Design and Analysis of Secure IP Networking Using RIP, NAT, and VPN

Dr. Dinakaran S[1], Mr. Ashok Raj R[1], Dr. Saravanan P[2], Dr. Felcy Judith[3]

[1] Associate Professor, T. John College, Bangalore
[2]Assistant Professor, T. John College, Bangalore
[3]Professor, T. John College, Bangalore

Abstract:

The growing reliance on IP-based networks has highlighted the importance of efficient routing, address management, and secure communication protocols. This paper describes the design and simulation-based analysis of a secure IP networking environment that utilizes the Routing Information Protocol (RIP), Network Address Translation (NAT), and Virtual Private Network (VPN) technologies. The proposed network architecture is implemented in Cisco Packet Tracer, utilizing RIP for dynamic intra-domain routing, NAT for address conservation and controlled external connectivity, and VPN mechanisms to ensure secure data transmission across untrusted networks. Basic firewall rules are also used to manage traffic and improve network security. The integrated mechanisms' performance and functionality are assessed in terms of connectivity, routing efficacy, address use, and secure communication. Simulation results show that combining RIP, NAT, and VPN improves network management, promotes efficient IP address usage, and ensures secure end-to-end communication in a controlled environment. The research emphasizes the usefulness of simulation tools for studying secure IP networking architectures and serves as a reference model for small to medium-sized enterprise networks.

Keywords: Secure IP Networking, RIP, NAT, VPN, Firewall, Cisco Packet Tracer

Introduction:

To meet expanding communication demands, modern IP networks must support fast routing, effective address management, and robust security. Dynamic routing methods, such as Routing Information Protocol (RIP), allow for automatic path selection, whereas Network Address Translation (NAT) addresses IPv4 address exhaustion by optimizing address usage. Furthermore, Virtual Private Networks (VPNs) provide safe communication across public networks. Integrating these methods is critical for creating stable and secure enterprise networks. This study examines the design and simulation-based analysis of secure IP networking employing RIP, NAT, and VPN in a controlled setting. The study demonstrates the design and simulation of a secure VPN using Cisco Packet Tracer as a cost-effective alternative to traditional leased lines. Results show that VPNs enable secure and reliable data transmission over the Internet. The authors recommend deploying servers in a distributed manner and using

Published: 14 February 2026
DOI: https://doi.org/10.70558/IJST.2026.v3.i1.241185

IPSec with tunnelling protocols to enhance security Forbacha, S. C., et, al., 2023). Secure IP networking is the process of designing, implementing, and managing IP-based networks to assure the confidentiality, integrity, authentication, and availability of data carried across the network. Because IP networks frequently run on public or shared infrastructures, security methods are required to safeguard data from illegal access, interception, modification, or disruption.

At the network layer, secure IP networking is dependent on proper routing and traffic management. Routing protocols like RIP, OSPF, and BGP allow for dynamic path selection, but they must be secured from threats such as route spoofing and misleading updates. Secure setups (for example, authentication in RIPv2) contribute to routing integrity. In addition, secure IP networking employs firewalls, intrusion detection/prevention systems (IDS/IPS), access control policies, and monitoring tools to detect and mitigate attacks. These methods work together to create a layered security architecture that secures both the control plane (routing and management) and the data plane (user traffic).

Virtual Private Networks (VPNs) are an essential part of secure IP networking. VPNs use encryption and tunneling (such as IPsec or SSL/TLS) to establish secure communication channels across untrustworthy networks such as the Internet. They provide data confidentiality and integrity during transmission and are commonly used for site-to-site communication and remote access. Network Address Translation (NAT) improves security by concealing internal IP addresses from external networks, hence limiting direct exposure of internal hosts. While NAT is not a complete security solution, it serves as a basic protective layer and allows for efficient address management. However, NAT can interfere with end-to-end security, necessitating careful integration of security mechanisms. To summarize, safe IP networking is accomplished by integrating secure routing, regulated address translation, encrypted communication, and constant monitoring, resulting in dependable and secure data exchange in current network environments.

Literature Review:

Secure IP networks must be designed with dynamic routing protocols, address translation algorithms, and encrypted communication channels. The Routing Information Protocol (RIP) is still an essential inside gateway protocol, recognized for its simplicity in small to medium-sized networks. Despite limitations in hop counts and slower convergence, innovations such as RIPv2 with authentication alleviate basic routing risks by offering safe updating mechanisms. However, the research emphasizes that older routing protocols, like RIP, frequently lack appropriate security for current attacks without additional control plane protections (Malkin, 1998).

Address translation via Network Address Translation (NAT) conserves IPv4 address space while providing basic obscurity by concealing internal network topologies. Recent security research has identified serious vulnerabilities in NAT implementations, including remote denial-of-service (DoS) mechanisms that attackers can use to disrupt TCP connections by altering NAT mappings. Such empirical tests reveal that NAT devices under varied networks

(LTE/5G, Wi-Fi, cloud VPS) remain extensively vulnerable, emphasizing compelling needs for robust NAT security configurations and countermeasures Feng, X., et al., 2024).

Virtual Private Networks (VPNs) are critical for ensuring secure connectivity over untrusted networks by encapsulating and encrypting traffic. A comprehensive survey on VPN technologies published in 2024 synthesizes evolving roles, taxonomies, and challenges of VPN deployment, emphasizing the importance of future design strategies to address cloud migration, regulatory changes, and advanced threats. Such surveys enrich understanding of VPN protocols such as IPsec, SSL/TLS, and emerging models like Wire Guard, detailing both practical and theoretical security considerations Tian, A., (2025).

Furthermore, cutting-edge research into peer-to-peer VPN communication suggests alternatives to traditional VPN and firewall dependencies. For example, a 2025 study shows that modern peer-to-peer network virtualization (e.g., Zero Tier) outperforms traditional VPN technologies by achieving faster connection establishment, lower latency, and direct device-to-device connections while maintaining encryption and NAT traversal efficiency. These findings suggest new architectural directions for safe network architecture beyond traditional VPN paradigms. Mehrab, A. I. (2025).

The interplay between routing, NAT, and VPN is also reflected in broader networking research. Although many works focus on secure routing protocol enhancements (e.g., resilient routing in mobile ad-hoc networks), such investigations underline the significance of routing integrity and adaptability in environments where VPN and NAT mechanisms operate concurrently Baumgartner, M., et al., 2024). Secure routing design principles that emerged from such studies contribute conceptual insights toward strengthening overall IP networking security, especially when integrating dynamic routing with secure tunnels.

The recent research emphasizes the importance of revisiting and improving established protocols while creating secure IP networks. While RIP's simplicity is useful in confined situations, true security necessitates combining routing advancements with strong NAT defences and complex VPN topologies. Emerging research in safe, decentralized VPN connectivity and increased NAT security contributes to best practices for future network designs, arguing for comprehensive approaches that address both control plane and data plane weaknesses.

Methodology:

Routing Information Protocol (RIP): This popular distance-vector routing technique uses hop count as a statistic to assist routers in figuring out the best route for data packets. RIP, which operates at Layer 3 of the OSI model, allows routers to dynamically exchange and update routing tables, guaranteeing network flexibility. RIP, and offers straightforward configuration and dependable communication by choosing routes with the fewest hops, is perfect for tiny networks. The Routing Information Protocol in computer networks encompasses the key ideas about the RIP protocol and how it operates. Enrolling in our online networking courses can also help you obtain hands-on experience if you want to learn more about these Internet protocols.

The Routing Information Protocol (RIP): has several unique features that define its operation in computer networking. RIP uses periodic updates, where routers exchange routing information at regular intervals, typically every 30 seconds, to keep routing tables up to date. These updates are broadcast to all neighbouring routers, ensuring that every connected device receives the latest routing information. Each update carries the entire routing table, allowing routers to maintain an accurate view of the network topology. RIP also follows the principle of "routing on rumours," meaning routers generally trust the routing information received from neighbouring routers without independently verifying it. RIP is best suited for small and medium-sized networks with a somewhat stable topology. RIP, despite its drawbacks, is still a significant protocol for education and basic routing ideas Forouzan, B. A. (2017). The number of routers a data packet must go through in order to reach its destination is known as the hop count. According to the Routing Information Protocol, the best route is the one with the fewest hops.

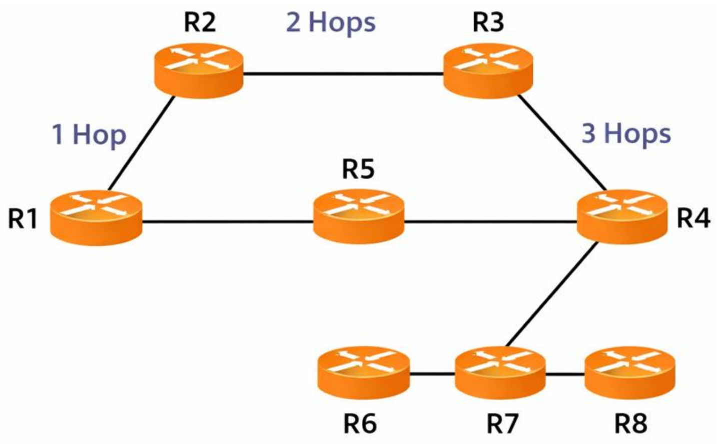


Fig 1: RIP Hop count calculation

Several studies have identified RIP's shortcomings in terms of convergence time, scalability, and bandwidth usage as a result of its periodic full-table updates. The sluggish convergence can cause routing loops and count-to-infinity difficulties, particularly in dynamic network contexts. To address these concerns, RIP version 2 (RIPv2) included innovations such as split horizon, route poisoning, and hold-down timers. RIPv2 enables classless routing and multicast updates, making it more efficient than RIPv1. However, when compared to newer routing protocols such as OSPF and EIGRP, RIP still underperforms in large or highly dynamic networks Huitema, C. (2000). To avoid routing loops, the RIP protocol restricts the number of hops to 15 and designates a hop count of 16 as unreachable. The network's stability and efficiency are preserved by this limitation.

The characteristics of RIP are

1. RIP calculates the distance to a destination using hop count. Preferred and noted in the routing table is the path with the fewest hops.
2. RIP's administrative distance (AD) rating of 120 shows how reliable it is in comparison to other routing protocols.
3. RIP functions at the OSI model's Network layer, or Layer 3.
4. RIP uses UDP port 520 for routing updates.

Working model of RIP

RIP functions by exchanging routing data among routers through a structured sequence of operations. Initially, when a router starts up, it builds its routing table using information about directly connected networks and assigns them a hop count of zero. At fixed intervals of 30 seconds, routers transmit updates that include their complete routing tables to neighboring routers, helping all devices maintain an updated understanding of the network structure.

When a router receives an update, it evaluates the new routing information against its existing table and modifies its entries if better or updated routes are available. This exchange continues until all routers reach a stable and consistent view of available paths, a state known as convergence. Compared to modern routing protocols, RIP generally requires more time to achieve convergence. If a router identifies a failed or unreachable route, it labels that route as invalid and activates a hold-down timer to avoid rapid or incorrect routing changes. Finally, each router determines the most efficient path by selecting the route with the smallest hop count and updates its routing table accordingly.

Network Address Translation (NAT): A single public IP address can be used by several devices connected to a private network to access the internet thanks to Network Address Translation (NAT). For extra security, it conceals internal systems and aids in IPv4 address conservation. Converts private IP addresses into public ones and the other way around. Keeps IPv4 addresses from running out increases security by hiding internal components. Enables the sharing of a single public IP among thousands of devices.

The addresses that need to be translated are referred to as "within." The term "outside" describes addresses that are not under an organization's control. The translation will take place at these network addresses.

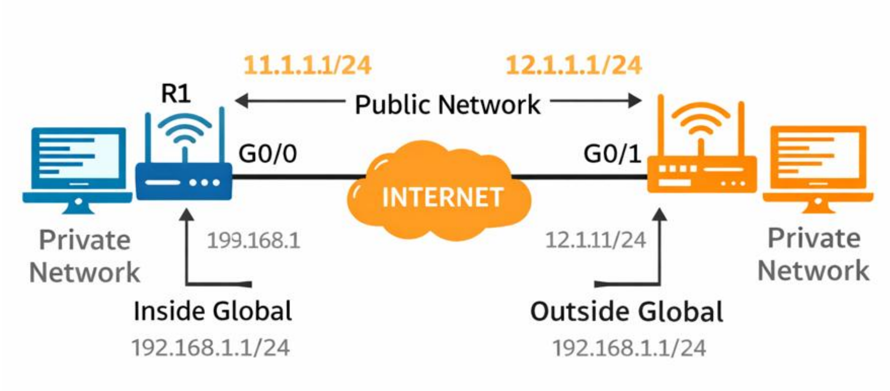


Fig 2: NAT Inside & Outside Address

The diagram illustrates how Network Address Translation (NAT) enables communication between private networks through the public Internet by translating IP addresses. On the left side, there is a private network containing a host with a private IP address (for example, 192.168.1.1/24). This host is connected to Router R1. The private IP used inside the local network is referred to as the Inside Local address. When traffic leaves the private network, Router R1 performs NAT by translating this private IP into a public IP address, known as the Inside Global address. This public IP is routable on the Internet. Network Address Translation

(NAT) is still a popular method for mitigating IPv4 address exhaustion by allowing numerous private hosts to share limited public IP addresses. Recent studies have highlighted the widespread deployment of Carrier-Grade NAT (CGNAT) by ISPs and examined its impact on scalability and address sharing efficiency Czyz, J et, al (2016). The Internet (Public Network) is shown in the center of the diagram. It carries traffic between different organizations using public IP addresses. Private IP addresses are not visible or routable across the Internet. On the right side, there is another network connected through a router to the Internet. The public IP address used by this external router is called the Outside Global address, while the private IP of the destination host inside that network is known as the Outside Local address. NAT performance optimization has gained traction in recent years, with an emphasis on lowering lookup latency and increasing throughput on high-speed networks. Journal articles suggest improved NAT architectures that use optimized state tables and parallel processing to handle modern traffic loads Zhang, Y., Bi, J., & Hu, C., (2019).

Virtual Private Networks (VPN): By establishing an encrypted connection that conceals your IP address, it enables you to join your computer to a private network and safely share data and browse the internet while safeguarding your identity. An encrypted connection made between a device and a network via the Internet is known as a virtual private network, or VPN. Sensitive data transmission is made safer by the encrypted connection. It enables the user to operate remotely and keeps unauthorized others from listening in on the conversation. In business settings, VPN technology is frequently utilized. Performance evaluations conducted after 2015 indicate that VPNs operating over NAT may introduce additional latency due to encapsulation and translation overhead. However, optimized VPN gateways and improved NAT handling significantly reduce performance degradation in modern network environment Bezahaf, M et al. (2017).

There are two key applications for VPN connections. To create VPN-based wide area network (WAN) connections between two remote networks that may be thousands of miles apart, yet each has access to the internet. To create remote access connections that allow distant users to use a public network, such as the internet, to access a private network.

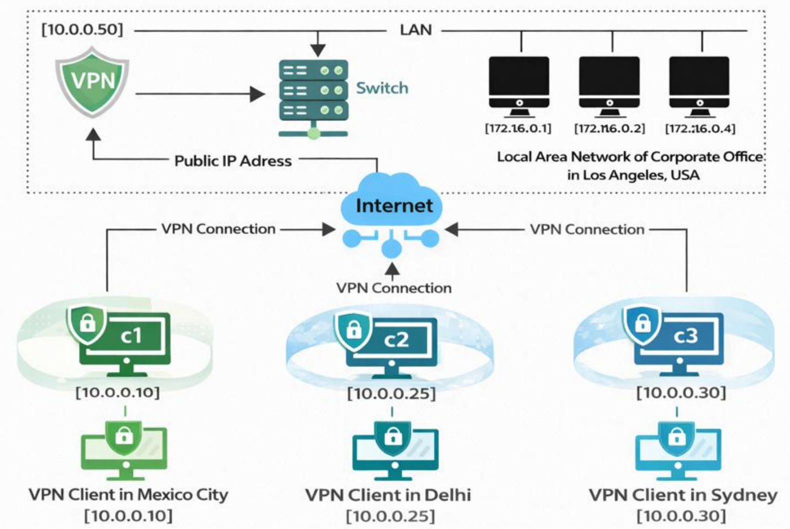


Fig 3: Working model of VPN

Recent research has emphasized the need for VPN-NAT integration in improving business and remote-access security, particularly for IPsec-based VPNs. NAT preserves addresses, whereas VPNs protect the confidentiality, integrity, and authentication of data transported across heterogeneous networks Alshamrani, A., et al (2019)

Results and Discussion:

The diagram represents a small routed network topology consisting of three Cisco 1841 routers interconnected in a linear (WAN) fashion and three separate LANs. Router0, Router1, and Router2 are connected through point-to-point links using the 10.0.0.0 and 11.0.0.0 networks, where Router0 connects to Router1 via IP addresses 10.0.0.1 ↔ 10.0.0.2, and Router1 connects to Router2 via 11.0.0.1 ↔ 11.0.0.2. Each router also connects to a local LAN through a 2960 switch. The left LAN uses the 192.168.1.0/24 network with Router0 as the default gateway (192.168.1.1) and two PCs assigned 192.168.1.2 and 192.168.1.3. The middle LAN uses the 192.168.2.0/24 network with Router1 as the gateway (192.168.2.1) and PCs configured as 192.168.2.2 and 192.168.2.3. The right LAN operates on the 192.168.3.0/24 network, where Router2 acts as the gateway (192.168.3.1) and hosts PCs with IP addresses 192.168.3.2 and 192.168.3.3. Overall, the diagram illustrates the interconnection of multiple LANs using routers and switches, demonstrating both intra-LAN communication through switches and inter-network communication through routing.

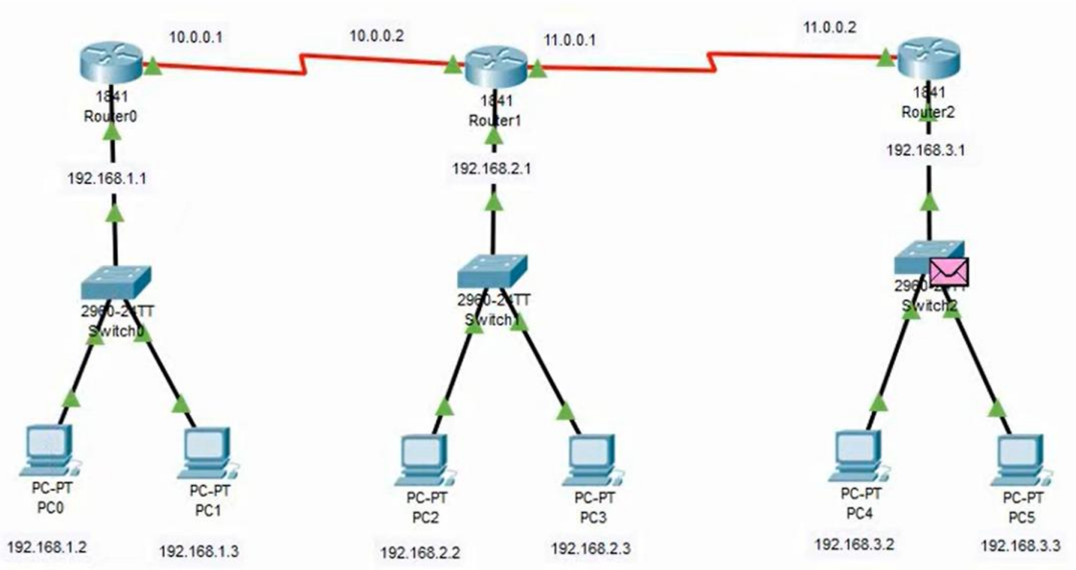
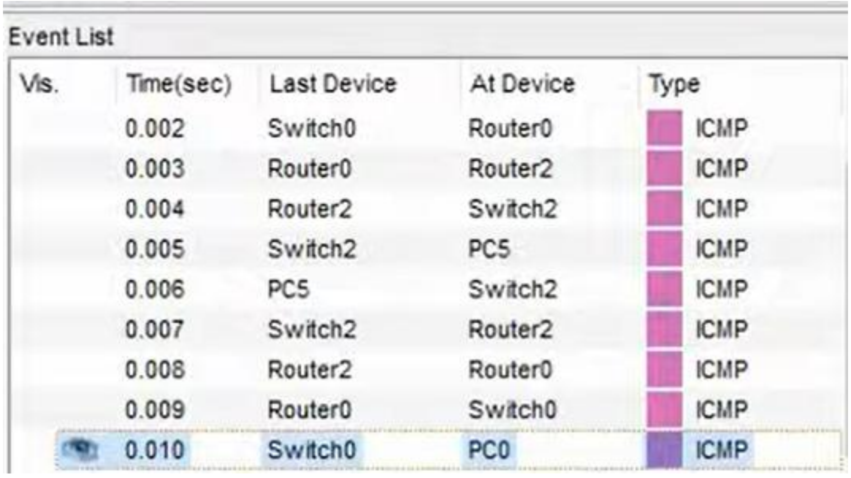


Fig 4: Experimental Setup of RIP-Enabled Network Topology

The diagram shows the Event List from Cisco Packet Tracer in Simulation Mode, detailing the step-by-step flow of an ICMP (ping) packet across the network. Each row represents a single event, indicating the time (in seconds), the last device the packet passed through, the current device, and the protocol type, which is ICMP throughout. The sequence begins when the ICMP packet moves from Switch0 to Router0, then travels across the routed network from Router0 to Router2, demonstrating inter-router communication over the WAN links. From Router2, the packet is forwarded to Switch2 and then delivered to the destination host PC5. After reaching PC5, the ICMP echo reply is generated and follows the reverse path: from PC5 back to Switch2, then to Router2, Router0, Switch0, and finally reaching the source device PC0. The increasing timestamps (from 0.002 to 0.010 seconds) illustrate the packet's traversal delay across devices, while the consistent ICMP type confirms successful ping request and reply, validating end-to-end network connectivity.



Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.002	Switch0	Router0	ICMP
	0.003	Router0	Router2	ICMP
	0.004	Router2	Switch2	ICMP
	0.005	Switch2	PC5	ICMP
	0.006	PC5	Switch2	ICMP
	0.007	Switch2	Router2	ICMP
	0.008	Router2	Router0	ICMP
	0.009	Router0	Switch0	ICMP
👁	0.010	Switch0	PC0	ICMP

Fig 5: Simulation Event Log for ICMP-Based Connectivity Testing-RIP

The diagram illustrates a small client–server network topology created in Cisco Packet Tracer, showing communication between a local LAN and a remote server through two routers. On the left side, two end devices—PC0 (192.168.0.100) and PC1 (192.168.0.200)—are connected to Switch1, forming a LAN in the 192.168.0.0/24 network. Switch1 connects to Router0 via the FastEthernet interface, with Router0's LAN-facing interface configured as 192.168.0.1, acting as the default gateway for the PCs. Router0 is connected to Router1 through a serial WAN link using the 200.10.0.0 network, where Router0 uses 200.10.0.1 and Router1 uses 200.10.0.2, representing inter-router communication. Router1 then connects to a remote network via its FastEthernet interface (10.0.0.1), which links to Server0 configured with the IP address 10.0.0.200. Overall, the diagram demonstrates how multiple PCs in a LAN can access a remote server across different networks using switches for local communication and routers for inter-network and WAN connectivity.

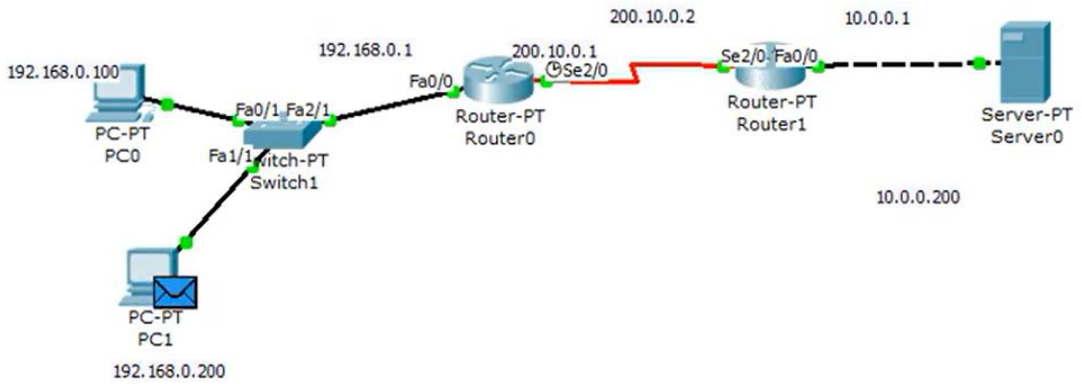
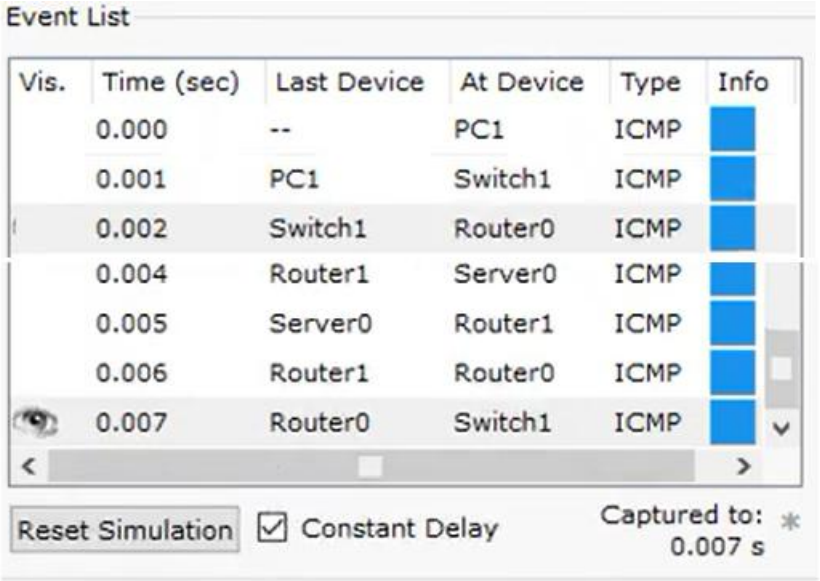


Fig 6: Experimental Setup of NAP-Enabled Network Topology

The diagram displays the Event List in Cisco Packet Tracer Simulation Mode, illustrating the complete path of an ICMP (ping) request and reply between PC1 and Server0 across multiple network devices. The process begins at time 0.000 seconds when the ICMP packet is generated at PC1, then forwarded to Switch1 at 0.001 seconds, and subsequently to Router0 at 0.002 seconds, showing the transition from the local LAN to the routed network. The packet is then delivered to Server0 via Router1, confirming successful inter-router communication. After receiving the echo request, Server0 generates an ICMP echo reply at 0.005 seconds, which travels back through Router1 and Router0, and finally reaches Switch1 at 0.007 seconds on its way to the source host. The consistent ICMP protocol type across all events and the steadily increasing timestamps indicate proper packet forwarding, routing, and return path operation, thereby confirming end-to-end connectivity between the client PC and the remote server.



Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	PC1	ICMP	🟦
	0.001	PC1	Switch1	ICMP	🟦
	0.002	Switch1	Router0	ICMP	🟦
	0.004	Router1	Server0	ICMP	🟦
	0.005	Server0	Router1	ICMP	🟦
	0.006	Router1	Router0	ICMP	🟦
👁	0.007	Router0	Switch1	ICMP	🟦

Reset Simulation ☑ Constant Delay Captured to: 0.007 s

Fig 7: Simulation Event Log for ICMP-Based Connectivity Testing-NAT

The diagram illustrates a multi-router network topology designed in Cisco Packet Tracer, showing end-to-end connectivity between two geographically separated LANs through a chain of routers. On the left side, PC0 (10.0.0.1) and PC1 (10.0.0.2) are connected to Switch0, forming a LAN using the 10.0.0.0 network, with Router0 acting as the default gateway via its LAN interface (10.0.0.3). Router0 is connected to Router1 through a point-to-point link using the 60.0.0.0 network, where Router0 uses 60.0.0.1, and Router1 uses 60.0.0.2. Router1 is further connected to Router2 over the 70.0.0.0 network, followed by a link from Router2 to Router3 over the 80.0.0.0 network, forming a routed backbone between the two LANs. On the right side, Router3 connects to Switch1, providing access to the 20.0.0.0 LAN, where PC2 (20.0.0.1) and PC3 (20.0.0.2) reside, with Router3's LAN interface configured as 20.0.0.3. The top labels (192.168.1.1 to 192.168.1.2) indicate logical end-to-end communication between the two LAN gateways across the routed path. Overall, the diagram demonstrates how multiple routers and networks work together to enable communication between distant LAN segments using hierarchical IP addressing and point-to-point links.

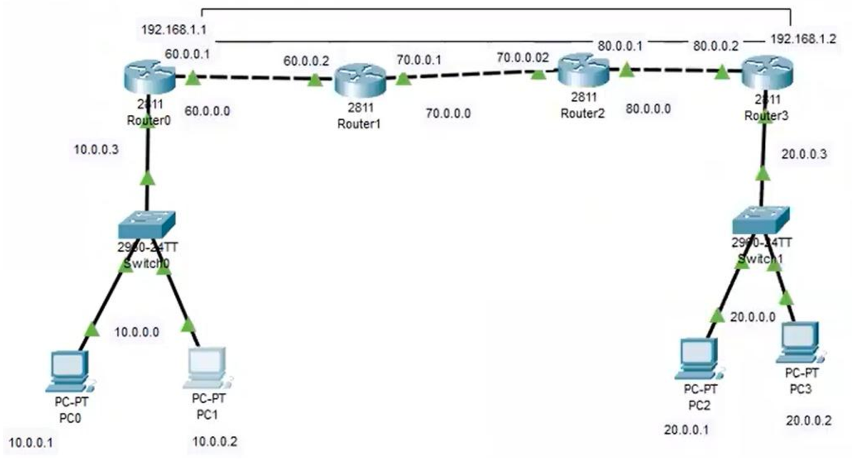
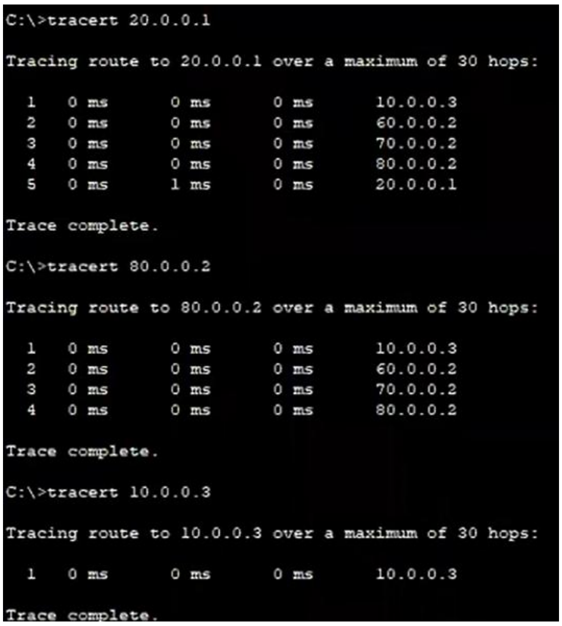


Fig 8: Experimental Setup of VPN-Enabled Network Topology

The diagram presents the traceroute (tracert) output used to analyze and validate packet traversal across a multi-router IP network, serving as an experimental verification of routing behavior in a research context. The first traceroute traces the path from a source host in the 10.0.0.0 network to the destination 20.0.0.1, revealing a sequential hop-by-hop progression through intermediate gateway and backbone routers with IP addresses 10.0.0.3, 60.0.0.2, 70.0.0.2, and 80.0.0.2 before reaching the destination, thereby confirming correct routing table configuration and end-to-end reachability. The second traceroute to 80.0.0.2 demonstrates partial path validation by terminating at the penultimate router, verifying the accessibility of intermediate backbone nodes. The final traceroute to 10.0.0.3 confirms immediate reachability of the local default gateway within a single hop, validating proper LAN-level configuration. The consistently low latency values (0–1 ms) indicate an idealized or simulated environment, typical of controlled network experiments. Collectively, these traceroute results provide empirical evidence of correct hierarchical routing, path determinism, and network convergence, supporting the reliability and correctness of the proposed network design.



```
C:\>tracert 20.0.0.1

Tracing route to 20.0.0.1 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.0.0.3
  2   0 ms      0 ms      0 ms      60.0.0.2
  3   0 ms      0 ms      0 ms      70.0.0.2
  4   0 ms      0 ms      0 ms      80.0.0.2
  5   0 ms      1 ms      0 ms      20.0.0.1

Trace complete.

C:\>tracert 80.0.0.2

Tracing route to 80.0.0.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.0.0.3
  2   0 ms      0 ms      0 ms      60.0.0.2
  3   0 ms      0 ms      0 ms      70.0.0.2
  4   0 ms      0 ms      0 ms      80.0.0.2

Trace complete.

C:\>tracert 10.0.0.3

Tracing route to 10.0.0.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      10.0.0.3

Trace complete.
```

Fig 9: Tracking route over hop count

Conclusion:

This paper presented the design and simulation-based evaluation of a secure IP networking architecture that integrates the Routing Information Protocol (RIP), Network Address Translation (NAT), and Virtual Private Network (VPN) technologies using Cisco Packet Tracer. The results demonstrate that RIP provides effective dynamic routing for small to medium-sized networks, while NAT supports efficient IPv4 address utilization and offers a basic level of network concealment. The inclusion of VPN mechanisms enables secure and encrypted data transmission over untrusted networks, thereby ensuring confidentiality, integrity, and authentication. Simulation-based validation using ICMP testing and traceroute analysis confirmed reliable end-to-end connectivity, accurate routing behavior, and stable network convergence across multiple network segments. Although RIP has inherent limitations related to scalability and convergence speed, its simplicity and ease of configuration make it suitable for controlled and educational environments. Overall, the combined deployment of RIP, NAT, and VPN presents a practical, cost-effective, and secure networking solution for small and medium enterprise scenarios. This study further highlights the effectiveness of network simulation tools in analyzing secure IP network designs and provides a solid foundation for future research involving advanced routing protocols and enhanced security frameworks.

Reference:

1. Malkin, G. (1998). RIP version 2 (RFC 2453). Internet Engineering Task Force.
2. Huitema, C. (2000). Routing in the Internet (2nd ed.). Prentice Hall.
3. Forouzan, B. A. (2017). Data communications and networking (5th ed.). McGraw-Hill Education.
4. Bezahaf, M., Pierre, S., & Gagnon, G. (2017). Performance analysis of IPsec VPNs under NAT environments. Journal of Network and Computer Applications, 87, 45–55.
5. Czyz, J., Allman, M., Zhang, J., Iekel-Johnson, S., Osterweil, E., & Bailey, M. (2016). Measuring IPv4 address exhaustion and carrier-grade NAT deployment. IEEE Internet Computing, 20(6), 26–34. https://doi.org/10.1109/MIC.2016.124
6. Alshamrani, A., Chowdhary, A., Pisharody, S., Huang, D., & Abdelhakim, M. (2019). A survey on VPN security: Threats, mechanisms, and challenges. IEEE Access, 7, 181781–181802. https://doi.org/10.1109/ACCESS.2019.2951514
7. Zhang, Y., Bi, J., & Hu, C. (2019). High-performance NAT design for large-scale networks. IEEE Access, 7, 112345–112354.
8. Forbacha, S. C., Agwu, M. J. A., & Anyam, M. J. (2023). Design and implementation of a secure virtual private network over an open network (Internet). American Journal of Technology, 2(1), 1–36. https://doi.org/10.58425/ajt.v2i1.134
9. Baumgartner, M., et al. (2024). Resilient enhancements of routing protocols in MANET. Peer-to-Peer Networking and Applications, 17, 3200–3221.
10. Feng, X., et al. (2024). ReDAN: An empirical study on remote DoS attacks against NAT networks. arXiv.
11. Tian, A. (2025). A survey on VPN technologies: Concepts, implementations, and anti-detection strategies. International Journal of Engineering Development Research, 13(1).

12. Mehrab, A. I. (2025). A new approach to peer-to-peer VPN connectivity: Achieving seamless communication without firewalls. ResearchGate Preprint.