Activity Based Learning

On

HIP (Host Identity Protocol)

Submitted By

Dhara Dhuvaviya (CS23181)

Submitted in partial fulfilment

Of

"TAE-1(ABL)"

Under the subject

Computer Network

(N-PCCCS502T)

(V Semester, B.Tech)

Guided By: -

Mrs. Arati Karadbhajane

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

S.B. JAIN INSTITUTE OF TECHNOLOGY, MANAGEMENT & RESEARCH, NAGPUR.

2025-2026

ABSTRACT

The Host Identity Protocol (HIP) is an experimental network layer protocol designed to separate a host's identity from its IP address, enhancing security, mobility, and session continuity. Traditional IP-based communication relies on static IP addresses for identification, which creates challenges in scenarios involving mobile hosts or dynamic networks. HIP addresses this by introducing Host Identifiers (HITs), cryptographic identifiers derived from public keys, allowing hosts to maintain secure sessions even when their IP addresses change.

This project demonstrates a HIP simulation using Cisco Packet Tracer, where two hosts are assigned, permanent identities represented as hostnames (simulating HITs). The network topology includes two routers and two switches, forming a multi-subnet environment. Secure communication is conceptually simulated through labelled "encrypted tunnels," representing HIP's session security.

The simulation highlights the HIP base exchange, where hosts authenticate each other using their HITs before establishing a session. Mobility is demonstrated by changing HostA's IP address to a new subnet while maintaining uninterrupted communication with HostB. Static routing ensures that routers correctly forward packets across subnets, preserving connectivity despite IP changes.

The project effectively illustrates HIP principles in a simulated environment, emphasizing host identity separation, secure communication, and mobility support. Although Cisco Packet Tracer does not natively implement HIP cryptography, this simulation provides a clear conceptual understanding of HIP functionality, making it a valuable educational tool for network security and mobility research.

INDEX

Sr.No.	Contents	Page No
Chapter 1	**Introduction**	4
Chapter 2	**Objective & Outcome**	5
Chapter 3	**Methodology/Implementation**	6
Chapter 4	**Observation**	9
Chapter 5	**Advantages**	10
Chapter 6	**Disadvantages**	11
Chapter 7	**Application**	11
Chapter 8	**Conclusion**	12
Chapter 9	**References**	13

Introduction

The Host Identity Protocol (HIP) is a network layer protocol designed to enhance security, mobility, and session continuity in IP networks. Traditionally, Internet communication relies on IP addresses, which serve two purposes:

1. Host identification – identifying a device on the network.
2. Location indication – specifying the host's network location.

This dual role creates several challenges:

- When a host changes its network location (due to mobility, dynamic IP assignment, or network reconfiguration), its IP address changes.
- Ongoing communication sessions may break because connections are tied to the IP address.
- Security can be compromised as IP addresses alone are insufficient for authentication, making networks vulnerable to spoofing and unauthorized access.

HIP addresses these challenges by introducing a separate host identity, known as the Host Identifier (HIT):

- HIT is a cryptographic identifier derived from the host's public key.
- It remains constant even if the host's IP address changes.
- This separation of identity from location allows ongoing sessions to persist across network changes.
- HIP also provides authentication and security, preventing spoofing attacks and ensuring trusted communication.

Purpose of the Project:

- To simulate HIP using Cisco Packet Tracer, demonstrating its core principles.
- Hostnames represent HITs, simulating permanent identities.
- Links are labeled as "secure tunnels" to conceptually illustrate HIP's encrypted communication.
- The simulation highlights key HIP features:
    - Host identification independent of IP
    - Session continuity during mobility
    - Secure communication

This simulation provides a clear understanding of HIP functionality and its importance in dynamic, secure, and mobile network environments.

Objectives

The main objectives of this project are:

1. Understand the Host Identity Protocol (HIP):
    - To learn how HIP separates host identity from IP addresses, improving security and mobility.
2. Simulate HIP in a controlled environment:
    - Use Cisco Packet Tracer to conceptually demonstrate HIP features like host identity (HIT), secure communication, and mobility.
3. Demonstrate session continuity:
    - Show that communication sessions persist even when a host's IP address changes.
4. Simulate secure communication:
    - Conceptually represent encrypted sessions using labeled tunnels between routers and hosts.
5. Provide practical learning:
    - Enable hands-on understanding of HIP principles and network configuration, routing, and mobility in a simulated network.

Outcomes

After completing this project, the following outcomes are achieved:

1. Conceptual understanding of HIP:
    - Clear understanding of how HIP works, including host identification, HIP base exchange, and session security.
2. Simulated HIP environment in Packet Tracer:
    - Hosts with permanent identities (HITs) communicating across multiple subnets.
3. Mobility support demonstration:
    - Show that a host can change its IP address while maintaining communication sessions.
4. Secure communication visualization:
    - Encrypted tunnels conceptually represent HIP's session security.
5. Enhanced learning of networking concepts:
    - Practical experience with IP addressing, static routing, subnetting, and host-router connectivity.

Methodology/Implementation

The methodology of this project focuses on conceptually simulating the Host Identity Protocol (HIP) using Cisco Packet Tracer, since the software does not natively support HIP. The main idea is to demonstrate host identity separation, secure communication, and mobility.

Step 1: Network Topology Design

- Two PCs (HostA and HostB) were used as hosts.
- Two routers (Router1 and Router2) were placed to connect the different subnets.
- Two switches connected the PCs to their respective routers.
- The topology ensured two subnets: one for HostA (192.168.1.0) and another for HostB (192.168.2.0), connected via routers.

Step 2: IP Address Assignment

- Each host and router interface was assigned a static IP to ensure communication across subnets.
- Gateways were configured on PCs to enable routing through routers.
- Example: HostA → 192.168.1.2, Gateway: 192.168.1.1; HostB → 192.168.2.2, Gateway: 192.168.2.1.

Step 3: Router Configuration

- Static routes were added to routers to allow cross-subnet communication.
- Serial interfaces were configured and activated, with clock rate on the DCE side.
- This setup ensured that packets could traverse from HostA to HostB and vice versa.

Step 4: Assign Host Identity (HIT)

- Hostnames of PCs were changed to simulate HIP's permanent host identities:
  - HostA → HostA_HIT
  - HostB → HostB_HIT
- This demonstrates identity independent of IP address.

Step 5: Testing Basic Connectivity

- The ping command was used to verify communication between hosts.
- Initial timeouts occurred due to ARP resolution, followed by successful replies.

Step 6: Simulate Secure Communication

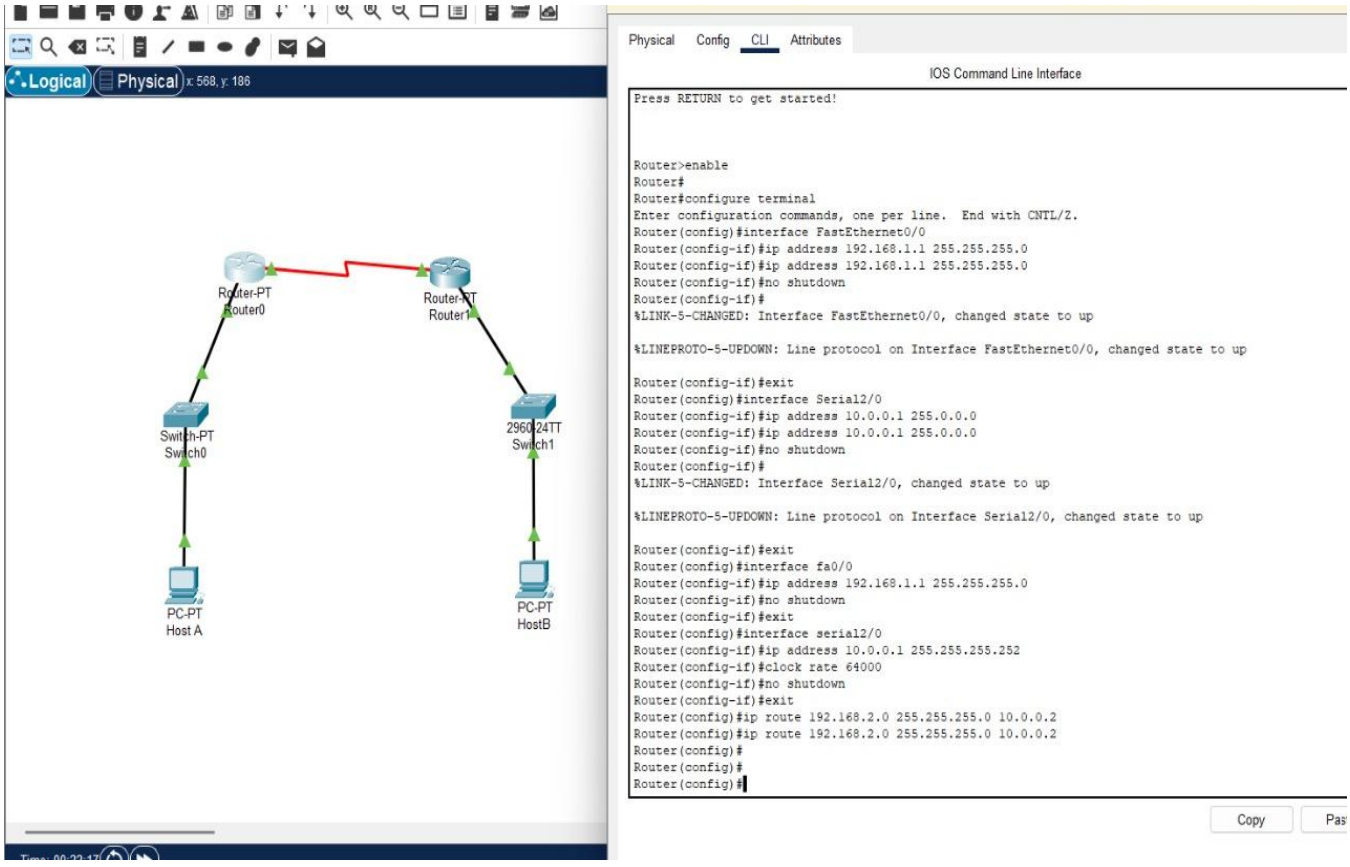
- Connections between routers were labeled “HIP Secure Tunnel” to conceptually represent HIP’s cryptographic sessions.

Step 7: Mobility Simulation

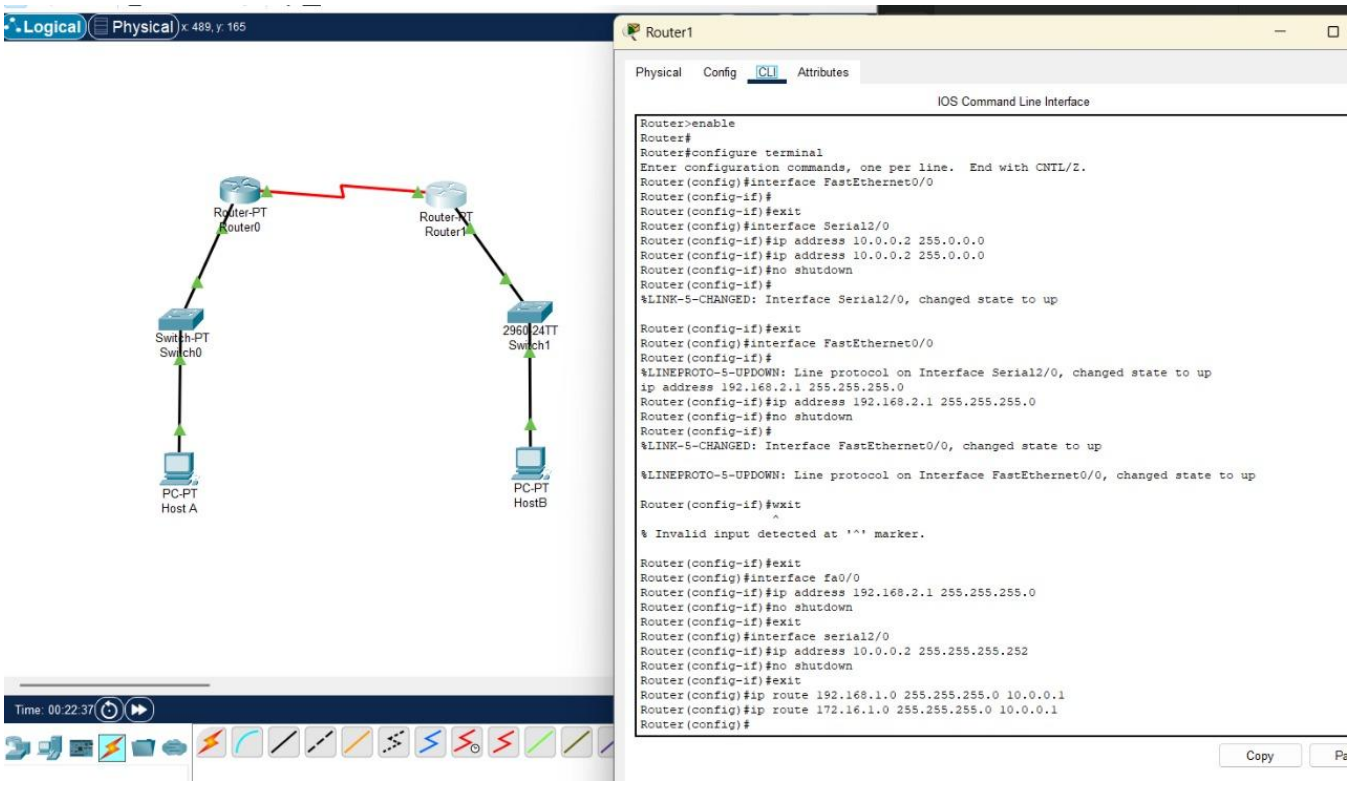
- HostA’s IP was changed to a new subnet (e.g., 172.16.1.2).
- Router interfaces and static routes were updated accordingly.
- Despite the IP change, communication with HostB continued uninterrupted, demonstrating HIP’s mobility support.

Implementation Snapshots:

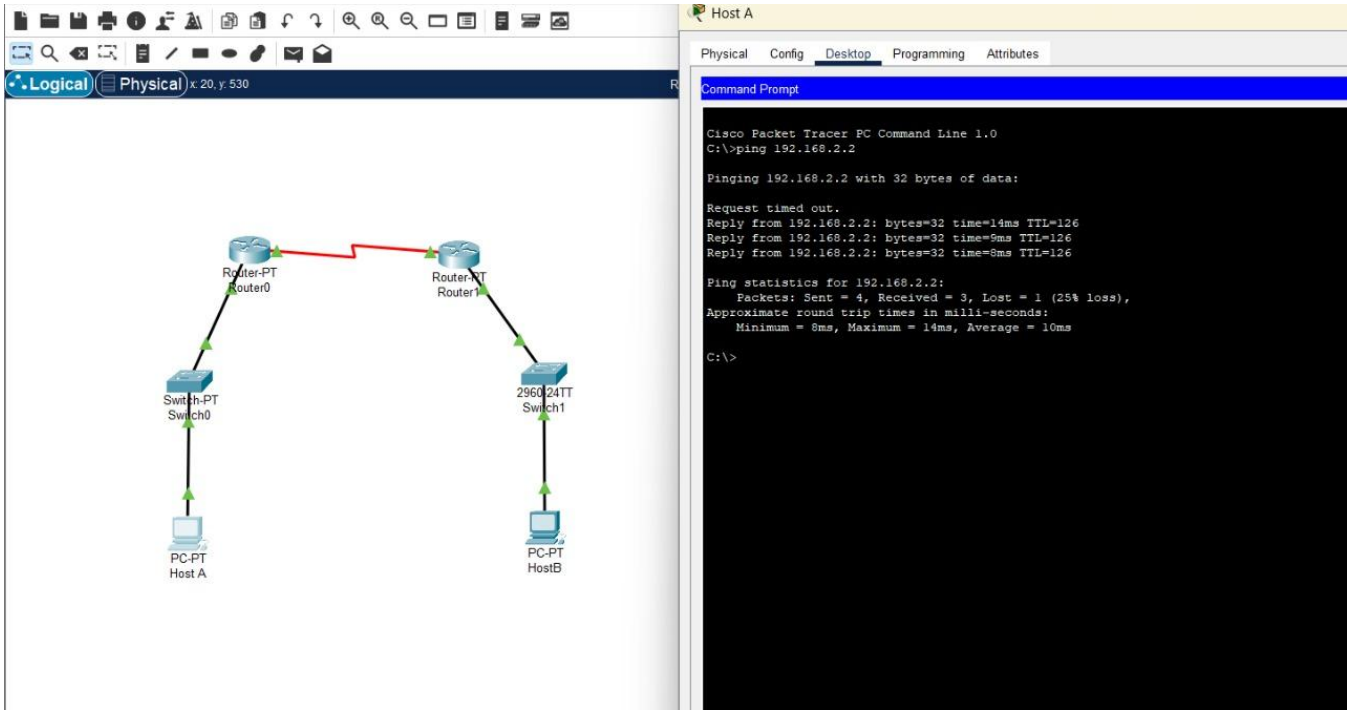
1. Router 0 configuration



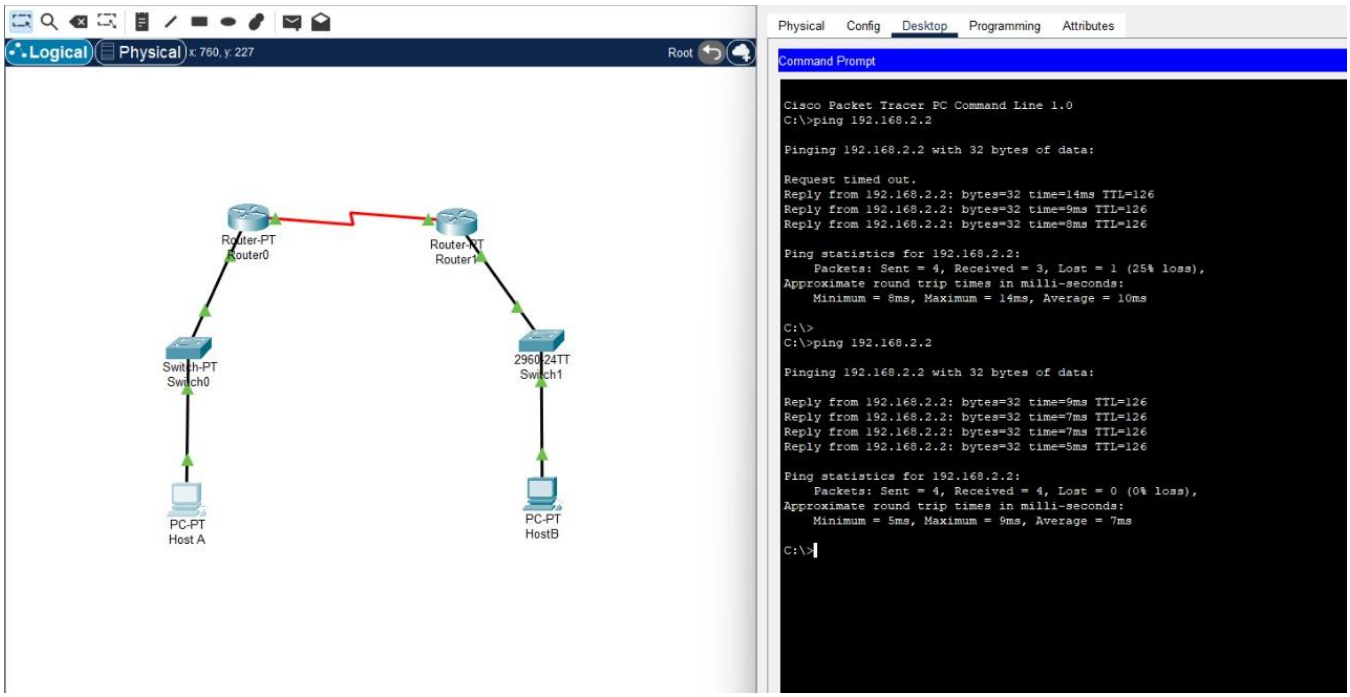
2. Router 1 Configuration



3. Pinging of Host A to Host B



4. Pinging Host A to Host B to verify the mobility



Observation

During the HIP simulation project, the following observations were made:

1. Host Identity (HIT) Persistence:
   - Even when HostA's IP address was changed to a new subnet, the hostname (HostA_HIT) remained unchanged.
   - This demonstrates HIP's principle of identity separation from IP address, allowing hosts to maintain a permanent identity regardless of location.
2. Session Continuity:
   - After changing HostA's IP, communication (ping) with HostB continued successfully once routing was updated.
   - This shows HIP's ability to maintain ongoing sessions even with dynamic IP addressing.
3. Routing Importance:
   - Static routes had to be configured on Router1 and Router2 after the IP change to maintain connectivity.
   - This highlights the necessity of proper routing in networks with multiple subnets and mobile hosts.
4. Conceptual Secure Communication:
   - Although Packet Tracer cannot implement real HIP cryptography, labeling links as "HIP Secure Tunnel" effectively simulates secure communication.
   - It helps visualize HIP's role in authenticated and encrypted sessions.

5. Mobility Simulation:
    - HostA successfully communicated across different subnets without changing its HIT.
    - This demonstrates HIP's support for mobility and multi-homing in dynamic network environments.
6. Practical Learning:
    - The simulation provided hands-on experience with IP addressing, subnetting, router configuration, and network troubleshooting.
    - It reinforced the conceptual understanding of HIP's benefits in real-world networks.

Advantages

Advantages of HIP

1. Separation of Host Identity from IP Address
    - HIP introduces Host Identifiers (HITs), which remain constant even if the host's IP address changes.
    - This allows mobility and multihoming, meaning devices can move across networks or use multiple IPs without breaking ongoing communication sessions.
2. Enhanced Security
    - By using cryptographic identifiers, HIP provides strong authentication between hosts.
    - It prevents common attacks such as IP spoofing, Man-in-the-Middle (MITM), and unauthorized access, ensuring that only verified hosts can communicate.
3. Session Continuity
    - HIP ensures that existing connections remain active even when a host changes its IP address.
    - This is particularly useful for mobile devices, IoT devices, or dynamic networks, where IP addresses frequently change.
4. Support for Multi-homing and Mobility
    - HIP allows a host to have multiple IP addresses simultaneously.
    - The host can switch between IPs without interrupting sessions, which is critical for networks with dynamic routing or mobile nodes.
5. Flexibility in Network Management
    - Since identity is independent of location, network administrators can reconfigure IP addressing or subnets without affecting sessions.

Disadvantages

Disadvantages of HIP

1. Complex Implementation
    - HIP is not widely supported in standard network devices.
    - Implementing HIP requires modified operating systems or software stacks, which can be technically challenging.
2. Increased Overhead
    - The use of cryptographic identifiers and base exchanges introduces extra processing.
    - This can slightly reduce network performance, especially on resource-constrained devices like IoT sensors.
3. Limited Compatibility
    - Many existing routers and firewalls do not natively support HIP.
    - Special configuration or software simulation (like in Packet Tracer) is often required.
4. Learning Curve
    - Understanding HIP concepts like HITs, base exchange, and mobility support requires additional training.
    - Network engineers need to grasp both networking fundamentals and cryptography concepts.
5. Simulation Limitations
    - In tools like Packet Tracer, HIP is conceptually simulated.
    - Real cryptographic and security features cannot be fully tested, which may limit hands-on experience.

Application

Applications of Host Identity Protocol (HIP)

1. Mobile Networks and Devices
    - HIP is particularly useful for mobile devices such as smartphones, laptops, and tablets.
    - It allows devices to change IP addresses while maintaining ongoing communication sessions, which is crucial for mobile users moving between networks (e.g., Wi-Fi to cellular networks).
2. Internet of Things (IoT)
    - IoT devices often have dynamic IPs and need secure communication.
    - HIP provides host-based identity and session continuity, enabling IoT devices

to connect securely across changing networks without disrupting communication.

3. Multi-homed Hosts and Load Balancing
    - Hosts with multiple network interfaces (multi-homed) can use HIP to switch between IP addresses seamlessly.
    - This supports load balancing and redundancy, ensuring continuous connectivity even if one network interface fails.
4. Secure Communications and VPNs
    - HIP enhances security by using cryptographic identifiers for host authentication.
    - It can be applied in VPNs and secure communication setups, providing an extra layer of trust beyond traditional IP-based identification.
5. Dynamic and Reconfigurable Networks
    - In networks with frequent IP address reassignments or network topology changes, HIP ensures that ongoing sessions are not interrupted.
    - Useful in enterprise networks, cloud environments, and research networks where flexibility is needed.
6. Research and Experimental Protocols
    - HIP is used in network research and experimental protocols to study mobility, multihoming, and secure host identification in next-generation Internet architectures.

Conclusion

The Host Identity Protocol (HIP) effectively separates a host's identity from its IP address, enhancing security, mobility, and session continuity. Through this simulation in Cisco Packet Tracer, the project demonstrated key HIP features, including permanent host identities (HITs), secure communication, and mobility support. Even when HostA's IP address changed, communication with HostB remained uninterrupted, illustrating HIP's principle of identity-location separation. Additionally, the project provided hands-on learning in IP addressing, routing, and network configuration, while conceptually simulating secure sessions. Overall, the simulation highlights HIP's potential for mobile networks, IoT devices, multi-homed hosts, and secure dynamic networks, making it a valuable protocol for modern network environments.

References

- Moskowitz, R., & Nikander, P. (2008). *Host Identity Protocol (HIP) Architecture*. RFC 4423. https://www.rfc-editor.org/rfc/rfc4423
- Nikander, P., & Laganier, J. (2006). *Host Identity Protocol (HIP) Overview*. IETF Journal. https://tools.ietf.org/html/rfc5201
- Cisco Systems. (2023). *Cisco Packet Tracer – User Guide*. Cisco Networking Academy. https://www.netacad.com/courses/packet-tracer

Rubrics	Contents & Description	Viva-Voce	Report Submission
Marks Scored			
Out of	**5M**	**3M**	**2M**
Remark & Sign			