IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 1, January 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

Configuration of IPv6 on EIGRP

A. Ramesh[1], G. Lakshman Reddy[2], T. Syam Kumar[3], N Sri Ganesh[4], R. Malleswar singh[5]

Asst. Professor, Dept of computer Science & Engineering, QIS College of Engineering and Technology, Ongole, India[1].

Students, Dept of computer Science & Engineering, QIS College of Engineering and Technology, Ongole, India[2,3,4,5].

ABSTRACT: Today networking has become an essential aspect of your job search. Networking being the backbone of computer industry faces the greatest challenge. Even if you are well established in your job and have no plans of moving or advancing your career soon, networking has proven to be a valuable tool.
This paper suggests and describes how to configure Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. EIGRP is an enhanced version of the IGRP developed by Cisco. It is an enhanced distance vector protocol that relies on the Diffused Update Algorithm to calculate the shortest path to a destination within a network. EIGRP for IPv6 works in the same way as EIGRP IPv4 where they can be configured and managed separately.

KEYWORDS: - CISCO Software, EIGRP.

I. INTRODUCTION TO NETWORKING

Networking is referred as connecting computers electronically for the purpose of sharing information. Resources such as files, applications, printers and software are common information shared in a networking. The advantage of networking can be seen clearly in terms of security, efficiency, manageability and cost effectiveness as it allows collaboration between users in a wide range. Basically, network consists of hardware component such as computer, hubs, switches, routers and other devices which form the network infrastructure. These are the devices that play an important role in data transfer from one place to another using different technology such as radio waves and wires.
There are many types of network available in the networking industries and the most common network are Local Area Network (LAN) and Wide Area Network (WAN). LAN network is made up of two or more computers connected together in a short distance usually at home, office buildings or school. WAN is a network that covers wider area than LAN and usually covers cities, countries and the whole world. Several major LAN can be connected together to form a WAN. As several devices are connected to network, it is important to ensure data collision does not happened when these devices attempt to use data channel simultaneously.

1.1Types of Networking

i)Breaking down Networking: -

Networking helps to develop professional relationships that may boost an individual's future business and employment prospects. Networking events, such as industry conferences and seminars, are common practice within professional organizations, which may also link up with other groups to stage a joint event or conference.

ii)Business Networking: -

Strategies for expanding a business network include developing relationships with people and companies as well as exchanging contact information. Connections within a network usually maintain regular contact with each other to build rapport and gain trust. Instead of having many contacts, a small selective network may provide more benefit, even though it often takes longer to establish. Successful networking involves regularly engaging and following up with contacts in the network to provide and receive valuable information that is not readily available outside the network.
For example, a business network consisting of accounting professionals may provide information to their connections about an upcoming employment.

iii)Online Networking: -

Business networking has increased in popularity due to social networking websites. Networking platforms, such as LinkedIn provides an online meeting place for business professionals to engage with other professionals, join groups,

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

post blogs, share content and create online profiles with the objective of connecting with other people that have similar interests. LinkedIn allows users to search for companies, people and jobs. LinkedIn members can reach out to potential employees and connect them with human resources managers or recruiters. Likewise, a business-to-business customer pipeline could develop through using a social networking site. Online networking through forums allows professionals to demonstrate their knowledge and connect with like-minded people.

iv)Computer Networking: -

Computer networking involves connecting computers in the same building or office so users can readily communicate with other computers or devices.

Switches connect multiple devices in one building on the same network. Computers, for instance, can connect to printers, fax machines, scanners and servers through a switch. Routers tie multiple networks together, such as when a computer connects to an internet router to access the web. Routers control the information going to and from computer networks through security software and programs.

1.2 DEVICES USED IN NETWORKING

Switches, routers, and wireless access points and firewalls perform different functions in a network.

i) Range

Networking devices may include gateways, routers, network bridges, modems, wireless access points, networking cables, line drivers, switches, hubs, and repeaters; and may also include hybrid network devices such as multilayer switches, protocol converters, bridge routers, proxy servers, firewalls, network address translators, multiplexers, network interface controllers, wireless network interface controllers, ISDN terminal adapters and other related hardware.

The most common kind of networking hardware today is a copper-based Ethernet adapter which is a standard inclusion on most modern computer systems. Wireless networking has become increasingly popular, especially for portable and handheld devices.

Other networking hardware used in computers includes data center equipment (such as file servers, database servers and storage areas), network services (such as DNS, DHCP, email, etc.) as well as devices which assure content delivery.

Taking a wider view, mobile phones, tablet computers and devices associated with the internet of things may also be considered networking hardware. As technology advances and IP-based networks are integrated into building infrastructure and household utilities, network hardware will become an ambiguous term owing to the vastly increasing number of network capable endpoints.

ii)Switches

A network switch (also called switching hub, bridging hub, officially MAC Bridge) is a computer networking device that connects devices on a computer network by using packet switching to receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kalpana in 1990. Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

Fig: - 1.5.1 the switch

Role in a network: -

Switches are most commonly used as the network connection point for hosts at the edge of a network. In the hierarchical internetworking model and similar network architectures, switches are also used deeper in the network to provide connections between the switches at the edge.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, Rapid IO, ATM, ITU-T G.hn and 802.11. This connectivity can be at any

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

of the layers mentioned. While the layer-2 functionality is adequate for bandwidth- shifting within one technology, interconnecting technologies such as Ethernet and token ring are performed more easily at layer 3 or via routing. Devices that interconnect at the layer 3 are traditionally called routers, so layer 3 switches can also be regarded as relatively primitive and specialized routers.

Where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall, network intrusion detection, and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules. Through port mirroring, a switch can create a mirror image of data that can go to an external device such as intrusion detection systems and packet sniffers.

iii)Routers:

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node.

A router is connected to two or more data lines from different networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.

Routers that forward data at high speed along the optical fiber lines of the Internet backbone. Though routers are typically dedicated hardware devices, software-based routers also exist.

Applications: -

A router may have interfaces for different types of physical layer connections, such as copper cables, fiber optic, or wireless transmission. It can also support different network layer transmission standards. Each network interface is used to enable data packets to be forwarded from one transmission system to another. Routers may also be used to connect two or more logical groups of computer devices known as subnets, each with a different network prefix.

Routers may provide connectivity within enterprises, between enterprises and the Internet, or between internet service providers' (ISPs') networks. The largest routers (such as the Cisco CRS-1 or Juniper PTX) interconnect the various ISPs or may be used in large enterprise networks. Smaller routers usually provide connectivity for typical home and office networks.

All sizes of routers may be found

inside enterprises. The most powerful routers are usually found in ISPs, academic and research facilities. Large businesses may also need more powerful routers to cope with ever-increasing demands of intranet data traffic. A hierarchical internetworking model for interconnecting routers in large networks is in common use.

Fig: - 1.5.2 the Router

Existing System:

RIP (Routing information protocol). It is the distance vector protocol. In this we differ only protocols.

Disadvantages: -

- Hop count
- It use only in smaller Organinsations.
- In these protocols have limitations.

Proposed system:

In this proposed system we use EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL). It is a link state protocol. We will overcome the RIP protocol we use Eigrp protocol.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

Advantages: -

- Speed
- Scalability
- Easy to management

II. INTERNET PROTOCOL VERSION 6(IPV6)

The Internet Protocol (IP) is the principal communications protocol in theInternet protocol suitefor relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information. Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahnin 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP.

2.1 IP ADDRESS(IP.add)

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: Host or Network interface identifying and location addressing. Internet Protocol version 4 (IPV4) it defines as an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPV4 addresses, a new version of IP (IPV6), using 128 bits for the IP address, was developed in 1995, and standardized in December 1998. In July 2017, a final definition of the protocol was published.

IPV6 deployment has been ongoing since the mid-2000s.IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 in IPV4, and 2001:db8:0:1234:0:567:8:1 in IPV6. The size of the routing prefix ofthe address is designated in CIDR Notation by suffixing the address with the number of significant bits, e.g., 192.168.1.15/24, which is equivalent to the historically used subnet mask 255.255.255.0. Each ISP or private network administrator assigns an IP address to each device connected to its network. The IP address space is managed globally by theInternet Assigned Numbers Authority (IANA), and by five regional Internet registries (RIRs) responsible in their designated territories for assignment to end users and local Internet registries, such as Internet service providers. IPV4 addresses have been distributed by IANA to the RIRs in blocks of approximately 16.8 million addresses each. Such assignments may be on a static (fixed or permanent) or dynamic basis, depending on its software and practices. An IP address serves two principal functions. It identifies the host, or more specifically its network interface, and it provides the location of the host in the network, and thus the capability of establishing a path to that host. Its role has been characterized as follows: "A name indicates what we seekThe subnet mask or CIDR notation determines how the IP address is divided into network and host parts. The term subnet mask is only used within IPV4. Both IP versions however use the CIDR concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the routing prefix. For example, an IPV4 address and its subnet mask may be 192.0.2.1 and 255.255.255.0, respectively.

The CIDR notation for the same IP address and subnet is 192.0.2.1/24, because the first 24 bits of the IP address indicate the network and subnet.

2.1.1 IPV6(InternetProtocolVersion6)

Internet Protocol Version 6 (IPV6) is an Internet Protocol (IP) used for carrying data in packets from a source to a destination over various networks. IPV6 was developed in hexadecimal format and contains 8 octets to provide large scalability. Like IPV4, IPV6 deals with address broadcasting without containing broadcast addresses in any class. IPV6 is the enhanced version of IPv4 and can support very large numbers of nodes as compared to IPV4. It allows for 2128 possible node, or address, combinations. IPV6 is also known as Internet Protocol Next Generation (IPNG). IPV6 provides other technical benefits in addition to a larger addressing space.

In particular, it permits hierarchical address allocation methods that facilitate routeaggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol. IPV6 provides other technical benefits in addition to a larger addressing space. The use of multicast addressing is expanded and simplified and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol. On the Internet, the data is transmitted in the form of network packets. In particular, it permits hierarchical address

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. IPV6 specifies a new packet format, designed to minimize packet header processing by routers. So, the headers of IPV4 packets and IPV6 packets are significantly different, the two protocols are not interoperable. However, most transport and application-layer protocols need little or no change to operate over IPV6; exceptions are application protocols that embed Internet-layer addresses, such as File Transfer Protocol (FTP) and Network Time Protocol (NTP), where the new address format may cause any such conflicts with existing protocol syntax.

Configuration of Router0 for IPv6

Router>en
Router#config t
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#ipv6 un
Router(config)#ipv6 unicast-routing Router(config)#int f0/0
Router(config-if) #ipv6 address 2002::1/64 Router(config-if) #no shut
Router(config-if) #
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up Router(config-if)#int f0/1
Router(config-if) #ipv6 address 2001::1/64 Router(config-if) #no shut
Router(config-if) #
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if) #
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit

2.2 EIGRP (ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL)

All routers contain a routing table that contains rules by which traffic is forwarded in a network. If the router does not contain a valid path to the destination, the traffic is discarded. EIGRP is a dynamic routing protocol by which routers automatically share route information. This eases the workload on a network administrator who does not have to configure changes to the routing table manually. In addition to the routing table, EIGRP uses the following tables to store information: Neighbor Table: The neighbor table keeps a record of the IP addresses of routers that have a direct physical connection with this router. Routers that are connected to this router indirectly, through another router, are not recorded in this table as they are not considered neighbors. Topology Table: The topology table stores routes that it has learned from neighbor routing tables. Unlike a routing table, the topology table does not store all routes, but only routes that have been determined by EIGRP. The topology table also records the metrics for each of the listed EIGRP routes, the feasible successor and the successors. Routes in the topology table are marked as "passive" or "active". Passive indicates that EIGRP has determined the path for the specific route and has finished processing. Active indicates that EIGRP is still trying to calculate the best path for the specific route. Routes in the topology table are not usable by the router until they are inserted into the routing table. Information in the topology table may be inserted into the router's routing table and can then be used to forward traffic. If the network changes (for example, a physical link fails or is disconnected), the path will become unavailable. EIGRP is designed to detect these changes and will attempt to find a new path to the destination. The old path that is no longer available is removed from the routing table. Unlike most distance vector routing protocols, EIGRP does not transmit all the data in the router's routing table when a change is made, but will only transmit.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

III. ARCHITECTURE

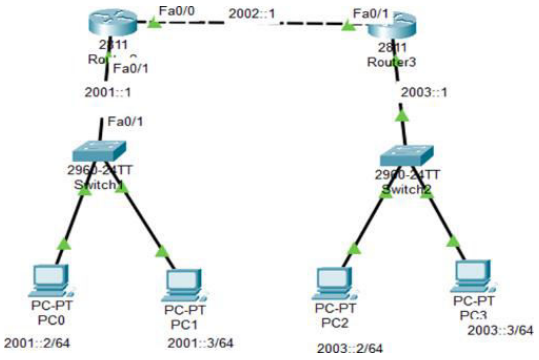


Fig: - 3.0.1 Topology

3.1CONFIGURATION IPv6 EIGRP ON A NETWORK:

•IPv6 packet forwarding is disabled by default. To enable IPv6 packet forwarding, use the ipv6 unicast-routing command in global configuration mode before enabling EIGRP.

R1(config)# ipv6 router eigrp 1

// IPv6 routing not enabled // R1(config)# ipv6 unicast routing

•A router ID is mandatory for IPv6 EIGRP to be functioning properly. If one isn't manually configured, one will be generated using the loopback or physical interface.

R1(config)# ipv6 router eigrp 1

R1(config-rtr) # router-id 1.1.1.1

R1(config-rtr) # no shutdown

•Unlike IPv4 EIGRP, IPv6 EIGRP does not require the use of network command to advertise its networks. Instead IPv6 EIGRP must be enabled on all of the router's interfaces.

R1(config)# int f0/1 R1(config-if) # ipv6 eigrp 1 R1(config-if) # int f0/0 R1(config-if)# ipv6 eigrp 1

•This command must be configured on all of the router's interfaces that are participating in EIGRP. If we fail to configure this command on an interface, that network will not be advertised, therefore, will not be learned by its neighbors.

•When IPv6 EIGRP is configured on all interfaces, a log message will inform you that an adjacency has formed.

Configuration of Router 2

R2(config)# int f0/1

R2(config-if) # ipv6 eigrp 1

R2(config-if) #

*Mar 1 00:01:25.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R2(config-if) # int f0/0

R2(config-if) # ipv6 eigrp 1

R2(config-if) #

*Mar 1 00:05:56.607: %DUAL-5-NBRCHANGE: IPv6-EIGRP (0) 100:

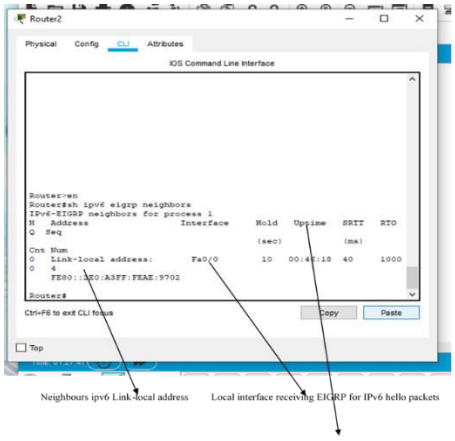
Neighbor FE80::C002:44FF:FE50:0 (Serial1/0) is up: new adjacency R2(config-if) #

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

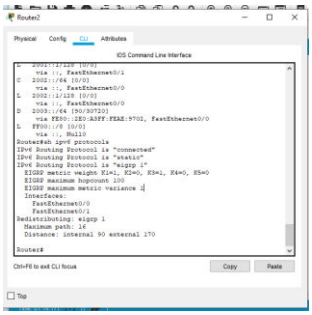
DOI:10.15680/IJIRSET.2021.1001081

3.2 IPV6 SHOW COMMANDS



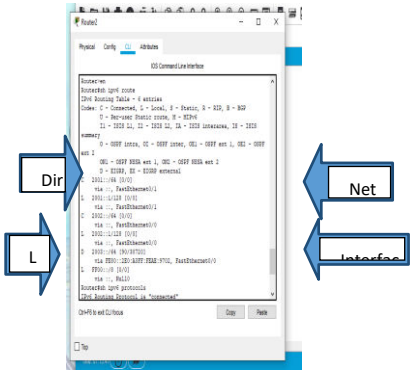
Seconds remaining before declaring neighbors down

IPv6 Protocols



- These are the ipv6 eigrp neighbour's with its local address and representing amount of time since this neighbour was added.

- Here we can see which are learned and directly connected networks and displaying network and interface addresses.



| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

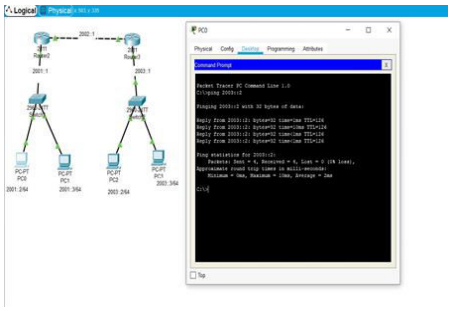
DOI:10.15680/IJIRSET.2021.1001081

3.4IPv6 END-DEVICE CONFIGURATION LOOKUP

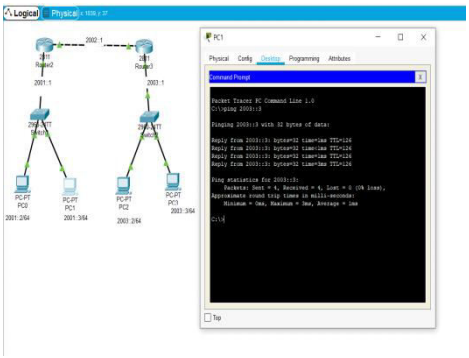
```
PC2> show ipv6

NAME            : PC2[1]
LINK-LOCAL SCOPE  : fe80::250:79ff:fe66:6801/64
GLOBAL SCOPE      : 4001::3/64
ROUTER LINK-LAYER : c2:01:50:f0:00:00
MAC             : 00:50:79:66:68:01
LPORT           : 10024
RHOST:PORT      : 127.0.0.1:10025
MTU:            : 1500
```

IV. RESULT

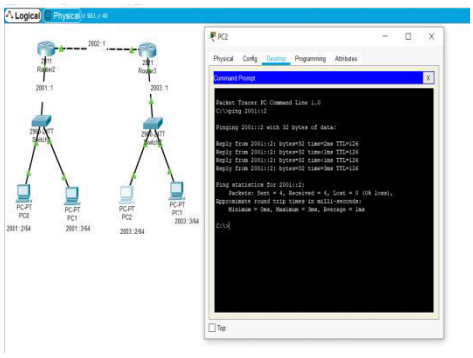
ipv6 pinging pc0 to pc2



ipv6 pinging pc1 to pc3



ipv6 pinging pc2 to pc0

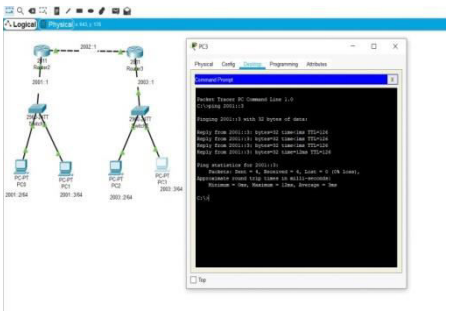


| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 1, January 2021 ||

DOI:10.15680/IJIRSET.2021.1001081

ipv6 pinging pc3 to pc1



V. CONCLUSION

This project proposes how to configure Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6. EIGR IPv6 will exchange the messages allowing a router to discover neighbors, and from the neighbour relationship as well as advertises the subnets along with a metric component for every route. The EIGRPv6 has the same successor as well as feasible successor concepts. From this section you can learn how to configure and verify the EIGRP for IPv6. After the configuration, it is very important to verify the EIGRP for IPv6.

REFERENCES

1. B. Carpenter & K. Moore. Connection of IPv6 Domains via IPv4 Clouds.RFC 3056, February 2001
2. R. Gilligan & E. Nordmark. Transition Mechanisms for IPv6 Hosts and Routers. RFC 2893, August 2000.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details