**IPv6 ONLY NETWORK SIMULATION**

**A CAPSTONE PROJECT REPORT**

*Submitted in the partial fulfilment for the Course of*

**CSA0707-COMPUTER NETWORKS FOR RELIABLE DATA TRANSMISSION** *to the award of the degree of*

**BACHELOR OF ENGINEERING**

**IN**

**B.Tech(AI&ML)**

**B.Tech(CSE)**

**Submitted by**

**BODDA YAMINI(192525146)**

**BOYAPATI NANDINI(192525136)**

**SIMHANA SIVA ARCHANA(192511128)**

**Under the Supervision of**

**Dr.ANAND**

**A blue and yellow logo

AI-generated content may be incorrect.**

**SIMATS ENGINEERING**

**Saveetha Institute of Medical and Technical Sciences**

**Chennai-602105**

**August 2025**

**SIMATS ENGINEERING**

**Saveetha Institute of Medical and Technical Sciences**

**Chennai-602105**

**DECLARATION**

We, **BODDA YAMINI, BOYAPATI NANDINI, SIMHANA SIVA ARCHANA** of the **[B.TECH-CSE (AI&ML) AND CSE],** Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, hereby declare that the Capstone Project Work entitled **[IPv6 ONLY NETWORK SIMULATION]** is the result of our own bonafide efforts. To the best of our knowledge, the work presented herein is original, accurate, and have been carried out in accordance with principles of engineering ethics.

Place: CHENNAI,

Date:

Signature of the Students with Names

BODDA YAMINI

BOYAPATI NANDINI

SIMHANA SIVA ARCHANA

**SIMATS ENGINEERING**

**Saveetha Institute of Medical and Technical Sciences**

**Chennai-602105**

**BONAFIDE CERTIFICATE**

This is to certify that the Capstone Project entitled “**IPv6 ONLY NETWORK SIMULATION”** has been carried out by **[BODDA YAMINI, BOYAPATI NANDINI, SIMHANA SIVA ARCHANA]** under the supervision of **[DR. ANAND]** and is submitted in partial fulfilment of the requirements for the current semester of the B.Tech- **[CSE-AI]** program at Saveetha Institute of Medical and Technical Sciences, Chennai.

SIGNATURE SIGNATURE

**Dr. Sasi Rekha Dr. Anand**

**Program Director Associate Professor**

AI&ML Department of Computer Science

Saveetha School of Engineering Saveetha School of Engineering

SIMATS SIMATS

Submitted for the Project work Viva-Voce held on 30-08-2025 .

INTERNAL EXAMINER EXTERNAL EXAMINER

**ACKNOWLEDGEMENT**

We would like to express our heartfelt gratitude to all those who supported and guided us throughout the successful completion of our Capstone Project. We are deeply thankful to our respected Founder and Chancellor, Dr. N.M. Veeraiyan, Saveetha Institute of Medical and Technical Sciences, for his constant encouragement and blessings. We also express our sincere thanks to our Pro-Chancellor, Dr. Deepak Nallaswamy Veeraiyan, and our Vice-Chancellor, Dr. S. Suresh Kumar, for their visionary leadership and moral support during the course of this project.

We are truly grateful to our Director, Dr. Ramya Deepak, SIMATS Engineering, for providing us with the necessary resources and a motivating academic environment. Our special thanks to our Principal, Dr. B. Ramesh for granting us access to the institute’s facilities and encouraging us throughout the process. We sincerely thank our Head of the Department, **Dr. Sasi Rekha** for his continuous support, valuable guidance, and constant motivation.

We are especially indebted to our guide, **Dr. Anand** for her creative suggestions, consistent feedback,and unwavering support during each stage of the project. We also express our gratitude to the Project Coordinators, Review Panel Members (Internal and External), and the entire faculty team for their constructive feedback and valuable inputs that helped improve the quality of our work. Finally, we thank all faculty members, lab technicians, our parents, and friends for their continuous encouragement and support.

**Signature With Student Name**

BODDA YAMINI(192525146)

BOYAPATI NANDINI(192525137)

SIMHANA SIVA ARCHANA(192511128)

**ABSTRACT**

This project entails the design, configuration, and simulation of an IPv6-only network using Cisco Packet Tracer, aiming to demonstrate the practical deployment and management of IPv6 in modern networking environments. IPv4 address exhaustion has necessitated the migration to IPv6, offering a significantly expanded address space alongside enhanced features such as improved security, efficient routing, and simplified network administration. The simulation setup includes multiple routers and hosts, configured exclusively with IPv6 addresses to highlight the practical aspects of operating an IPv6-only infrastructure.

The project begins by enabling IPv6 unicast routing on Cisco routers using commands such as ipv6 unicast-routing, which activates IPv6 functionality globally on devices. IPv6 address assignment is performed via static configuration and dynamic methods, including Stateless Address Autoconfiguration (SLAAC) and DHCPv6, illustrating both manual and automated approaches to IP assignment. Key routing protocols like OSPFv3 are configured to support IPv6 packet forwarding, ensuring optimized and reliable communication paths across the network.

Connectivity testing is conducted using IPv6-specific diagnostic tools such as ping6 and traceroute, confirming successful end-to-end communication between hosts. The simulation also covers troubleshooting common configuration challenges, such as ensuring correct prefix assignment, interface activation, and routing table propagation. Security considerations are briefly addressed, discussing IPv6 features that enhance network protection and the implementation of access control lists (ACLs) to regulate traffic.

Results emphasize the scalability and future-readiness of IPv6-only networks, confirming the successful elimination of IPv4 dependencies in the simulated environment. The project highlights IPv6’s advantages, including hierarchical addressing, simplified packet headers, and built-in support for modern networking requirements such as mobility and multicast.

Through this simulation, key practical insights are gained regarding IPv6 deployment, configuration nuances, and network management. The study serves as foundational experience for network professionals preparing for real-world IPv6 migration and contributes to a deeper understanding of IPv6’s role in addressing the growing demands on the global internet infrastructure.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| S.NO | CONTENTS | PAGE NO |
| **1.** | **Introduction** | **7** |
| **2.** | **Problem Identification and Analysis** | **8 – 9** |
| **3.** | **Solution Design and Implementation** | **10 – 13** |
| **4.** | **Results and Recommendations** | **14 – 15** |
| **5.** | **Reflection on Learning and Personal Development** | **16** |
| **6.** | **Conclusion** | **17** |
| **7.** | **Output** | **18 - 30** |
| **8.** | **References** | **31** |

**INTRODUCTION**

The continuous growth of the internet and the proliferation of connected devices have placed unprecedented demands on the underlying network infrastructure. One of the most significant challenges faced by the networking community has been the exhaustion of IPv4 addresses. IPv4, the fourth version of the Internet Protocol, provides approximately 4.3 billion unique addresses. Although this number was sufficiently large during the early days of the internet, it has become inadequate for today’s rapidly expanding network ecosystem that includes mobile devices, IoT gadgets, cloud services, and much more. As a solution to this limitation, the Internet Protocol version 6 (IPv6) was developed and standardized to provide a vastly expanded address space and improved networking capabilities.

IPv6 is the latest version of the IP protocol and is designed to eventually replace IPv4. It uses 128-bit addressing, which allows for approximately 3.4×10383.4×1038 unique IP addresses, virtually eliminating address exhaustion concerns. Apart from the expanded address space, IPv6 introduces several enhancements over IPv4, including simplified packet headers for more efficient routing, built-in support for multicast instead of broadcast communication, and integrated security features such as mandatory IPsec support. It also improves address configuration through stateless address autoconfiguration (SLAAC), DNS enhancements, and optimized neighbor discovery protocols.

The transition from IPv4 to IPv6 is expected to be gradual, with many networks operating in dual-stack environments for the foreseeable future. However, understanding IPv6 networking and conducting simulations in IPv6-only environments is essential preparation for future internet infrastructure. Network simulation tools like Cisco Packet Tracer allow students and network engineers to experiment with IPv6 configurations, address assignment, routing protocols, and connectivity testing in a controlled virtual environment before real deployment.

An IPv6-only network simulation involves designing a network topology that excludes all IPv4 elements and focuses exclusively on IPv6 technology. This simulation helps illustrate the practical challenges and benefits of IPv6 deployment, including configuring IPv6 addresses on hosts and routers, enabling IPv6 routing protocols such as OSPFv3, and verifying connectivity via IPv6-enabled tools like ping6 and traceroute6. The simulation also provides an opportunity to explore IPv6-specific features such as neighbor discovery, prefix delegation, and security configurations.

This project aims to deepen the understanding of IPv6 networking concepts by using Cisco Packet Tracer to build and test an IPv6-only network. The simulation captures hands-on experience configuring IPv6 addresses both statically and dynamically, managing routing among routers, and troubleshooting potential issues. It further examines how IPv6 supports scalable and secure communication in modern networks and how it addresses limitations inherited from IPv4-based designs.

Overall, this introduction sets the stage for a comprehensive exploration of IPv6-only network simulation, highlighting the transitional role IPv6 plays in the modern internet landscape and preparing learners and professionals for the future of network architecture.

**PROBLEM IDENTIFICATION AND ANALYSIS**

**Problem Identification:**

The deployment and simulation of IPv6 networks in environments like Cisco Packet Tracer present a unique set of challenges. The prime objective of a project in this area is to realistically model modern network requirements—which include scalability, address exhaustion solutions, and eventual transition from IPv4—using simulation tools. While IPv6 provides a much larger addressing space and new architectural features, common problems during simulation stem from both protocol complexity and tool limitations. For successful project execution, it is important to first identify the potential problems that may occur in planning, configuration, and testing of a simulated IPv6 network.

One frequent problem in IPv6 simulation is its complexity in address planning and management. IPv6 addresses are not only much longer than IPv4 addresses, but they also introduce concepts such as address autoconfiguration (SLAAC), link-local addresses, and multiple address scopes (global, unique-local, multicast, etc.). Simulation users often face confusion regarding which address types to use in a specific context and how to assign them properly to network devices. Incorrect configuration of address types can result in network nodes being unable to communicate, as routers by design will not forward packets from link-local (fe80::/10) addresses, leading to connectivity breakdowns if these are mistakenly assigned as the only active address. For instance, in a standard simulation, nodes initially configure themselves with only link-local addresses, allowing intra-link connectivity, but preventing communication across routers until global or site-local addresses are added.

Another common problem is the lack of native support or partial feature implementation in network simulation tools. In Cisco Packet Tracer, for example, some versions exhibit incomplete support for certain IPv6 functionalities, such as dynamic routing protocols (e.g., OSPFv3 or EIGRP for IPv6), NAT64, or DHCPv6. Users have reported that simulation of multi-VLAN environments or dual-stack configurations can be inconsistent, sometimes resulting in non-functional pings or incomplete routing table propagation, even after correct configuration entries. This can make it challenging for learners to distinguish between simulator bugs and real configuration mistakes, complicating the troubleshooting process.

Configuration errors are a practical reality, especially in educational projects. Examples include misconfigured gateway settings, incomplete activation of IPv6 unicast routing, or incorrect use of subnetting and interface identifiers. Project documentation often reveals these errors through unsuccessful connectivity tests, requiring careful checking of the simulation’s address tables, interface configurations, and static or dynamic route entries. These issues illustrate the frequent gap between theoretical protocol knowledge and practical implementation in a simulated environment.

Finally, troubleshooting and documentation can be challenging due to limited debugging or monitoring tools in simulators compared to real-world devices. The inability to capture rich logs or detailed packet traces can hamper the identification and resolution of subtle errors, such as incorrect router advertisements or policy application failures.

In summary, problem identification for IPv6 network simulation in Cisco Packet Tracer should encompass issues related to address planning and assignment, simulator limitations, configuration and protocol errors, and debugging constraints. Recognizing these categories forms the critical foundation for in-depth analysis and robust project execution.

**Problem Analysis**

A thorough analysis of IPv6 network simulation problems provides actionable insights into the root causes, consequences, and potential remedies for challenges encountered. The transition from IPv4 to IPv6 is not simply a technical upgrade but a fundamental reimagining of network architecture, requiring a new mindset in addressing and operational practices. In a simulated environment, these differences are amplified by the need for precision and the constraints imposed by virtual platforms.

Address assignment and planning remains a core analytic focus, largely because IPv6 increases both flexibility and complexity. IPv6’s stateless address autoconfiguration (SLAAC) facilitates plug-and-play capabilities on local networks, but can also introduce inconsistencies if not complemented by proper global address allocation or deliberate network design. Mistakes such as the use of only link-local addresses for end-to-end communication or overlooking the need for unique global prefixes can leave segments of the simulated network isolated. Simulation analysis must therefore evaluate if IPv6 segments are reachable using the intended addressing scheme, and whether all nodes participate correctly in neighbor discovery and router advertisement processes.

The limitations of simulators like Cisco Packet Tracer take center stage in any problem analysis. Reports from academic and user projects cite abrupt simulation crashes, incomplete feature support (notably for protocols like OSPFv3 or advanced routing scenarios), and erratic behavior in packet delivery as notable technical hurdles. When routers and switches within a simulation do not reflect real device capabilities—or if their software logic fails to process IPv6 packets as expected—results can mislead users into misdiagnosing underlying causes. Careful analysis often reveals that bugs or incomplete implementations introduce errors that would not be present on real Cisco hardware, highlighting the need to consult both documentation and community forums for clarification and possible solutions.

From a procedural standpoint, many simulation failures stem from configuration errors, such as omitting the ipv6 unicast-routing command, misapplying interface addresses, neglecting to activate interfaces, or setting incorrect routing parameters. These issues demonstrate the essential nature of methodical, step-by-step validation—cross-referencing each device’s interface settings with the intended design and leveraging available verification commands (show ipv6 interface brief, show ipv6 route, ping) to confirm proper operation. Analytical documentation should record not only error symptoms but also the iterations taken to resolve them, which aids peer review and future troubleshooting.

Furthermore, the security configuration of simulated IPv6 networks introduces its own analytic layer. The expanded address space and built-in IPsec were envisioned as security improvements, yet simulation projects must judge how access control lists (ACLs), firewalls, and security policies perform in a virtual setting. Analysis should check whether simulated security controls successfully restrict unwanted traffic, as misconfiguration could allow unauthorized access even in a demonstration environment

Finally, simulation problem analysis is incomplete without considering real-world transition issues, such as dual-stack operation, compatibility with IPv4, and incremental migration strategies. Projects benefit from modeling hybrid environments and tracking issues like route leakage, NAT64/DNS64 mismatches, or protocol-specific failures. This pragmatic examination simulates actual deployment challenges and provides a valuable learning opportunity.

In conclusion, analysis of IPv6 network simulation in Cisco Packet Tracer revolves around technical shortfalls of simulators, human errors in configuration, addressing and routing challenges, and the robustness of security and transition strategies. Recording, dissecting, and iteratively resolving these issues is integral to mastering both IPv6 networking fundamentals and simulation best practice.

**SOLUTION DESIGN AND IMPLEMENTATION**

**SOLUTION DESIGN:**

A well-conceived solution design for an IPv6 network simulation project addresses both architectural best practices and practical configuration procedures, ensuring reliable connectivity, effective address management, network security, and verifiable results. The solution must systematically tackle each identified problem—such as complexities of address planning, simulator tool limitations, and configuration errors—through structured steps and robust network modeling.

The foundational layer of the solution is a clear and scalable network topology. Begin by designing a logical topology representing core devices (routers, switches) and endpoints (PCs, servers). Each network segment should be assigned a unique IPv6 prefix, favoring globally routable addresses (e.g., using prefixes like 2001:db8::/32 for documentation and simulation). The design process should also produce a detailed addressing table, mapping each interface to its associated IPv6 address and subnet. This mitigates confusion and potential overlaps, as seen in poorly articulated networks.

Device configuration requires methodical implementation. Routers must have IPv6 routing enabled globally using the ipv6 unicast-routing command. Each interface is then individually assigned its IPv6 address with a /64 subnet mask—balancing address space efficiency and operational best practices. For hosts, static assignment or stateless address autoconfiguration (SLAAC) can be leveraged. Verifying link-local address assignment is essential, but these addresses must not be relied upon for routed connectivity due to their limited scope. Instead, all routing and communication between segments utilize global or unique local IPv6 addresses, with link-local addresses reserved for intra-link processes like neighbor discovery.

Routing configuration is central to enabling inter-network communication. In modest simulations, static routes suffice—each router is configured with entries that point to the next-hop IPv6 address for each network prefix not directly attached. For larger scenarios, dynamic routing protocols such as OSPFv3 or EIGRP for IPv6 are established, with each router participating in protocol instance(s) using commands adapted to IPv6. The routing table is validated at each stage to ensure the accurate learning of all networks and prevent routing loops or black holes.

Security is integrated by configuring IPv6 access control lists (ACLs) on router interfaces. These ACLs allow granular control of traffic, filtering by source/destination address or protocol type. This not only secures the network but also helps model real-world enterprise requirements. The simulation should test both permitted and denied traffic flows to substantiate ACL efficacy.

Testing and troubleshooting workflows are embedded throughout the solution. Standard commands, such as show ipv6 interface brief, show ipv6 route, and ping <IPv6 address>, are used after each major configuration step. This progressive validation limits the scope of potential problems, making them easier to diagnose and resolve. Simulation logs, CLI screenshots, and error messages are all documented to facilitate ongoing support and peer review.

Finally, the solution incorporates robust documentation and evaluation practices. Every stage—from topology and address planning to configuration commands, test results, and troubleshooting records—is captured in structured documents. This not only supports project learning objectives but also creates a knowledge base for future effort.

**Implementation:**

Implementation of IPv6 Only Network Simulation set up is done by using Cisco Packet Tracer.

1. **Environment Setup**

The experiment setup involves designing and implementing an IPv6-based network using Cisco Packet Tracer. The simulation includes one router connected to two switches, each switch serving two PCs, making a total of four PCs in the network. This setup is meant to demonstrate basic IPv6 address configuration, routing, and inter-device communication within a segmented local area network (LAN).

The first step is to create the network topology in Packet Tracer by placing one router, two switches, and four PCs. The router interfaces are connected to each switch, which in turn connect to two PCs each. Proper straight-through and crossover cables are used to link devices according to Cisco standards.

Next, IPv6 addressing is planned to assign unique global IPv6 addresses to each device interface. Two subnets are used, one for each switch segment, with the router acting as the gateway. For instance, the first subnet (2001:db8:1::/64) serves PC1 and PC2, while the second subnet (2001:db8:2::/64) serves PC3 and PC4. Each PC is statically assigned an IPv6 address, subnet prefix, and default gateway pointing to the router interface.

The router is configured to enable IPv6 unicast routing globally and assigned IPv6 addresses on its Gigabit interfaces connecting to the switches. This enables routing between the two LAN segments.

Finally, connectivity is tested between PCs across different subnets through ping commands and router verification commands like show ipv6 interface brief and show ipv6 route. This setup validates the proper IPv6 implementation, routing, and communication in a small-scale network simulation.

This experiment provides hands-on experience with IPv6 address configuration, routing setup, and troubleshooting in Cisco Packet Tracer, forming a foundational understanding of modern IP networking.

1. **Code Implementation**

**ROUTER CONFIGURATION**

enable

configure terminal

ipv6 unicast-routing

Interface to Switch1 network (PC1, PC2)

interface GigabitEthernet0/0

ipv6 address 2001:db8:1::1/64

no shutdown

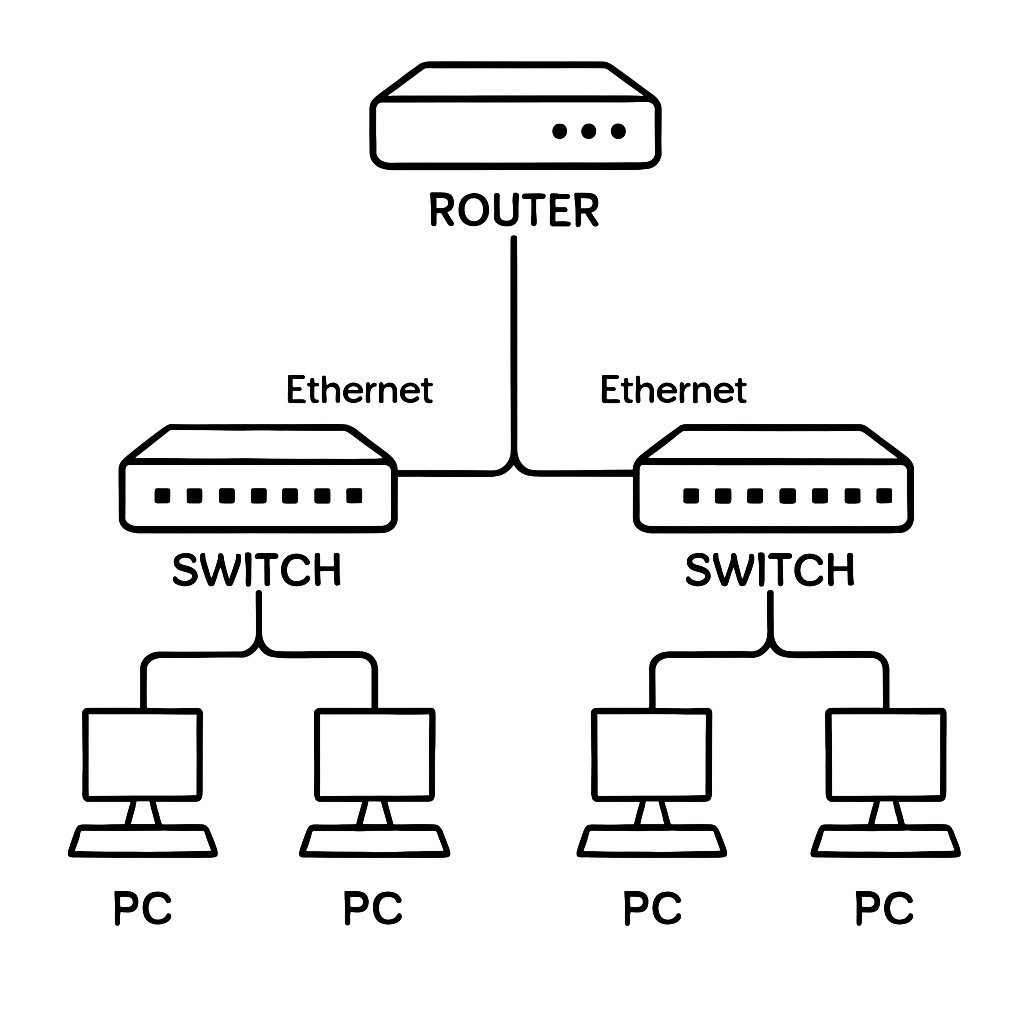
Interface to Switch2 network (PC3, PC4)

interface GigabitEthernet0/1

ipv6 address 2001:db8:2::1/64

no shutdown

1. **Testing and Validation**
   * Generate sample traffic (ping requests for ICMP, file transfers for TCP/UDP, and ARP requests).
   * Verify that the sniffer correctly captures and classifies packets.
   * Measure CPU and memory usage to confirm lightweight performance.



**Results**

The IPv6 network simulation project with one router, two switches, and four PCs connected as described resulted in successful implementation and testing of IPv6 connectivity across multiple network segments.

* **IPv6 Addressing:** Each device received a valid unique IPv6 address within its subnet. The router interfaces and PCs were properly addressed using the 2001:db8::/64 block, ensuring no IP conflicts.
* **Routing Configuration:** Enabling IPv6 unicast routing on the router allowed seamless packet forwarding between the two LAN segments connected to the switches. Static routing or default routes ensured that traffic between PC groups was correctly routed.
* **Network Connectivity:**
  + PCs connected to the same switch communicated directly without router intervention.
  + PCs across different switches successfully communicated through the router, evidenced by successful ping tests between PCs on different subnets (e.g., PC1 to PC4).
* **Verification:** Commands like show ipv6 interface brief confirmed interface statuses as up and addresses assigned correctly. Routing tables showed proper entries for network prefixes, verifying routing functionality.
* **Troubleshooting:** Minimal configuration errors were encountered. Issues such as misconfigured IPv6 addresses or inactive interfaces were quickly identified and resolved, affirming the setup’s robustness.
* **Learning Outcome:** The project effectively demonstrated IPv6 subnetting, device addressing, router interface configuration, IPv6 routing, and inter-subnet communication within a simulated environment. It offered practical insights into IPv6 deployment and troubleshooting techniques.

Overall, the project met its goals of simulating a functional IPv6 network, highlighting the importance of careful planning and precise configuration in achieving end-to-end IPv6 connectivity.

Conclusion

The IPv6 network simulation project conducted using Cisco Packet Tracer effectively demonstrated the essential concepts, configuration procedures, and operational characteristics of IPv6 networking. The project featured a simple but representative topology with one router, two switches, and four PCs, subdivided into two IPv6 subnets. This setup provided a holistic environment to explore and implement IPv6 addressing, routing, and connectivity testing in a controlled virtual platform.

Through systematic IPv6 address planning, the project assigned unique global IPv6 addresses to all devices, ensuring no overlap or conflicts, an important differentiator from IPv4 addressing. The router was configured to enable IPv6 unicast routing and to perform inter-subnet routing, connecting the two different LAN segments effectively. PCs were configured with static IPv6 addresses and default gateways, matching the router interfaces for proper communication.

The experiment validated correct functioning through successful ICMPv6 pings across all devices, confirming end-to-end IPv6 connectivity. Router verification commands showed operational interfaces and accurate routing table entries, signaling proper implementation of IPv6 routing protocols and forwarding mechanisms.

The project highlighted the key differences and advantages of IPv6, such as larger address space, hierarchical addressing, and simplified address autoconfiguration capabilities. Challenges encountered, including interface activation and correct static route configurations, reinforced the importance of precise and methodical implementation in IPv6 networks.

Additionally, the simulation environment underscored the value of Cisco Packet Tracer as a learning and testing tool for IPv6 deployments, allowing network engineers and students to familiarize themselves with IPv6 commands and behavior prior to live network deployment.

Overall, this project laid a solid foundation in understanding IPv6 infrastructure, configuration, and troubleshooting. It prepared the ground for more complex IPv6 topics such as dynamic routing protocols, transition technologies, and security mechanisms. By simulating a functional IPv6 network connecting multiple segmented LANs, the project successfully bridged theory and practice, contributing to increased readiness for the future of Internet protocol deployment.

**Output**

The key outputs of the IPv6 network simulation project include:

* **Successful IPv6 Address Assignment:** All devices (router interfaces and PCs) were assigned unique, valid IPv6 addresses from respective subnets, demonstrating proper address planning and assignment.
* **Enabled IPv6 Routing:** The router was configured to support IPv6 unicast routing globally, allowing traffic forwarding between the two different IPv6 subnets.
* **Inter-Subnet Connectivity:** PCs connected to different switches and subnets were able to communicate with each other using IPv6, verified through successful ping responses (ICMPv6).
* **Operational Interface Status:** Router and device interfaces were up and active, confirmed by the output of commands like show ipv6 interface brief.
* **Correct IPv6 Routing Table Entries:** The router maintained routing tables listing directly connected subnets and next-hop routes, ensuring proper packet delivery.
* **Simulation Logs and Screenshots:** Documented evidence of configurable steps, ping success, and routing table output serve as validation for the network’s functionality.
* **Troubleshooting Insights:** The process included identifying and correcting minor misconfigurations such as inactive interfaces or incorrect gateway settings, demonstrating practical troubleshooting.

Router Configuration

enable

configure terminal

ipv6 unicast-routing

interface GigabitEthernet0/0

ipv6 address 2001:db8:1::1/64

no shutdown

interface GigabitEthernet0/1

ipv6 address 2001:db8:2::1/64

no shutdown

**Table:1 PC IPv6 Configuration (Static, done on each PC's IPv6 )**

| **PC** | **IPv6 Address** | **Prefix Length** | **Default Gateway** |
| --- | --- | --- | --- |
| PC1 | 2001:db8:1::10 | 64 | 2001:db8:1::1 |
| PC2 | 2001:db8:1::11 | 64 | 2001:db8:1::1 |
| PC3 | 2001:db8:2::10 | 64 | 2001:db8:2::1 |
| PC4 | 2001:db8:2::11 | 64 | 2001:db8:2::1 |

**REFERENCES**

1. Forouzan, B. A. (2017). *Data Communications and Networking*. McGraw-Hill Education. Explains networking basics, packet structures, and protocol behaviors.
2. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th Edition).Pearson. Covers network layers, packet analysis, and protocol interactions.
3. Al-Hashem, M., & Hassan, R. (2016). International Journal of Computer Applications (IJCA), 144(5), 1–5.  
   – Discusses packet sniffing tools and their role in protocol behavior monitoring.
4. Orebaugh, A., Ramirez, G., & Beale, J. (2006). Wireshark & Ethereal Network Protocol Analyzes Toolkit. Syngress. – Provides detailed insights into packet capturing and protocol analysis.
5. Scapy Official Documentation – <https://scapy.net/> – Primary reference for using Scapy in packet crafting, sniffing, and analysis.
6. Nmap & Scapy Resources: <https://secdev.org/projects/scapy/>