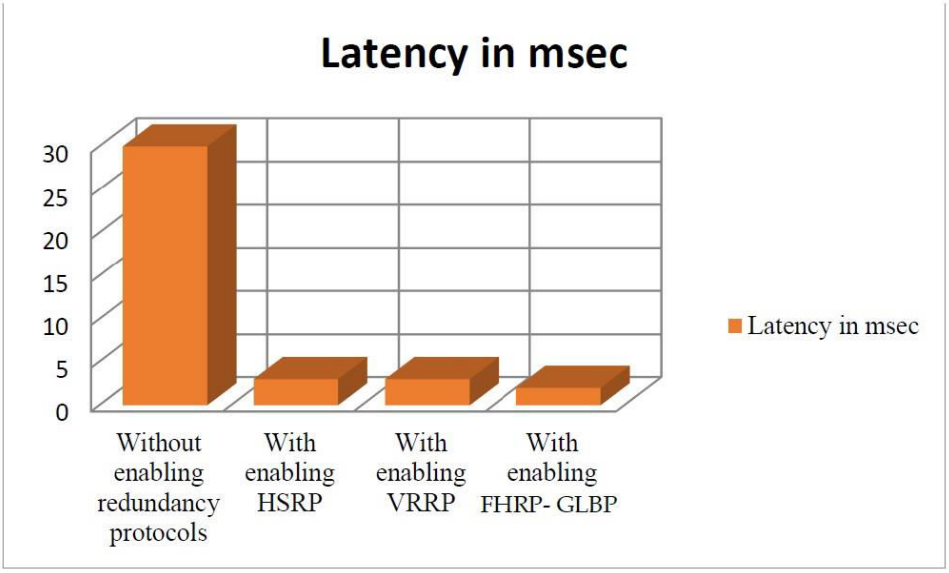

Figure-11. Latency of different Redundancy Protocols.

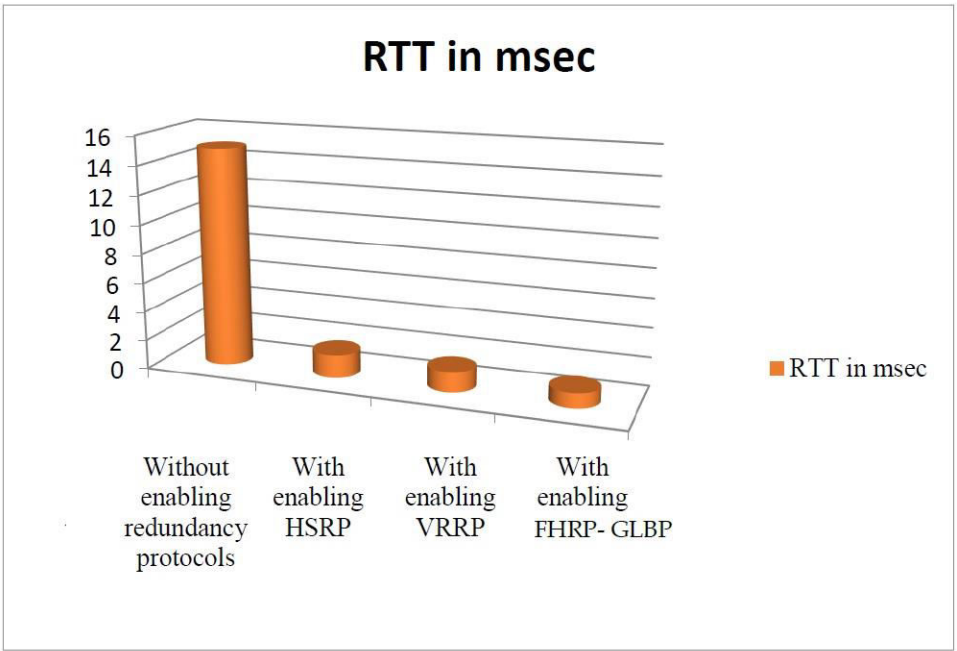

Figure-12. RTT of different Redundancy Protocols.

In the FHRP-GLBP protocol in Figure-4, R1 is shown as a live switch, whereas R2 is shown as a backup. The performance comparison of the various protocols in terms of packet loss, latency, and RTT has been displayed in Figure-10, Figure-11, and Figure-12, respectively. Here, a single router (R1) will handle packet forwarding, while another router (R2) will provide backup. Bundle tragedy is avoided if R1 fails since R2 serves as a reinforcing switch. Figure-4 further displays an FHRP-GLBP topology in which R1's gigabit Ethernet connection was severed. Customers can now access their Internet service providers (ISPs) over the R2 switch. One of our switches, R1, is currently in standby mode, while another, R2, is a dynamic switch. With FHRP-GLBP, the client can reroute objects through R2 even if they were first entered through the default entry. Table-1 compares the significance of the FHRP-GLBP protocol as compared to the HSRP and VRRP protocols.

Table-1. Comparison of all routing protocols.

Protocol	Packet loss	Latency in msec	RTT in msec
HSRP	2	3	1.6
VRRP	1	3	1.4
FHRP-GLBP	1	2	1
Without FHRP	25	30	15

5. CONCLUSIONS

Following an in-depth examination of the research, we have realized that the redundancy protocol was responsible for the increased reliability and redundancy of the topology. The failure of any device will not affect the functioning of the network. The performance of the FHRP-GLRP was analyzed, and the results led us to the conclusion and knowledge that every procedure has both positive and negative aspects. According to the study's findings, VRRP and GLBP both have the same amount of packet loss; however, HSRP has more delay and packet loss than the other two protocols. On the other hand, when there was a device failure, FHRP-GLRP acted quickly, and the amount of time that FHRP-GLRP required to complete its tasks in that scenario was almost the same as that required by HSRP and VRRP.

Redundancy Protocols Abbreviations
First-Hop Redundancy Protocol (FHRP)
Hot Standby Router Protocol (HSRP)
Virtual Router Redundancy Protocol (VRRP)
Gateway Load Balancing Protocol (GLBP)

REFERENCES

[1] Ravikumar C. V., Kalapraveen B. 2016. Robust neural network-based multiuser detector in MC-CDMA for multiple access interference mitigation. Indian Journal of Science and Technology. Vol. 9.

[2] Ravikumar C. V, Kala Praveen Bagadi. 2019. Design of MC-CDMA receiver using RBF network to mitigate MAI and nonlinear distortion, Neural Computing and Applications. 31(2).

[3] Karthick A. V., Gopalsamy S. 2023. Role of IoT in Business Sustainability. In: Aloysius Edward, J., Jaheer Mukthar, K. P., Asis, E. R., Sivasubramanian, K. (eds) Current Trends in Economics, Business and Sustainability. ICEBS 2023. Contributions to Environmental Sciences & Innovative Business Technology. Springer, Singapore. https://doi.org/10.1007/978-981-99-3366-2_2

[4] Mohammed M. N., Alfiras M., Alani S., Sharif A., Abdulghaffar A., Al Jowder F. and Tamer H. 2023, October. Design and Development of the GU CyberCar. A Solar-Powered Electric Vehicle Based on IoT Technology. In 2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS) (pp. 1-6). IEEE.

[5] Navabharat Reddy G., Rajesh A. 2022. Literature Review and Research directions towards channel estimations and hybrid pre-coding in mm-wave massive MIMO communication systems. J Reliable Intell Environ. https://doi.org/10.1007/s40860-022-00174-5

[6] Ravikumar C. V., Kalapraveen B. 216. Performance analysis of HSRP in provision-ing layer-3 gateway redundancy for corporate networks. Indian Journal of Science and Technology. Vol. 20.

[7] Jayaprabath, Rahul Varma C. 2019. Performance analysis of interior and exterior routing protocols. Journal of Engineering and Applied Sciences. 14(17).

[8] Reddy G. N. and Kumar C. R. 2023. Deep learning-based channel estimation in MIMO system for pilot decontamination. International Journal of Ad Hoc and Ubiquitous Computing. 44(3): 148-166.

[9] Ravikumar C. V., and Kalapraveen B. 2016. Performance analysis of ipv4 to ipv6 transition methods. Indian Journal of Science and Technology. Vol. 20.

[10] Ravikumar C. V, Kala Praveen Bagadi. 2017. MC-CDMA receiver design using recurrent neural network for eliminating MAI and nonlinear distortion. International Journal of Communication Systems (IJCS). 10(16).

[11] Ravikumar C. V. and Kalapraveen B. 2017. Receiver design using artificial neural network for signal detection in MC-CDMA system. International Journal of Intelligent Engineering & Systems. 10(3).

[12] K. Bagadi et al. 2022. Detection of Signals in MC–CDMA Using a Novel Iterative Block Decision Feedback Equalizer. in IEEE Access, 10: 105674-105684, doi: 10.1109/ACCESS.2022.3211392.

[13] S. P. Tera, et al. 2024. CNN-Based Approach for Enhancing 5G LDPC Code Decoding Performance. in IEEE Access, 12: 89873-89886, doi: 10.1109/ACCESS.2024.3420106.

[14] Chinthaginjala et al. 2024. Enhancing handwritten text recognition accuracy with gated mechanisms. Scientific Reports. 14.1: 16800.

[15] Jyothi Koganti Krishna, et al. 2024. A novel optimized neural network model for cyber-attack detection using enhanced whale optimization algorithm. Scientific Reports 14.1: 5590.

[16] M. Chinnusami et al. 2023. Low Complexity Signal Detection for Massive MIMO in B5G Uplink System. in IEEE Access, 11: 91051-91059, doi: 10.1109/ACCESS.2023.3266476.

[17] Kaveripakam S. and Chinthaginjala R. 2023. Optimal path selection and secured data transmission in underwater acoustic sensor networks: LSTM-based energy prediction. PLoS One. 18(9): e0289306.

[18] Anbazhagan Rajesh, et al. 2023. Structural analysis of nano core PCF with fused cladding for supercontinuum generation in 6G networks. Radio Science. 58.9: 1-18.

[19] Ravikumar C. V. 2023. Developing novel channel estimation and hybrid precoding in millimeter-wave communication systems using heuristic-based deep learning. Energy. 268: 126600.

[20] Cv R. and Sathish K. 2022, August. Performance Analysis of Clustered-Based Underwater Wireless Sensor Network by Deploying Application as CBR. In 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) (pp. 1678-1686). IEEE.

[21] V. Annepu et al. 2022. Review on Unmanned Aerial Vehicle Assisted Sensor Node Localization in Wireless Networks: Soft Computing Approaches. in IEEE Access, 10: 132875-132894, doi: 10.1109/ACCESS.2022.3230661.

[22] Yash Mr, et al. 2020. A smart wheelchair for health care systems. International Journal of Electrical Engineering and Technology. 11.4.

[23] Mohit et al. 2020. Investigation of Inter Vlan Routing and Deploying Access Control List for Corporate Network. International Journal of Electrical Engineering and Technology. 11.3.

[24] Kumar B, et al. Secure Data Communication with Cryptography and Steganography. International Journal of Electrical Engineering and Technology. 11(3).

[25] Prathyusha M. and Kumar C. R. 2019, March. A survey paper on debugging tools and frameworks for debugging real-time industrial problems and scenarios. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-4). IEEE.

[26] CV R. K. and Goyal H. 2019, March. IPv4 to IPv6 migration and performance analysis using GNS3 and Wireshark. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-6). IEEE.

[27] Ravikumar C. V., Venugopal P., Jagannadha Naidu K., Satheesh Kumar S. and Koppu S. 2018. Adaptive cruise control and cooperative cruise control in real-life traffic situations. International Journal of Mechanical Engineering and Technology. 9(13): 578-585.