Alqalam Journal of Medical and Applied Sciences. 2025;8(4):2974-2980
https://doi.org/10.54361/ajmas.2584129

Original article

IPv6 Addressing and Configuration: Building a Dual-Stack Network with OSPFv3

Hussam ALgzite[1], Nuredin Ahmed[2]

[1]*Department of Information Technology, Libya Academy for Graduate Studies, Tripoli, Libya*
[2]*Department of Computer Engineering, University of Tripoli, Tripoli, Libya*
Corresponding email. *workingonprogram5522@gmail.com*

Abstract
With the rapid growth of Internet-connected devices, IPv4 addressing has become insufficient to meet global demand. IPv6 was introduced to overcome this limitation by providing a significantly larger address space and improved routing efficiency. This project focuses on designing and implementing a dual-stack network that supports both IPv4 and IPv6. The network primarily operates using IPv6 while maintaining compatibility with IPv4 through a controlled and realistic transition model. The implementation includes IPv6 Global Unicast Addressing (GUA), Link-Local Address configuration, dynamic routing using OSPFv3, static routing for IPv4, and end-to-end connectivity testing using IPv6 ping and traceroute. The project successfully demonstrates the deployment of an IPv6-based network with seamless IPv4 integration, reflecting real-world enterprise transition scenarios.
Keywords. IPv4, IPv6, OSPFv3, Dual-Stack Network, Global Unicast Address.

Introduction

With the rapid growth of internet-connected devices, IPv4 addressing has become insufficient to meet global demand. IPv4 provides approximately 4.3 billion unique addresses, which have proven inadequate for the expanding number of devices requiring network connectivity. Several studies have highlighted the urgency of IPv6 deployment due to IPv4 exhaustion and the rapid growth of Internet of Things (IoT) devices, which significantly increase global address demand [5,6]. IPv6 was developed to address this limitation by providing a significantly larger address space using 128-bit addresses compared to IPv4's 32-bit addresses, offering an almost unlimited number of unique addresses. This study focuses on designing and implementing a dual-stack network that supports both IPv4 and IPv6 protocols simultaneously. The dual-stack approach allows networks to transition gradually from IPv4 to IPv6 without disrupting existing services, providing a practical migration strategy for organizations. The network topology consists of multiple interconnected locations to demonstrate real-world deployment scenarios. The primary objectives of this research are to configure IPv6 addresses on all network routers and establish communication between network segments. Additionally, this study implements OSPFv3, a routing protocol designed specifically for IPv6, to automatically share routing information between routers. The implementation also ensures that IPv4 devices continue to function in network segments that have not fully transitioned to IPv6, demonstrating backward compatibility and gradual migration capabilities.

Previous studies published between 2021 and 2024 have explored IPv6 implementation and migration strategies in network environments. Most research has focused on theoretical analysis or performance comparisons between IPv4 and IPv6, with emphasis on protocol efficiency and transition mechanisms. Several researchers have examined different transition mechanisms for moving from IPv4 to IPv6 networks [1]. These studies compared various approaches, including tunneling, translation, and dual-stack implementations. The findings indicate that dual-stack provides the most straightforward migration path while maintaining backward compatibility with existing IPv4 infrastructure. These studies also highlighted the importance of proper address planning and routing protocol configuration during the transition period. Research on OSPFv3 routing protocol implementation in IPv6 networks has demonstrated the differences between OSPFv2 (for IPv4) and OSPFv3 (for IPv6) [2]. Experimental studies have shown that OSPFv3 provides efficient dynamic routing for IPv6 networks, with better scalability compared to static routing approaches, particularly in larger network topologies. These findings support the use of OSPFv3 in enterprise networks transitioning to IPv6.

Comprehensive studies on IPv6 addressing schemes and configuration practices have analyzed different types of IPv6 addresses, including Global Unicast Addresses (GUA), Link-Local addresses, and Unique Local Addresses (ULA) [3]. These studies provided guidelines for proper address allocation and subnet planning in IPv6 networks, emphasizing the importance of using /64 prefix lengths for subnets, which is standard practice in IPv6 network design. Recent work on network information systems and IPv6 deployment strategies has examined real-world case studies of organizations implementing IPv6 [4]. This research documented various challenges encountered during IPv6 deployment, including routing configuration issues, address management complexity, and interoperability concerns. The authors provided recommendations for successful IPv6 migration, which informed the approach taken in this study. In contrast to previous theoretical studies, this research presents a practical implementation of a dual-stack network with detailed interface-level configuration and testing. The study demonstrates how different

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

network segments can coexist using both IPv4 and IPv6 protocols simultaneously, with OSPFv3 handling dynamic routing for IPv6 segments while maintaining static routing for IPv4 connectivity.

Methods

This research methodology employs a case study approach based on the simulation of IPv6 addressing and configuration using Cisco Packet Tracer, a network simulation tool widely used in academic and professional training settings. This simulation approach was chosen because it provides a controlled and reproducible environment suitable for educational purposes and allows for repeated testing without physical hardware limitations. It is important to clarify that this study is based on network simulation, not real-world experimentation. Cisco Packet Tracer is a network simulator that mimics the behavior of actual network devices and protocols.

Network Design Overview

The network consists of four main segments that work together to create a complete dual-stack environment. (Figure 1) shows the overall network topology.

Table 1. Description of Network Segments, Addressing Type, and Routing Protocols

Network Segment	Type	Routing Protocol	Description
HQ	Dual-Stack	OSPFv3	Central router connecting all segments, supports both IPv4 and IPv6
ISP	IPv6 Only	OSPFv3	Internet Service Provider router, IPv6 dynamic routing
Branch2	IPv6 Only	OSPFv3	Fully migrated IPv6 network segment
Branch1	Dual-Stack	Static (IPv6), DHCP (IPv4)	IPv4 LAN with IPv6 WAN connection

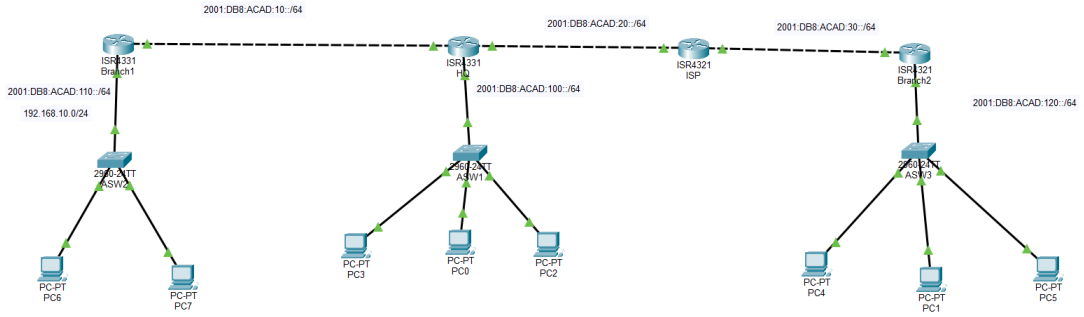

Figure 1. Network Topology: Dual-Stack Network with HQ, Branch1, Branch2, and ISP. The diagram shows four routers (Branch1, HQ, ISP, and Branch2) connected via WAN links, with each router connected to a switch serving local area networks

The network is organized as follows:

HQ (Headquarters)

The central router that interconnects all network segments. This dual-stack router handles both IPv4 and IPv6 traffic. OSPFv3 is enabled on this router to share routing information with other routers in the network automatically. The HQ router acts as the core routing point where different parts of the network converge.

ISP

This router represents an Internet Service Provider connection. It is configured as an IPv6-only router and uses OSPFv3 for dynamic routing. The ISP router connects the HQ to Branch2, creating a path for traffic to flow between these locations.

Branch2

An IPv6-only network segment. All devices in Branch2 use IPv6 addresses, and the router uses OSPFv3 to learn routes to other parts of the network dynamically. This branch demonstrates a fully migrated IPv6 environment.

Branch1

This branch implements a dual-stack configuration. The LAN side uses IPv4 with DHCP for automatic address assignment, while the WAN connection to HQ uses IPv6. This setup demonstrates a mixed

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

environment where some parts of the network still use IPv4 while the connections between locations use IPv6.

Simulation Setup

The simulation topology consists of four routers with the following specifications, as shown in (Table 1).

Implementation Details

IPv6 Global Configuration

Before implementing IPv6 functionality, IPv6 forwarding was enabled on all routers. This is similar to enabling IP routing for IPv4, but requires a separate command for IPv6. On each router, the following command was entered:

ipv6 unicast-routing

This command tells the router that it should forward IPv6 packets between its interfaces. Without this, the router would only handle IPv6 traffic for itself, not route it to other networks.

***HQ* Router Configuration**

The HQ router serves as the central node in the network, interconnecting all segments. It was configured as a dual-stack router, enabling it to handle both IPv4 and IPv6 traffic simultaneously.

Table 2. Router Specifications and Simulation Environment Configuration

Interface	Description	IPv6 GUA	Link-Local	OSPFv3
G0/0/0	WAN-to-Branch1	2001:DB8: ACAD:10::1/64	FE80::1	No
G0/0/1	WAN-to-ISP	2001:DB8: ACAD:20::1/64	FE80::1	Area 0
G0/0/2	HQ-LAN	2001:DB8: ACAD:100::1/64	FE80::1	Area 0

Interface G0/0/0 - WAN to Branch1

This interface provides connectivity between HQ and Branch1. It was configured with an IPv6 Global Unicast Address (GUA) of 2001:DB8:ACAD:10::1/64. A Link-Local address (FE80::1) was also assigned to this interface. Link-Local addresses are automatically used by IPv6 for communication on the same physical link, similar to how IPv4 uses addresses in the 169.254.0.0/16 range.

- *interface GigabitEthernet0/0/0*
- *description WAN-to-Branch1*
- *no ip address*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:10::1/64*
- *no shutdown*

Interface G0/0/1 - WAN to ISP

This interface connects HQ to the ISP router. It was configured with IPv6 addresses, and OSPFv3 was enabled on the interface. This configuration allows the router to exchange routing information with the ISP router automatically.

- *interface GigabitEthernet0/0/1*
- *description WAN-to-ISP*
- *no ip address*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:20::1/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

Interface G0/0/2 - HQ LAN:

This interface connects to the local network at headquarters. It was configured with IPv6 address 2001:DB8: ACAD:100::1/64, and OSPFv3 was enabled so that routes to this network are advertised to other routers.

- *interface GigabitEthernet0/0/2*
- *description HQ-LAN*
- *no ip address*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:100::1/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

https://doi.org/10.54361/ajmas.2584129

OSPFv3 Configuration

OSPFv3 was configured on the HQ router with router ID 1.1.1.1. Static route redistribution was enabled, which means any static routes configured will be shared with other routers using OSPFv3.

- *IPv6 router ospf 1*
- *router-id 1.1.1.1*
- *log-adjacency-changes*
- *redistribute static*

Static IPv6 Route

A static route was added to reach Branch1's LAN network. This route directs traffic to the 2001:DB8:ACAD:110::/64 network through Branch1's router.

- *ipv6 route 2001:DB8:ACAD:110::/64 2001:DB8:ACAD:10::2*

ISP Router Configuration

The ISP router configuration is simpler than HQ, as it only handles IPv6 traffic. Two interfaces were configured:

Interface G0/0/0 - WAN to Branch2:

This connects the ISP router to Branch2.

- *interface GigabitEthernet0/0/0*
- *description WAN-to-Branch2*
- *no ip address*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:30::1/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

Interface G0/0/1 - WAN to HQ

This connects the ISP router back to HQ.

- *interface GigabitEthernet0/0/1*
- *description WAN-to-HQ*
- *no ip address*
- *ipv6 address FE80::2 link-local*
- *ipv6 address 2001:DB8:ACAD:20::2/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

OSPFv3 Configuration

OSPFv3 was configured with router ID 5.5.5.5

- *IPv6 router ospf 1*
- *router-id 5.5.5.5*
- *log-adjacency-changes*

Branch2 Router Configuration

Branch2 is a fully IPv6 network; all configuration is focused on IPv6 implementation.

- *Interface G0/0/0 - WAN to ISP:*
- *This connects Branch2 to the ISP router.*
- *interface GigabitEthernet0/0/0*
- *description WAN-to-ISP*
- *no ip address*
- *ipv6 address FE80::2 link-local*
- *ipv6 address 2001:DB8:ACAD:30::2/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

Interface G0/0/1 - Branch2 LAN

This connects to the local network at Branch2.

- *interface GigabitEthernet0/0/1*
- *description Branch2-LAN*
- *no ip address*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:120::1/64*
- *IPv6 OSPF 1 area 0*
- *no shutdown*

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

OSPFv3 Configuration
OSPFv3 was configured with router ID 2.2.2.2.
- *IPv6 router ospf 1*
- *router-id 2.2.2.2*
- *log-adjacency-changes*

Branch1 Router Configuration
Branch1 implements a dual-stack configuration, utilizing both IPv4 and IPv6. The LAN side uses IPv4 with DHCP, while the WAN connection uses IPv6.

DHCP Configuration (IPv4)
A DHCP pool was configured for the Branch1 LAN to enable automatic IPv4 address assignment for connected devices.
- *ip dhcp pool Branch1*
- *network 192.168.10.0 255.255.255.0*
- *default-router 192.168.10.1*
- *dns-server 8.8.8.8*

Interface G0/0/1 - Branch1 LAN (Dual Stack)
This interface was configured with both IPv4 and IPv6 addresses, making it a true dual-stack interface.
- *interface GigabitEthernet0/0/1*
- *description Branch1-LAN*
- *ip address 192.168.10.1 255.255.255.0*
- *ipv6 address FE80::1 link-local*
- *ipv6 address 2001:DB8:ACAD:110::1/64*
- *no shutdown*

Interface G0/0/0 - WAN to HQ (IPv6)
This interface only uses IPv6 to connect to HQ.
- *interface GigabitEthernet0/0/0*
- *description WAN-to-HQ*
- *no ip address*
- *ipv6 address FE80::2 link-local*
- *ipv6 address 2001:DB8:ACAD:10::2/64*
- *no shutdown*

Static IPv6 Routing
Static routes were added to enable Branch1 to reach other parts of the network. One route directs traffic to HQ's LAN, and another is a default route that sends all other IPv6 traffic to HQ.
- *ipv6 route 2001:DB8:ACAD:100::/64 2001:DB8:ACAD:10::1*
- *ipv6 route ::/0 2001:DB8:ACAD:10::1*

Results
This section presents the results obtained after network implementation and activation within the simulation environment. The testing phase included three basic components: connectivity verification, routing table verification, and protocol behavior analysis.

IPv6 Connectivity Tests
We started by testing IPv6 connectivity between different network segments. From a device in one location, we tried to ping devices in other locations using their IPv6 addresses.

Table 3. Connectivity and Routing Verification Results

Test Type	Source	Destination	Result
IPv6 Ping	HQ LAN	Branch2 LAN (2001:DB8:ACAD:120::10)	Success - No packet loss
IPv6 Traceroute	Branch1	Branch2	Success - Path: Branch1 → HQ → ISP → Branch2
IPv4 Ping	Branch1 LAN	192.168.10.10	Success - No packet loss
OSPFv3 Adjacency	All Routers	Neighbors	Success - All adjacencies formed

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

IPv6 Ping Test

We tested connectivity to a device in Branch2 (2001:DB8:ACAD:120::10) from different locations in the network. The ping command for IPv6 is slightly different from IPv4:

- *ping ipv6 2001:DB8:ACAD:120::10*

All ping tests were successful, showing that IPv6 routing was working correctly across all network segments.

IPv6 Traceroute

We also used traceroute to see the path that packets take through the network. This helped us verify that routing was working as expected and that packets were following the correct path through the routers.

- *tracert ipv6 2001:DB8:ACAD:120::10*

The traceroute showed that packets traveled through the correct routers (HQ, ISP, and Branch2) to reach their destination.

IPv4 Connectivity Tests

We also tested IPv4 connectivity in Branch1 to make sure the dual-stack configuration was working properly. We pinged devices in the Branch1 LAN using their IPv4 addresses:

- *ping 192.168.10.10*

All IPv4 tests were successful, confirming that both IPv4 and IPv6 could work simultaneously on the same network segment.

OSPFv3 Verification

We verified that OSPFv3 was working correctly by checking the OSPFv3 neighbor relationships and routing tables on each router. We used commands like:

- *show ipv6 ospf neighbor*
- *show ipv6 route*

These commands showed that routers were forming OSPFv3 adjacencies with their neighbors and learning routes dynamically. We could see routes to all the IPv6 networks in the routing tables, which confirmed that OSPFv3 was sharing routing information correctly.

All tests were successful with no packet loss, confirming that our network configuration was working as intended.

Discussion

IPv6 addressing and configuration represent essential components of modern network infrastructure, addressing the limitations of IPv4 address space exhaustion. The dual-stack approach implemented in this study demonstrates a practical migration strategy that allows organizations to transition gradually from IPv4 to IPv6 without disrupting existing services. The dual-stack mechanism has been widely adopted as one of the most practical IPv6 transition strategies, enabling IPv4 and IPv6 to coexist during migration phases while maintaining service continuity [7,8].

In the implemented network, each protocol operates independently. IPv4 traffic is routed using IPv4 routing tables, and IPv6 traffic is routed using IPv6 routing tables. The router maintains separate routing tables for each protocol, ensuring they do not interfere with each other. No protocol translation mechanisms, such as NAT64 or tunneling, were used in this implementation. Instead, each protocol operates independently. This approach is more straightforward and demonstrates a realistic transition strategy from IPv4 to IPv6. Organizations can gradually migrate different parts of their network to IPv6 while maintaining IPv4 functionality in areas that have not been migrated yet. The use of OSPFv3 for dynamic routing proved effective in automatically sharing routing information between routers. When network topology changes occurred, OSPFv3 automatically updated routing tables on all routers, demonstrating superior efficiency compared to manual static route configuration. This finding is consistent with existing literature that highlights the advantages of dynamic routing protocols in network management [2].

In Branch1, the LAN uses IPv4 because the devices may not support IPv6 yet, or the organization may not have migrated that part of the network. However, the connection to HQ uses IPv6, demonstrating how organizations can begin using IPv6 for new connections while maintaining existing IPv4 networks. The results demonstrate that IPv6 routing works efficiently across all network segments, OSPFv3 successfully shares routing information between routers, and IPv4 and IPv6 can coexist on the same network without conflicts. The network topology created represents a realistic enterprise scenario where different branches may be at different stages of IPv6 migration. Compared to tunneling and translation-based transition mechanisms, the dual-stack approach used in this study avoids protocol encapsulation overhead and translation complexity. While tunneling mechanisms such as 6to4 and ISATAP introduce additional processing delays, the dual-stack model enables native protocol operation for both IPv4 and IPv6, resulting in simpler network management and improved performance, as reported in previous studies [9,10]. Although this study was conducted using a simulation environment, the results closely reflect real-world enterprise network behavior. Simulation-based research provides a cost-effective and repeatable method for evaluating network configurations before real deployment. However, future research could validate these findings

Received*: 29-05-2025 -* ***Accepted****: 23-07-2025 -* ***Published****: 30-07-2025*

through physical testbeds or production environments. Additionally, security considerations such as IPv6 firewall configuration, RA Guard, and OSPFv3 authentication were not addressed in this implementation. These aspects represent important areas for future work, particularly for organizations planning large-scale IPv6 deployments.

Conclusion

The findings of this study demonstrate that IPv6 addressing and configuration can be successfully implemented in a dual-stack network environment. The network supports both IPv4 and IPv6 protocols simultaneously, enabling organizations to transition gradually from IPv4 to IPv6 without disrupting existing services. This study demonstrates that different parts of a network can use different protocols while maintaining connectivity. Branch1 uses IPv4 on the local network, Branch2 is fully IPv6, and HQ connects everything using the appropriate protocol as needed. OSPFv3 proved effective for IPv6 routing, automatically sharing routes between routers. The dual-stack implementation ensures that legacy IPv4 systems continue to function while IPv6 is being deployed. This approach reflects how most organizations will implement IPv6 migration in real-world scenarios. For organizations planning to migrate to IPv6, this study demonstrates that a gradual transition is practical and effective. Organizations do not need to change everything at once. They can begin using IPv6 for new connections and gradually migrate existing networks as devices and applications are updated to support IPv6. Future work could explore more advanced topics such as IPv6 security features, quality of service (QoS) configuration for IPv6, or integration with other routing protocols. However, for demonstrating IPv6 addressing and routing fundamentals, this study provides a solid foundation and practical model that can be adopted in network management and security designs.

Conflict of interest. Nil

References

1. IEEE. IPv6 migration strategies. In: IEEE Conference Proceedings. 2023.
2. IPv6 migration OSPFv3 routing based on IPv6 and IP. J Article. 2022.
3. International Journal of Engineering and Computing. IJEC. 2024;3(1).
4. Information Journal. Information systems and IPv6 deployment. 2021;12.
5. Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. IETF RFC 8200. 2017.
6. Cisco Systems. IPv6 deployment guide and migration strategies. Cisco White Paper. 2022.
7. Colitti L, Gunderson S, Kline E, Refice T. Evaluating IPv6 adoption and dual-stack deployment in enterprise networks. IEEE Commun Mag. 2021.
8. Huitema C. IPv6: The new internet protocol. 2nd ed. Prentice Hall; 2021.
9. Li X, Bao C. Performance comparison of IPv6 transition mechanisms in enterprise networks. IEEE Access. 2022.
10. Internet Society (ISOC). Best practices for IPv6 transition and deployment. ISOC Report. 2023.

Received: *29-05-2025* - ***Accepted***: *23-07-2025* - ***Published***: *30-07-2025*