IPv6Next – Enterprise Migration to IPv6

Students:

Mohamed Ali - 230102751

Marwan Hossam - 230104805

Rany Wael - 230103861

Ahmed Ramadan - 230104353

Belal Mahmoud - 230101227

Table of Contents

1. Summary 2. Introduction

2.1. Why IPv6?

3. Network Design

3.1. Network Topology

3.2. Router–Router Links

3.3. LAN Segments (Router ↔ Switch ↔ PCs)

4. Routing Protocols

4.1. OSPFv3 vs EIGRP Comparison

4.2. Justification for Protocol Choice

5. Implementation

5.1. Interface Configuration

5.2. IPv4/IPv6 Dual Stack Setup

5.3. OSPFv3 Configuration

6. Migration Strategy

6.1. Migration Steps

6.2. Device Configuration Changes

6.3. Rollback Plan

7. Testing

7.1. ICMP Testing

7.2. SLAAC Testing

7.3. DHCPv6 Testing

7.4. OSPFv3 Neighbor and Route Verification

8. Results and Discussion 9. Conclusion

1. Summary:

This report presents the design, implementation, and validation of a dualstack IPv4/IPv6 network architecture tailored for a mid-sized enterprise environment. The project aims to facilitate a seamless transition to IPv6 while maintaining full backward compatibility with IPv4 infrastructure. Using Cisco Packet Tracer as a simulation platform, the network topology includes eight routers, ten inter-router links, and eight local area networks (LANs), all configured to support dual-stack addressing. The routing protocol selected for IPv6 is OSPFv3, chosen for its scalability, open-standard compatibility, and fast convergence. The implementation includes core IPv6 services such as Stateless Address Autoconfiguration (SLAAC), stateless DHCPv6, and ICMPv6. Comprehensive testing was conducted to ensure end-to-end connectivity, routing stability, and fault recovery under various failure scenarios. This document provides a detailed addressing plan, protocol comparison, configuration steps, and a migration guide, offering a practical blueprint for future enterprise-grade IPv6 deployments.

2. Introduction

With the depletion of IPv4 addresses and evolving network demands, the transition to IPv6 is imperative. This report presents a simulated enterprise network deployment utilizing a dual-stack configuration. It covers design rationale, routing protocol evaluation, implementation procedures, testing methodologies, and operational verification.

2.1. Why IPV6?

The transition to IPv6 is driven by the limitations of IPv4 and the evolving needs of modern networks. IPv4's 32-bit address space provides approximately 4.3 billion addresses, which is no longer sufficient due to the rapid growth of internet-connected devices, IoT, and cloud infrastructure.

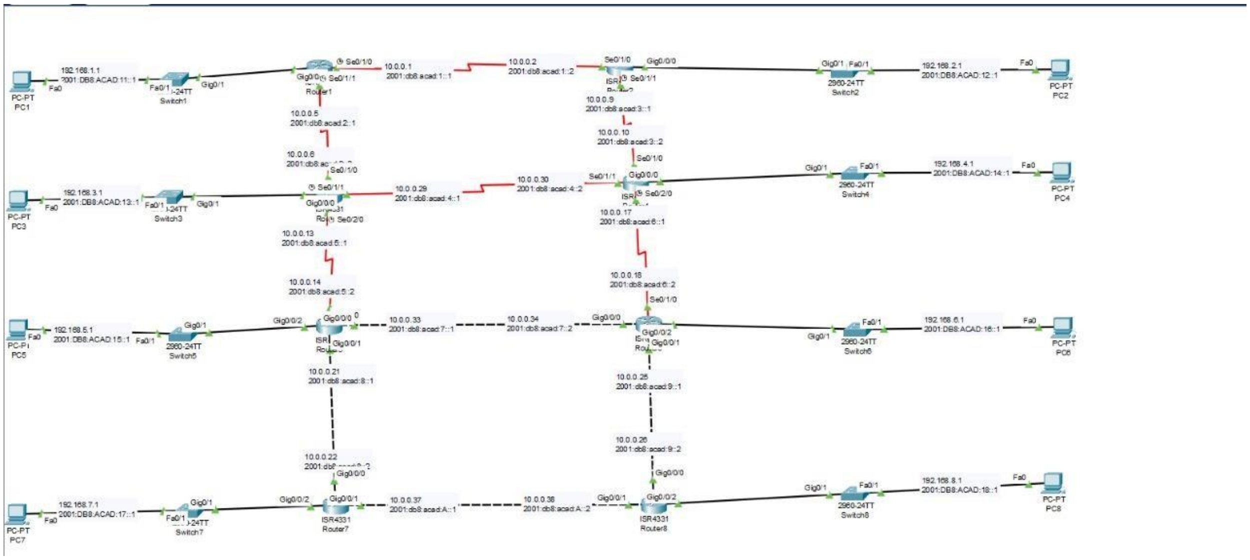
IPv6, with its 128-bit addressing, offers an almost limitless number of unique IP addresses, enabling end-to-end connectivity without the need for NAT (Network Address Translation). In addition to expanded address space, IPv6 introduces advantages such as:

- **Improved routing efficiency** with simplified headers and hierarchical addressing
- **Enhanced security**, with IPsec support built into the protocol
- **Better support for mobile and real-time applications**
- **Simplified network configuration** through stateless address autoconfiguration (SLAAC)

For enterprises, adopting IPv6 is essential to ensure scalability, maintain global reach, and stay aligned with current and future internet standards.

3. Network Design

3.1. Network Topology:



3.2. Router – Router Links

Router number	IPV4	IPV6
R1	192.168.1.0/24	2001\:db8\:acad:11::1
R2	192.168.2.0/24	2001\:db8\:acad:12::1
R3	192.168.3.0/24	2001\:db8\:acad:13::1
R4	192.168.4.0/24	2001\:db8\:acad:14::1
R5	192.168.5.0/24	2001\:db8\:acad:15::1
R6	192.168.6.0/24	2001\:db8\:acad:16::1
R7	192.168.7.0/24	2001\:db8\:acad:17::1
R8	192.168.8.0/24	2001\:db8\:acad:18::1

3.3. LAN segments (Router ↔ Switch ↔ PCs)

Links	IPV4
R1 ↔ R2 (S0/0/0 ↔ S0/0/0)	10.0.0.1 / 10.0.0.2
R1 ↔ R3 (S0/0/1 ↔ S0/0/0)	10.0.0.5 / 10.0.0.6
R2 ↔ R4 (S0/1/0 ↔ S0/0/0)	10.0.0.9 / 10.0.0.10
R3 ↔ R4 (S0/1/1 ↔ S0/1/1)	10.0.0.29 / 10.0.0.30
R3 ↔ R5 (S0/2/0 ↔ S0/1/0)	10.0.0.13 / 10.0.0.14
R4 ↔ R6 (S0/1/0 ↔ S0/0/0)	10.0.0.17 / 10.0.0.18
R5 ↔ R6 (G0/0/1 ↔ G0/0/0)	10.0.0.33 / 10.0.0.34
R5 ↔ R7 (G0/0/2 ↔ G0/0/0)	10.0.0.21 / 10.0.0.22
R6 ↔ R8 (S0/1/0 ↔ S0/1/0)	10.0.0.25 / 10.0.0.26
R7 ↔ R8 (S0/1/1 ↔ S0/1/1)	10.0.0.37 / 10.0.0.38

4. Routing Protocols

4.1. OSPFv3 vs EIGRP Comparison

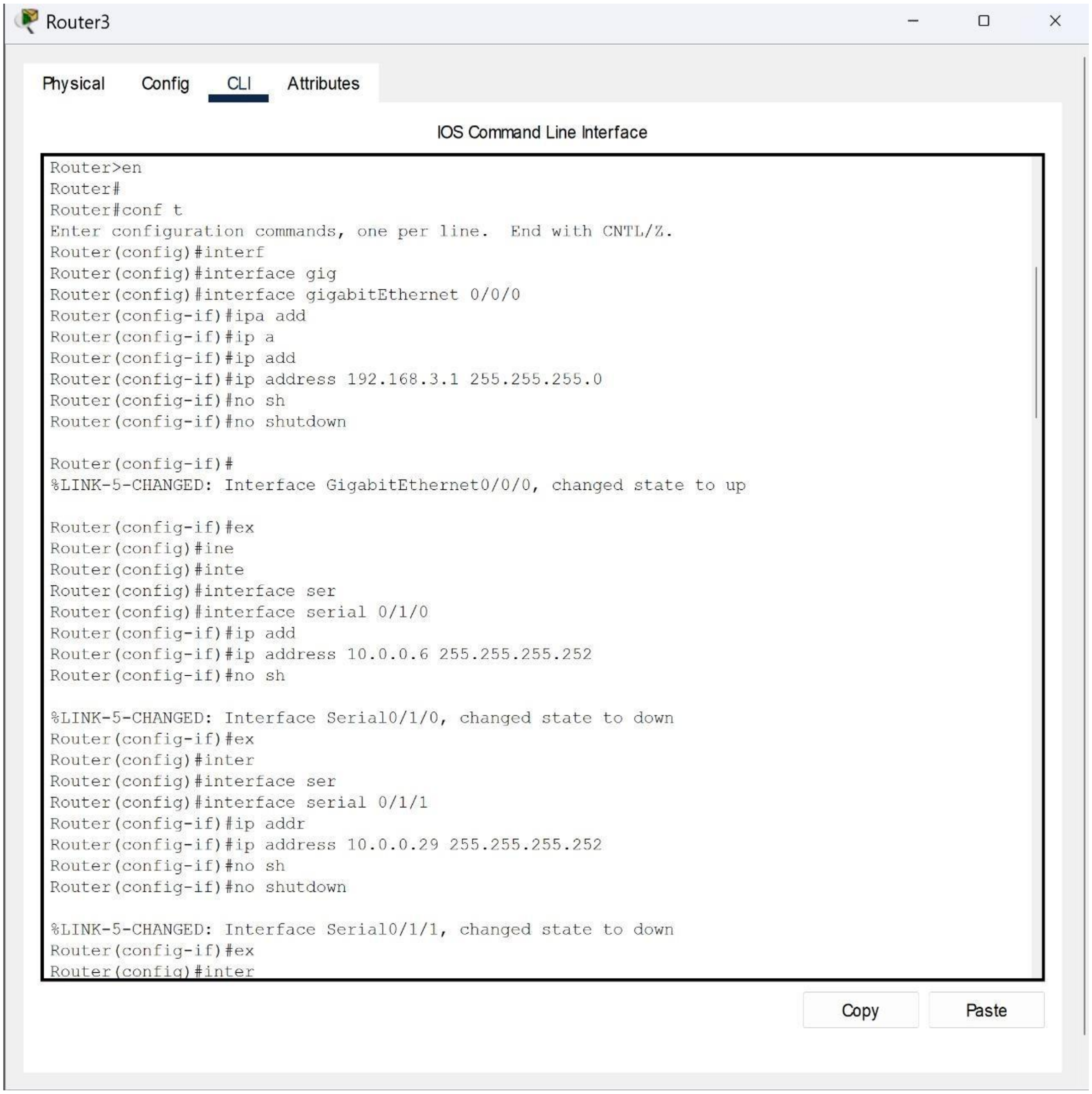
Protocol	Type	Scalability	Convergence	Complexity	Suitability
OSPFv3	Link-State	High	Fast	Moderate	Open Standard
EIGRP	Enhansed Distance Vector	High	Very fast	Moderate	Cisco - Proprietary

4.2. Justification for Protocol Choice

Based on the comparison, OSPFv3 was selected due to its open-standard nature, making it more suitable for multi-vendor environments than Ciscoproprietary EIGRP. While both offer high scalability and moderate complexity, OSPFv3 provides fast convergence and greater flexibility in enterprise networks. Its compatibility, structure, and long-term support make it a more strategic choice for this dual-stack deployment.

5. Implementation

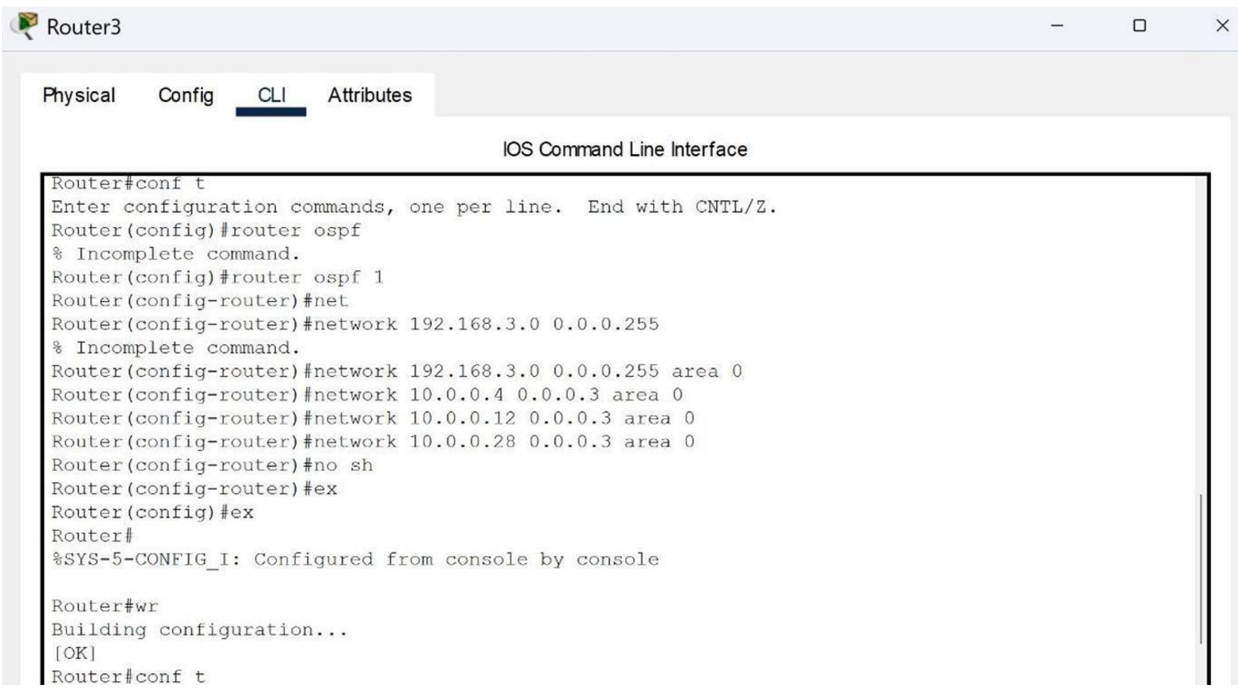
5.1. Interface Configuration



5.2. IPv4/IPv6 Dual Stack Setup

A dual-stack configuration was implemented on all routers to support both IPv4 and IPv6 protocols simultaneously. Each router interface was assigned both an IPv4 and an IPv6 address, allowing devices to communicate over either protocol based on availability and compatibility. The ipv6 unicastrouting command was used to enable IPv6 routing functionality on each router. This setup ensures continued support for IPv4 services while enabling IPv6 capabilities, facilitating a smooth transition without disrupting existing operations.

5.3. OSPFv3 Configuration



6. Migration Strategy

6.1. Migration Steps

1. Configure IPv4/IPv6 interfaces
2. Enable IPv6 routing
3. Configure OSPFv3

4. Enable DHCPv6 and SLAAC

6.2. Device Configuration Changes

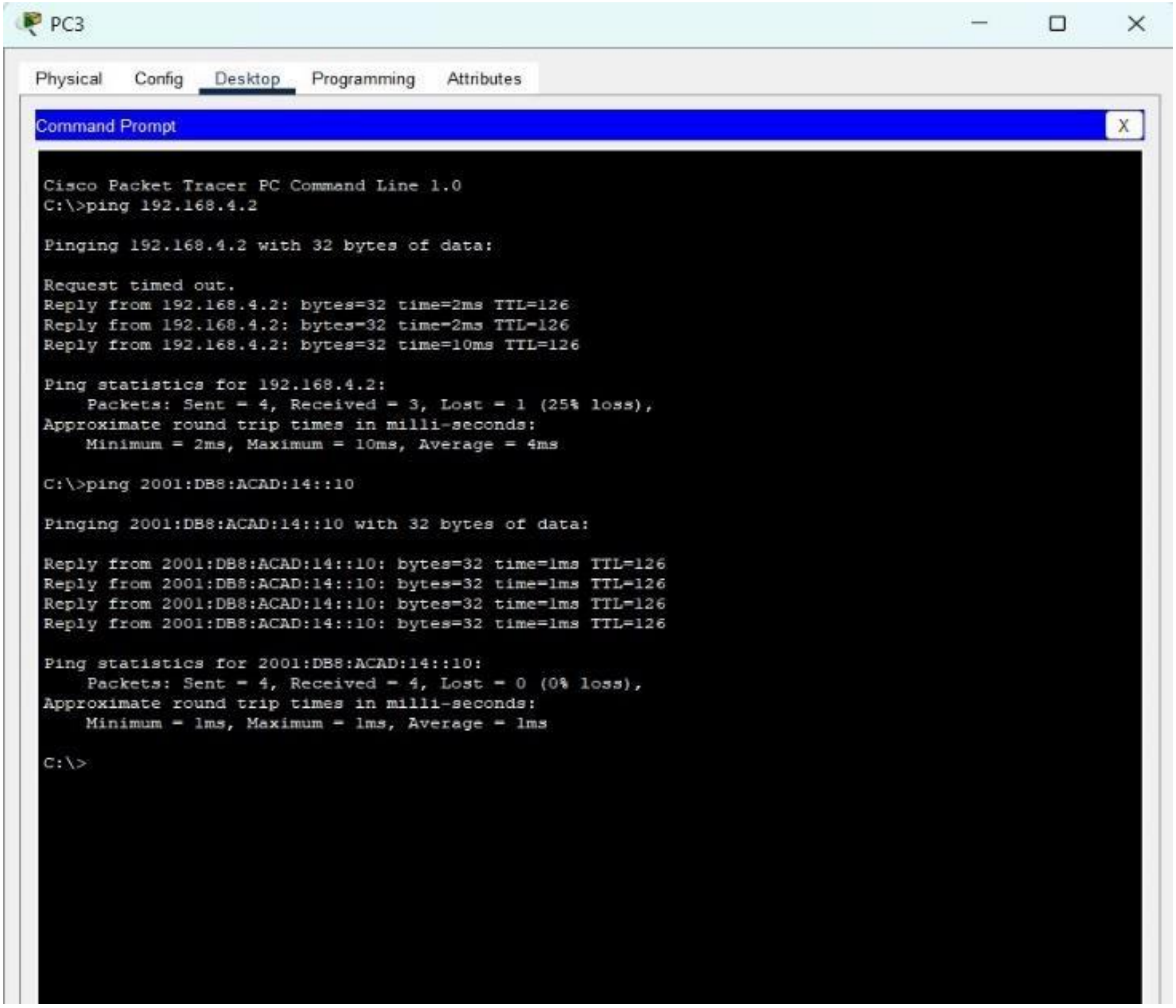
- Routers: Interface configs, routing protocols
- PCs: IPv6 auto config, IPv4 DHCP
- Switches: VLAN setup

6.3. Rollback Plan

- Static IPv6 fallback if OSPFv3 fails
- IPv4 routing retained throughout

7. Testing

7.1. ICMP Testing



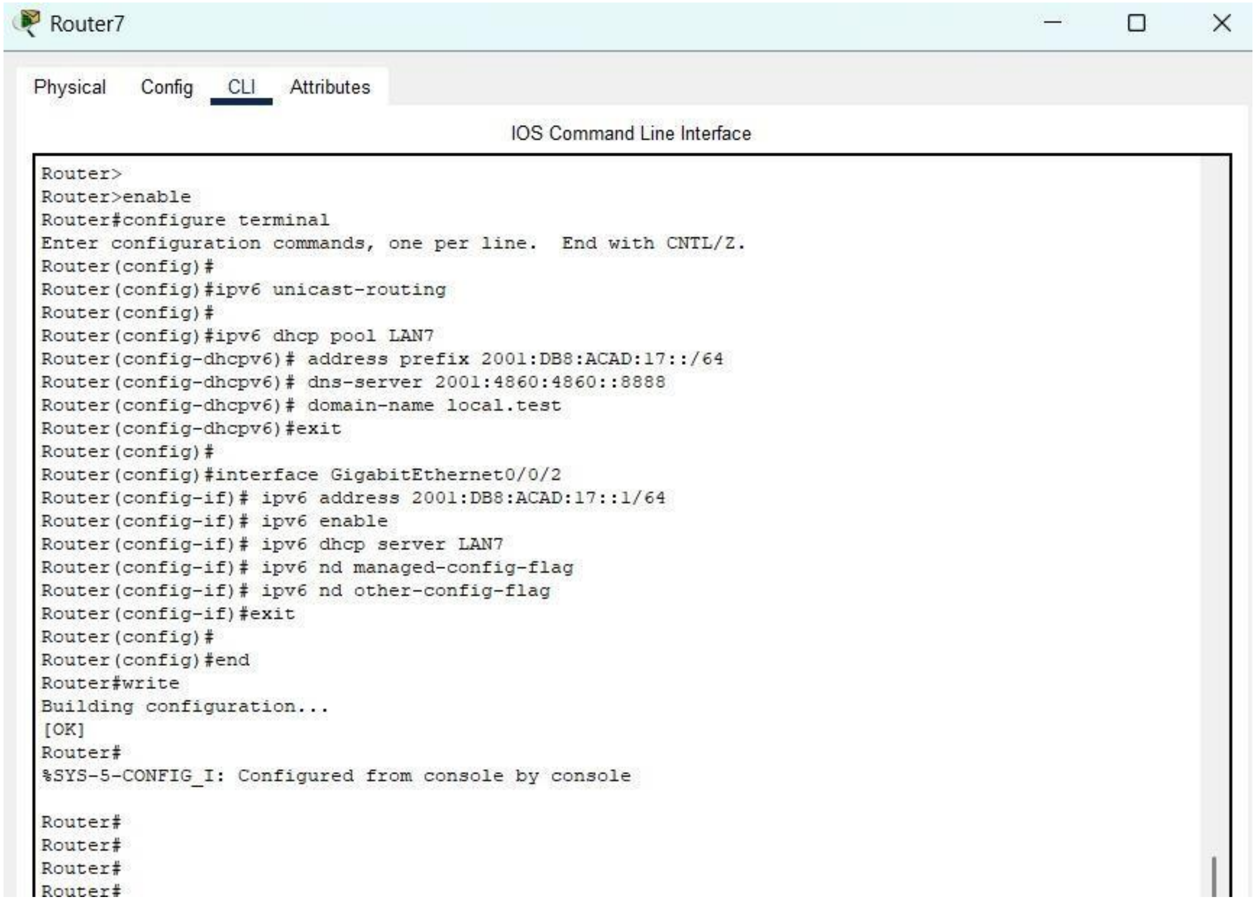
The above screenshot show successful ICMPv6 ping tests between various network devices. These tests verify that IPv6 addressing and routing are correctly configured, and that ICMPv6 messages are properly exchanged, confirming reliable end-to-end IPv6 connectivity.

7.2. **SLAAC**

```
C:\>
C:\>IPCONFIG /ALL

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 000C.CF29.99AE
   Link-local IPv6 Address.........: FE80::20C:CFFF:FE29:99AE
   IPv6 Address....................: 2001:DB8:ACAD:11::10
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 2001:DB8:ACAD:11::1
                                     192.168.1.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-34-AA-1B-0C-00-0C-CF-29-99-AE
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0040.0B9A.EA89
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-34-AA-1B-0C-00-0C-CF-29-99-AE
   DNS Servers.....................: ::
                                     0.0.0.0
```

The PC received a global IPv6 address (2001:DB8:ACAD:11::10) via SLAAC, confirming successful IPv6 autoconfiguration from the router's advertisement.

7.3. **DHCPv3 Testing**

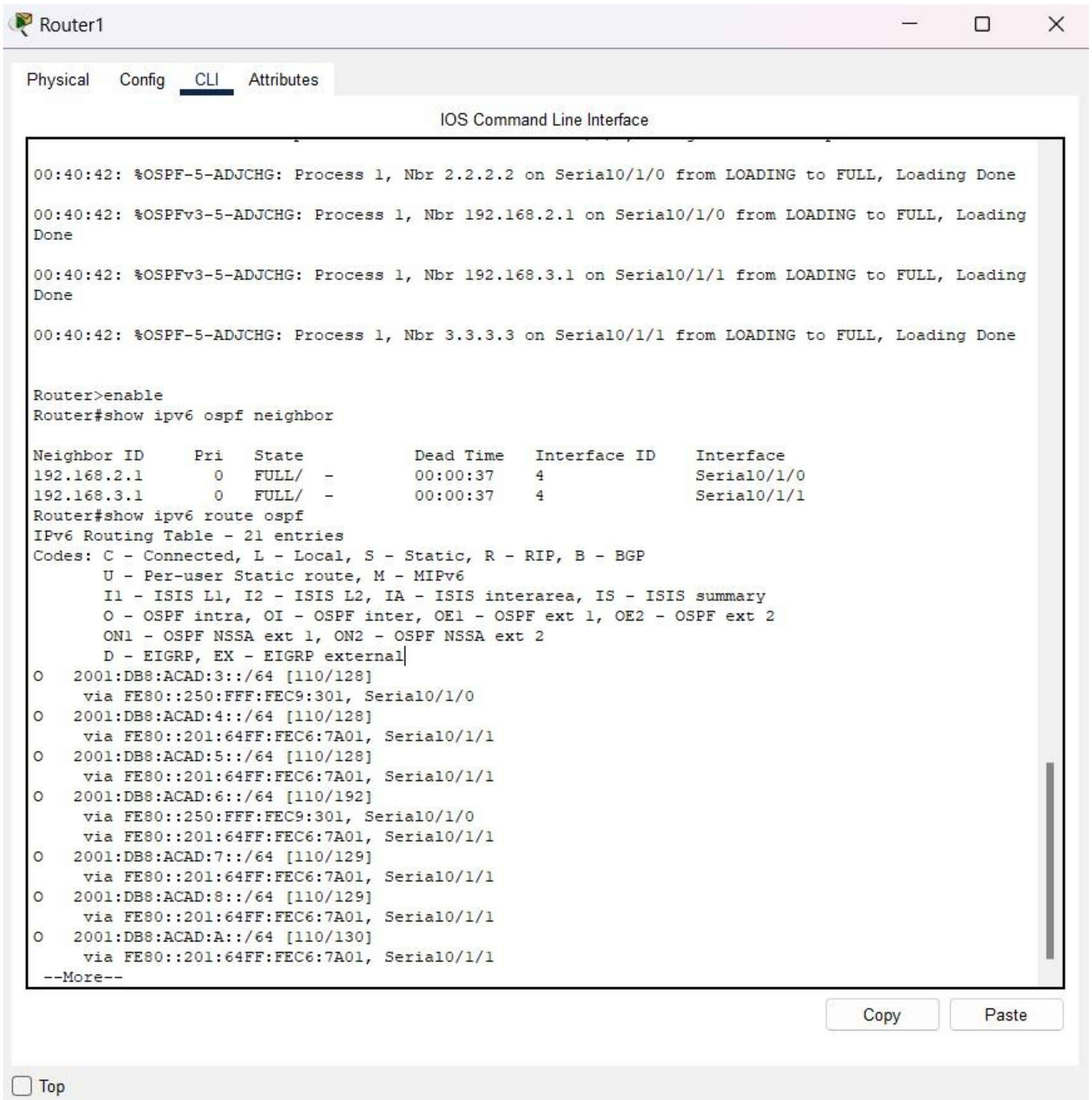


This screenshot displays the configuration of DHCPv6 on the router using the CLI. The router is set to provide IPv6 addresses with the prefix 2001:DB8:ACAD:17::/64 via a DHCPv6 pool named LAN7. It also advertises DNS and domain settings, and enables RA flags to inform hosts to use DHCPv6 for both addressing and other configurations.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..: local.test
   Physical Address................: 000C.8575.E67E
   Link-local IPv6 Address.........: FE80::20C:85FF:FE75:E67E
   IPv6 Address....................: 2001:DB8:ACAD:13:FF4A:AA5F:62F7:3831
   IPv4 Address....................: 192.168.3.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: FE80::201:64FF:FEC6:7A01
                                     192.168.3.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 2107409215
   DHCPv6 Client DUID..............: 00-01-00-01-DB-94-BC-2B-00-0C-85-75-E6-7E
   DNS Servers.....................: 2001:4860:4860::8888
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..: local.test
   Physical Address................: 000B.BE53.ED2B
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 2107409215
   DHCPv6 Client DUID..............: 00-01-00-01-DB-94-BC-2B-00-0C-85-75-E6-7E
   DNS Servers.....................: ::
                                     0.0.0.0
```

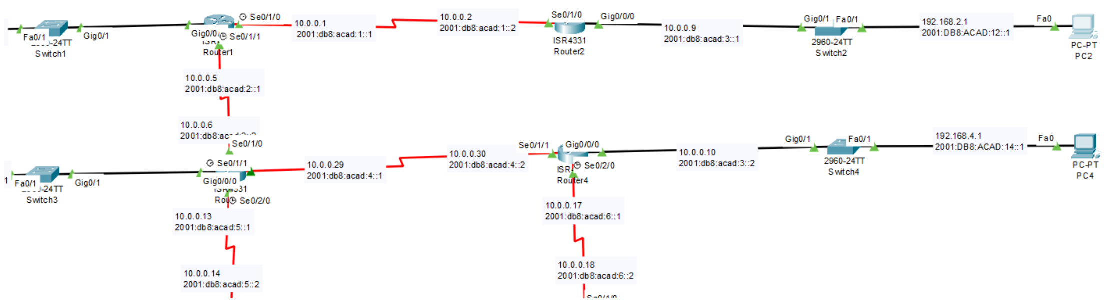
This screenshot shows the output of the ipconfig /all command on a PC, verifying that DHCPv6 is functioning correctly. The PC received an IPv6 address, DNS server, and domain name from the router’s DHCPv6 pool. This confirms that the PC is successfully communicating with the DHCPv6 server and obtaining configuration dynamically.

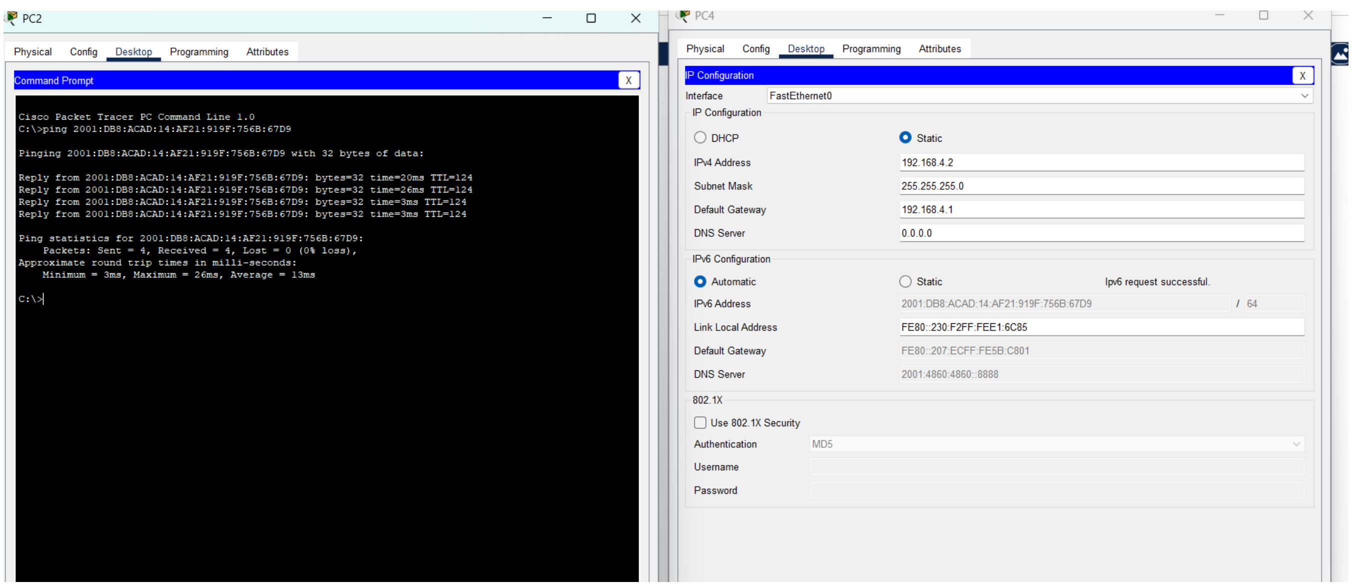
7.4. OSPFv3 Neighbor and Route Verification

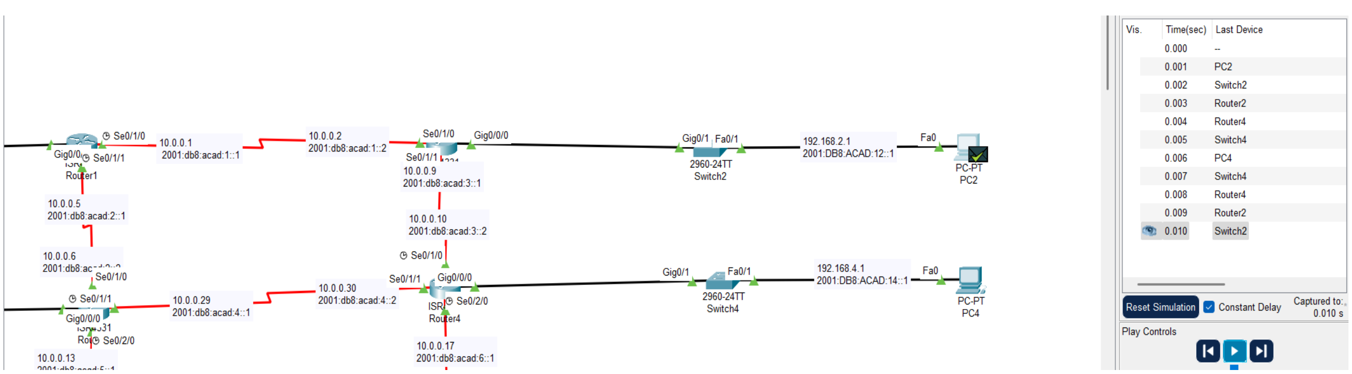


OSPFv3 neighbors are fully established, and multiple IPv6 routes are learned via OSPF, confirming proper OSPFv3 operation on the router.

7.5. Simulate link failures to test OSPFv3 Recovery







8. Results and Discussion

- The **dual-stack design** successfully maintained uninterrupted IPv4 and IPv6 connectivity throughout the migration process.
- **OSPFv3** demonstrated quick and stable reconvergence after link failures, ensuring minimal downtime in the IPv6 routing domain.
- Both **SLAAC** and **DHCPv6** configurations were validated and worked as expected, providing efficient IPv6 address assignment to hosts.
- The migration strategy allowed seamless integration of IPv6 routing alongside the existing IPv4 infrastructure without service disruption.
- Overall, the network showed strong resilience and flexibility, confirming the effectiveness of the chosen protocols and configurations.

9. Conclusion

The dual-stack network successfully demonstrated seamless IPv6 readiness while maintaining legacy IPv4 support. OSPFv3 provided reliable and efficient routing across all devices, and the combination of SLAAC and DHCPv6 ensured robust and automated IPv6 address assignment. This project establishes a strong foundation for a future migration towards IPv6-exclusive environments, highlighting the network's scalability and resilience.