MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2024) 7 (2) 1-15
©UNIVERSITI SULTAN ZAINAL ABIDIN
DOI: *https://doi.org/10.37231/myjcam.2024.7.2.124*

Article: Received 17.07.2024; Accepted 16.09.2024; Published 30.09.2024

UNISZA CAMPUS NETWORK: BACKUP USING HSRP AND OSPF INPACKET TRACER

Muhammad Syhakirin Yahya, Raja Hasyifah Raja Bongsu

Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia
muhammadsyhakirin@gmail.com

Abstract: Our campus, like many others in the changing world of higher education, is strongly dependent on a wide range of data, which serves as the foundation for our educational experience and institutional memory. Examples of this data include academic records, research findings, administrative information, and digital communications. However, campus networks are naturally susceptible to a variety of risks, including human error, natural disasters, and hardware problems, which calls for a proactive approach to data protection. By creating and putting into place a reliable backup and restoration system, the "UNISZA Campus Network: Backup Using Hot Standby Router Protocol (HSRP) and Open Shortest Path First (OSPF) inPacket Tracer" project seeks to protect all campus data from unanticipated calamities. This study presents the usage of Open Shortest Path First (OSPF) and Hot Standby Router Protocol (HSRP) to improve network backup procedures within the campus network of UNISZA. This study assesses network resilience during disasters using Packet Tracer simulations. The findings show enhanced throughput, decreased latency, and efficient failover capabilities, guaranteeing continuous operations. The results emphasise how crucial strong redundancy mechanisms are for academic networks.

Keywords: Campus network resilience, Data protection, Backup and restoration system, HSRP and OSPF protocols, Disaster recovery, Packet Tracer simulations

1. INTRODUCTION

The main objective of this study is to reduce the impact of network outages on all of UNISZA's campuses by designing and implementing a robust backup system that makes use of the HSRP and OSPF protocols. Like the dynamic world of higher education, our campus depends on a multitude of data, including digital communications, research discoveries, academic records, and administrative information. This data is the basis of our educational experience and institutional memory; it is not just informational. Proactive data protection is crucial because campus networks are inherently vulnerable to various risks, such as hardware failures, natural disasters, and human error. This program ensures that every piece of data is carefully saved in recognition of the vital importance of data from the main campus and its satellite locations.This project use a multi-tiered backup system [1], tailoring backup frequencies to data criticality and using localizedbackups for emergency scenarios. The system is thoroughly designed, tested, and assessed using PacketTracer for virtual simulations before being used in the real world, guaranteeing its dependability and efficiency. Understanding the fine line between cost-effectiveness and data relevance, this project adds flexibilityso administrators can set backup priorities based on data value. Furthermore, external server backups are recommended as an additional security measure outside of school boundaries. This all-inclusive strategy is intended to lessen the weaknesses caused by hardware malfunctions, natural calamities, and human mistakes, eventually strengthening campus networks' resistance to unanticipated attacks. This case study attempts to offer valuable solutions that guarantee administrative and academic continuity by examining the difficulties of backup and restoration in learning environments, developing an intricate multi-tiered backup and recovery system, and testing its efficacy in actual disaster situations [2][3]. We are dedicated to protecting our campus from the uncertainties of the digital age by merging best practices for datamanagement with the smooth continuation of educational activities through this initiative.

2. RELATED WORKS

Improve network resilience and reduce downtime, a great deal of research has been done on failover and redundancy solutions. As a Cisco-only protocol, Hot Standby Router Protocol (HSRP) has been widelyused to guarantee network continuity in the case of device failures. For example, prior studies have shownthat by offering an effective failover mechanism between active and standby routers, HSRP can greatly reduce packet loss and latency during network outages. Research comparing High-Availability Routing Protocol (HSRP) with alternative redundancy protocols, like Virtual Router Redundancy Protocol (VRRP), has demonstrated that HSRP frequently offers better performance in terms of quicker failover times and more reliable network operations during peak loads. This has been examined in order to improve network performance overall and optimise route convergence times. These tests demonstrate the efficiency of HSRPin preserving network stability and reliability, laying a strong platform for further research into the technologyin a variety of real-time network settings [4]. Comparison the performance of HSRP and VRRP has highlighted key differences in their operational efficiencies and effectiveness in network redundancy. Studies have shown that while both protocols aim toprovide seamless failover and high availability, HSRP often outperforms VRRP in specific metrics such as failover time and packet loss. For instance, it has been observed that HSRP exhibits a quicker transition from backup to master states, resulting in reduced downtime during failover events. Moreover, the packet loss rate during failover in HSRP implementations tends to be lower compared to VRRP, making it a preferred choice in environments where minimal data loss is critical. Analyses have also indicated that HSRP offers more consistent performance in handling network traffic and maintaining stable connections during dynamic network conditions. These comparative evaluations are crucial for network designers in selecting the appropriate redundancy protocol based on specific network requirements and operational goals [5].

Explored the new paradigm of controller-based networks, which became popular in 2010 because of their programmable and centralised architecture. The fundamental elements of these networks have been established in this research. This has demonstrated how having many controllers can improve QoS measurements and network availability. Building on this, the study investigates how numerous controllers utilising OSPF and OpenFlow affect jitter and packet delivery ratio (PDR) in mobile IP networks. It models these networks using simulation tools like as OMNeT++, OpenFlow, and simuLTE and offers insights into the QoS gains provided by multi-controller topologies over conventional OSPF-based networks [6]. The study [7] explored the historical evolution and performance of various dynamic routing protocols. It references early work by Golap et al., which utilized GNS3 software to compare RIPV2, EIGRP, and OSPF,finding EIGRP superior in performance for large networks, while RIPV2 performed better in smaller ones. Another notable study involved OPNET simulations to compare convergence durations of EIGRP, RIP, andOSPF, with EIGRP again showing superior results. Additionally, research by Anibrika Bright focused on real-time applications, confirming EIGRP's superior performance. The paper also discusses the practical benefits of route redistribution for ensuring network convergence and providing backup routes in case of failures, thus enhancing overall network resilience.

Guaranteed ongoing operation even in the event of a breakdown, redundancy mechanisms are implemented and the failover performance of link systems inside network infrastructures is assessed in this study. Utilising multiple pathways and backup links can greatly increase network dependability, according to earlier study. To ensure service availability, strategies like dynamic routing modifications and link aggregation are frequently used. Research has indicated that appropriately set up failover methods can reduce downtime and stop data loss in the event of a link breakdown. The efficacy of these methods is frequently assessed using metrics like recovery time, packet loss, and failover time. Through the implementation and testing of several failover mechanisms, this research helps to clarify the practical effectsof redundancy on network stability and performance [8]. Recent years have seen a large amount of study conducted on the effectiveness of routing protocols, including RIP, OSPF, and EIGRP, and how well they perform in different network contexts. Previous research has looked into many facets of these methods. Masruroh et al., for example, assessed how well various protocols performed in DMVPN contexts, noting variations in convergence times and resource usage. In a study comparing RIP with OSPF, Jayakumar et al. emphasised the ease of configuration and simplicity of RIP in contrast to the quicker convergence and shorter latency times of OSPF. Yang and Yongalso examined RIP's failure processes, offering insights into its shortcomings and possible enhancements.In their study of RIP and EIGRP performance under IEEE 802.3u standards, Atefi et al. demonstrated the superiority of EIGRP in terms of convergence and delay. Furthermore, Athira et al.'s analysis of RIP, EIGRP,and OSPF network performance indicators led them to the conclusion that EIGRP performs better in large-scale networks because of its effective resource usage. When taken as a whole, these studies improve ourknowledge of routing protocol behaviours across a variety of network configurations, which helps us selectthe best protocols for our needs [9].

Numerous approaches have been investigated to guarantee data resilience and integrity in the context of disaster recovery and data security for campus networks. Using fault-tolerant multi-cloud data backup strategies, like the one outlined by Sengupta and Annervaz (2014), which distributes data over several geographic sites, is one well-known method. This strategy optimises storage costs and protection levels while also improving data recoverability in the event of catastrophic failures. Furthermore, traditional backup techniques have been transformed by developments in cloud computing and online storage, which now provide more effective and scalable disaster recovery solutions. In order to ensure uninterrupted network operations in the face of disruptions, other research have concentrated on the deployment of High Availability Network solutions employing protocols like OSPF (Open Shortest Path First) and HSRP (Hot Standby Router Protocol). These integrated tactics emphasise the value of a multifaceted strategy that balances cost, effectiveness, and resilience against different risks when it comes to data protection in educational institutions [10]. Considerable study has been done in the field of disaster recovery (DR) planning and optimisation, especially in the areas of network resilience, resource supply, and data replication. Erasure Coding (EC) isa distributed data coding method that has been thoroughly explored in the past for fault tolerance in large- scale archival systems. Several EC algorithms, including Reed-Solomon and Cauchy Reed-Solomon coding, have been highlighted. Furthermore, studies addressing the assignment and allocation of nodes fordata files to enable resilience against site failures have examined multi-site replication for data availability. These studies, however, frequently concentrate on recovery models that do not have strict recovery time objectives (RTOs). The goal of recent approaches to DR storage planning has been to optimise data centrezones, storage volume, and pathways using heuristic and cost-based methods. Routing protocols have been divided into three groups in the context of MANETs (Mobile Ad Hoc Networks) for disaster recovery scenarios: proactive, reactive, and hybrid. Each group has advantages and disadvantages with regard to network performance and stability during high mobility. By presenting an effective gateway routing strategydesigned for disaster recovery situations and addressing both routing complexity and network performanceunder dynamic settings, this study adds to the body of information already in existence [11].

3. METHODOLOGY

A. Framework:

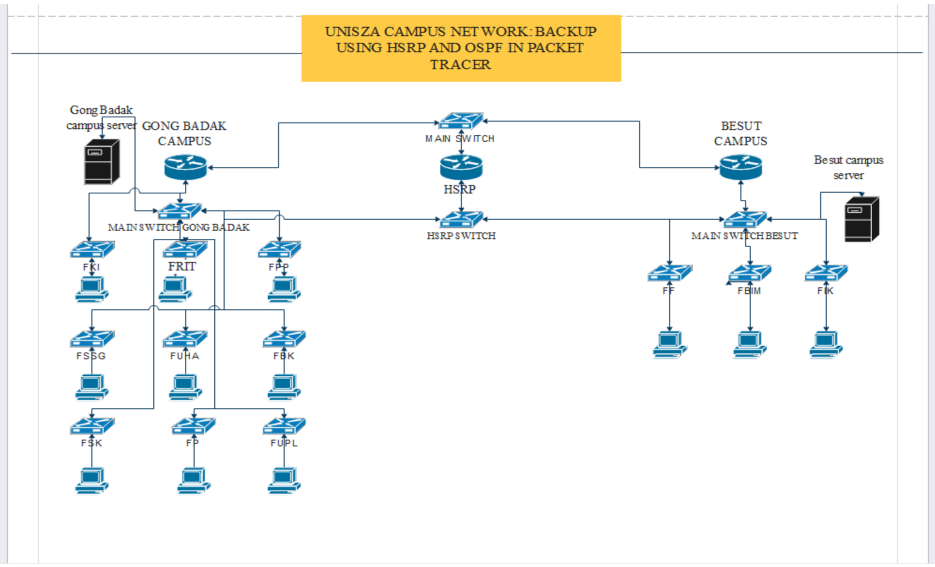


Figure 1: UNISZA Network Topology for Gong Badak and Besut Campuses

Figure 1 above showed this framework of UNISZA Campus Network topology. The two UniSZA campuses are situated in Besut, Terengganu, and Gong Badak, respectively. The UNISZA network topology simulation is organized as follows: At the Gong Badak campus, the network is structured with the Gong Badak main switch connected to the Gong Badak router. Under this main switch, there are seven switches,each connecting to various departments and the Gong Badak server. Specifically, the FKI switch connectsto 10 PCs, the FRIT switch connects to 10 PCs, the FPP switch connects to 10 PCs, the FSSG switch connects to 10 PCs, the FUHA switch connects to 10 PCs, the FBK switch connects to 10 PCs, and the FSK switch connects to 10 PCs. Additionally, the FP switch and the FUPL switch each connect to 10 PCs.

At the Besut campus, the Besut main switch is connected to the Besut router. Below this main switch are three additional switches connected to the Besut server: the FF Switch connects to 10 PCs, the FBIM switch connects to 10 PCs, and the FIK switch connects to 100 PCs. The routers of both campuses, Besut and Gong Badak, are connected to a main switch, which is in turn linked to the HSRP router. The Gong Badak main switch and the Besut main switch are connected to the HSRP router through the HSRP switch. This setup ensures a comprehensive and resilient network structure, enabling effective data backup and restoration across both campuses.

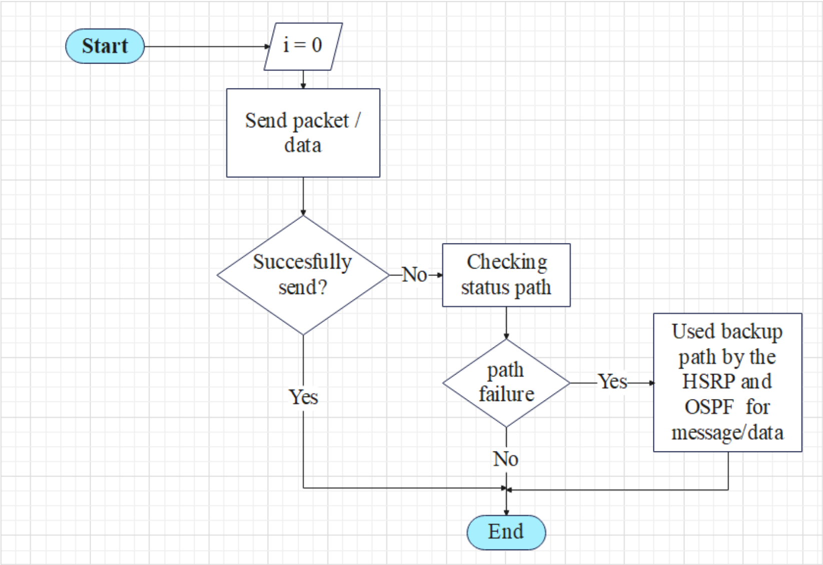


Figure 2. Data Transmission and Backup Path Flowchart in UNISZA Network

Figure 2 illustrated the flowchart of the data/packet transmission process over the assigned pathways within the network topology. Initially, data or packets are sent through the primary path. If the data/packets are successfully transmitted, the process concludes. However, if an issue arises and the data/packets cannot reach their destination, the system checks the status of the network paths using OSPF. In the eventof a path failure, the backup path provided by the HSRP and dynamically managed by OSPF is utilized. This ensures that the data/packets are rerouted and successfully delivered to their intended destination, maintaining network reliability and data integrity.

4. IMPLEMENTATION AND RESULTS

B. Configuration and setup of topology

The configuration of servers, PCs, routers, switches, and switches within the UNISZA Campus Network is shown in Figure 3, 4, 5, 6, 7, 8, and 9. The network architecture and connectivity that guarantee effective data transmission and communication throughout the campus are shown in these diagrams, which offer a thorough visual representation of how the network's component parts are connected.

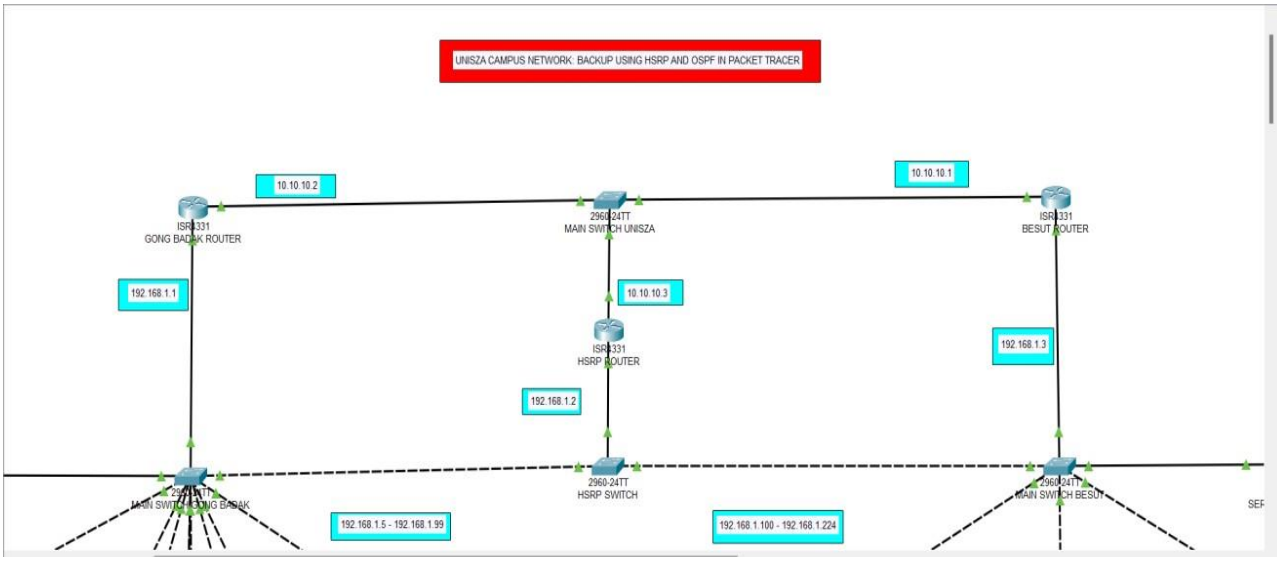


Figure 3. UNISZA Campus Network Topology

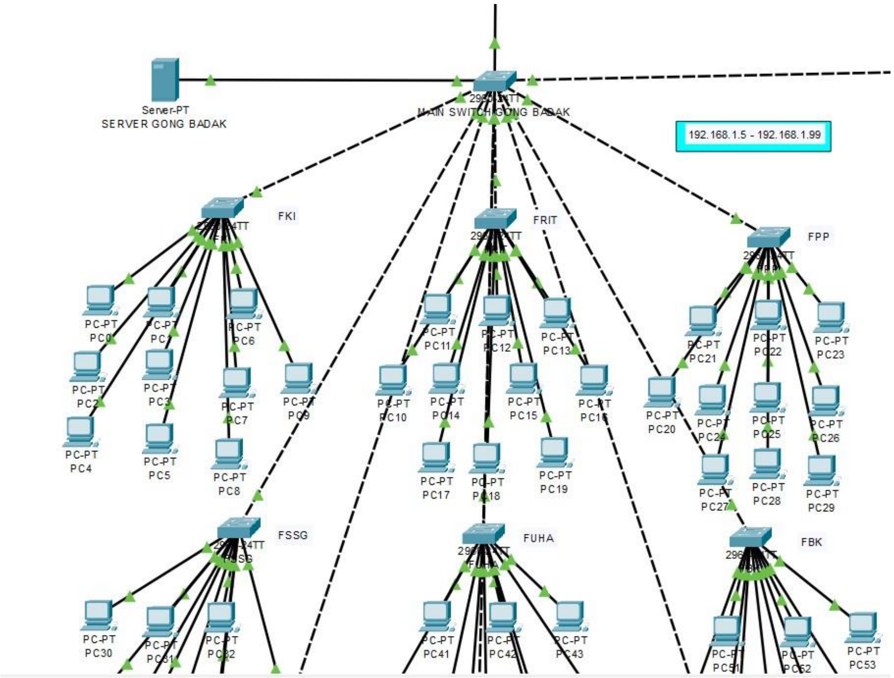


Figure 4. UNISZA Network Topology for Gong Badak (i)

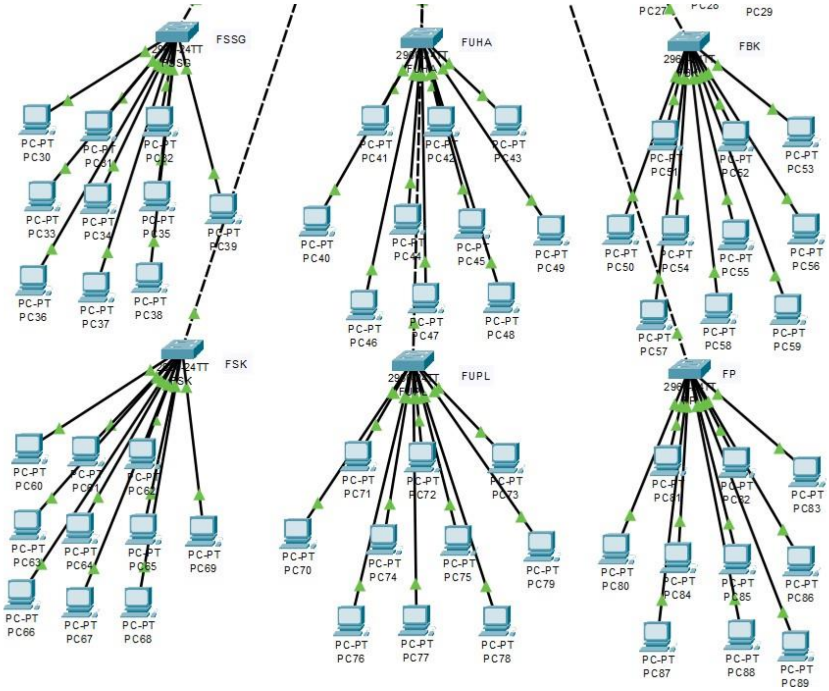


Figure 5. UNISZA Network Topology for Gong Badak (ii)

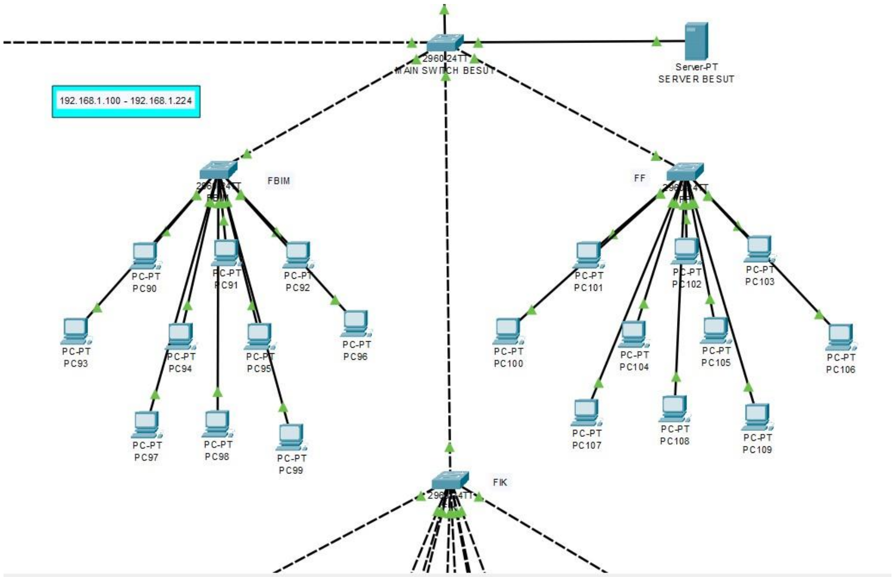


Figure 6. UNISZA Network Topology for Besut (i)

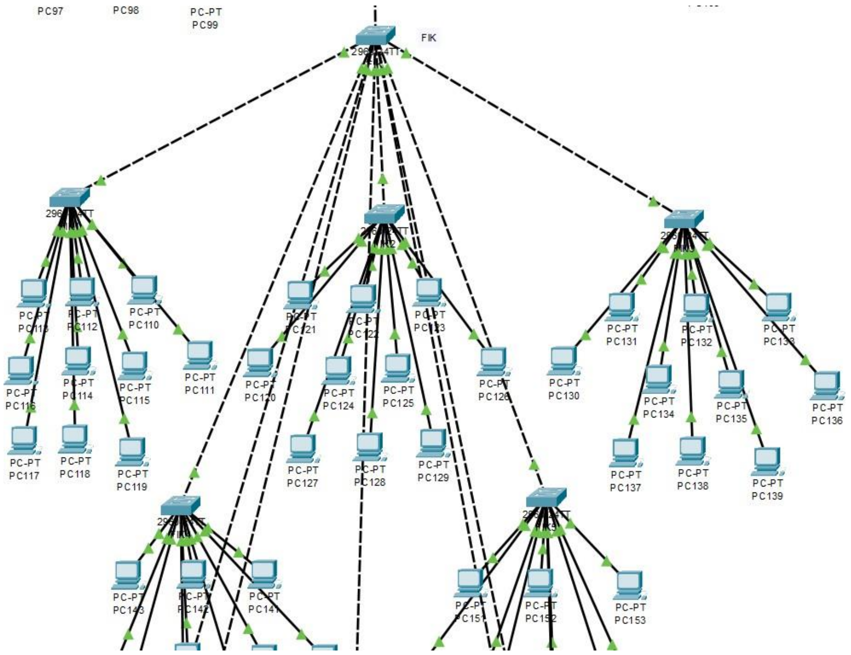


Figure 7. UNISZA Network Topology for Besut (ii)

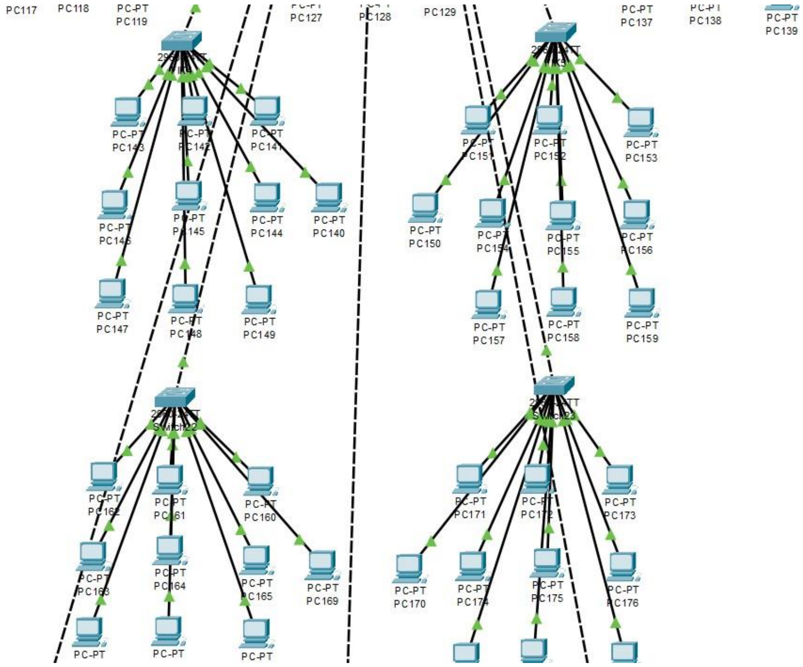


Figure 8. UNISZA Network Topology for Besut (iii)

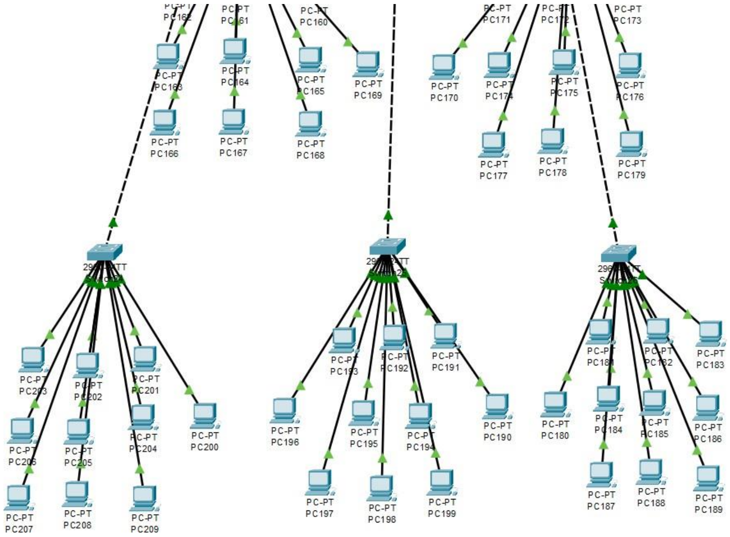
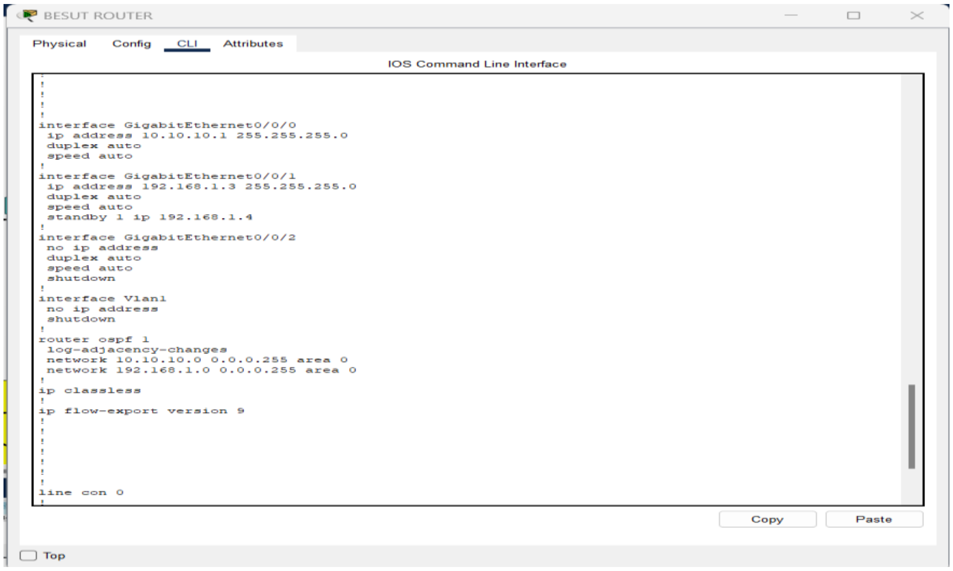


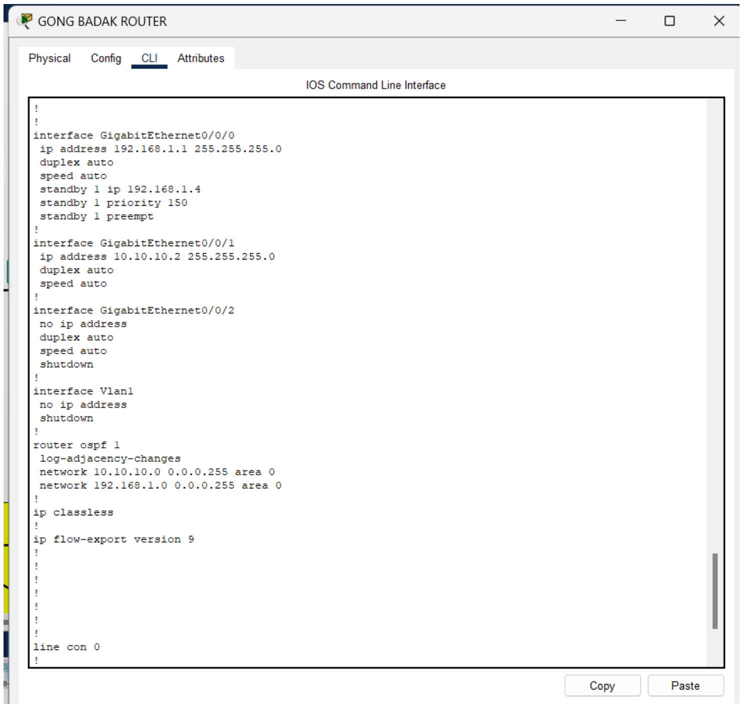
Figure 9. UNISZA Network Topology for Besut (iv)

The Besut Router, Gong Badak Router, and HSRP Router configurations inside the UNISZA Campus Network are shown in Figures 10, 11, and 12. These diagrams show the precise configuration procedures and options needed to set up every router, guaranteeing dependable backup routes and uninterrupted communication. Essential parameters and protocols, such HSRP and OSPF, are included in the setups to improve network resilience and data transmission efficiency. For configuration Besut Router which is interface GigabitEthernet0/0/0 ip address 10.10.10.1 255.255.255.0, interface GigabitEthernet0/0/1 ip address 192.168.1.3 255.255.255.0 standby 1 ip 192.168.1.4, router ospf 1 network 10.10.10.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255.area 0. For configuration Gong Badak Router which is interface GigabitEthernet0/0/0 ip address 192.168.1.1 255.255.255.0 standby 1 ip 192.168.1.4 standby priority 150 standby preempt, router ospf 1 network 10.10.10.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255.area 0, interface GigabitEthernet0/0/1 ip address 10.10.10.2 255.255.255.0. For configuration HSRP Router whichis interface GigabitEthernet0/0/0 ip address 10.10.10.3 255.255.255.0, interface GigabitEthernet0/0/1 ip address 192.168.1.2 255.255.255.0 standby 1 ip 192.168.1.4, router ospf 1 network 10.10.10.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255.area 0 .



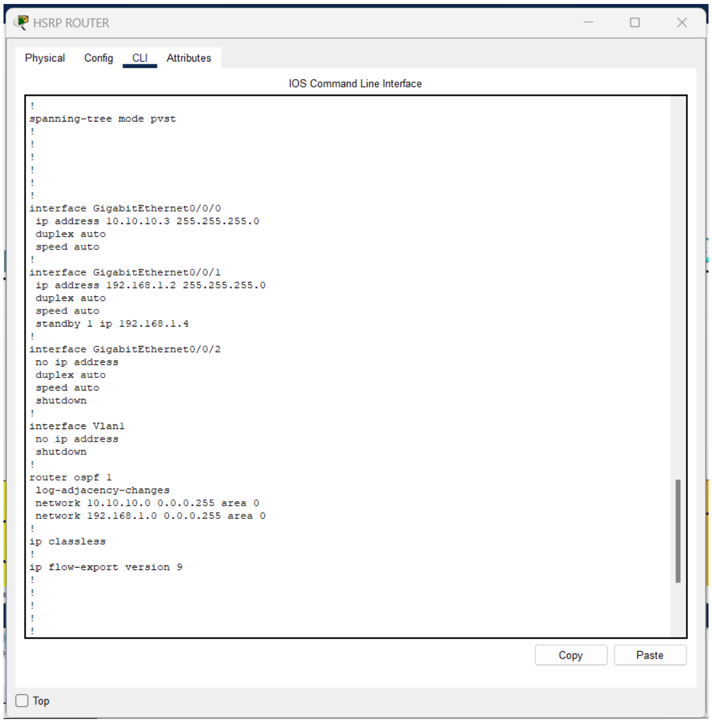
```
!
!
!
!
interface GigabitEthernet0/0/0
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.1.3 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 192.168.1.4
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
line con 0
!
```

Figure 10. Configuration for Besut Router



```
!
!
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 192.168.1.4
 standby 1 priority 150
 standby 1 preempt
!
interface GigabitEthernet0/0/1
 ip address 10.10.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
```

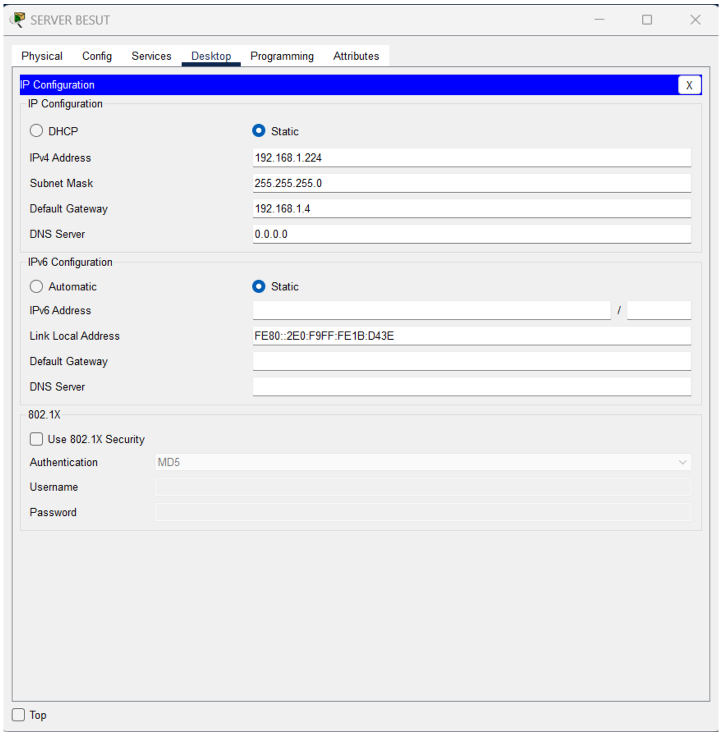
Figure 11. Configuration for Gong Badak Router



```
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 ip address 10.10.10.3 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 standby 1 ip 192.168.1.4
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 10.10.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
```

Figure 12. Configuration for HSRP Router

The Besut Server and the Gong Badak Server setups within the UNISZA Campus Network are shown in Figures 13 and 14. The processes and parameters needed to configure each server are shown in detail in these figures, guaranteeing peak performance and a smooth network integration. Using IP address for Besut Server is ‘192.168.1.224’ and for Gong Badak Server is ‘192.168.1.5’



IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.224

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.4

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2E0:F9FF:FE1B:D43E

Default Gateway:

DNS Server:

802.1X

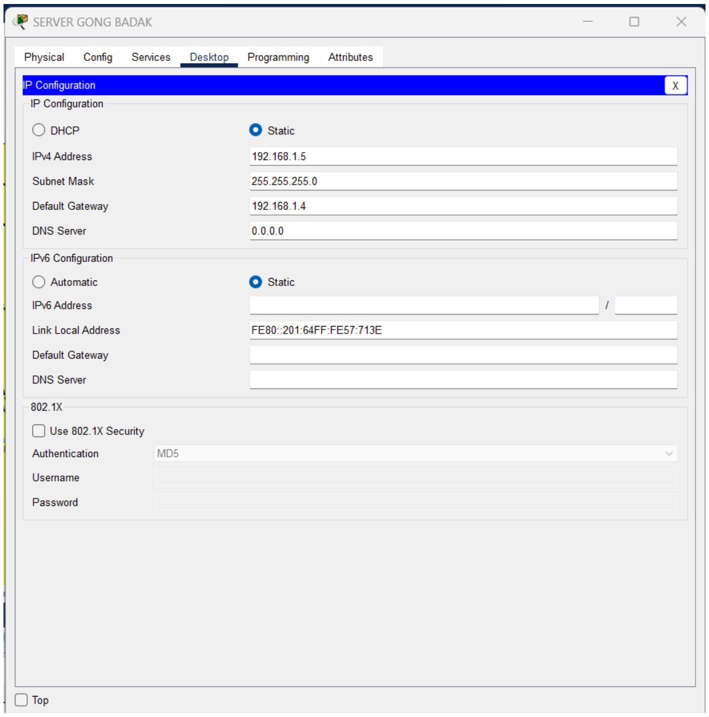
□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 13. Configuration for Besut Server



IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.5

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.4

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::201:64FF:FE57:713E

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

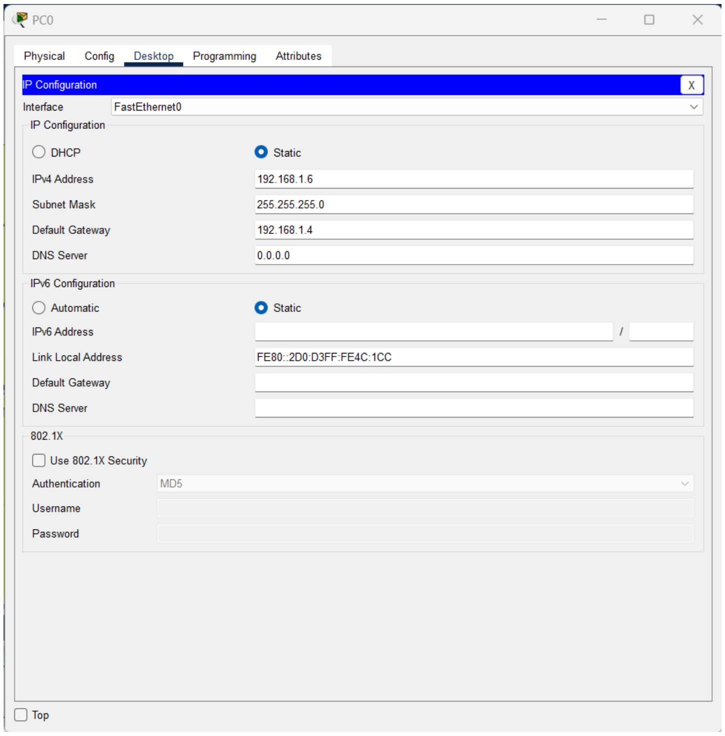
Authentication: MD5

Username:

Password:

Figure 14. Configuration for Gong Badak Server

Figure 15 illustrates the configuration for the PCs within the UNISZA Campus Network. This figure providesdetailed steps and settings used to configure each PC, ensuring they are properly integrated into the network. Using ip address for all pcs '192.168.1.5 until 192.168.1.223'.



PC0

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.6

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.4

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:D3FF:FE4C:1CC

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

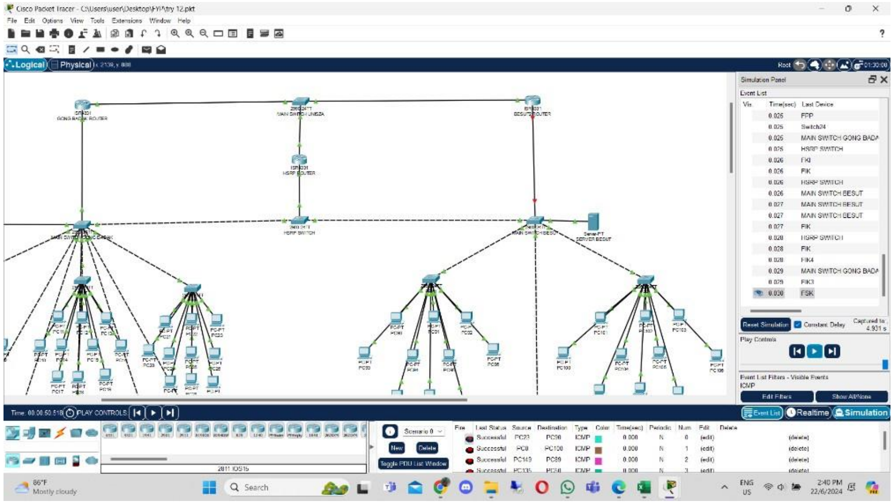
Authentication: MD5

Username:

Password:

□ Top

Figure 15. Configuration for PC



Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.026	FPP
	0.025	Switch24
	0.025	MAIN SWITCH GONG BADA
	0.025	HSRP SWITCH
	0.026	FKI
	0.026	FIK
	0.026	HSRP SWITCH
	0.026	MAIN SWITCH BESUT
	0.027	MAIN SWITCH BESUT
	0.027	MAIN SWITCH BESUT
	0.027	FIK
	0.028	HSRP SWITCH
	0.028	FIK
	0.028	FIK4
	0.029	MAIN SWITCH GONG BADA
	0.029	FIK3
👁	0.030	FSK

Reset Simulation ☑ Constant Delay Captured to: 4.931 s

Play Controls

Event List Filters - Visible Events

ICMP

Edit Filters | Show All/None

Event List | Realtime | Simulation

Scenario 0

New | Delete | Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC23	PC98	ICMP	🟩	0.000	N	0	(edit)	(delete)
●	Successful	PC8	PC100	ICMP	🟫	0.000	N	1	(edit)	(delete)
●	Successful	PC149	PC89	ICMP	🟪	0.000	N	2	(edit)	(delete)
●	Successful	PC135	PC50	ICMP	🟩	0.000	N	3	(edit)	(delete)

Figure 16. Simulation for throughput takes

$$Throughput = \frac{number\ of\ packet\ x\ size\ of\ packet}{times} \qquad (1)$$

Eq (1) used to calculate throughput from simulation in packet tracer.

Table 1. Throughput Table

	Number of intakes	Size of Packets	Number of packets	Without Disaster	Disaster
Time (s)	1	32	5	0.016	0.030
Time (s)	2	32	5	0.017	0.020
Time (s)	3	32	5	0.015	0.040
Average (s)	4	32	5	0.016	0.030

In order to observe the failover and recovery processes of OSPF and HSRP, disaster situations were simulated by purposefully turning off important network links. Throughput, latency, and recovery times were measured using Packet Tracer simulations in a variety of scenarios. Five packets with a size of 32 bytes each are sent throughout each simulation. In the event that there is nodisaster, the first time around is 0.016 seconds, the second time is 0.017 seconds, and the third time is 0.015 seconds. It takes 0.016 seconds on average. Five packets with a size of 32 bytes each are sent throughout each simulation. For the first, second, and third times, the results in the disaster scenario are 0.030, 0.020, and 0.040 seconds, respectively. It takes 0.030 seconds on average.

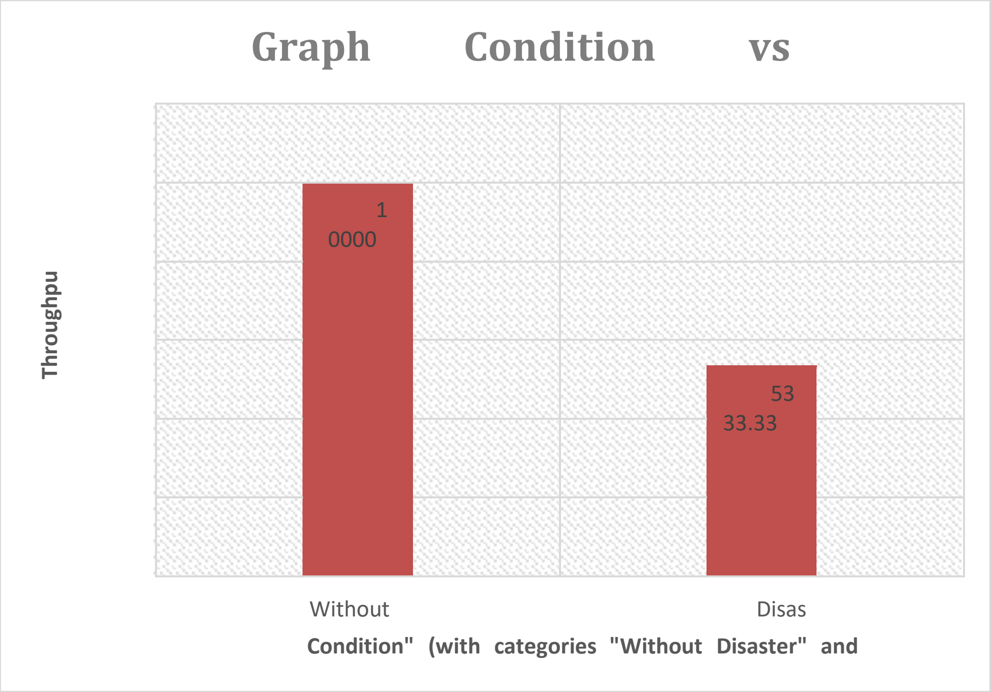
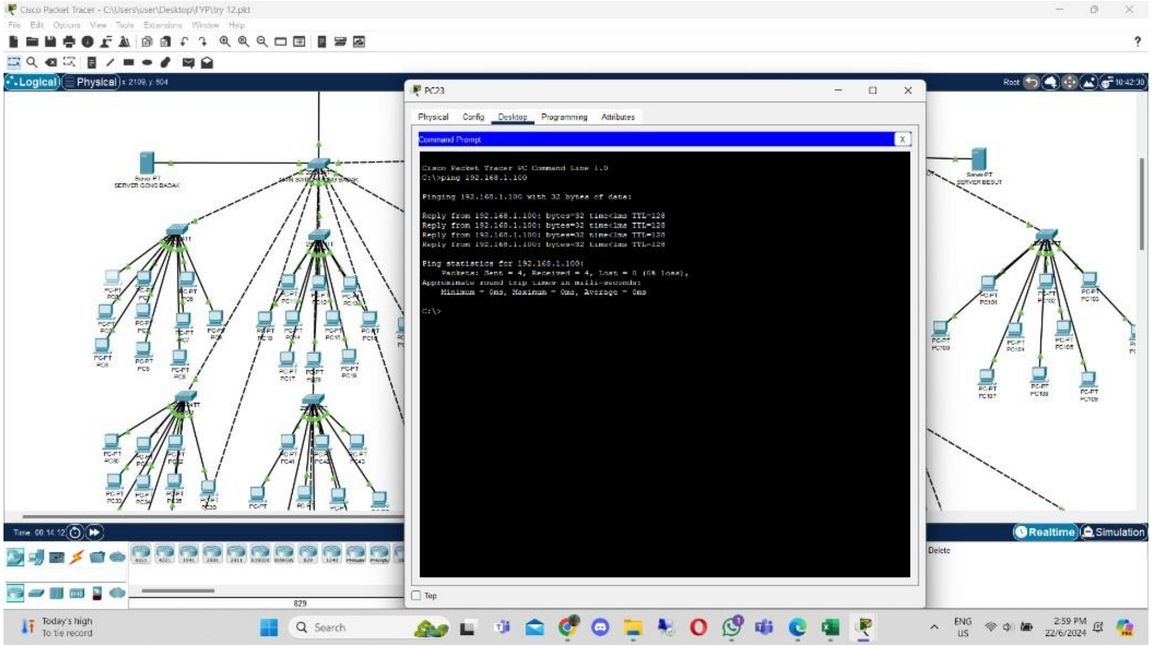


Figure 17. Graph of Condition vs Throughput

We can see from the results of the above Figure 17,that the throughput produced by a topology without a disaster is higher, at 10,000 bps, compared to the throughput of a topology with a disaster, which is 5,333.33 bps. This is due to the possibility that a disaster would disrupt the network, resulting in packet loss and the requirement for retransmissions. In the event of a disaster, these interruptions decrease data transmission efficiency and lower total throughput.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 18. ping pc for average loss takes

Table 2. Latency Table

Pinging PC fromA to B	Average Loss (ms)	
	Without Disaster,	Disaster
23 to 90	0	0
0 to 100	2	6
149 to 89	0	2
135 to 50	0	0
60 to 200	0	0
TotalAverage Loss(ms)	2	8

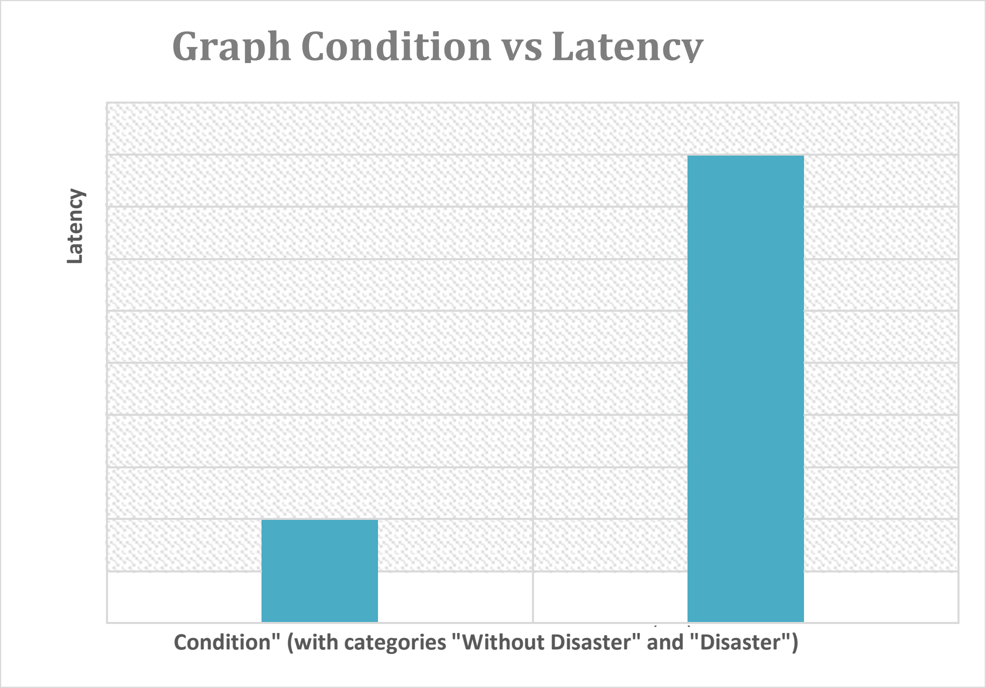


Figure 19. Graph Condition vs Latency

The average latency is found for the latency portion by using the ping method from PC to PC. Pinging PCsin an environment free of disasters yields the following results: 0 ms for the first ping from PC 23 to PC 90,2 ms for the second from PC 0 to PC 100, 0 ms for the third from PC 149 to PC 89, 0 ms for the fourth fromPC 135 to PC 50, and 0 ms for the fifth from PC 60 to PC 200. The following happens in a disaster scenario:the first ping time from PC 23 to PC 90 is 0 ms, the second ping time from PC 0 to PC 100 is 6 ms, the fourth is 0 ms from PC 135 to PC 50, the fifth is 0 ms from PC 60 to PC 200, and the third is 2 ms from PC149 to PC 89. It has been determined what the overall average latency is for each scenario: 2 ms for the disaster-free environment and 8 ms for the disaster scenario.

We can see from the results of the above Figure 19 that the latency produced by a topology without a disaster is lower, at 2 ms, compared to the latency of a topology with a disaster, which is 8 ms. This is due to the fact that a disaster throws off the regular network paths, forcing packets to choose longer detours and perhaps resulting in network congestion. In times of calamity, these factors lead to greater latency because they lengthen the time it takes packets to travel from their source to their destination.

5. CONCLUSION

This study shows how to improve network resilience in educational institutions by combining Open Shortest Path First (OSPF) and Hot Standby Router Protocol (HSRP). Through the use of Packet Tracer simulations, the study offers network managers practical advice on how to put in place reliable backup systems that guarantee uptime in the event of a network loss. These results demonstrate how important redundancy procedures are to preserving continuous administrative and academic operations. In the future, the knowledge acquired from this study will be useful in continuing conversations aboutimproving data security procedures in educational environments. The effective deployment of sophisticatedbackup and recovery systems highlights UNISZA's dedication to preserving uninterrupted academic and administrative activities while fortifying its defences against possible attacks. In order to keep UNISZA at the forefront of data protection and educational quality, network resilience methods will need to be continuously improved and adapted as technology advances.

REFERENCES

[1] Vishwa Nand Chandra, & Kumar, K. (2015). *QoS Improvement in AOMDV through Backup and Stable Path Routing*. https://doi.org/10.1109/csnt.2015.128

[2] Takashi Kurimoto, Yamada, H., Shigeo Urushidani, Syoko Mikawa, Eisuke Kaneyoshi, & Oki, E. (2017). *Multi-campus ICT equipment virtualization architecture for cloud and NFV integrated service*. https://doi.org/10.1109/codit.2017.8102662

[3] Rahman Mohamed, H. A. (2014). A Proposed Model for IT Disaster Recovery Plan. *International Journal of Modern Education and Computer Science*, *6*(4), 57–67. https://doi.org/10.5815/ijmecs.2014.04.08

[4] Simanjuntak, I. U. V., Haidi, J., Heryanto, & Silalahi, L. M. (2023). Simulation and Performance Analysis of Network Backup Systems Using Hot Standby Router Protocol (HSRP) Method on Real-Time Networks. *International Journal of Electronics and Telecommunications*. https://doi.org/10.24425/ijet.2023.147698

[5] Firmansyah, M. W. R. a. P. (2018). Analisis Perbandingan Kinerja Jaringan CISCO Virtual Router Redundancy Protocol (VRRP) Dan CISCO Hot Standby Router Protocol (HSRP). *Repository Universitas Bina Sarana Informatika (RUBSI)*, 764–769. https://repository.bsi.ac.id/index.php/unduh/item/221191/Analisis-Perbandingan-Kinerja-Jaringan-CISCO-VRRP-&-CISCO-HSRP.pdf

[6] Omumbo, N. J., Muhambe, T. M., & Ratemo, C. M. (2021). Evaluation of Routing Performance using OSPF and Multi-Controller Based Network Architecture. *International Journal of Computer Networkand Information Security*, *13*(4), 45–61. https://doi.org/10.5815/ijcnis.2021.04.05

[7] Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. *Computer Standards & Interfaces*,*68*, 103391. https://doi.org/10.1016/j.csi.2019.103391

[8] Fiade, A., Agustian, M. A., & Masruroh, S. U. (2019). *Analysis of Failover Link System Performance in OSPF, EIGRP, RIPV2 Routing Protocol with BGP*. https://doi.org/10.1109/citsm47753.2019.8965373

[9] Biradar, A. G. (2020). *A Comparative Study on Routing Protocols: RIP, OSPF and EIGRP and Their Analysis Using GNS-3*. https://doi.org/10.1109/icraie51050.2020.9358327

[10] Sengupta, S., & Annervaz, K. M. (2014). Multi-site data distribution for disaster recovery—A planning framework. *Future Generation Computer Systems*, *41*, 53–64. https://doi.org/10.1016/j.future.2014.07.007

[11] Nor Aida Mahiddin, & Nurul I.Sarkar. (2019). An Efficient Gateway Routing Scheme for Disaster Recovery Scenario. *Tuwhera (Auckland University of Technology)*. https://doi.org/10.1109/icoin.2019.8718189