Lab Implementation of IPv6 in Enterprise Network Using Cisco Packet Tracer

Mohammad Ali Sadat[a], Priyanka Meel[b]

[a,b] Department of Information Technology, Delhi Technological University, India

[a] mali.sadat789@gmail.com, [b] priyankameel86@gmail.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: As technology is growing fast, using technologies is also increasing because the previous technologies cannot support the new requirements. In this case, every company is trying to implement newly released technologies. As IPv4 was introduced, it has been used for a long time in networking. But now, the limitations of IPv4 are too much, such as address limitation, subnet-ting with complex structure, inefficient NAT employment. This is why IPv4 is not considered to be used anymore. Because of IPv4 problems, the IPv6 protocol is designed and developed to overcome IPv4 limitations. The efficiency of IPv6 is more in packet processing, and routing pro-vides a simple network configuration and improves the QoS by decreasing latency in the time of the data packet transformation. As IPv6 has many features and new supported services.

With the emergence of IPv6, any enterprise companies are interested in implementing IPv6 in the enterprise network. An enterprise network includes protocols, virtual and physical networks that connect all systems and users on a LAN, and all applications in the cloud and data center. The main purpose of this research is to implement ipv6in the enterprise network. We used the latest version of the Cisco packet Tracer for simulation purposes. Cisco packet Trace can simulate necessary routing using EIGRPv6, OSPVv3, and RIPng and application layer protocols.

Keywords: Enterprise Network, Frame Relay IPv6, LAN, VLAN, Routing Protocol, Cisco Packet Tracer

1. Introduction

IPv4 is the network layer protocol used to identify network devices' physical locations in a network or on theInternet. As technology is growing, the need and requirements are also increasing. The previous technologies are not sufficient for the new requirements, and every organization is trying to be updated with the latest technologies. However, in networking, IPv4 is a protocol almost used for 30 years for communication purposes. IPv4 faces many challenges and limitations like routing scalability, address shortage and exhaustion, complex structure for subnetting, address translation is inefficient and slows down the network between other networks. As the internet scale is growing too fast (use of mobile devices) and the space address of IPv4 had already been run out and cannot support new devices to connect to the Internet, for the reason IPv6 [1]has been introduced. The latest Internet Protocol is IPv6, which uses a simplified and new IP header, IP options support, further address architecture expansion, flow labeling, auto-configuration, neighbor discovery, and integrated security mechanisms. These features of IPv6 keep the growth of the Internet-scale when the issue of new devices gets increased [2,3]. The efficiency of IPv6 is more in packet processing, and routing provides a simple network configuration and improves the QoS by decreasing latency in the time of the data packet transformation. As IPv6 has many features and new supported services, any enterprise companies are interested in implementing IPv6 in their enterprise network.

By coming IPv6 as a new protocol, any organization must move to the IPv6 platform. However, this process is not easy or straightforward to do automatically. Still, the requirements demand that any company should do the movement from IPv4 to IPv6 to deal with the complexities and challenges of the IPv4 network. There are different solutions for this transition like IPv6 tunneling [4],that IPv6 domain is allowed to communicate with each other via IPv4 network or vice versa, and IPv4 to IPv6 dual-stack mechanism [5], that can be used when there is not a perfect implementation of ipv6 in both WAN and LAN.Fig 1 shows the Google IPv6[6] users that access Google over IPv6. We can see the graph that shows the ascending state of IPv6 users accessing Google. From the performed statistic on IPv6 users. See Fig 1.

Figure 1: IPv6 adaptation on the Internet, Image source [6]

We can analyze that the use and adoption of IPv6 are increasing day by day.So,this research aims to implement IPv6 in the enterprise network becausethe usage of IPv6 is growing up, as Fig1 shows, and IPv6 may be implemented in Internet backbones[7]. All IPv4 users will move to IPv6 completely. In this research, we supposed that ISP has already implemented IPv6;we aim to completely implement IPv6 to an enterprise network from LAN complete configuration up to WAN configuration with dynamic routing protocol and technologies thatIPv6 can support.

LAN configuration includes VLAN creation, wireless access point configuration, IP telephony set up, DHCPV6 implementation, VTP server configuration, STP configuration. WAN configuration includes EIGRPv6 dynamic routing protocol, Frame relay multipoint configuration to connect several LANs via WAN, web server, and mail server set up.

The Contribution of this paper is as follows:

1. We considered a new company that wants to implement IPv6 without having IPv4 network infrastructure before.
2. We developed and designed an IPv6 network infrastructure to support the enterprise plan. (IPv6 supported topologies).
3. We identified external connectivity with ISP using static IPv6 route; we supposed that ISP has already implemented IPv6.
4. We connected multiple sites by leased lines technology.
5. We performed a complete simulation of IPv6 implementation in an enterprise network;it can be used as a prototype for further implementation of IPv6 in a real scenario.
6. We used technologies and other supported protocols by IPv6 duringits implementation.
7. The proposed research is advantageous and outperforms the existing state-of-the-art methods of IPv4.

The rest of the paper is structured as follows: Section 2 overview of the related work on enterprise networks. Section 3 methodology and design of the project to be simulated in Cisco packet Tracer, Section 4Implementation includes configuration commands, Section 5 result and discussion contains the project's output.Section6 is the conclusion.

2. Related Work

Many studies and researches have been done on the enterprise network; ina studyby Nahid, M. H[8], Cisco Packet Tracer is usedto simulate the network. Datacenter model was designed in this research, and the model contains pcs, TFTP server, HTTP server, NTP server. Switch 2980-24TT is used to build up the entire network system. The 2811 model router is used to connect the data center, branches & internet cloud.

In a study by Enoch, Orike, &Ahiakwo[9],a solution has been developed that enables Network/Communication Engineers to deploy the design of a scalable, secured, manageable, andavailable campus network. They configured Adaptive Security Appliance (ASA), Core Router, and Distribution Switches to provide network coverage to the entire Faculty Infrastructure. They used the integrated service of routers/access points to create a point of presence (POP) for network coverage between the buildings, enablinga wireless connection between the PCs, Laptops, and other devices withWi-Fi technologies; their campus network was working based on IPv4.

Michael,in his study [10],on-campus network security, identified the threats and security issues in a campus network and the types ofnetwork attacks. They suggested creating a Virtual LAN (VLAN), implementing the firewall for external and internal security, and Virtual Private Networks (VPN)as solutions for the secured campusnetworks.

In the studyby Andry, J. F[11], Cisco Packet Tracer is used as a simulator to implement the LAN switching method to break down the broadcast domain into segments by using the VLAN concept.

Tarkaa, N. S., Iannah, P. I., &Iber,[12]used Cisco Packet Tracer to simulate the LAN model for the engineering college, University of Agriculture, Makurdi, Nigeria. They described that how a simulator software offers a way to prototype a local Area Network without using hardware devices in our proposed work.

Xiaonan, W., & Shan, in their research [13],designedandimplemented IPv6 address auto configuration in a Wireless Sensor Network (WSN). They created a structure of IPv6 addresses for nodes of the sensor. The address recovery algorithm is also proposed by the research[13].

Wang, X., Le, D., & Cheng, H in their study[14], proposed the configuration of IPv6 addresses for vehicular networks on location-based information. Theirproposed addressing scheme does the combination of stateful and stateless address configuration mechanismand also does the performance evaluation of the scheme.

In research by Eric and Neudith[15], IPv6 is implemented at the Central University of Venezuela; they identified two big problems:the fast growth of users, but still, there was low throughput. The second isNAT's inefficiencybecause NAT (Network Address Translation) is not working in many Internet Services and shortage ofpublic IPv4. Their proposed solution for IPv4 address shortage is IPv6 deployment in the university network.

3. Methodology

Many different modelsare used to design a physical network topology, but the hierarchical and Cisco enterprise architecture models are the most considered model to create enterprise networks. A hierarchical network design model can break down network design's complex problems into more minor and manageable issues. The hierarchical model is flexible; it allows the network to be scaled up when it grows up. This model can help the network in the case to control the traffic, and the traffic should not be infiltrated to other parts of the network and have to stay local. The bandwidth can be optimized by localizing the traffics to be managed effectively in the network. [16].

This research aims to enable ipv6 to the enterprise network and then focus ontraffic management in every branch called VLAN-based traffic management, which breaks down a large-sized network into manageable and smaller segments to decrease the broadcast trafficin each department. Traffic management is one of the factors that positively affect network performance and speeds. However, the practical part is more focused rather than the physical design because the functionality, availability, and flexibility of a computer network depend on the practical part ofthe project, so this research helps that how a network engineer ups the steps to implement an enterprise network with the help of IPv6.

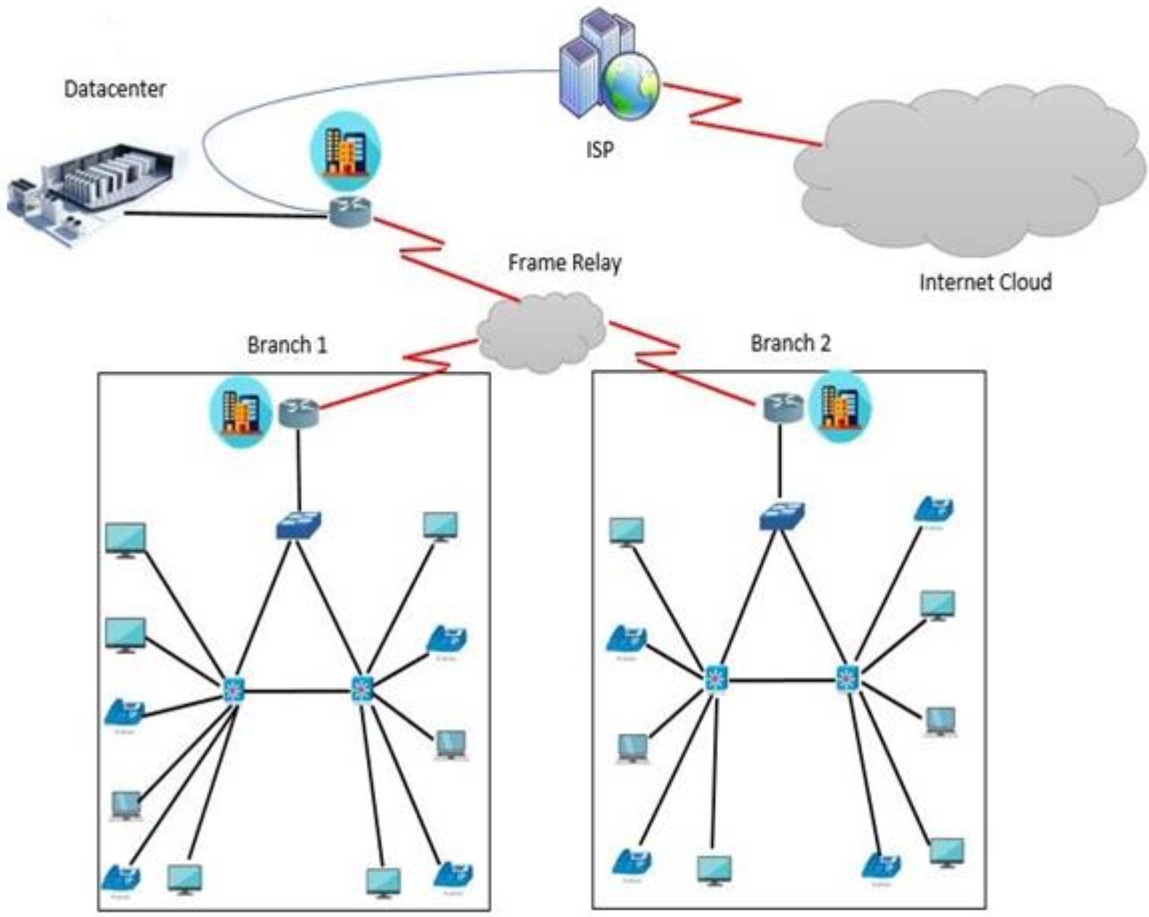

Figure 2 Conceptual Design of proposed Enterprise Network

Since the network's physical and conceptual design depends on the physical building structure, we showed the network's conceptual and physical designin Fig 2 and 3, respectively.

Elaborate on IPv6 network design:

The methodology principles of this research aim at enabling IPv6 all over in different companies, offices, hosts, applications, and services that can be run inside a corporate network. We focus on iteratively planning, implementing, and launching the different parts of the network. Further, IPv6 is implemented with reliability, as ipv4 has reliable and capable connectivity. While IPv6 gets implemented, it should support new protocol connectivity and provide a capable and dependable connection for any organization's companies. The next task is to auto-assignthe ipv6 address to the host and end-users. Finally, the implementation completes with securitymechanisms, using pap and chap authentication. Cisco Packet Tracer softwareis used to designand simulate the network.The simulation aims to include up-to-date configuration, Telnet abilities, administrative control, and prevent failure in internetworks communications and Internet Service Provider (ISP).The proposed network diagram in Fig (3) was designed and simulated, which comprised core layer switches (3560) in each branch, access layer switches (2960), routers (2811), frame relay device, and IP telephony for call communications among the branches.

The Access layer switches can provide endpoint access to local segments in the network. IPv6-based configuration with appropriate dynamic routing protocol (EIGRP for IPv6), which has better security and performance than OSPFv3 [17], DHCPv6, and other necessary configurations are implemented.

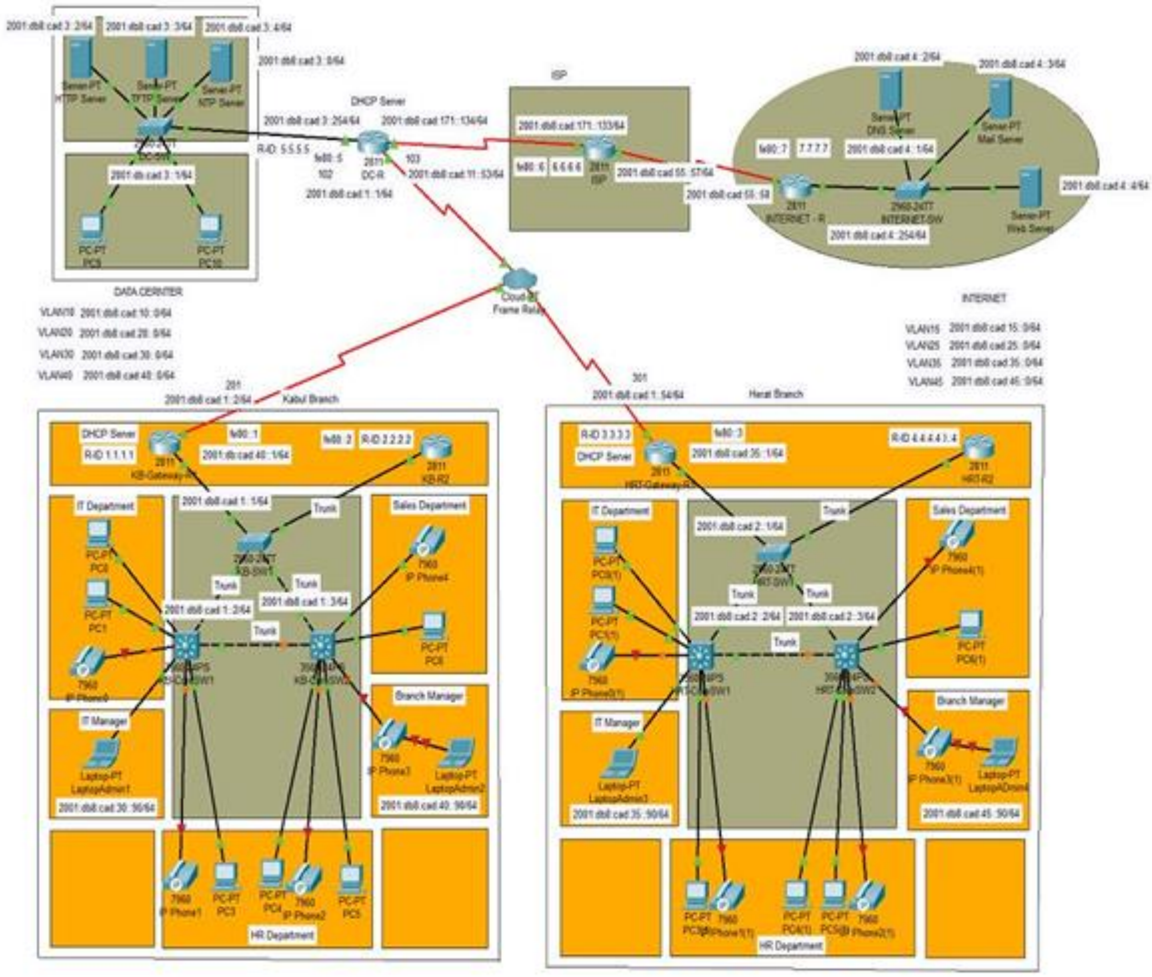

Figure 3: Proposed Enterprise Network Physical Design

4. Implementation

Planning and deployment phases:

Firstly, a comprehensive IPv6 addressing plan is created for branches, offices, and data centers. In this case, the guideline in [18] is followed for the Ipv6 addressing scheme.

DHCPv6 [19] is used in Datacenter's router and each branches' router to assign IPv6 addresses dynamically for end hosts and users.

Dhcpv6 is configured in each branch's routerto help a host to obtain IPv6 address automatically from the range of VLANs' IP. The auto-assigned address is the composition of routeradvertised information and MAC address which is locally available. Manual address assignment is not required furthermore when DHCPv6 is implemented. IP addresses manual configuration has never been suggested as an option.

DHCPv6 provides three types of dynamic address assignment, stateful[20], stateless [21], and SLAAC (Stateless Address Auto configuration) [22].

Default addressing mode is not used by DHCPv6 for OSs, while DHCP can do it in IPv4. The protocol is offering management and configuration options thatare useful in large and intricate networks.

Next, frame relay technology has been implemented to establish the connection between branches;a virtual path can be set in a frame relay network that frames can take the ability to be transferred from one switching node to another over a virtual circuit. DLCI has a predetermined value used to indicate the control message's purpose for identifying a virtual path aggregating.Data Link Connection Identifier (DLCI) can be transferred from one switch node to another switch node by a control message. Control message acts as a transferor in a frame relay network[23].

To build up the IPv6 network on the top existing, we tried to keep IPv6 and IPv4 network design closer in terms of traffic flows and routing because the traffic flows almost are same in both IPv4 and IPv6 computer network.

To keep the IPv6 network design simple, we ensure manageability and scalability; and also it will be much easier for the network operations team to support it. The following routing protocol and policies are considered: There are several dynamic routing protocols (DRP) that IPv6 supports, like EIGRPv6 [24], OSPFv3 [25], RIPng[26], Multiprotocol BGP [27], etc.

But the preferable routing protocol in this project is EIGRPv6 which has a better security mechanism and performance [17].

Cisco designed and developed the Enhanced Interior Gateway Routing Protocol (EIGRP),a dynamic routing-protocol;it works based on Diffusing Update Algorithm [28]. EIGRP can be used in IPv4 as well as in the IPv6 environment. The IPv4 EIGRP's features are integrated with IPv6,which includes the following [24]:

- DUAL is used for computing EIGRP Successors and Feasible Successors.
- Bandwidth and delay are used as default metrics.
- No need for updates periodically.
- The same mechanism is implemented for authentication (MD5) as EIGRP in IPv4.

Besides the similarities between EIGRPv6 and EIGRP, some changes help the protocol to routes within the IPv6 environment.Instead of IP subnet, Link-Local Addresses are used for neighbor adjacencies.

- EIGRP routers use the FF02::10 ipv6 multicast address instead of the previous multicast address(224.0.0.10).
- EIGRPv6 configuration can alsobe done in each interface of a router,preferably enabling globally.
- The creation of router ID is mandatory for routing operations to be started successfully.

EIGRPv6 does not require to use IPsec security mechanism for routing updates encryption; instead, MD5 (Message-Digest Algorithm 5) authentication method is used for security purposes and was also used previously by EIGRP in IPv4.

Creating VLANs:

Virtual Local Area Network [29] or VLAN is recently developed to manage theLAN network traffic. It can be used to limit network traffic or prevent a network from overload. VLAN can design the internal network of enterprise network or campus network or any other organizations' network. It is a Data Link Layer technology used to build many logical networks from a physical network. The networks created by VLAN can be divided into various logical segments named broadcast domains. VLAN is used to breakdown a complicated network into smaller parts or smaller networks for easy maintains, better manageability, improved security,flexibility, and improved performance.

Table 1: Creating VLAN

```
KB-CoreSW1(config)#vlan 10
KB-CoreSW1(config-vlan)#name VOICE_A
KB-CoreSW1(config-vlan)#exit
KB-CoreSW1(config)#vlan 20
KB-CoreSW1(config-vlan)#name IT_A
KB-CoreSW1(config-vlan)#exit
KB-CoreSW1(config)#vlan 30
KB-CoreSW1(config-vlan)#name HR_A
KB-CoreSW1(config-vlan)#exit
KB-CoreSW1(config)#vlan 40
KB-CoreSW1(config-vlan)#name Sales_A
KB-CoreSW1(config-vlan)#exit
KB-CoreSW1(config)#do wr
KB-CoreSW1(config)#int range fa0/3, fa0/5
```

Table 2: Assigning port to VLANs

```
KB-CoreSW1(config-if-range)#switchport voice vlan 10
KB-CoreSW1(config-if-range)#do wr
KB-CoreSW1(config-if-range)#exit
KB-CoreSW1(config)#int range fa0/2-4, fa0/7
KB-CoreSW1(config-if-range)#switchport mode access
KB-CoreSW1(config-if-range)#switchport access vlan 20
KB-CoreSW1(config-if-range)#exit
KB-CoreSW1(config)#int range fa0/5-6
KB-CoreSW1(config-if-range)#switchport mode access
KB-CoreSW1(config-if-range)#switchport access vlan 30
KB-CoreSW1(config-if-range)#exit
KB-CoreSW1(config)#exit
```

Implementing IPv6:

Ipv6 protocol is developed by Internet Engineering Task Force (IETF) [30]for solving IPv4 limitations and security issues. The addressing scheme of ipv6 is 16 bytes or 128 bits, which can be represented by hexadecimal numbers or eight blocks of 16 bits, and colons separate each block. IPv6 format is x: x: x: x: x: x: x: x, that each x can be 16 bits of hexadecimal number, each field with zero is represented as following format: 2001:0000:0000:0000:0000:0000: 0db8:0001. This format can also be written as a short form by removing all zeros, for example, 2001:: db8:1. The new features such as hierarchical addressing, routing infrastructure, large address space, stateful[20] address auto configuration and, stateless [22] address IPv6 supports auto configuration, IPv6 security provides encryption and authentication.

The goal of auto configuration is to configure addresses in end-devices or hosts automatically merely. IPv6 supports auto-configuration; stateless (auto address configuration can be done without DHCPv6 server) and stateful (auto-configuration is done by DHCPv6 server). The DCPv6 server routers send RAs (Router Advertisements) to help the nodes to do the auto-configuration process. An RA message is an ICMP message sent periodically by the router or per request of a node.

The IPv6 serviceis disabled by default; for enabling this servicecisco routers, the command **ipv6 unicast-routing** is used. Assigning ipv6 address on a port of a router: Router (config-if)#<ipv6 address x:x:x:x::/prefix>.

Implementing DHCPv6:

IPv6Dynamic Host Configuration Protocol [31]is used to enable the DHCP server to transit configuration parameters like the network addresses of ipv6 to the end-users of IPv6. Reusable network addresses allocation and any other additional configuration also can be done dynamically by DHCPv6.

In this project, Branches' routers are configured as DHCPv6 servers to assign ipv6 addresses automatically following different VLANs IP addresses for various departments.

```
KB-Gatewat-R1(config)#ipv6 dhcp pool VLAN10
KB-Gatewat-R1(config-dhcpv6)#prefix-delegation pool VLAN10
KB-Gatewat-R1(config-dhcpv6)#dns-server 2001:db8:cad:4::2
KB-Gatewat-R1(config-dhcpv6)#exit
KB-Gatewat-R1(config)#ipv6 general-prefix VLAN10 2001:db8:cad:10::/64
KB-Gatewat-R1(config)#ipv6 local pool VLAN10 2001:db8:cad:10::/64 64
KB-Gatewat-R1(config)#int fa0/1.10
KB-Gatewat-R1(config-subif)#ipv6 dhcp server VLAN10
KB-Gatewat-R1(config-subif)#exit
KB-Gatewat-R1(config)#ipv6 dhcp pool VLAN20
KB-Gatewat-R1(config-dhcpv6)#prefix-delegation pool VLAN20
KB-Gatewat-R1(config-dhcpv6)#dns-server 2001:db8:cad:4::2
KB-Gatewat-R1(config-dhcpv6)#exit
KB-Gatewat-R1(config)#ipv6 general-prefix VLAN20 2001:db8:cad:20::/64
KB-Gatewat-R1(config)#ipv6 local pool VLAN20 2001:db8:cad:20::/64 64
KB-Gatewat-R1(config)#int fa0/1.20
KB-Gatewat-R1(config-subif)#ipv6 dhcp server VLAN20
KB-Gatewat-R1(config-subif)#exit
KB-Gatewat-R1(config)#ipv6 dhcp pool VLAN30
KB-Gatewat-R1(config-dhcpv6)#prefix-delegation pool VLAN30
KB-Gatewat-R1(config-dhcpv6)#dns-server 2001:db8:cad:4::2
KB-Gatewat-R1(config-dhcpv6)#exit
KB-Gatewat-R1(config)#ipv6 general-prefix VLAN30 2001:db8:cad:30::/64
KB-Gatewat-R1(config)#ipv6 local pool VLAN30 2001:db8:cad:30::/64 64
KB-Gatewat-R1(config)#int fa0/1.30
KB-Gatewat-R1(config-subif)#ipv6 dhcp server VLAN30
KB-Gatewat-R1(config-subif)#exit
KB-Gatewat-R1(config)#ipv6 dhcp pool VLAN40
KB-Gatewat-R1(config-dhcpv6)#prefix-delegation pool VLAN40
KB-Gatewat-R1(config-dhcpv6)#dns-server 2001:db8:cad:4::2
KB-Gatewat-R1(config-dhcpv6)#exit
KB-Gatewat-R1(config)#ipv6 general-prefix VLAN40 2001:db8:cad:40::/64
KB-Gatewat-R1(config)#ipv6 local pool VLAN40 2001:db8:cad:40::/64 64
KB-Gatewat-R1(config)#int fa0/1.40
KB-Gatewat-R1(config-subif)#ipv6 dhcp server VLAN40
KB-Gatewat-R1(config-subif)#exit
```

Table 3: DHCPv6 configuration for each VLANs

Datacenter's routerisalso configured as a DHCPv6 server to assign ipv6 address dynamically to end-users in the data center.

Implementing Frame Relay:

Frame relay[32]is packet-switched technology; it is a WANprotocol with high speed;this technology is designed to establish an interconnection between LAN and WAN via a shared network geographically dispersed. In the OSI model frame, relay operations and functions can be done at the data link layer to transfer routed protocols. Therouted protocols' data packets can be encapsulated within the frame relay packets known as frames.Before IP packets are sent to the frame relay network,the IP packets will be encapsulated in frames [32].

Table 4: Frame Relay Configuration

Herat Branch Router: HRT-Gateway-R1(config)#int s1/0 HRT-Gateway-R1(config-if)#encapsulation frame-relay HRT-Gateway-R1(config-if)#frame-relay lmi-type cisco HRT-Gateway-R1(config-if)#frame-relay map ipv6 2001:db8:cad:1::1 301 HRT-Gateway-R1(config-if)#frame-relay map ipv6 2001:db8:cad:1::2 302 Data Center Router: DC-R(config)#int s1/0 DC-R(config-if)#encapsulation frame-relay DC-R(config-if)#frame-relay lmi-type cisco DC-R(config-if)#frame-relay map ipv6 2001:db8:cad:1::54 103 DC-R(config-if)#frame-relay map ipv6 2001:db8:cad:1::2 102	DC-R(config-if)#frame-relay map ipv6 fe80::3 103 broadcast DC-R(config-if)#frame-relay map ipv6 fe80::2 102 broadcast Kabul Branch Router: KB-Gateway-R1 (config)#int s1/0 KB-Gateway-R1 (config-if)#encapsulation frame-relay KB-Gateway-R1 (config-if)#frame-relay lmi-type cisco KB-Gateway-R1 (config-if)#frame-relay map ipv6 2001:db8:cad:1::1 201 KB-Gateway-R1 (config-if)#frame-relay map ipv6 2001:db8:cad:1::54 203 KB-Gateway-R1 (config-if)#frame-relay map ipv6 fe80::1 201 broadcast KB-Gateway-R1 (config-if)#frame-relay map ipv6 fe80::3 203 broadcast

Table 4 includes the frame relay configuration code;**encapsulation frame-relay** command is used to enable frame-relayin each serial interface of the routers; these routers are connected to the frame-rely device to establish the connection between enterprise branches. The **frame-relay lmi-type** command lets a frame relay interface detect LMI (Local Management Interface) type, which is connected directly to the frame relay switch; here, the lmi type is Cisco. The third command **frame-relay map ipv6** is used to map DLCI value to the IPv6 address implemented on the S1/0 serial interface of the router.

Implementing EIGRPv6:

EIGRPis a dynamic routing protocol; asmentioned earlier, it works based on Diffusing Update Algorithm [28]. It can learn about the other routing routes using rumors from the neighboring routers [17]called distance vectorprotocol. EIGRP is a proprietary protocol that Cisco introduced. It is a hybrid of link state advertisement and distance vector protocols. EIGRP uses the concept of autonomous systems to group routers that are performing the same tasks. EIGRP keeps the topology of the network partially; three tables are used to make decisions for routing. The Neighbor Table, Routing table, and Topology table. Delay and bandwidth[17]are the metrics used by EIGRP to determine the best route in the network.

Table 5: EIGRPv6 configuration

```
EIRGPv6 configuration on Kabul Router:

KB-Gatewat-R1>enable
KB-Gatewat-R1#conf t
KB-Gatewat-R1(config)#ipv6 unicast-routing
KB-Gatewat-R1(config)#ipv6 router eigrp 1
KB-Gatewat-R1(config-rtr)#eigrp router-id 1.1.1.1
KB-Gatewat-R1(config-rtr)#no shutdown
KB-Gatewat-R1(config-rtr)#exit
KB-Gatewat-R1 (config)#int S0/0/0
KB-Gatewat-R1 (config-if)#ipv6 eigrp 1
KB-Gatewat-R1 (config-if)#ipv6 enable
KB-Gatewat-R1 (config-if)#exit
KB-Gatewat-R1(config)#int fa0/1
KB-Gatewat-R1 (config-if)#ipv6 eigrp 1
KB-Gatewat-R1 (config-if)#ipv6 enable

EIRGPv6 configuration on Herat Router:

HRT-Gateway-R1>enable
HRT-Gateway-R1#conf t
HRT-Gateway-R1 (config)#ipv6 unicast-routing
HRT-Gateway-R1 (config)#ipv6 router eigrp 1
HRT-Gateway-R1 (config-rtr)#eigrp router-id 2.2.2.2
HRT-Gateway-R1 (config-rtr)#no shutdown
HRT-Gateway-R1 (config-rtr)#exit
        HRT-Gateway-R1 (config)#int S0/0/0
HRT-Gateway-R1 (config-if)#ipv6 eigrp 1
HRT-Gateway-R1 (config-if)#ipv6 enable
HRT-Gateway-R1 (config-if)#exit
HRT-Gateway-R1#(config)#int fa0/1
HRT-Gateway-R1 (config-if)#ipv6 eigrp 1
HRT-Gateway-R1 (config-if)#ipv6 enable

EIGRPv6 configuration on DataCenter Router:

DC-R#conf t
DC-R(config)#ipv6 unicast-routing
DC-R(config)#ipv6 route ::/0 2001:db8:cad:171::133 / Configure static routing between DC-R and ISP router:
DC-R(config)#ipv6 router eigrp 1
DC-R(config-rtr)#eigrp router-id 5.5.5.5
DC-R(config-rtr)#no shutdown
DC-R(config-rtr)#redistribute static
DC-R(config-rtr)#exit
DC-R(config)#int serial 0/0/0
DC-R(config-if)#ipv6 eigrp 1
DC-R(config-if)#ipv6 enable
DC-R(config-if)#exit
        DC-R(config)#int serial 0/2/0
DC-R(config-if)#ipv6 eigrp 1
DC-R(config-if)#ipv6 enable
DC-R(config-if)#exit
DC-R(config)#do wr
DC-R(config)#exit
```

5. RESULT AND DISCUSSION

VLANs verification:

We have created four VLANs for different departments in each branch to reduce traffic congestion for better network availability.

Table 6: VLAN verification

```
KB-CoreSW1#show vlan brief

VLAN        Name          Status        Ports
---- -------------------------------- --------- -------------------------------
1           default       active        Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                   Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Gig0/1, Gig0/2
10          VOICE_A       active        Fa0/3, Fa0/5
20          IT_A          active        Fa0/2, Fa0/3, Fa0/4, Fa0/7
30          HR_A          active        Fa0/5, Fa0/6
40          Sales_A       active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

In table 6, we just verified the first branch's VLANs because all branches have similar configurations.

DHCPv6 verification

```
Rapid-Commit: disabled
FastEthernet0/1.30 is in server mode
Using pool: VLAN30
Preference value: 0
Hint from client: ignored
Rapid-Commit: disabled
FastEthernet0/1.40 is in server mode
Using pool: VLAN40
Preference value: 0
Hint from client: ignored
Rapid-Commit: disabled
```

Table 7: DHCPv6 verification in each interface

Table 7 shows the configured DHCPv6 in each subinterface. Subinterfaces are created for each Vlans and using the related DHCPv6 pool for IPv6 address auto-assignment, end users get IPv6 addresses from the VLAN range.

Table8:DHCPv6 verification for each VLAN

In Table 8, there are four Vlans 10, 20, 30, and 40. DHCPv6 is configured for eachVlan to assign IPv6 addresses to relatedVlan users;for example, those users who are in Vlan 10 can get IPv6 addresses from the range of Vlan10, Vlan 20 users can get their IPv6 address from Vlan 20, and so on.

```
KB-Gatewat-R1#show ipv6 dhcp pool
DHCPv6 pool: VLAN10
Prefix pool: VLAN10
preferred lifetime 604800, valid lifetime 2592000
Active clients: 0
DHCPv6 pool: VLAN20
Prefix pool: VLAN20
preferred lifetime 604800, valid lifetime 2592000
Active clients: 0
DHCPv6 pool: VLAN30
Prefix pool: VLAN30
preferred lifetime 604800, valid lifetime 2592000
DNS server: 2001:DB8:CAD:4::2
Active clients: 0
```

```
KB-Gatewat-R1#show ipv6 dhcp interface
FastEthernet0/1.10 is in server mode
Using pool: VLAN10
Preference value: 0
Hint from client: ignored
Rapid-Commit: disabled
FastEthernet0/1.20 is in server mode
Using pool: VLAN20
Preference value: 0
Hint from client: ignored
```

Frame Relay verification

Table 9: Frame relay verification in three branches

Table 9 shows the verification of Frame Relay, which was configured to connect the enterprise branches. Here we could ping from Data Center to Branch 1 and Branch 2, from Branch 1 to Data Center and Branch 2, and from

```
Frame relay verification from DATACENTER to Bramch 1 and Branch 2:

DC-R#ping 2001:db8:cad:1::54

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::54, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/17/34 ms

DC-R#ping 2001:db8:cad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/18 ms

Frame relay verification from Branch 1 to datacenter and Branch 2:

HRT-Gateway-R1#ping 2001:db8:cad:1::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/11/22 ms
HRT-Gateway-R1#ping 2001:db8:cad:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/9/14 ms

Frame relay verification from Branch 2 to datacenter and Branch 1:

KB-Gateway-R1#ping 2001:db8:cad:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/16/26 ms
KB-Gateway-R1#ping 2001:db8:cad:1::54

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:cad:1::54, timeout is 2 seconds:
!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/17 ms
```

Branch 2 to Data Center and Branch 1 successfully.

IPv6 Routes in three Datacenter, Branch 1 and 2

Table 10: IPv6 route in Datacenter **Table 11:** IPv6 route in Branch 1

Table 10 shows EIGRP for the IPv6 routing table. A router stores the routing table as a data table that contains all necessary routes to specific network destinations. EIGRP v6 is used to find the best path for data packet

DC-R#show ipv6 route IPv6 Routing Table - 8 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP U - Per-user Static route, M - MIPv6 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 D - EIGRP, EX - EIGRP external C 2001:DB8:CAD:1::/64 [0/0] via ::, Serial1/0 L 2001:DB8:CAD:1::1/128 [0/0] via ::, Serial1/0 C 2001:DB8:CAD:3::/64 [0/0] via ::, FastEthernet0/0 L 2001:DB8:CAD:3::254/128 [0/0] via ::, FastEthernet0/0 D 2001:DB8:CAD:40::/64 [90/20514560] via FE80::2, Serial1/0 C 2001:DB8:CAD:171::/64 [0/0] via ::, Serial1/1 L 2001:DB8:CAD:171::134/128 [0/0] via ::, Serial1/1 L FF00::/8 [0/0] via ::, Null0	KB-Gateway-R1#show ipv6 route IPv6 Routing Table - 5 entries Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP U - Per-user Static route, M - MIPv6 I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2 ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 D - EIGRP, EX - EIGRP external C 2001:DB8:CAD:1::/64 [0/0] via ::, Serial1/0 L 2001:DB8:CAD:1::2/128 [0/0] via ::, Serial1/0 C 2001:DB8:CAD:40::/64 [0/0] via ::, FastEthernet0/1 L 2001:DB8:CAD:40::1/128 [0/0] via ::, FastEthernet0/1 L FF00::/8 [0/0] via ::, Null0

transitions.In the Datacenter router, the routing table shows from which interface we can go to which network is connected to which interface.

Table 12: IPv6 route in Branch 2

In Branch 1 and Branch 2, we have two networks: LAN and WAN.LAN network is connected with the local

```
 HRT-Gateway-R1#show ipv6 route
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
    U - Per-user Static route, M - MIPv6
    I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
    ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
    O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
    ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
    D - EIGRP, EX - EIGRP external
C   2001:DB8:CAD:1::/64 [0/0]
    via ::, Serial1/0
L   2001:DB8:CAD:1::54/128 [0/0]
    via ::, Serial1/0
C   2001:DB8:CAD:35::/64 [0/0]
    via ::, FastEthernet0/1
L   2001:DB8:CAD:35::1/128 [0/0]
    via ::, FastEthernet0/1
L   FF00::/8 [0/0]
    via ::, Null0
```

switches in each branch, and WAN is connected to the frame relay switch.

6. Baseline Comparison

As Ipv4 is already implemented and used in every organization, either small or large, private or public, governmental or nongovernmental, and different network projects are designed and implemented based on Ipv4, and a lot of papers are written and published to discuss IPv4, its implementation, and supported technologies. Each of them has applied their methodto create a network usingIPv4 for having network connection and Internet connection.

Table 13:comparative analysis with related works

S.No	Reference	Task	Identified Problems	Solutions	Advantages	Disadvantages
1.	[8]	An enterprise network of a city was designed and simulated	The infrastructural problem of an enterprise network	A hierarchal design of enterprise network only based on software	Enterprise Network overview. New design methodology. Benefits of an enterprise network.	Some limitations: Bandwidth, Encryption, NAT, Proxies, Tunneling. All these limitations are because of IPv4 implementation in an enterprise network.
2.	[9]	A Secured Enterprise Network for Faculty of Engineering, Rivers State University was designed and simulated.	The other designed and simulated project does not meet the security requirement of an enterprise network; the other researcher did not implement Cisco ASA	Deployed a secure design for Network Engineers to design and implement a scalable, manageable, available, and secured enterprise network for the River State University of Nigeria.	Minimize the cost. Ease manageability, connectivity, improved security, availability.	IPv4 provides network connectivity. IPv4 implementation causes many limitations in any network nowadays. From the low bandwidth up to network security issues.
3.	[10]	A Secure Campus Networkis designed and implemente d	Network architecture and Network security problems	They proposed the hierarchical network design, cost-effective and secure campus network	Maintaining the network is easy, scalability, performance, and security are improved	There are several security threats and network attacks that can be occurred as long as IPv4 is adapted.

4.	[11]	Designed and Simulated VLAN Using Cisco Packet Tracer	Poor network design, In VLAN trunking protocol reduces administration in a switched network	They used VLAN and ACL to redesign the Local Area Network as a solution	It is better in the case of reducing network traffics by creating multiple broadcast domains using VLAN.	The paper talks about the VLAN, so it cannot fulfill the connection because it is not working at layer 3 (router), only runs at the switch (layer 2).
5.	[12]	An IPv6 address configuration scheme for wireless sensor networks	IPv6 address configuration was on the base of a hierarchical cluster-based structure. A node should join to cluster tree to acquire an IPv6 address.	Ipv6 address configuration is based on flat architecture, and the neighbor node can provide IPv6 address to a sensor node.	The deployment of IPv6 in Wireless Sensor Network Removed any address shortage and limitations.	IPv6 deployment in Wireless Sensor Network is different than the enterprise network.
6.	[13]	Location-Based IPv6 Address Configuration for Vehicular Networks	Stateful and stateless address configuration is not efficient in Vehicular networks.	IPv6 configuration based on information of location for Vehicular Network.	IPv6 deployment in Vehicular Network.	IPv6 cannot work in vehicular networks efficiently because there is an addressing delay when a vehicleobtains an IPv6 address from a remote server.
7.	[15]	Implementing IPv6 at the University of Venezuela	Fast growth and Low throughput, the inefficacy of ANT	Deploy IPv6 in the network of the university.	WAN link to ISP was upgraded, Better throughput is available, IPv4 address shortage was solved	A native connection is not provided just by IPv6, IPv6 over IPv4 tunneling is used, and address spoofing is an issue on tunnels of IPv6 over IPv4. Mismatch of IPv4 address of the relay router with IPv6 address of source.
8.	Our Work	Implementing IPv6 in Enterprise Network Using Cisco Packet Tracer Simulator	IPv4 addressesexhaustion and limitations. Security challenges and problems. Do not support new technologies in the case of IoT and Cloud.	We deployed IPv6 and didthe infrastructural design for IPv6 network and.All design and implementations are simulated in Cisco Packet Tracer. A successful and secure IPv6 connectivity is provided. Native IPv6 implementation is done. IPv4 address shortage is removed.	Move forward to IPv6. To know IPv6 implementation mechanisms. Help in business development. As internet users are growing and also new modern equipment comes with supported IPv6. Can go forward for more use of IPv6 in future coming technologies according to an enterprise plan.	Maybe there is a topological problem because it is simulated in software; it can be different from a real scenario. For the implementation of IPv6 in a real scenario, maybe this approach is not sufficient.

Table 13 presents the detailed comparisons of all related works with our work and shows how our work is better as a solution for IPv6 implementation in an enterprise network. The first four projects are implemented using IPv4 but not entirely implemented as an enterprise network. An enterprise network combines LANs and WAN; in the mentioned projects, they focused on the LANs network, designed and implemented in Cisco Packet Tracer. The last projects indicate the implementation of IPv6 in the networks, which are utterly different from enterprise networks; we just mentioned those projects here for the widespread use of IPv6 in other networks.In this research,IPv6 is implemented in the network of an industrial company. The following network concepts are implemented, such as IPv6 address configuration in LAN and WAN, topology design of the network, Virtual

Local Area Networks (VLANs), DHCPv6, VoIP set up in each department for voice communication, EIGRPv6 routing protocol, frame relay, which can support IPv6 connectivity in between.Finally,all the necessary configurations for the LANs and WAN of an enterprise network had wholly done.

7. Conclusion

IPv6 is an upgraded form of IPv4,as IPv4 is not enough to support globally unique addresses for more devices to connect to the Internet, for the reason IPv6 is developed to remove this limitation of IPv4.

Any small or large enterprise company needs to have a computer network to manage and control their workflow and work progress and connect to the Internet. By implementing IPv6 in an enterprise network, it will remove the IPv4 problems and challenges, and the organizations can pave the way to go ahead with IPv6 implementation in their network for the usability ofservices that will be provided by upcoming technologies in the future, separate of the services which are providing by IPv6 right now.

In our future work, we willimplement IPv6 on MPLS [33] in the enterprise core networkto provide fast connectivity overall in an enterprise network. Additionally, we focus on IPv6 network security included CCTV and Biometric technologies, to provide security and advance access control for end-to-end security in the network.

References

1. Baki, A. (2008). *Kuramdan uygulamaya matematik eğitimi*. Ankara: Harf Eğitim Yayıncılığı
2. Loshin, P. (2004). IPv6: Theory, protocol, and practice.
3. Narayanan, A. S., Mohideen, M. S. K., & Raja, M. C. (2012). IPv6 Tunneling Over IPV4. International Journal of Computer Science Issues (IJCSI), 9(2), 599.
4. Bi, J., Wu, J., &Leng, X. (2007). IPv4/IPv6 transition technologies and univer6 architecture. International Journal of Computer Science and Network Security, 7(1), 232-243.
5. Chuangchunsong, N., Kamolphiwong, S., Kamolphiwong, T., Elz, R., &Pongpaibool, P. (2014, February). Perfor-mance evaluation of IPv4/IPv6 transition mechanisms: IPv4-in-IPv6 tunneling techniques. In The International Conference on Information Networking 2014 (ICOIN2014) (pp. 238-243). IEEE.
6. Park, E. Y., Lee, J. H., &Choe, B. G. (2004, June). An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 hosts and IPv4 hosts in integrated IPv6/IPv4 network. In 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577) (Vol. 2, pp. 1024-1027). IEEE.
7. https://www.google.com/intl/en/ipv6/statistics.html accessed on March 2, 2021.
8. Zhang-Shen, R., &McKeown, N. (2004, November). Designing a predictable Internet backbone network. HotNets.
9. Nahid, M. H. (2015). Design an Enterprise Network Infrastructure of a City. International Journal of Advanced Research in Computer and Communication Engineering, 4(9), 4.
10. Enoch, J. D., Orike, S., &Ahiakwo, C. O. (2019). Design and Simulation of a Secured Enterprise Network for Faculty of Engineering, Rivers State University. IISTE-Computer Engineering and Intelligent Systems, 10(5), 26-41.
11. Michael, G. (2017). Design and implementation of a secure campus network. International Journal of Pure and Applied Mathematics, 116(8), 303-307.
12. Andry, J. F. (2016). Design and simulation VLAN using Cisco packet tracer: A case study. In The International Seminar of Mathematics, Science, and Computer Education (pp. 66-72).
13. Tarkaa, N. S., Iannah, P. I., &Iber, I. T. (2017). Design and simulation of local area network using cisco packet trac-er. The International Journal of Engineering and Science, 6(10), 63-77.
14. Xiaonan, W., & Shan, Z. (2013). An IPv6 address configuration scheme for wireless sensor networks based on loca-tion information. Telecommunication Systems, 52(1), 151-160.
15. Wang, X., Le, D., & Cheng, H. (2016). Location-based ipv6 address configuration for vehicular networks. Journal of Network and Systems Management, 24(2), 257-284.
16. Gamess, E., & Morales, N. (2007, October). Implementing IPv6 at central university of venezuela. In Proceedings of the 4th international IFIP/ACM Latin American conference on networking (pp. 43-51).
17. Roşu, S. M., &Drāgoi, G. (2010, June). Virtual enterprise network general architecture. In 2010 8th International Conference on Communications (pp. 313-316). IEEE.
18. Krishnan, Y. N., &Shobha, G. (2013, March). Performance analysis of OSPF and EIGRP routing protocols for greener internetworking. In 2013 International Conference on Green High Performance Computing (ICGHPC) (pp. 1-4). IEEE.

19. Van de Velde, G., Popoviciu, C., Chown, T., Bonness, O., & Hahn, C. (2008). IPv6 unicast address assignment con-siderations. IETF Request for Comment, 5375.
20. Groat, S., Dunlop, M., Marchany, R., &Tront, J. (2011, February). What DHCPv6 says about you. In 2011 World Congress on Internet Security (WorldCIS-2011) (pp. 146-151). IEEE.
21. Talipov, E., Shin, H., Han, S., & Cha, H. (2011). A lightweight stateful address autoconfiguration for 6LoWPAN. Wireless Networks, 17(1), 183-197.
22. Droms, R. (2004). Stateless dynamic host configuration protocol (DHCP) service for IPv6. RFC 3736, April.
23. Gont, F. (2014). A method for generating semantically opaque interface identifiers with ipv6 stateless address auto-configuration (slaac). RFC 7217, DOI 10.17487/RFC7217, April 2014,< http://www. rfc-editor. org/info/rfc7217.
24. Basu, A., Jha, K. K., &Mohanty, S. (2015). Wide area networking using frame relay cloud. International Journal of Computer & Mathematical Sciences, 4(7), 80-85.
25. Goyal, V., & Arora, G. (2017). Implementation of enhanced interior gateway routing protocol (EIGRP) in IPv6 network. Research Journal of Advanced Engineering and Science, 2(1), 90-95.
26. Jian, S., & Fang, Y. Y. (2011, July). Research and implement of Ospfv3 in Ipv6 network. In Proceedings of 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (Vol. 1, pp. 743-746). IEEE.
27. Malkin, G., &Minnear, R. (1997). RFC2080: RIPng for IPv6.
28. Bates, T. O. N. Y., Rekhter, Y., Chandra, R., & Katz, D. (2000). RFC2858: Multiprotocol Extensions for BGP-4.
29. Trujillo, V., Expósito, J., &Gamess, E. (2010). An alternative way of teaching the advanced concepts of the diffus-ing update algorithm for EIGRP. In The 2010 International Conference on Computer Science and Applications (ICCSA'10). San Francisco, California, USA.
30. V. Rajaravivarma, "Virtual local area network technology and applications," Proceedings The Twenty-Ninth Sou-theastern Symposium on System Theory, Cookeville, TN, USA, 1997, pp. 49-52, doi: 10.1109/SSST.1997.581577.
31. https://en.wikipedia.org/wiki/IPv6#:~:text=IPv6%20was%20developed%20by%20the,Standard%20on%2014%20July%202017. Accessed on February 17, 2021.
32. Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., & Carney, M. (2003). Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315, July.
33. Chin, J. Cisco Frame Relay Solutions Guide. Cisco Press. 2nd ed. 800 East 96th Street, Indianapolis, Indiana 46240 USA, (2004), pp. 5-6.
34. Vanaubel, Y., Mérindol, P., Pansiot, J. J., &Donnet, B. (2016, March). A brief history of MPLS usage in IPv6. In International Conference on Passive and Active Network Measurement (pp. 359-370). Springer, Cham