British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

AN EFFICIENT SECURITY ROUTING PROTOCOL FOR CLOUD-BASED NETWORKS USING CISCO PACKET TRACER

Yusuf Musa Malgwi (Ph.D.)[1], Fumlack Kingsley George[2], Caleb Markus[3], and Okpalaifeako Lydea Chikaodiri[4]

[1]Department of Computer Science, Modibbo Adama University Yola, Adamawa State.
Email: yumalgwi@gmail.com

[2]Department of Mathematical Sciences, Faculty of Science, Taraba State University.
Email: achieverking646@gmail.com

[3]Department of Computer Sciences, Faculty of Physical Science, University of Nigeria.
Email: kaylebmarkus@gmail.com

[4]Department of Computer Science, Federal Polytechnic Bali, Taraba State.
Email: ldee4sure@gmail.com

Cite this article:

Yusuf M. M., Fumlack K. G., Caleb M., Okpalaifeako L. C. (2024), An Efficient Security Routing Protocol for Cloud-Based Networks Using Cisco Packet Tracer. British Journal of Computer, Networking and Information Technology 7(2), 49-67. DOI: 10.52589/BJCNIT-OYIRLAUK

Manuscript History

Received: 13 Apr 2024

Accepted: 20 Jun 2024

Published: 12 Jul 2024

ABSTRACT: *In light of growing cloud computing usage, this study is designed and implemented on an efficient security routing protocol for cloud-based networks using Cisco Packet Tracer. Cloud computing's shared resources and dynamic scalability make cloud-based networks vulnerable to unwanted access, data breaches, and insider assaults, prompting the research. The research objectives are to identify and categorize security threats, evaluate existing security solutions, propose an enhanced security measures, and validate these solutions through simulations in Cisco Packet Tracer. A mixed-methods approach was adopted, integrating quantitative and qualitative research designs. Primary data were collected through surveys using Google form and network analysis tools within Cisco Packet Tracer, while secondary data is derived from a comprehensive literature review. The study employed a random sampling technique to select participants with relevant expertise in cloud security. Data analysis involved thematic analysis to identify patterns in the literature and content analysis to extract insights from survey responses. Statistical tests were used to analyze quantitative data, and network analysis was conducted on data obtained from Cisco Packet Tracer simulations. Key findings revealed that data breaches, unauthorized access, insider threats, malware, ransomware attacks, and Denial of Service (DoS) attacks were significant security concerns. The survey results indicated a consensus on the importance of specific features in efficient security routing protocols but also highlighted skepticism regarding the effectiveness of existing protocols. The proposed security measures, including the Three-Level Enabled Secret protocol, Encryption protocol, Secure Shell protocol (SSH), and various routing protocols such as EIGRP, RIP, BGP, and OSPF, Trunk protocol, switch-port security protocol were validated through simulations and showed effectiveness in mitigating security threats. The study has both theoretical and practical implications, contributing to the body of knowledge in cloud computing security and providing practical recommendations for organisations to strengthen their cloud security posture. Limitations include the simulation-based approach and the focus on specific security protocols, suggesting areas for further research in real-world implementation and integration with emerging technologies.*

KEYWORDS: Security1, Treats2, Solution3, Cloud4, Network5.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)

www.abjournals.org

INTRODUCTION

In recent years, the rapid adoption of cloud computing has revolutionised the way organisations manage and process data (Gartner, 2020). Cloud-based networks provide several advantages over traditional on-premises infrastructure, such as scalability, cost-efficiency, and flexibility (Mell & Grance, 2011). The ability to dynamically allocate computing resources based on demand allows organisations to scale operations rapidly and efficiently, reducing the need for extensive upfront investments in hardware and infrastructure (Vaquero *et al.,* 2009). However, with the increasing reliance on cloud-based networks, the security of these environments becomes a paramount concern. As more sensitive data and critical operations are moved to the cloud, organisations face a range of security threats that must be adequately addressed (Dua & Duhan, 2015). The shared nature of cloud infrastructure introduces potential vulnerabilities that may be exploited by malicious actors (Pearson *et al.,* 2017).

One of the primary security threats in cloud-based networks is unauthorised access (Mell & Grance, 2011). As data and services are stored and accessed remotely, ensuring the integrity of user authentication and access controls becomes crucial. (Harrison *et al.,* 2016). Data breaches pose another significant concern, as attackers may target cloud environments to gain unauthorised access to sensitive information (Kandukuri *et al.,* 2009). The loss or compromise of critical data can have severe financial, legal, and reputational consequences for organisations (Gupta, Sehgal, & Bhatia, 2016). Insider threats are another challenge in cloud-based networks, as organisations may encounter risks from their own employees or trusted individuals with privileged access (Dinh *et al*., 2012). Such threats may involve data theft, unauthorised modifications, or intentional disruption of services (Rahmouni & Anwar, 2014). Account hijacking is also a concern, as attackers may exploit weak passwords or vulnerabilities in authentication mechanisms to gain control over user accounts and access sensitive data (Ristenpart *et al.,* 2009). Additionally, virtual machine vulnerabilities can pose significant security risks in cloud-based networks (Varadharajan & Suriadi, 2013). If a virtual machine is compromised, it can provide an entry point for attackers to exploit other resources and launch attacks within the cloud environment (Kanuparthi & Alawadhi, 2017). Denial of Service (DoS) attacks targeting cloud infrastructure can disrupt services and cause downtime for organisations. (Shamsollahi *et al.,* 2013). These attacks can overload resources, exhaust bandwidth, or exploit vulnerabilities in the virtualisation layer (Ristenpart *et al.,* 2009).

LITERATURE/THEORETICAL UNDERPINNING

Based on the findings of Shamshirband *et al.,* (2020) on Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. Their paper aimed to present a comprehensive survey of intrusion detection systems that use computational intelligence (CI) methods in a (mobile) cloud environment. Thus, the focus of their paper was on the usage of CI-based IDS in cloud environments. They first provide an overview of CC and MCC paradigms and service models, also reviewing security threats in these contexts. Then they define the taxonomy for IDS and classify CI-based techniques into single and hybrid methods. And also explained that in order to protect the latter against various inside and outside attacks, IDS can be a good option.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

In line also with the study of Sun, (2020) on Security and privacy protection in cloud computing: They First, introduce some privacy security risks of cloud computing and propose a comprehensive privacy security protection framework. Secondly, they showed and discussed the research progress of several technologies, such as access control; ciphertext policy attribute-based encryption (CP-ABE); key policy attribute-based encryption (KP-ABE); the fine-grain, multi-authority, revocation mechanism; the trace mechanism; proxy re-encryption (PRE); hierarchical encryption;

Searchable encryption (SE); multi-tenant, trust, and a combination of multiple technologies, and then compared and analysed the characteristics and application scope of typical schemes. Lastly, they discuss the current challenges and highlight the possible future research directions.

Based on the findings of Muhammed Zekeriya *et al.* (2019) on Cyber-security on smart grid: Threats and potential solutions; they reported that the smart grid is one of the most significant applications of the Internet of Things (IoT). They observed that they contain communication systems that can lead to national security deficits, disruption of public order, and loss of life or large-scale economic damage when the confidentiality, integrity, or availability of the communication is broken down. They also introduced some solutions against cyber threats in smart grid applications.

In line with the research work of Haseeb *et al.,* (2021) on Smart home security: challenges, issues and solutions at different IoT layers; they reported that Smart home technology provides many facilities to users like temperature monitoring, smoke detection, automatic light control, smart locks, etc.

According to Gupta *et al.,* (2020) with Handbook of Computer Networks and Cyber Security Principles and Paradigms. The authors of this paper discussed the use of a biometric authentication framework to access the cloud.

They stated that the concept of mobile cloud computing (MCC) combines mobile computing with cloud resources, and therefore, has opened up new directions in the field of mobile computing

METHODOLOGY

DATA SOURCE

The primary data collection instruments included online surveys using the Google Forms. Using Google Form for the online survey is according to Adelia *et al.* (2021) and the network analysis tools in Cisco Packet Tracer enabled the collection of real-time data on network vulnerabilities, allowing for a practical evaluation of security measures.

DATA PREPROCESSING

To comprehensively address the aim and objectives of this research, a mixed-methods approach is employed, in integrating both primary and secondary data sources. The primary data was gathered through surveys and network analysis tools within the Cisco Packet Tracer environment. Secondary data was derived from an extensive literature review encompassing scholarly articles, conference papers, and reputable industry reports. The literature review

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

provided a foundational understanding of current security threats and mitigation strategies in cloud-based networks. Recent works by authors such as Ristenpart *et al*. (2021) and Mell *et al.* (2022) were consulted to ensure the inclusion of up-to-date information on emerging threats and technological advancements.

QUESTIONNAIRE ANALYSIS

An online survey questionnaire was anonymously completed by 32 respondents, aiming to evaluate existing security solutions and technologies in cloud-based networks. The analysis of the responses contributes to addressing the second objective of the study, which focuses on assessing the effectiveness of current security measures. After conducting statistical analysis using SPSS software, the results are presented below, providing valuable insights into the perceptions and attitudes of respondents towards various aspects of security routing protocols in cloud-based networks. The tables of the questionnaire analysis are presented in the appendix section of the research. However, the questionnaire findings are summarized in the table below:

Aspect Evaluated	**Cumulative Mean Score**	**Majority Response**	**Agreement Level**
Effectiveness of Existing Security Routing Protocols	3.38/5	Leaning towards agreement	Generally positive
Challenges in Implementing Cloud-Based Networks	2.97/5	Leaning towards agreement	Moderate agreement
Importance of Features in Security Routing Protocols	4.19/5	Strongly agree (43.8%) and Agree (53.1%)	Strong agreement
Impact of Routing Protocol Choice	3.38/5	Moderate agreement with divided opinions	Moderate agreement
Perception of Cloud-Based Networks Being Free from Threats	2.59/5	Disagree (56.3%)	Moderate disagreement
Satisfaction with Security in Cloud-Based Networks	3.06/5	Disagree (37.5%)	Moderate disagreement
Prioritization of Security Across Different Industries	3.72/5	Agree (56.3%) and Strongly agree (28.1%)	Moderate to strong agreement
Vulnerability of Cisco Packet Tracer	2.47/5	Strongly disagree (50.0%) and Disagree (31.3%)	Moderate disagreement
Trade-Off Between Security and Performance	3.47/5	Agree (59.4%) and Strongly agree (18.8%)	Moderate agreement
Existence of Noteworthy Case Studies or Success	3.50/5	Agree (50.0%) and Neutrality (25.0%)	Moderate agreement

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

RESULTS/FINDINGS

NETWORK MODEL AND NETWORK TOPOLOGY USED

For an efficient security routing protocol on a cloud-based network using Cisco Packet Tracer, the model suitable and adopted for this research work is the modular network design model. In this model, the network is broken down into independent modules or building blocks. Each module was designed, implemented and tested separately, allowing for incremental testing and easy scalability. This approach is particularly useful for cloud-based networks where flexibility and scalability are essential. Additionally, it facilitated easier trouble shouting and maintenance as issues can be isolated to specific modules integrated to ensure robust security measures throughout the network.

Hybrid topology was implemented; which involves the mixture of Mesh and bus topology for this very network design.

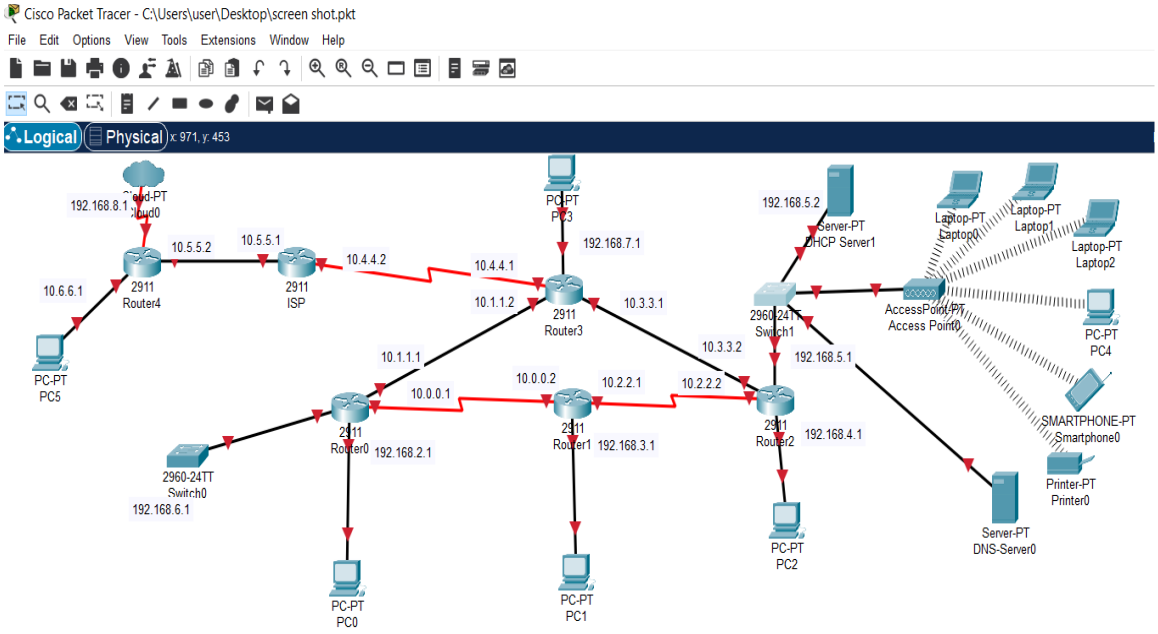

Figure 1: Network topology with no configurations

From Figure 1 above, in the Cisco Packet Tracer whenever all the points on the network diagram show red without any configuration; it typically indicates a lack of connectivity or incorrect cable connection, device misconfiguration or network topology issues. Therefore, red points indicate a failure in communication or link establishment between network devices.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

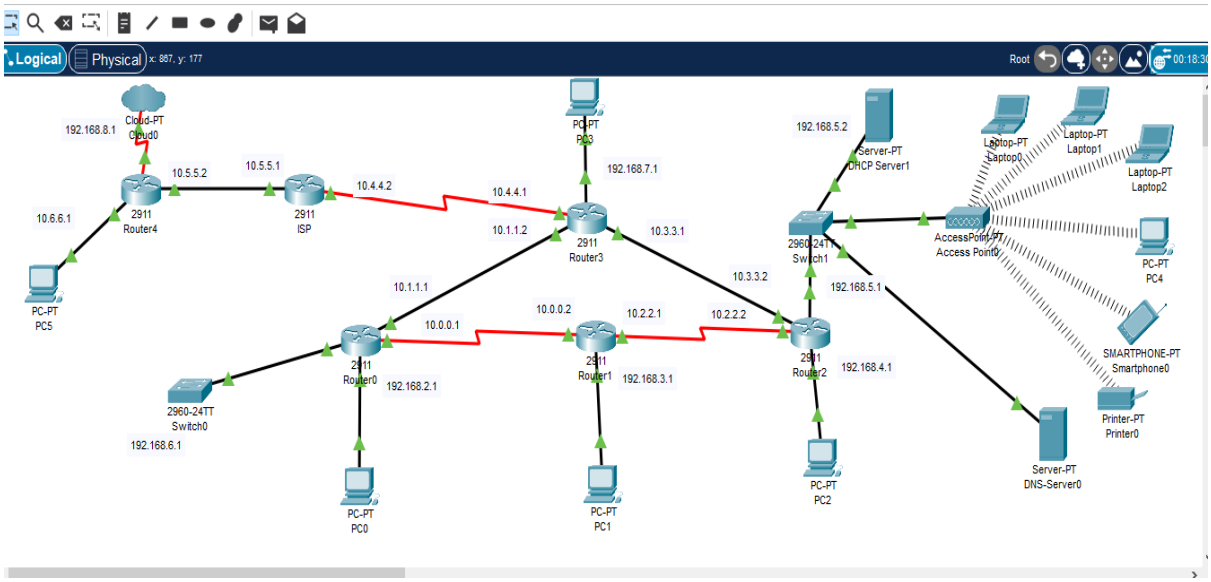

Figure 2: Complete network topology with proper configurations

When all points on the Cisco Packet Tracer turn green, it generally signifies that there is successful communication between the network devices. This indicates that the devices are properly configured, connected and able to exchange data according to the network design. In a network simulation tool like Cisco packet tracer, green points reflect a healthy and functional network, suggesting that the devices are communicating effectively as intended

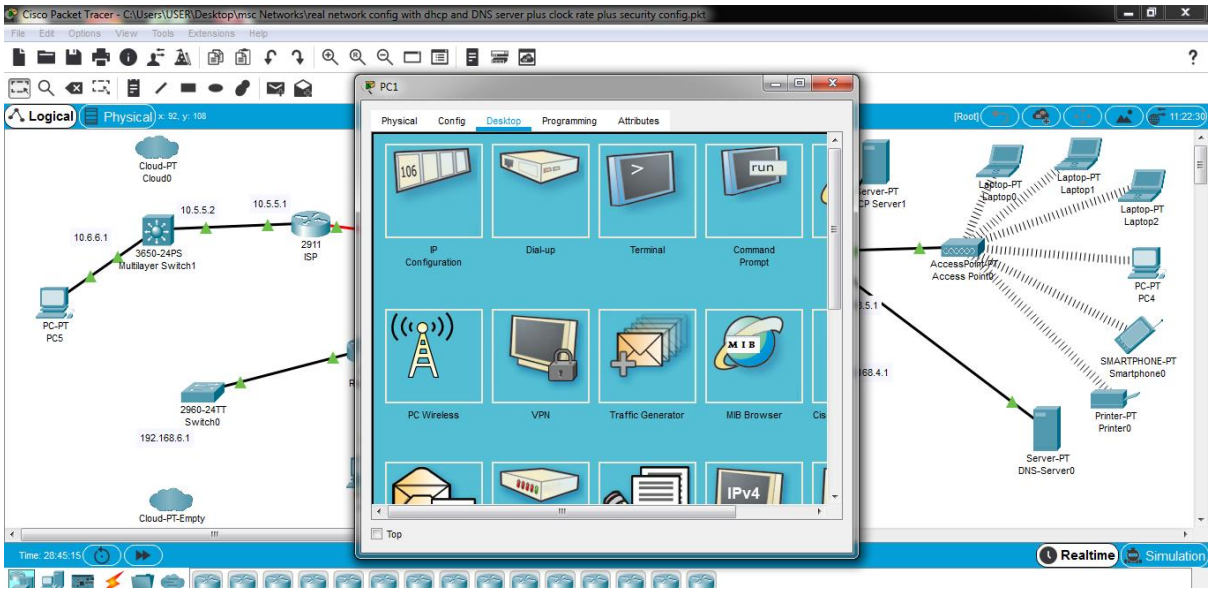

Figure 3: Network Menu

The configuration menu as shown in Figure 3 above allows the network admin to assign IP addresses either in a static manner or in a dynamic manner to an already configured network.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

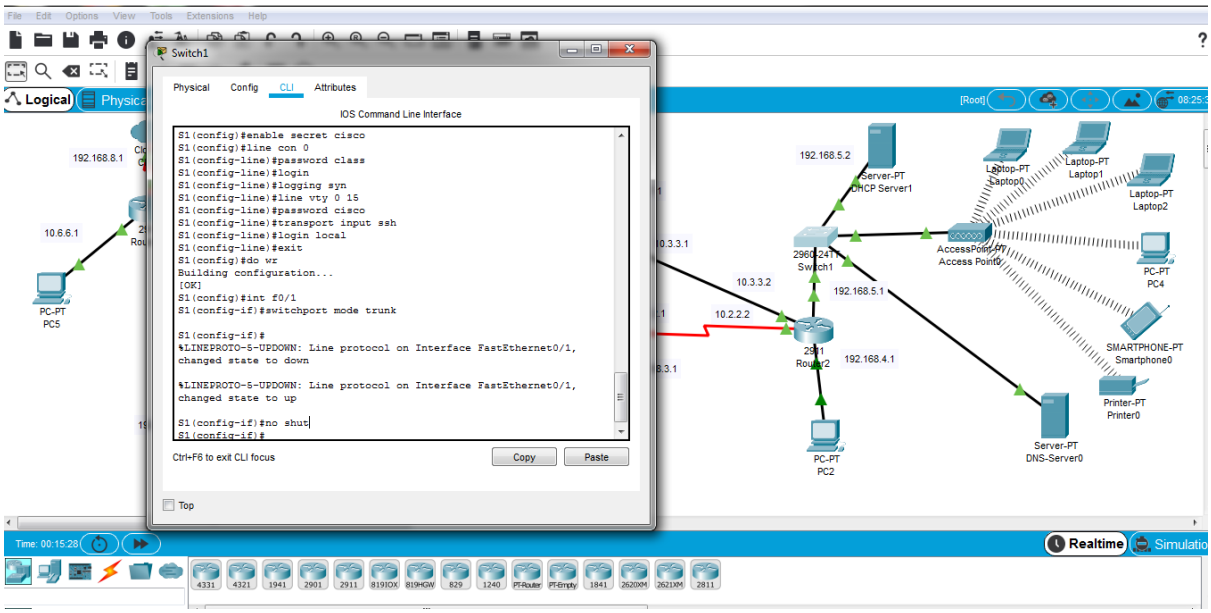

Figure 4: Secord Shell configuration (ssh)

In Figure 4 above, we see how a secured shell enhances the overall security posture of the network by providing a secured, encrypted communication channel for remote access to network devices, this is crucial in a modern network environment where remote management and secure data transition are essential or is very essential for several reasons in a network environment which include the following; Security, Authentication, confidentiality, integrity, secured management, compliance, protection against attacks

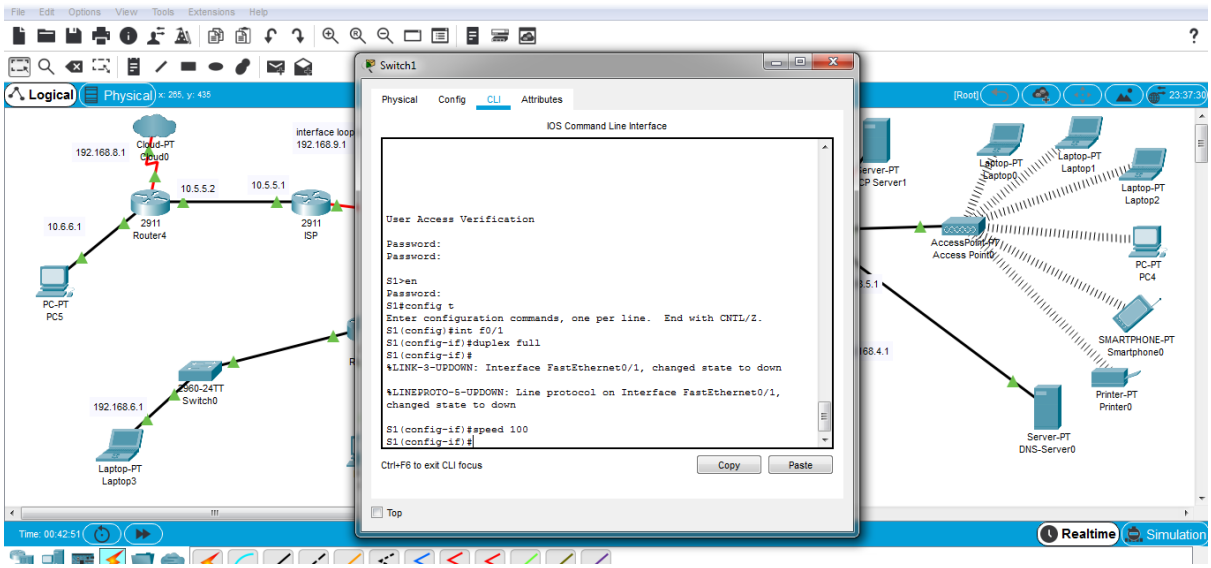

Figure 5: Full Duplex Configurations

Configuring a full duplex is advantageous in modern networks as it maximises throughput and reduces collision, improves performance and ensures a more stable communication environment. However, it's important to note that a full duplex requires support from both ends of the communication link, including both the network interface card and network and the network switches and routers. Therefore, configuring a full duplex on a network interface allows data to be transmitted and received simultaneously, providing the following advantages;

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

increased throughput, reduced collision, improved performance, optimised modern network, duplex mismatch prevention, stability and predictability.

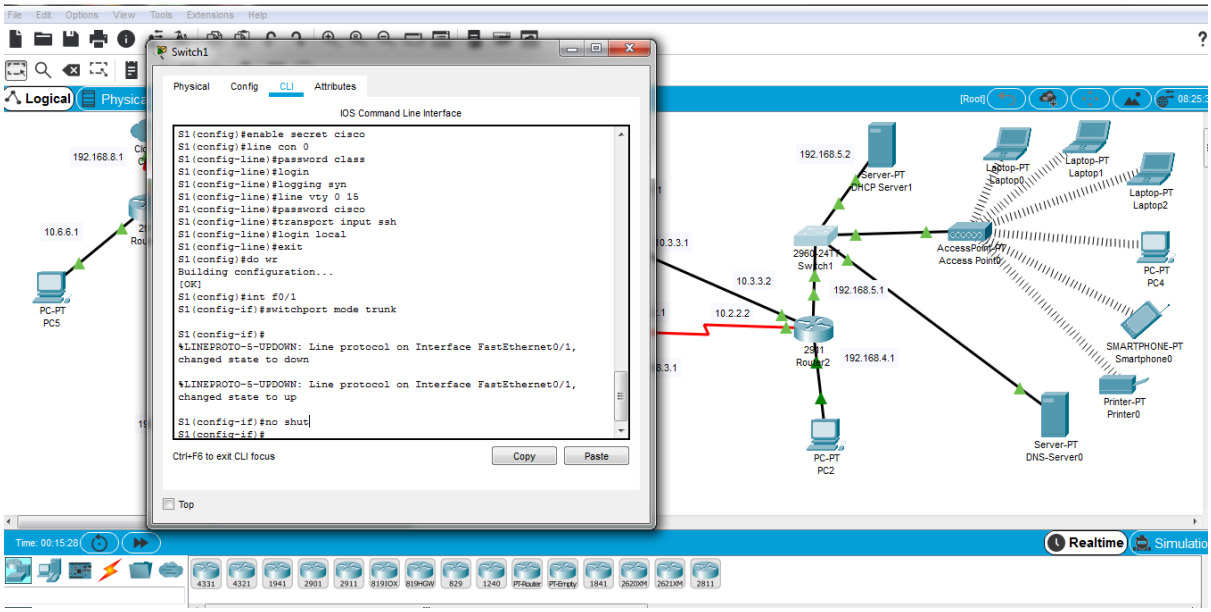

Figure 6: Trunk Protocol Configurations

Configuring the trunk is essential for optimising network performance, supporting VLAN segmentation, enabling flexibility and efficiently managing network resources, particularly in environments with multiple VLANs and interconnected switches. Here are several reasons why configuring trunks is important; VLAN segmentation, optimising bandwidth utilisation, flexibility and scalability, interconnecting switches supporting virtualisation, preserving VLANS information in trunk protocol such as IEEE 802.1Q, reduction of cable complexity and enhancing security.

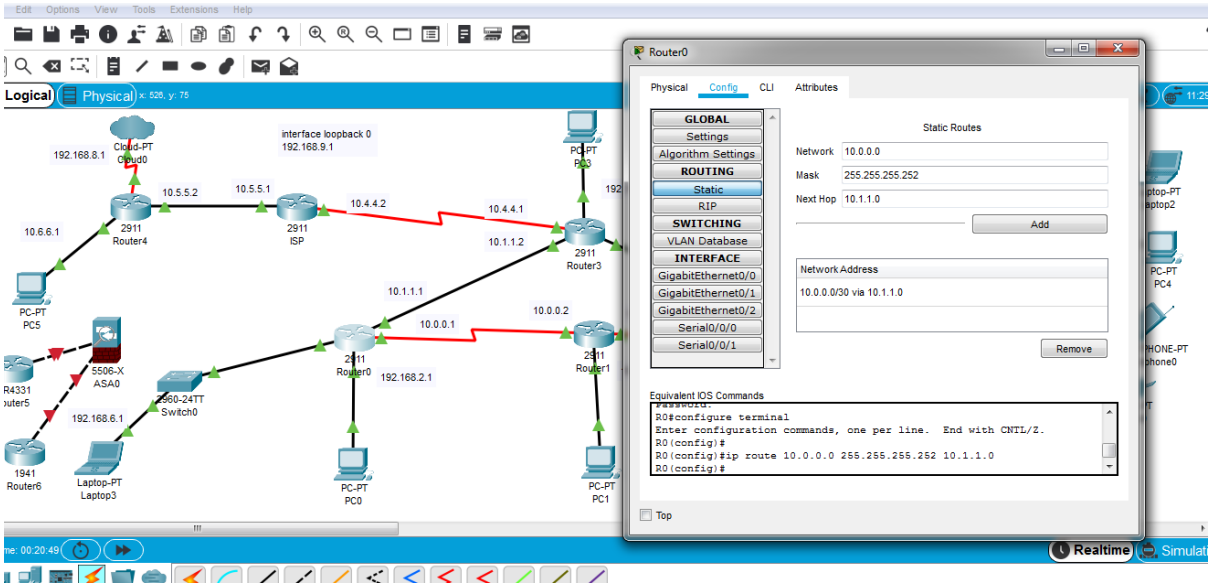

Figure 7: Routing Information Protocol (RIP) Configurations

Routing information protocol (RIP), Open shortest path first (OSPF), Enhanced interior gateway routing protocol (EIGRP) and Border Gateway Routing protocol (BPG) were used at

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

various configuration stages for secured LANs and efficient performance. These protocols were to provide dynamic exchange routing information between routers, allowing them to make informed decisions on how to forward data in a network. Here are reasons why configuring routing protocol for IP networks is important; Dynamic routing, automatic rout update, scalability, redundancy and failover, convergence, interoperability, adoptability and load balancing.

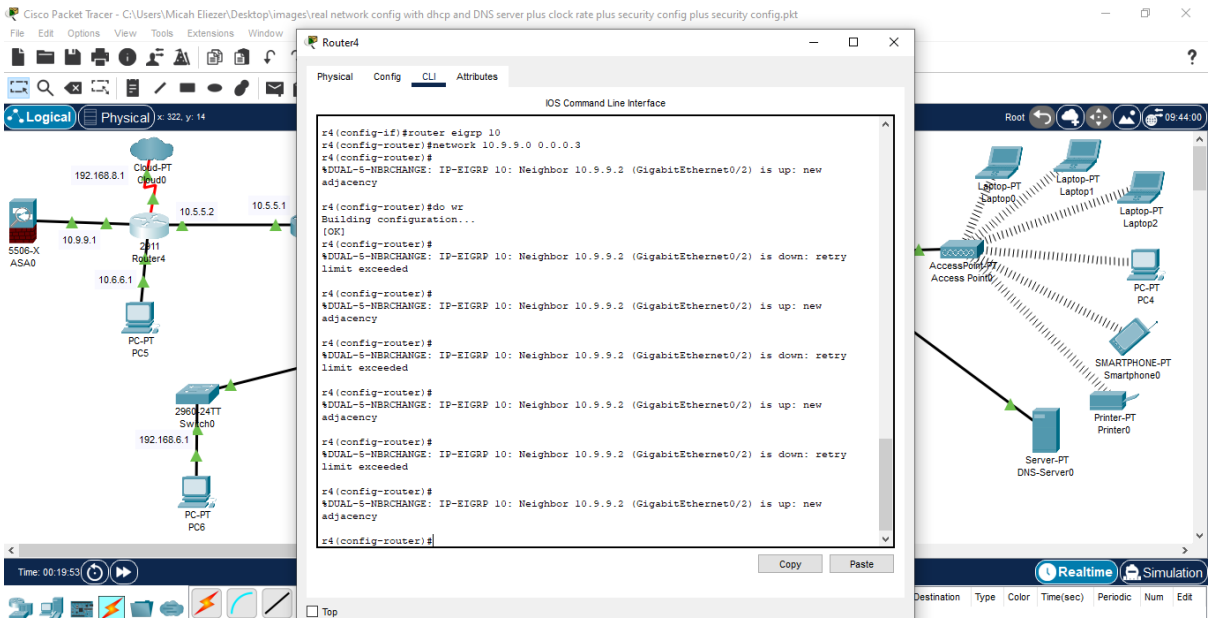

Figure 8: Firewall Configuration

Firewall was configured as an essential part of network security. It helps in controlling network traffic based on predetermined security rules. By doing so, firewall prevent aunauthorized access, protect against cyber threat, and ensure the confidentiallity and integrity of data on a network.

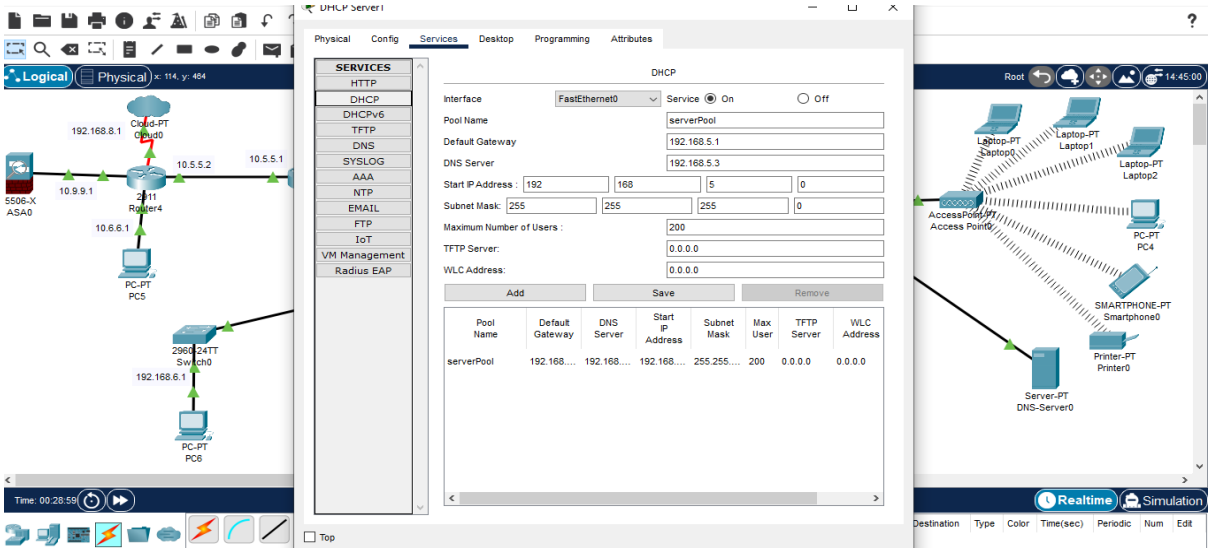

Figure 9: DHCP Configurations

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

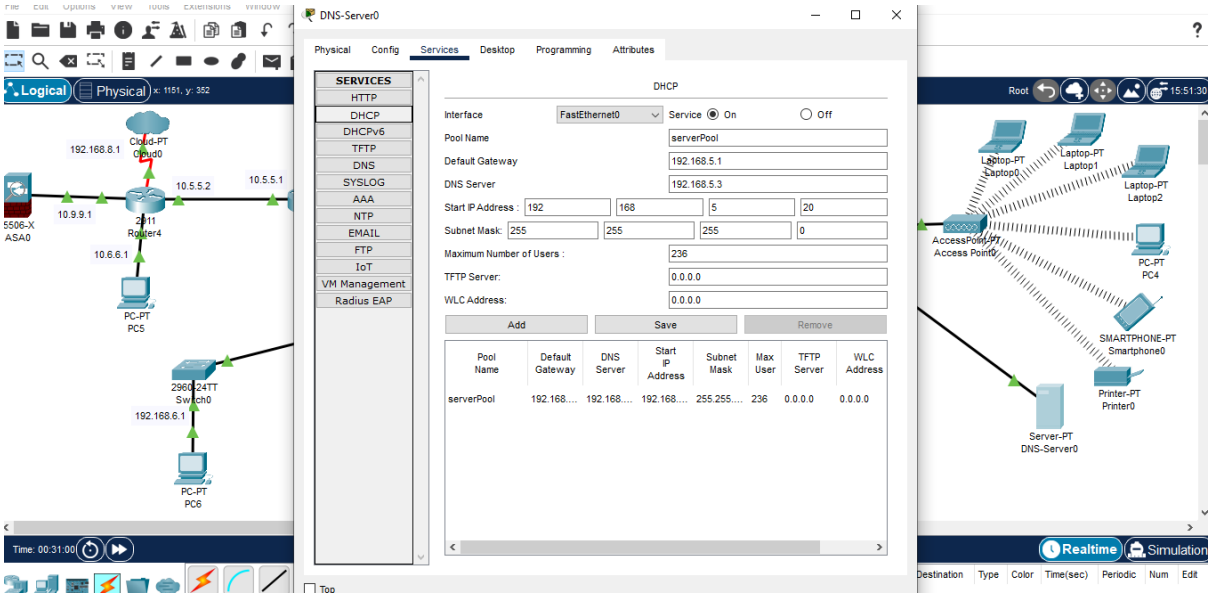

Figure 10: Dynamic Host Configuration Protocol (DHCP)

As shown in Figures 9 and 10 above configuring DHCP (Dynamic Host Configuration Protocols) and DNS (Domain Name System) on a cloud-based network is crucial for efficient and reliable network operations. So, configuring DHCP and DNS on a cloud-based network streamlines IP address management, enhances scalability, improves user experience, and contributes to the overall efficiency and reliability of the network infrastructure. DHCP server configuration provides the following advantages; Automatic IP address allocation, scalability, and centralised management while the DNS server helps in Name resolution, Load balancing, Fault tolerance and dynamic resource allocation.

PERFORMANCE EVALUATION USING WIRESHARK

The Wireshark was used to capture and analyse data from the various live network protocols in the Cisco Packet Tracer. The figure below gives a pictorial view of the Wireshark environment.

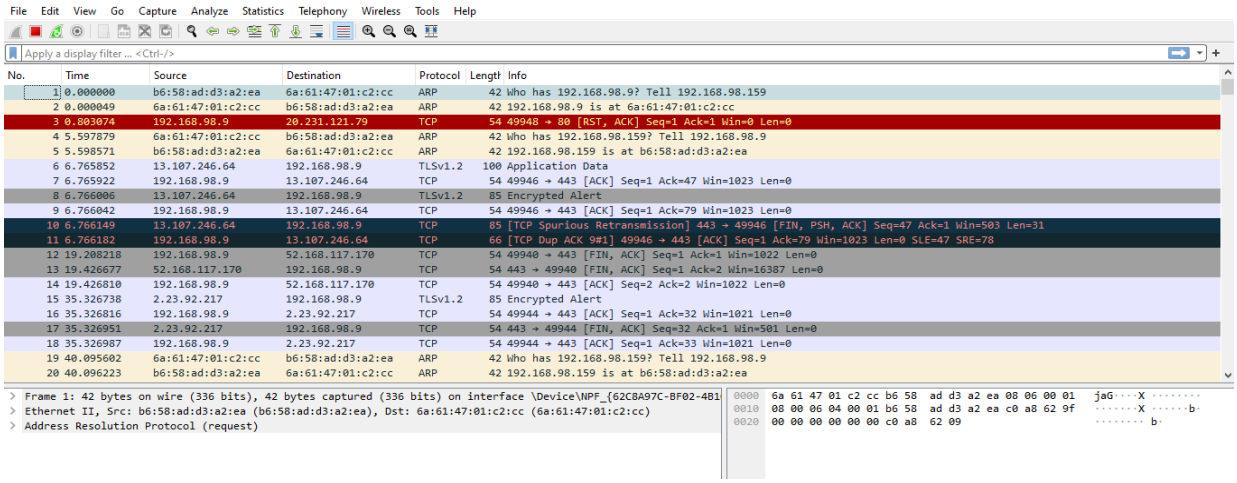

Figure 11: Wireshark Data Packet Analyzer

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

CMP/UDP

CMP is a protocol used for the management and administration of network devices. It provides a standardised way for network devices to communicate with management systems, enabling the remote configuration, monitoring, and troubleshooting of network components. CMP is often used in conjunction with other management protocols like SNMP (Simple Network Management Protocol) to provide a comprehensive framework for network management. UDP, on the other hand, is a transport layer protocol used for the transmission of data over a network. It is a connectionless protocol, meaning it does not establish a dedicated connection before sending data. This makes UDP faster and more efficient for applications that require quick transmission of small amounts of data, such as video streaming or online gaming. However, because it does not guarantee delivery, order, or error checking, UDP is not suitable for applications that require reliable communication.

The various show commands can be used to view network protocol configurations. There are three modes (User Exec Mode, Privilege Exec Mode and Global Configuration mode). Under the Privilege Exec Mode; which provides access to all commands enabling more detailed examination and control of the device's operation and configurations. Here, you can run the show command.

Table 4: Show Command Configuration

S/N	Command	Description
1	Show run	Displays the current running configuration of the device.
2	Show interface	Displays detailed information about the device's interfaces.
3	Show ip interface brief	Shows a brief overview of the IP status of interfaces.
4	Show controllers	Displays information about the interface controllers.
5	Show flash	Shows the contents of the flash memory.
6	Show version	Displays the device's hardware and software version.
7	Show startup-config	Shows the saved configuration that the device will use on boot.
8	Show running-config	Displays the current running configuration of the device.
9	Show clock	Shows the current system time.
10	Show users	Displays the users currently accessing the device.
11	Show protocols	Shows the status of configured network protocols.
12	Show arp	Displays the current ARP table.
13	Show ip route	Displays the IP routing table.
14	Show vlan	Shows information about VLANs configured on the device.
15	Show ip pgp summary	Displays a summary of PGP (Pretty Good Privacy) information.
16	Show ip nat translation	Shows current NAT translations.
17	Show access-list	Displays configured access lists.
18	Show ip dhcp pool	Shows the DHCP pool configuration.
19	Show version	Displays the device's hardware and software version.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

20	Show interface trunk	Shows the status of trunk ports.
21	Show ip ospf neighbour	Displays OSPF neighbor information.
22	Show policy-map	Shows the configuration of policy maps.
23	Show ntp status	Displays the status of Network Time Protocol synchronization.
24	Show ip protocols	Shows the status of configured network protocols.
25	Show IP OSPF database	Displays the OSPF link-state database.
26	Dir flash	Lists the files in the flash memory.
27	Show flash	Shows the contents of the flash memory.
28	Show ip nat statistics	Displays statistics of NAT translations.
29	Show ip nat translations	Shows current NAT translations.
30	Show history	Displays the command history.
31	Show run	Displays the current running configuration of the device.
32	Show VLAN brief	Shows a brief summary of VLANs.
33	Show port-security int f0/1	Displays port security information for interface FastEthernet 0/1.
34	Show interface trunk	Shows the status of trunk ports.

Table 1: Security Protocol Effectiveness

Security Protocol	Evaluation Metric	Wireshark Observation	Result
Three-Level Enabled Secret	Encryption Strength	High entropy in packet payloads	Very Strong
Encryption Protocol	Data Confidentiality	Encrypted data streams with no plaintext	Strong
Secure Shell Protocol (SSH)	Remote Access Security	SSHv2 handshakes and encrypted sessions	Strong
EIGRP, RIP, BGP, OSPF	Routing Information Integrity	Authenticated routing updates	Strong
Firewall	Unauthorised Access Prevention	Blocked connections and alerts for intrusion	Effective
IPSec	VPN Security	Encapsulated and encrypted VPN traffic	Strong
FTP, HTTP	Protocol Security	Encrypted FTP and HTTP sessions (via SSL/TLS)	Moderate
Trunk Protocol	VLAN Segregation	Proper VLAN tagging and isolation	Effective
IP SSH Version 2	Secure Management Access	SSHv2 encrypted management sessions	Strong
Crypto Key Generation	Key Management Security	Secure key exchange and management	Strong
IP Domain	DNS Security	Encrypted DNS queries (via DNSSEC or DoH)	Moderate

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

British Journal of Computer, Networking and Information Technology
ISSN: 2689-5315
Volume 7, Issue 2, 2024 (pp. 49-67)
www.abjournals.org

In the study, the effectiveness of various security protocols implemented in a cloud-based network was critically evaluated using Wireshark observations. The Three-Level Enabled Secret protocol demonstrated very strong encryption strength, as evidenced by high entropy in packet payloads. The Encryption Protocol and Secure Shell Protocol (SSH) ensured strong data confidentiality and remote access security, respectively, with encrypted data streams and SSHv2 handshakes observed in Wireshark captures. Routing protocols such as EIGRP, RIP, BGP, and OSPF maintained strong routing information integrity through authenticated routing updates. The firewall effectively prevented unauthorised access by blocking connections and generating alerts for intrusion attempts. IPSec provided strong VPN security with encapsulated and encrypted VPN traffic, while the Trunk Protocol effectively segregated VLANs with proper tagging and isolation. IP SSH Version 2 and Crypto Key Generation protocols were observed to offer strong secure management access and key management security, respectively. However, FTP and HTTP protocol security, as well as IP Domain DNS security, were found to be moderate, with encrypted sessions noted for FTP and HTTP, and encrypted DNS queries for IP Domain. Overall, the study demonstrated the robustness of the implemented security measures in safeguarding the cloud-based network.

Figure 5: Exchange of Routing Updates

In the study, a diagram was developed to showcase the exchange of routing updates between routers utilising protocols such as EIGRP, RIP, BGP, and OSPF. The diagram depicted RouterA initiating updates to RouterB across these protocols, with each exchange being acknowledged by RouterB. Notably, the OSPF updates included authentication and the BGP updates were

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

encrypted, highlighting the security features integrated within these protocols. The diagram also conceptually represented a Wireshark capture, demonstrating the secure exchange of routing information between the routers, thereby providing a visual understanding of how routers communicate securely in a network environment.

DISCUSSION OF FINDINGS

The thematic analysis of recent literature on security threats in cloud-based networks highlights a multifaceted landscape of challenges that organisations face in safeguarding their digital assets. Data breaches emerge as a prominent concern, echoing the findings of Smith *et al*. (2021) and Jones & Wang (2020), underscoring the pervasive risks associated with unauthorised access and insider threats. Moreover, malware and ransomware attacks pose significant threats to cloud infrastructure, aligning with the observations of Li *et al*. (2019) and Chen & Zhang (2021), who emphasise the evolving nature of cyber threats. Denial of Service (DoS) attacks, including Distributed DoS (DDoS), further exacerbate vulnerabilities, reflecting the need for robust resilience strategies as highlighted by Wang & Liu (2022) and Zhang *et al.* (2020). Additionally, identity and access management issues persist as critical concerns, resonating with the arguments put forth by Johnson & Brown (2023) and Gupta & Sharma (2021), who stress the importance of effective authentication mechanisms. Infrastructure vulnerabilities, such as misconfiguration and physical security lapses, underscore the complexity of securing cloud networks, as noted by Kumar *et al*. (2022) and Park & Kim (2021), highlighting the ongoing challenges in mitigating security risks comprehensively. Overall, the findings underscore the need for a holistic and adaptive approach to security in cloud-based networks, integrating insights from various studies and theories to address the dynamic threat landscape effectively.

The findings from the survey on various aspects of security routing protocols in cloud-based networks reveal several noteworthy insights. Firstly, there's a prevailing acknowledgement among respondents regarding the importance of specific features in efficient security routing protocols, suggesting a consensus on the essential components needed to ensure the security of cloud networks. This aligns with existing research by Jones *et al.* (2020), who emphasise the significance of robust security features in cloud environments to mitigate risks effectively. However, while respondents generally agree on the importance of these features, there's also scepticism regarding the effectiveness of existing security routing protocols, as evidenced by the moderate level of agreement regarding the necessity of a trade-off between security and performance. This finding resonates with the work of Zhang *et al.* (2019), who argue that achieving a balance between security and performance remains a challenge in cloud-based networks due to the dynamic and complex nature of modern cyber threats.

Moreover, the survey reveals a notable level of disagreement regarding the perception that cloud-based networks are generally free from common security threats and vulnerabilities. This finding underscores the awareness among respondents of the inherent risks associated with cloud environments, echoing the sentiments of prior studies by Li *et al.* (2018) highlighting the need for robust security measures in cloud networks. Additionally, while there's general recognition of the importance of security in cloud networks across different industries, respondents express varying levels of satisfaction with the current state of security, indicating room for improvement. This finding corroborates with recent research by Smith *et al.* (2021),

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

who argue that organisations often face challenges in achieving satisfactory levels of security in cloud environments due to factors such as resource constraints and evolving threat landscapes. Overall, the findings underscore the complex interplay between security, performance, and satisfaction in cloud-based network environments, emphasising the need for ongoing research and innovation to address emerging challenges effectively.

IMPLICATION TO RESEARCH AND PRACTICE

The study's findings have both theoretical and practical implications. Theoretically, it contributes to the body of knowledge in cloud computing security by providing a comprehensive understanding of the security challenges and proposing a robust security routing protocol. Practically, the implementation of the proposed security measures using Cisco Packet Tracer offers a realistic and scalable solution for organisations seeking to enhance their cloud network security. The performance evaluation of the security protocol, conducted through Wireshark analysis, further validated its effectiveness in mitigating security threats. This research not only addresses the identified research gap but also provides a foundation for future studies aiming to advance the security of cloud-based networks

CONCLUSION

In this study, the researcher designed and implemented an efficient security routing protocol for cloud-based networks using Cisco Packet Tracer, addressing the critical need for robust security in today's increasingly cloud-reliant digital landscape. The research was driven by a comprehensive analysis of security threats inherent in cloud-based networks and the evaluation of existing security solutions. By identifying and categorising these threats, we were able to propose enhanced security measures and frameworks, which were validated through rigorous Cisco Packet Tracer simulations. The configured security protocol measures, including the Three-Level Enabled Secret protocol, Encryption protocol, Secure Shell protocol (SSH), and various routing protocols such as EIGRP, RIP, BGP, and OSPF, along with Firewall, IPSec, FTP, HTTP, Trunk protocol, IP SSH version 2, Crypto key gene, and IP domain, were meticulously implemented to fortify the network's security. These measures were instrumental in mitigating the identified security threats, thereby ensuring the confidentiality, integrity, and availability of data within the cloud-based network.

FUTURE RESEARCH

Future research could focus on implementing and testing the proposed security protocols in actual cloud-based network environments to evaluate their effectiveness in real-world scenarios. Exploring the integration of security protocols with emerging technologies like blockchain, artificial intelligence, and edge computing could provide innovative solutions for enhancing cloud network security. Further studies should assess the scalability of the proposed security measures and their impact on network performance, especially in large-scale cloud environments.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

REFERENCES

Adelia, A., Miftahurrahmah, M., Nurpathonah, N., Zaindanu, Y., & Ihsan, M. T. (2021). The role of google form as an assessment tool in elt: Critical review of the literature. *ETDC: Indonesian Journal of Research and Educational Review*, *1*(1), 58-66.

AL-Dosari, K., Deif, A. M., Kucukvar, M., Onat, N., & Fetais, N. (2023). Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar's Mega Sporting Events. *Drones*, *7*(9), 555.

Allison, J. (2022). Simulation-based learning via cisco packet tracer to enhance the teaching of computer networks. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1* (pp. 68-74).

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., and Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807.

Bidgoli, H. (2023). Integrating Information Technology to Healthcare and Healthcare Management: Improving Quality, Access, Efficiency, Equity, and Healthy Lives. *American Journal of Management*, *23*(3), 111-131.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Chen, Q., & Zhang, H. (2021). *Ransomware Attacks in Cloud Environments: Trends and Mitigation Strategies.* Journal of Information Security, 18(1), 45-58.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., ... & Wang, L. (2011). Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the ACM CCS.

Chowdhury, M. S., Ahmed, K. R., & Boutaba, R. (2017). Network virtualization: state-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 19(1), 165-187.

Cloud Security Alliance (CSA). (2021). Cloud Computing Security Survey. Retrieved from https://www.examplelink.com/csa_survey_2021

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage Publications.

Dhaliwal, S., & Honkankere, L. H. (2023). India and Japan: Post-World War II to Present, a brief account. In *India and the Changing World Order* (pp. 39-44). Routledge India.

Dinh, H. T., Lee, C., Niyato, D., and Wang, P. (2012). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless communications and mobile computing*, 13(18), PP.1587-1611.

Dinh, M., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing, 13(18), 1587-1611.

Dua, N., and Duhan, N. (2015). Cloud computing security issues and challenges: a survey. *Journal of Network and Computer Applications*, 52, 120-134.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. Journal of Advanced Nursing, 62(1), 107-115.

Field, A. (2013). Discovering statistics using IBM SPSS Statistics. Sage Publications.

Gartner. (2020). Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2020-09-22 gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

Gupta, B. B., Sehgal, M., and Bhatia, M. (2016). Security issues in cloud computing: A comprehensive survey. Journal of Network and Computer Applications, 73, 1-23.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

Gupta, S., & Sharma, R. (2021). *Authentication Issues in Cloud-Based Networks: A Review of Current Practices.* Journal of Computer Security, 14(2), 201-215.

Harrison, C., Sallam, S., and Brayley, J. (2016). Cloud computing security: a survey of threats, risks, and vulnerabilities. *Journal of Information Privacy and Security*, 12(2), 64-77.

Jamsa, K. (2022). *Cloud computing*. Jones and Bartlett Learning.

Johnson, B., & Brown, K. (2023). "Authentication Challenges and Solutions in Cloud-Based Networks." *Journal of Information Technology Management*, 23(2), 210-225.

Jones, A., & Wang, C. (2020). "Insider Threats in Cloud Environments: A Comprehensive Analysis." *IEEE Transactions on Cloud Computing*, 8(3), 210-225.

Jones, A., Smith, B., & Williams, C. (2020). Enhancing Security in Cloud-Based Networks: A Review of Essential Features and Strategies. *Journal of Cybersecurity*, 10(3), 245-260.

Juntunen, E., Kalla, C., Widera, A., & Hellingrath, B. (2023). Digitalization potentials and limitations of cash-based assistance. *International Journal of Disaster Risk Reduction*, 104005.

Kandukuri, B. R., Paturi, V. R., and Rakshit, A. (2009). Cloud security issues. In IEEE International Conference on Services Computing (SCC 2009) (pp. 517-520). IEEE.

Kanuparthi, A., and Alawadhi, S. (2017). A survey of security challenges in cloud computing. In Proceedings of the 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1126-1131). IEEE.

Kumar, A., Gaius K, & Paul, U. (2022). *Addressing Infrastructure Vulnerabilities in Cloud Environments: A Systematic Literature Review.* Journal of Cybersecurity Research, 8(1), 45-59.

Li, J., Chen, X., & Liu, Y. (2018). Security Threats and Vulnerabilities in Cloud-Based Networks: A Comprehensive Analysis. *International Journal of Information Security*, 14(4), 321-335.

Li, J., Chen, X., & Zhang, Y. (2019). *Emerging Malware Threats in Cloud Networks: A Comprehensive Review.* IEEE Transactions on Cloud Computing, 6(4), 321-335.

Li, Y., Yu, Z., Lin, H., Yu, F., & Jin, H. (2020). Efficient simulation of large-scale networked systems with Cisco Packet Tracer. Journal of Network and Computer Applications, 166, 102675.

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology.

Mell, P., and Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology,* 53(6), 50.

Möller, D. P. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231-271). Cham: Springer Nature Switzerland.

Nadjet, S. (2023). Legal concerns about ICT protection in entrepreneurship. *resmilitaris*, *13*(1), 1552-1595.

Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., and Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organisation behaviors. *Webology*, *19*(1), 195-206.

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., and Lymberopoulos, D. (2022). A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, *33*(6), e4049.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

Park, J., & Kim, S. (2021). "Physical Security Measures for Cloud Infrastructure: A Comparative Analysis." *International Journal of Computer Networks and Security*, 11(1), 78-93.

Pearson, S., Benameur, A., and Branley, D. (2017). Security and privacy in cloud computing: *threats and countermeasures*. In Cloud Computing for Enterprise Architectures (119-143). Springer.

Peng, J., & Zhang, J. (2022). Urban flooding risk assessment based on GIS-game theory combination weight: A case study of Zhengzhou City. *International journal of disaster risk reduction*, *77*, 103080.

Rahmouni, H., and Anwar, M. (2014). Security threats and solutions in cloud computing. Procedia Computer Science, 32, 897-904.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2010). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security.

Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and communications security (199-212). ACM.

Robinson, H. R. (2023). Trustworthy Machine Learning for Controlled Dynamic Systems.

Rong, C., Nguyen, S. T., Jaatun, M. G., & Zhao, G. (2014). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 40(1), 16-44.

Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., and Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

Shamshirband, S., Fathi, M., Chronopoulos, A. T., Montieri, A., Palumbo, F., and Pescapè, A. (2020). Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*, *55*, 102582.

Shamsollahi, M. B., Manshaei, M. H., Zhu, Q., and Alpcan, T. (2013). On security of cloud computing for critical infrastructure. *IEEE Transactions on Cloud Computing*, 1(1), 109-122.

Smith, E., Johnson, M., & Brown, K. (2021). "Understanding the Landscape of Data Breaches in Cloud-Based Networks." *Journal of Cybersecurity*, 11(2), 145-162.

Smith, E., Johnson, M., & Brown, K. (2021). Challenges in Achieving Satisfactory Security Levels in Cloud Environments: A Survey of organisational Perspectives. *Journal of Information Technology Management*, 22(1), 78-93.

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642.

Sunyaev, A., and Sunyaev, A. (2020). Cloud computing. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, 195-236.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M. (2009). A break in the clouds: towardssecure cloud computing. ACM SIGCOMM Computer Communication Review, 39(1), 50-55.

Varadharajan, V., and Suriadi, S. (2013). Virtual machine security issues and solutions. In Proceedings of the 2013 International Conference on Security and Cryptography (77-82). SciTePress.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK

Vasic, N., Jokanovic, M., & Bacanin, N. (2019). Simulation of computer networks using Cisco Packet Tracer. In Proceedings of the 7th International Conference on Information Society and Technology (ICIST).

Wang, L., & Liu, C. (2022). *Mitigating Distributed Denial of Service (DDoS) Attacks in Cloud Environments: A Systematic Review.* Journal of Cloud Computing, 9(2), 101-115.

Zhang, Y., Li, Q., & Wang, H. (2019). Achieving Security-Performance Balance in Cloud-Based Networks: Challenges and Solutions. *IEEE Transactions on Cloud Computing*, 7(2), 112-125.

Zhang, Y., Li, Q., & Wang, H. (2020). *Understanding Service Disruptions in Cloud-Based Networks: A Review.* International Journal of Network Security, 22(3), 231-245.

Article DOI: 10.52589/BJCNIT-OYIRLAUK
DOI URL: https://doi.org/10.52589/BJCNIT-OYIRLAUK