# NATIONAL INSTITUTE OF TECHNOLOGY SILCHAR

2020-2022

MINI PROJECT REPORT

ON

# ICMP IMPLEMENTATION

MASTER OF TECHNOLOGY

SECOND SEMESTER

SUBMITTED TO

SIR UMAKANTA MAJHI

SUBMITTED BY

ROHIT THINGBAIJAM
2022120

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

# Abstract

IP convention needs the assistance of distinguishing sending blunder and control messages since it doesn't have an inbuilt component, the utilization of ICMP has been presented, which has utilized by network gadgets as a supporting convention. The examination objective is to show the setup of ICMP, interfacing two switches and confirm ICMP and utilizing ICMP to test the Network which neglected to arrive at the worker and right its organization availability. The examination will be performed by utilizing the Cisco Packet Tracer.

***Keywords***: ICMP, IP,Ping,Trace,Cisco packet tracer

# Contents

# List of Figures

# 1 INTRODUCTION

## 1.1 Internet Protocol

The underneath Figure for example Fig. no. 1. relates the web convention stack and the OSI reference convention. The Internet convention stack gives an association arranged solid branch (TCP) and a connectionless, untrustworthy branch (UDP) expand on top of the Internet Protocol.

All actual execution subtleties are covered up underneath the IP layer. The

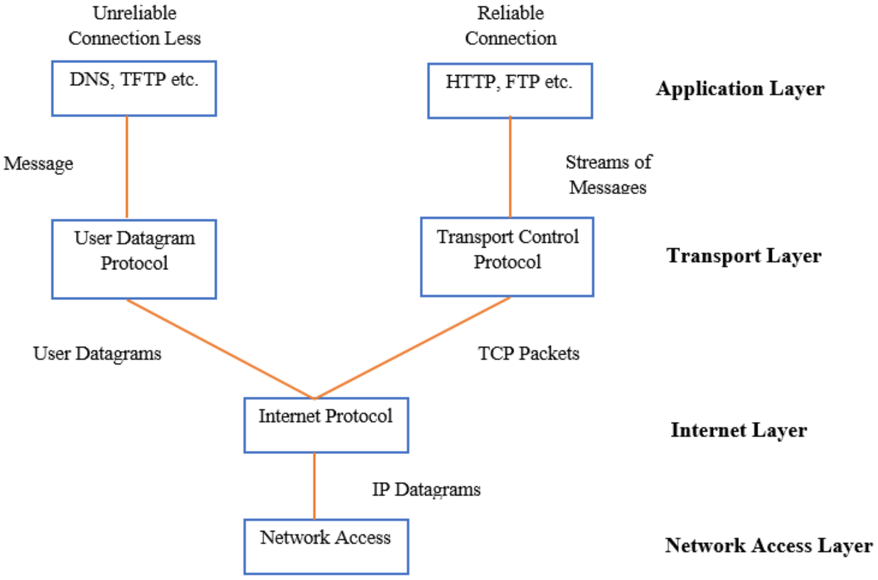


Figure 1: Internet Protocol Stack.

IP layer gives a problematic, connectionless conveyance framework. The motivation behind why it is temperamental originate from the reality the convention doesn't give any usefulness to blunder recuperating for datagrams that are either copied, lost or show up at the far off have in another request than they are sent. On the off chance that no such blunders happen in the actual layer, the IP convention ensures that the transmission is ended effectively. The essential unit of information trade in the IP layer is the Internet Datagram. The organization of an IP datagram and a short portrayal of the main fields are remembered for Fig. no. 2.:

1. LEN: The number of 32 bit-segments in the IP header

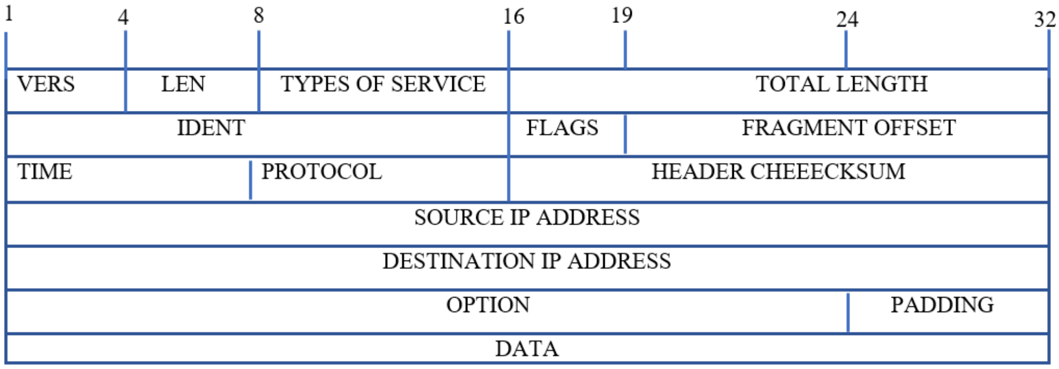


Figure 2: Internet Protocol Datagram.

2. TYPES OF SERVICE: Each IP datagram can be given a precedence value ranging from 0-7, showing the importance of the datagram. This is to allow out-of-band data to be routed faster than normal data.

3. IDENT, FLAGS AND FRAGMENT OFFSET: These fields are used to describe the fragmentation of a datagram.

4. TIME: This is the remaining Time To Live (TTL) for a datagram when it travels on the Internet.

5. SOURCE IP-ADDRESS AND DESTINATION IP-ADDRESS: Both the source and the destination address is indicated in the datagram header so that the recipient can send an answer back to the transmitting host.

## 1.2 ICMP

ICMP is designed to overcome the following two problems with IP Protocol

1. No Error reporting(Correcing mechanism)
2. Lacks a mechanism for queries

It is a network layer protocol, but its msg are not passed to the data link layer. Its msg are first encapsulated inside an IP datagram before going to the lower layer.

ICMP position is shown in below Fig. no. 3. ICMP messages are not directly passed to the Data link layer. The message is first encapsulated inside IP datagrams before going to the lower layer.

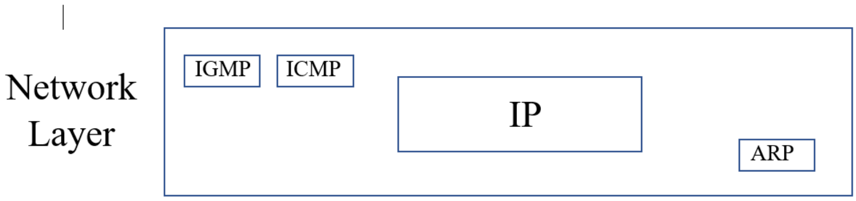


Figure 3: ICMP position.

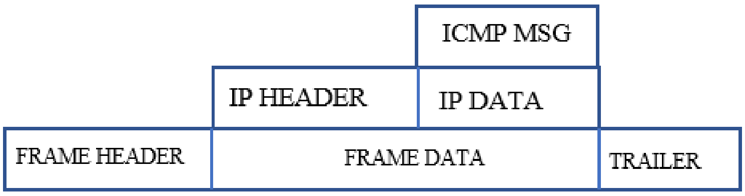


Figure 4: ICMP Encapsulation.

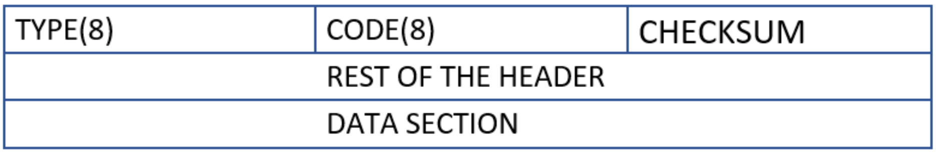
### 1.2.1 ICMP message

Two type of messages in ICMP:

1. ERROR REPORTING: They report problem that are router or a host may encounter whille processing of IP pocket.

2. QUERY: Fetch important/specific information from a router or host.

### 1.2.2 ICMP message format



| | | |
|---|---|---|
| TYPE(8) | CODE(8) | CHECKSUM |
| REST OF THE HEADER | | |
| DATA SECTION | | |

Figure 5: ICMP Format.

1. TYPES: Defines the msg type

2. CODE: Reason for message type

3. CHECKSUM: Error Checking

4. REST OF HEADER: Specified for each msg type

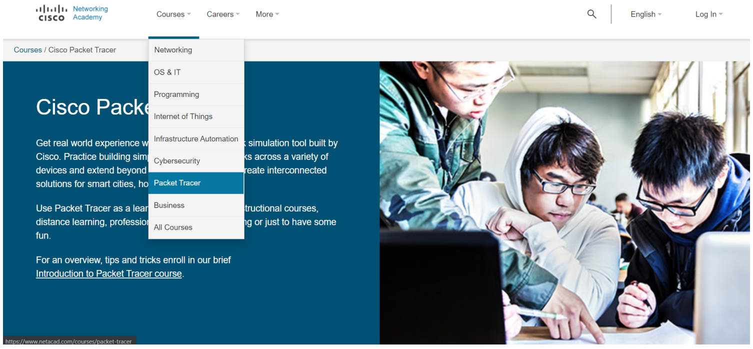
5. DATA SECTION: Find the original packet with error.for queries it carries extra infomartaion.

# 2 IMPLEMENTATION SETUP

## 2.1 Cisco Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command-line interface.

Step 1: Go to the website www.netacad.com



Get real world experience w k simulation tool built by Cisco. Practice building sim ks across a variety of devices and extend beyond reate interconnected solutions for smart cities, ho

Use Packet Tracer as a lear tructional courses, distance learning, professio ng or just to have some fun.

For an overview, tips and tricks enroll in our brief Introduction to Packet Tracer course.

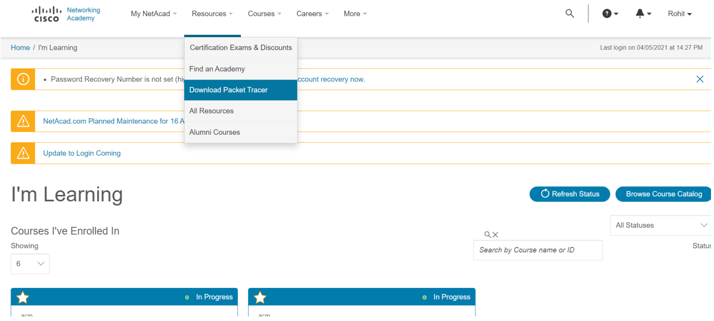
https://www.netacad.com/courses/packet-tracer

Step 2: Click the course tab and select Packet Tracer

Step 3: Click on the learn more button in the course intro to packet tracer

Step 4: Create an account

Step 5: After redirecting to new page, click on resources tab and download Packet Tracer



Last login on 04/05/2021 at 14:27 PM

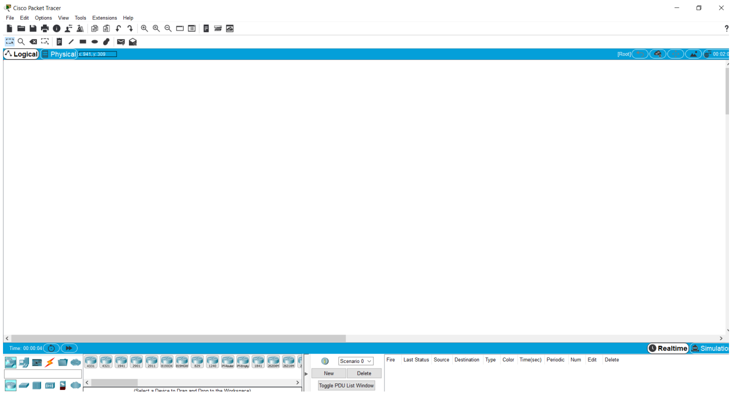
- Password Recovery Number is not set (hi ccount recovery now.

NetAcad.com Planned Maintenance for 16 A

Update to Login Coming

Step 6: Download the version according to your system

Step 7: Cisco Packet Tracer is ready to start the project



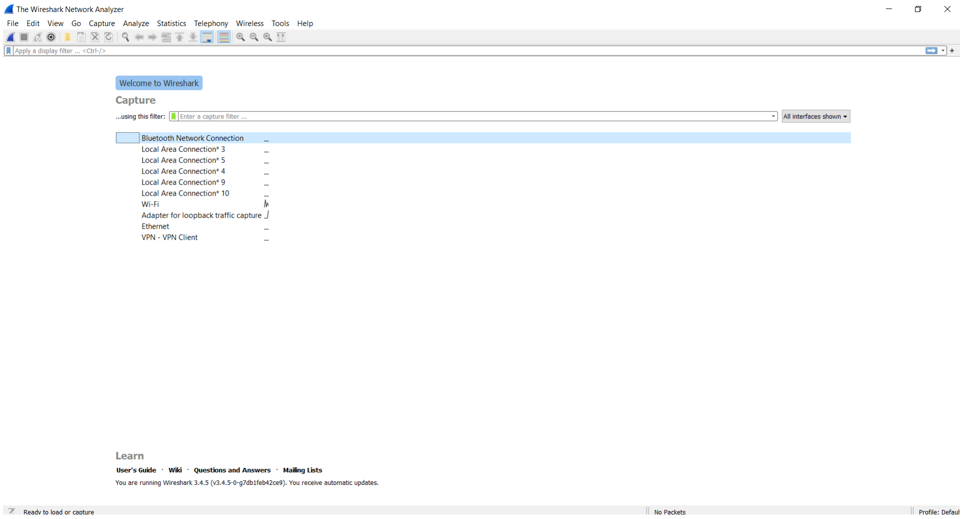
## 2.2 Wireshark

Wireshark is a free and open-source parcel analyzer. It is utilized for network investigating, examination, programming and interchanges convention improvement, and training.

Step 1: Go to the website www.wireshark.org/download.html

Step 2: Download the software according to your system

Step 3: Wireshark is ready to start


The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Bluetooth Network Connection
Local Area Connection* 3
Local Area Connection* 5
Local Area Connection* 4
Local Area Connection* 9
Local Area Connection* 10
Wi-Fi
Adapter for loopback traffic capture
Ethernet
VPN - VPN Client

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.4.5 (v3.4.5-0-g7db1feb42ce9). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Defaul

# 3 IMPLEMENTATION

## 3.1 ICMP Configuration

ICMP Protocol is generally used for troubleshooting activities. The main two troubleshooting commands for network engineers are “ping” and “traceroute” that works with Internet Control Message Protocol .

Ping is a utility used in computer network administration software to test the reachability of a host on an Internet Protocol (IP) network.

In the cisco packet tracer environment, we create a network that is shown in Fig. no. 6.

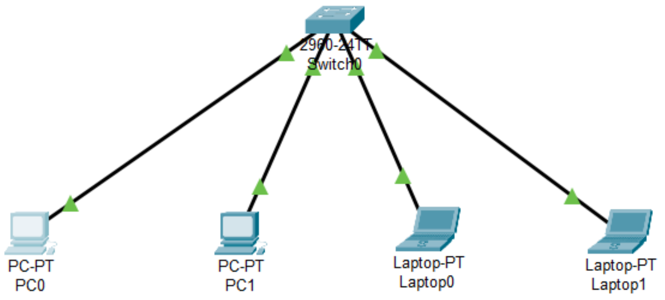
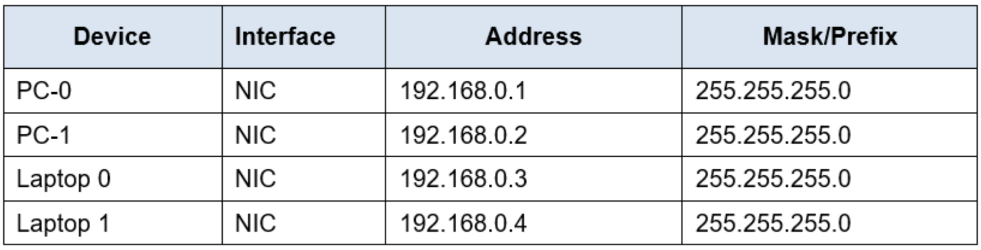


Figure 6: ICMP Configuration.

The 4 devices are connected with a switch and we assigned there stactic IP addresses and subnet masks.

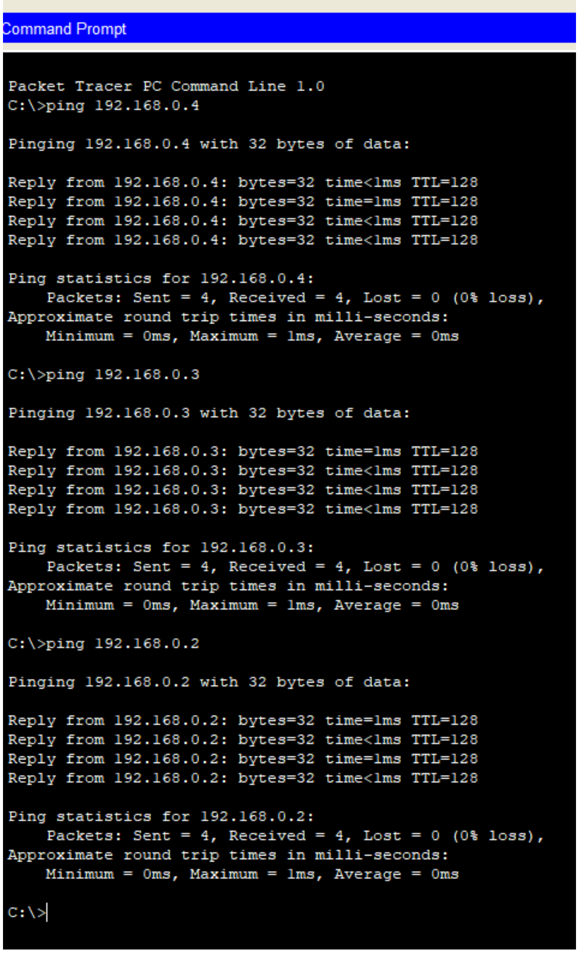


| Device | Interface | Address | Mask/Prefix |
|---|---|---|---|
| PC-0 | NIC | 192.168.0.1 | 255.255.255.0 |
| PC-1 | NIC | 192.168.0.2 | 255.255.255.0 |
| Laptop 0 | NIC | 192.168.0.3 | 255.255.255.0 |
| Laptop 1 | NIC | 192.168.0.4 | 255.255.255.0 |

Figure 7: IP address configuration.

Pinging from PC-0 to the other three systems is giving us a response as shown in Fig. No. 8. so that means the message can be sent among the system through the switch and has been checked by using ICMP protocol.

Table 1: Addressing table.



```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.4

Pinging 192.168.0.4 with 32 bytes of data:

Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Reply from 192.168.0.4: bytes=32 time=1ms TTL=128
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128
Reply from 192.168.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Reply from 192.168.0.3: bytes=32 time=1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128
Reply from 192.168.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128
Reply from 192.168.0.2: bytes=32 time=1ms TTL=128
Reply from 192.168.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

## 3.2 Connect two router and verify ICMP

In this experiment, there are 4 systems, 2 switch and 2 routers, as shown in Fig. No. 9. Two systems have been assigned with class A IP configuration, and the other two has been with class C configuration, and we are going to connect the class A and class C network and ping it.

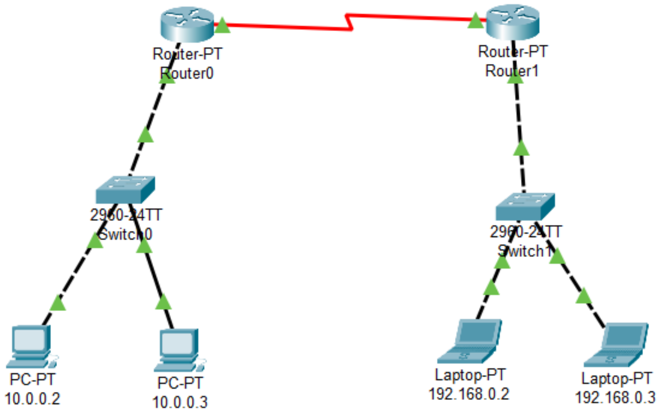
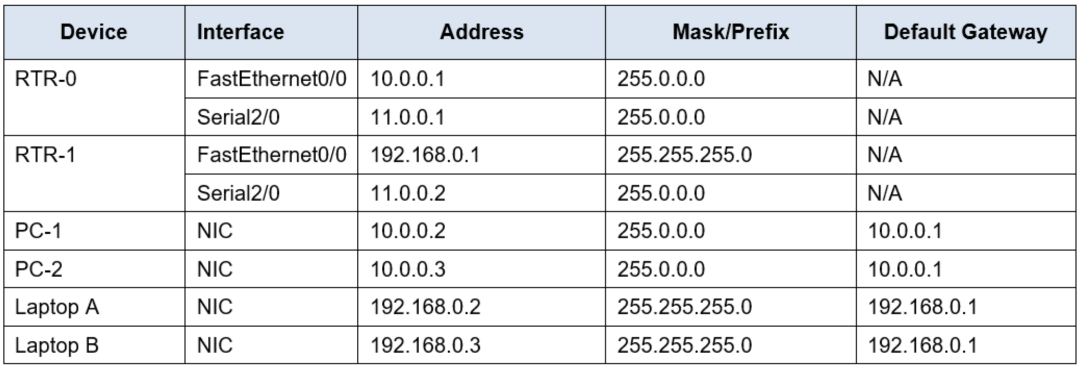


Figure 8: Experiment connection.

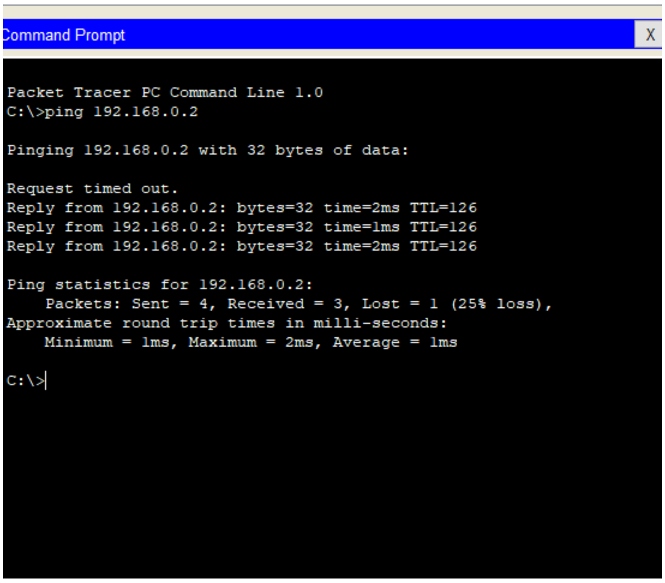
The IP addresses, the subnet mask and the default gateway has been configured as shown in the table no. 2. Running the ping command from

Table 2: Addressing table.



| Device | Interface | Address | Mask/Prefix | Default Gateway |
|---|---|---|---|---|
| RTR-0 | FastEthernet0/0 | 10.0.0.1 | 255.0.0.0 | N/A |
| | Serial2/0 | 11.0.0.1 | 255.0.0.0 | N/A |
| RTR-1 | FastEthernet0/0 | 192.168.0.1 | 255.255.255.0 | N/A |
| | Serial2/0 | 11.0.0.2 | 255.0.0.0 | N/A |
| PC-1 | NIC | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| PC-2 | NIC | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 |
| Laptop A | NIC | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 |
| Laptop B | NIC | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 |

the 10.0.0.2 to 192.168.0.2 we successfully get the response as shown in Fig. no. 10.



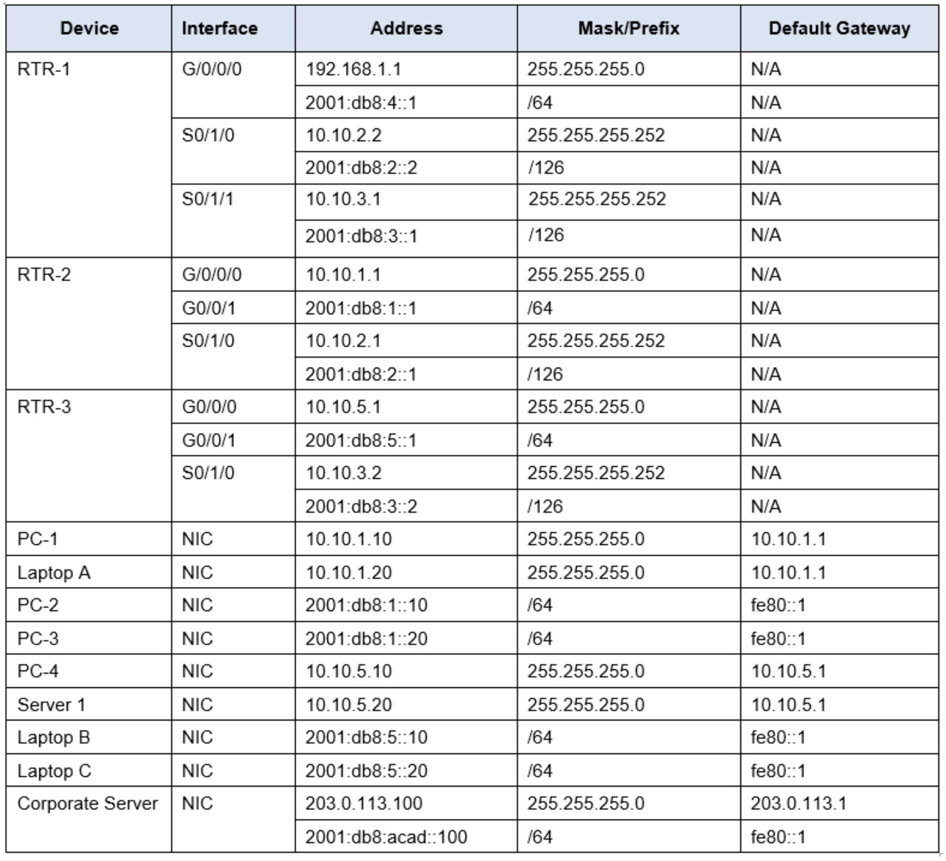
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.2: bytes=32 time=2ms TTL=126
Reply from 192.168.0.2: bytes=32 time=1ms TTL=126
Reply from 192.168.0.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Figure 9: Pinging to system.

## 3.3 Use ICMP to test and correct network connectivity

In this experiment, ICMP is used to test network connectivity and locate network problems and to correct simple configuration issues and restore connectivity to the network.

Table 3: Addressing table.



| Device | Interface | Address | Mask/Prefix | Default Gateway |
|---|---|---|---|---|
| RTR-1 | G/0/0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | | 2001:db8:4::1 | /64 | N/A |
| | S0/1/0 | 10.10.2.2 | 255.255.255.252 | N/A |
| | | 2001:db8:2::2 | /126 | N/A |
| | S0/1/1 | 10.10.3.1 | 255.255.255.252 | N/A |
| | | 2001:db8:3::1 | /126 | N/A |
| RTR-2 | G/0/0/0 | 10.10.1.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 2001:db8:1::1 | /64 | N/A |
| | S0/1/0 | 10.10.2.1 | 255.255.255.252 | N/A |
| | | 2001:db8:2::1 | /126 | N/A |
| RTR-3 | G0/0/0 | 10.10.5.1 | 255.255.255.0 | N/A |
| | G0/0/1 | 2001:db8:5::1 | /64 | N/A |
| | S0/1/0 | 10.10.3.2 | 255.255.255.252 | N/A |
| | | 2001:db8:3::2 | /126 | N/A |
| PC-1 | NIC | 10.10.1.10 | 255.255.255.0 | 10.10.1.1 |
| Laptop A | NIC | 10.10.1.20 | 255.255.255.0 | 10.10.1.1 |
| PC-2 | NIC | 2001:db8:1::10 | /64 | fe80::1 |
| PC-3 | NIC | 2001:db8:1::20 | /64 | fe80::1 |
| PC-4 | NIC | 10.10.5.10 | 255.255.255.0 | 10.10.5.1 |
| Server 1 | NIC | 10.10.5.20 | 255.255.255.0 | 10.10.5.1 |
| Laptop B | NIC | 2001:db8:5::10 | /64 | fe80::1 |
| Laptop C | NIC | 2001:db8:5::20 | /64 | fe80::1 |
| Corporate Server | NIC | 203.0.113.100 | 255.255.255.0 | 203.0.113.1 |
| | | 2001:db8:acad::100 | /64 | fe80::1 |

The addressing table of the given network is shown in Fig. no. 12, and in Fig. no. 11 it shows the connection, and there is some error in that some devices are unreachable from the corporate server, and our objective is to find that and restore the connectivity with the help of ping and trace with comparison to the addressing table.

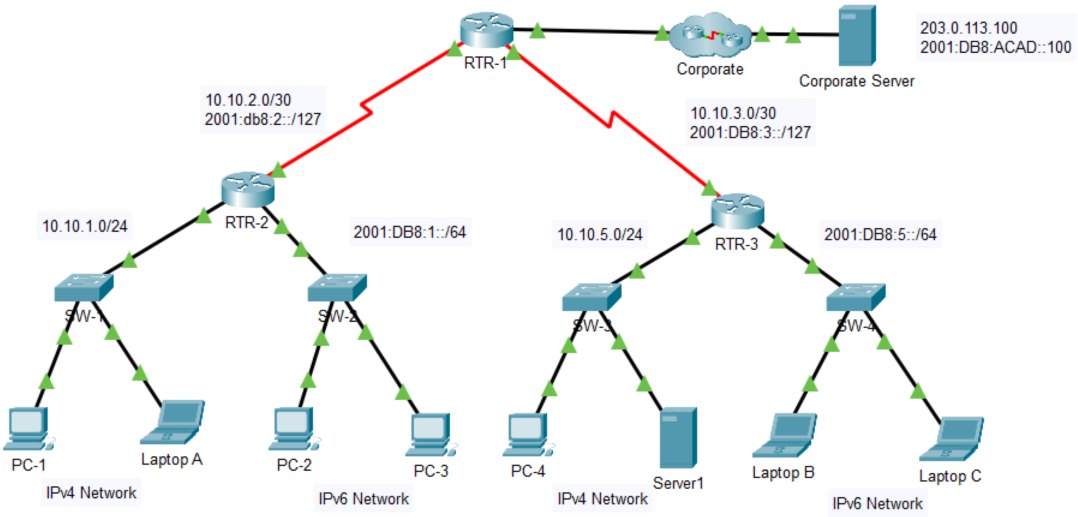


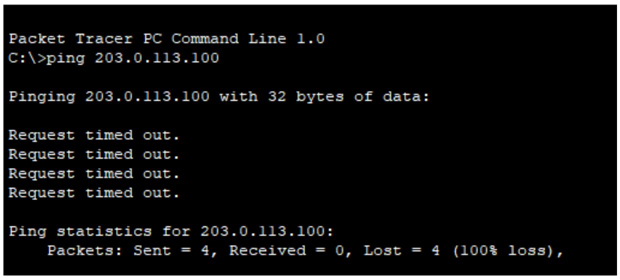
Figure 10: Experiment network connectivity.

Pinging to corporate server(IPv4:203.0.113.100 or IPv6:2001:db8:acad::100 ) from all the devices let us know which is unreachable.

First of all, for PC-1 of IPv4 address, we get a response from the server and again from Laptop-A of IPv4 address, we also get a response.

Next, we ping from PC-2 and PC-3 of IPv6 addresses we get a response.

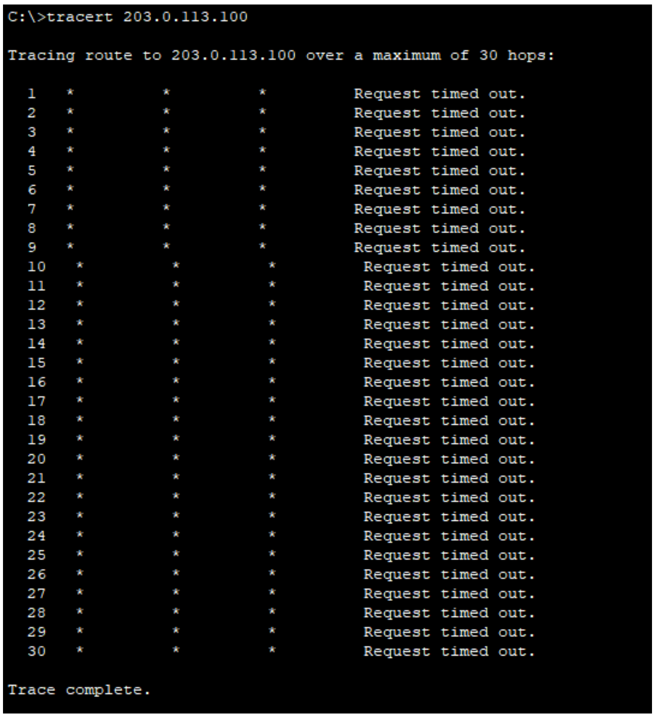
Next, we ping from PC-4 of IPv4 address, but we don't get a response as shown in Fig. no. 11.



```
Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.100

Pinging 203.0.113.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 203.0.113.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 11: Ping not response from PC-4 to coperate server.

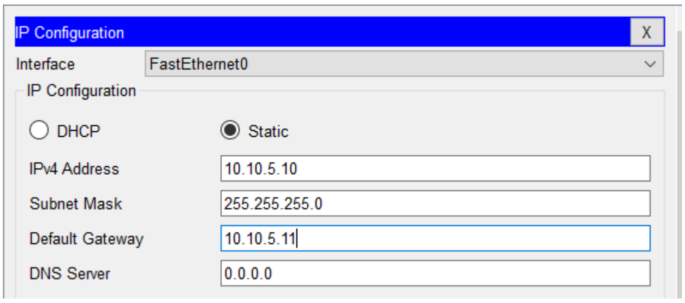
So, we will trace and identify the problem as shown in Fig. no. 12. Tracert is commands that display possible paths and measuring transit delays of packets across an IP network.



```
C:\>tracert 203.0.113.100

Tracing route to 203.0.113.100 over a maximum of 30 hops:

  1   *         *         *         Request timed out.
  2   *         *         *         Request timed out.
  3   *         *         *         Request timed out.
  4   *         *         *         Request timed out.
  5   *         *         *         Request timed out.
  6   *         *         *         Request timed out.
  7   *         *         *         Request timed out.
  8   *         *         *         Request timed out.
  9   *         *         *         Request timed out.
  10   *         *         *         Request timed out.
  11   *         *         *         Request timed out.
  12   *         *         *         Request timed out.
  13   *         *         *         Request timed out.
  14   *         *         *         Request timed out.
  15   *         *         *         Request timed out.
  16   *         *         *         Request timed out.
  17   *         *         *         Request timed out.
  18   *         *         *         Request timed out.
  19   *         *         *         Request timed out.
  20   *         *         *         Request timed out.
  21   *         *         *         Request timed out.
  22   *         *         *         Request timed out.
  23   *         *         *         Request timed out.
  24   *         *         *         Request timed out.
  25   *         *         *         Request timed out.
  26   *         *         *         Request timed out.
  27   *         *         *         Request timed out.
  28   *         *         *         Request timed out.
  29   *         *         *         Request timed out.
  30   *         *         *         Request timed out.

Trace complete.
```

Figure 12: Tracing.

Now, we know that it didn't go to its default gateway. So, we verify PC-4 with its addressing table, and now we get to know that the default gateway is 10.10.5.11 instead of 10.10.5.1. Now replace with correct default gateway as shown in Fig. No. 13.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.10.5.10

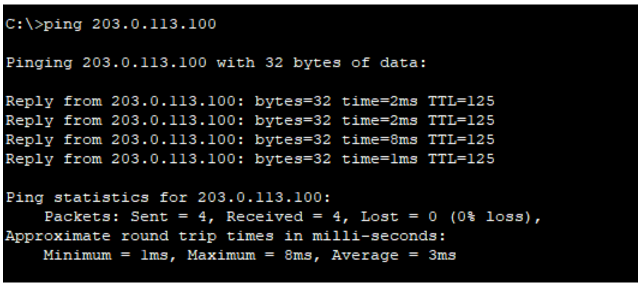
Subnet Mask: 255.255.255.0

Default Gateway: 10.10.5.11

DNS Server: 0.0.0.0

Figure 13: IP configuration.

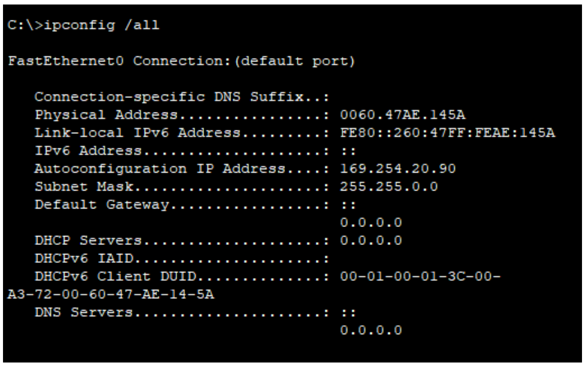
Now, we will trace again from PC-4 and it is showing response and get ping response as shown in Fig. no. 14.



```
C:\>ping 203.0.113.100

Pinging 203.0.113.100 with 32 bytes of data:

Reply from 203.0.113.100: bytes=32 time=2ms TTL=125
Reply from 203.0.113.100: bytes=32 time=2ms TTL=125
Reply from 203.0.113.100: bytes=32 time=8ms TTL=125
Reply from 203.0.113.100: bytes=32 time=1ms TTL=125

Ping statistics for 203.0.113.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

Figure 14: Pinging.

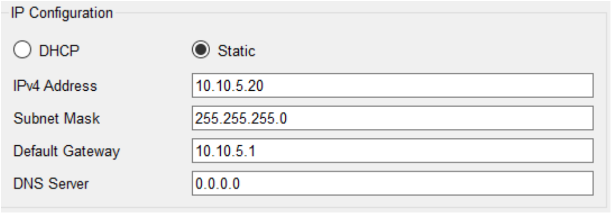
Next, we ping from server 1 to cooperate server, and it didn't get a response. So, we check the configuration using the command "ipconfig /all" as shown in Fig. no. 15, and we get to know that its IP address is DHCP.



```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.47AE.145A
   Link-local IPv6 Address.........: FE80::260:47FF:FEAE:145A
   IPv6 Address....................: ::
   Autoconfiguration IP Address....: 169.254.20.90
   Subnet Mask.....................: 255.255.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-3C-00-
A3-72-00-60-47-AE-14-5A
   DNS Servers.....................: ::
                                     0.0.0.0
```

Figure 15: Showing IP configuration.

Now we convert it to static IP address using the adressing table as shown in Fig. no. 16.



IP Configuration

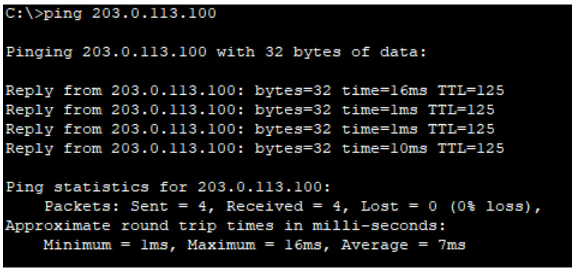
○ DHCP ● Static

| | |
|---|---|
| IPv4 Address | 10.10.5.20 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 10.10.5.1 |
| DNS Server | 0.0.0.0 |

Figure 16: Converting to static IP.

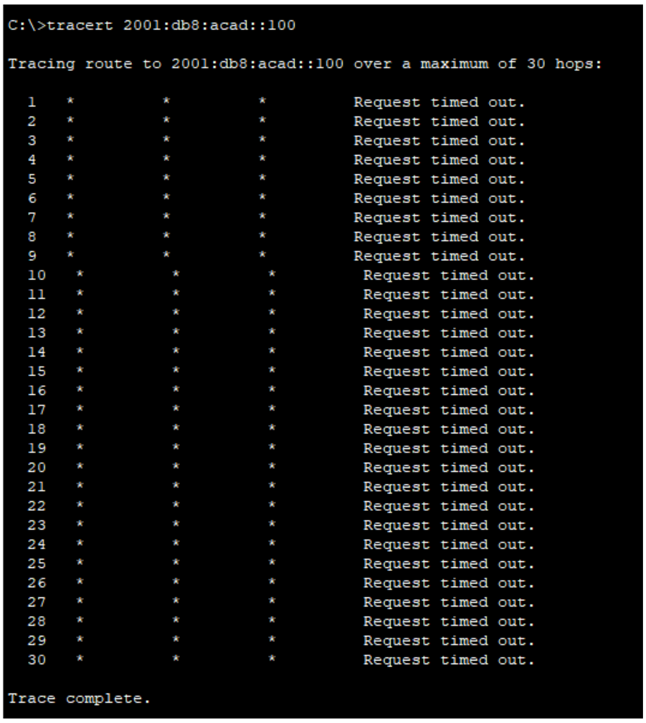
After that we again check for ping and we get the reply as shown in Fig. no. 17.

Next we go to laptop B and ping to coperate server and we didn't get a response and we used the "tracert" command to check and we found out that it didn't go to default gateway as shown in Fig. no. 18.



```
C:\>ping 203.0.113.100

Pinging 203.0.113.100 with 32 bytes of data:

Reply from 203.0.113.100: bytes=32 time=16ms TTL=125
Reply from 203.0.113.100: bytes=32 time=1ms TTL=125
Reply from 203.0.113.100: bytes=32 time=1ms TTL=125
Reply from 203.0.113.100: bytes=32 time=10ms TTL=125

Ping statistics for 203.0.113.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 16ms, Average = 7ms
```

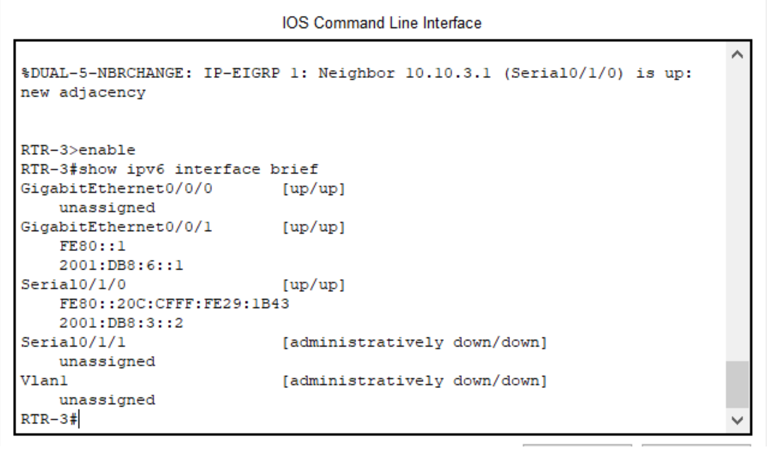
Figure 17: Ping response from coperate server to server 1 .



```
C:\>tracert 2001:db8:acad::100

Tracing route to 2001:db8:acad::100 over a maximum of 30 hops:

  1   *         *         *         Request timed out.
  2   *         *         *         Request timed out.
  3   *         *         *         Request timed out.
  4   *         *         *         Request timed out.
  5   *         *         *         Request timed out.
  6   *         *         *         Request timed out.
  7   *         *         *         Request timed out.
  8   *         *         *         Request timed out.
  9   *         *         *         Request timed out.
  10   *         *         *         Request timed out.
  11   *         *         *         Request timed out.
  12   *         *         *         Request timed out.
  13   *         *         *         Request timed out.
  14   *         *         *         Request timed out.
  15   *         *         *         Request timed out.
  16   *         *         *         Request timed out.
  17   *         *         *         Request timed out.
  18   *         *         *         Request timed out.
  19   *         *         *         Request timed out.
  20   *         *         *         Request timed out.
  21   *         *         *         Request timed out.
  22   *         *         *         Request timed out.
  23   *         *         *         Request timed out.
  24   *         *         *         Request timed out.
  25   *         *         *         Request timed out.
  26   *         *         *         Request timed out.
  27   *         *         *         Request timed out.
  28   *         *         *         Request timed out.
  29   *         *         *         Request timed out.
  30   *         *         *         Request timed out.

Trace complete.
```

Figure 18: Tracing.

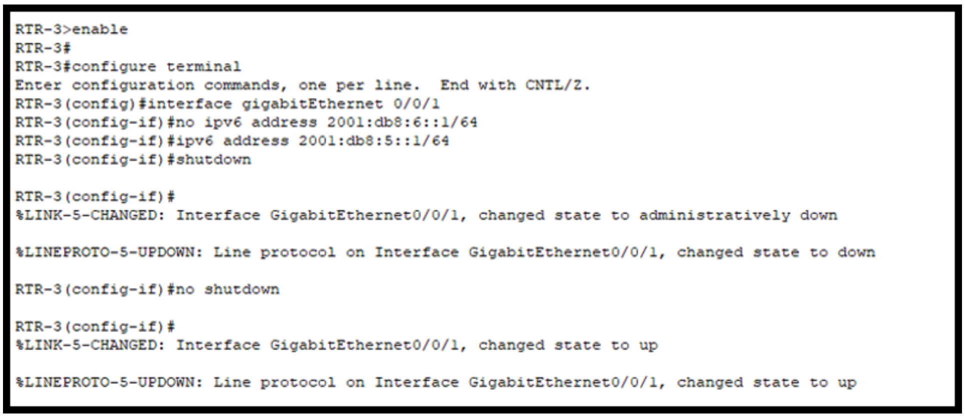
Next, we verify IP configuration with the addressing table, and we found it to be correct. Now, we go to router RTR-3 and proceed with the following command as shown in the Fig. no. 19 and we found out that IP configuration is incorrect while comparing with the addressing table.



```
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.3.1 (Serial0/1/0) is up:
new adjacency


RTR-3>enable
RTR-3#show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    unassigned
GigabitEthernet0/0/1       [up/up]
    FE80::1
    2001:DB8:6::1
Serial0/1/0                [up/up]
    FE80::20C:CFFF:FE29:1B43
    2001:DB8:3::2
Serial0/1/1                [administratively down/down]
    unassigned
Vlan1                      [administratively down/down]
    unassigned
RTR-3#
```

Figure 19: Checking IP confirugation in router.

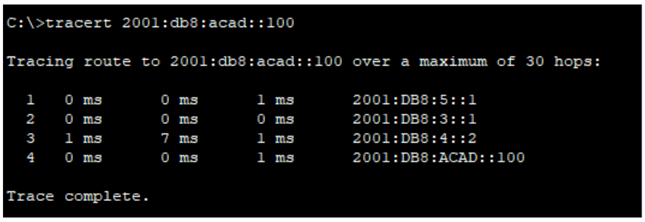
Now we re-assigned the IP address using the follwing command as shown in the Fig. no. 20.



```
RTR-3>enable
RTR-3#
RTR-3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-3(config)#interface gigabitEthernet 0/0/1
RTR-3(config-if)#no ipv6 address 2001:db8:6::1/64
RTR-3(config-if)#ipv6 address 2001:db8:5::1/64
RTR-3(config-if)#shutdown

RTR-3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to down

RTR-3(config-if)#no shutdown

RTR-3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

Figure 20: Changing IP address in router.

And now we re-do the trace in laptop B and it got response and ping was successfull.



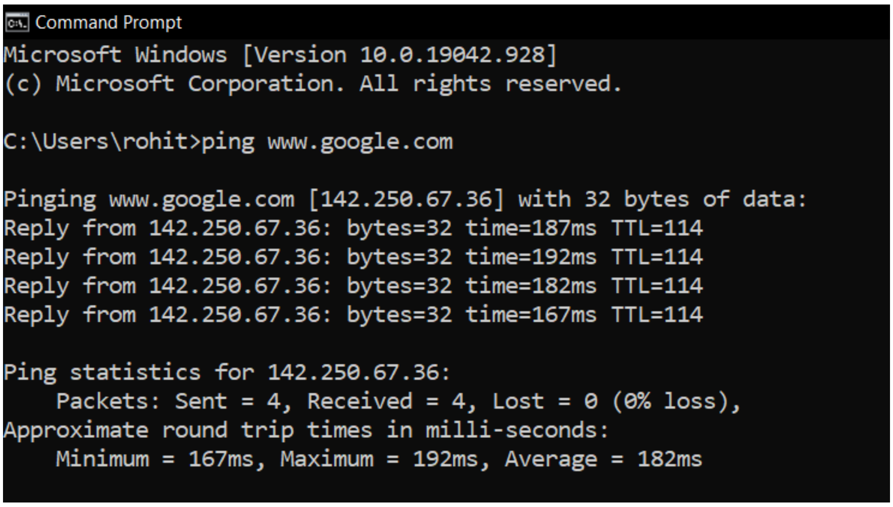
```
C:\>tracert 2001:db8:acad::100

Tracing route to 2001:db8:acad::100 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      2001:DB8:5::1
  2    0 ms      0 ms      0 ms      2001:DB8:3::1
  3    1 ms      7 ms      1 ms      2001:DB8:4::2
  4    0 ms      0 ms      1 ms      2001:DB8:ACAD::100

Trace complete.
```

Figure 21: Tracing.

Finally, we check for last system laptop C and we get responsed.

## 3.4 ICMP packets capture using Wireshark

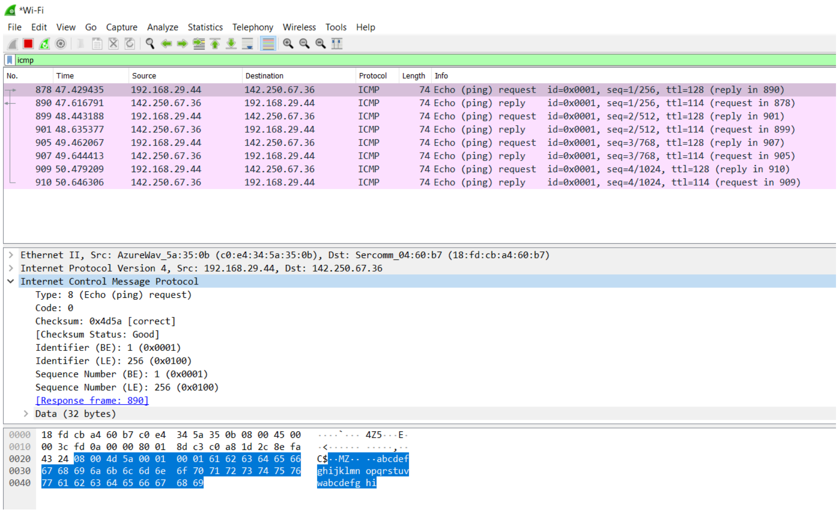
First we ping to www.google.com in the command prompt and we get a reply.As this is ICMP request packet so we can see source IP as my system IP address and destination IP as Google's one IP address. Also IP layer mentioned the protocol as ICMP.



```
Microsoft Windows [Version 10.0.19042.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rohit>ping www.google.com

Pinging www.google.com [142.250.67.36] with 32 bytes of data:
Reply from 142.250.67.36: bytes=32 time=187ms TTL=114
Reply from 142.250.67.36: bytes=32 time=192ms TTL=114
Reply from 142.250.67.36: bytes=32 time=182ms TTL=114
Reply from 142.250.67.36: bytes=32 time=167ms TTL=114

Ping statistics for 142.250.67.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 167ms, Maximum = 192ms, Average = 182ms
```

Figure 22: Pinging to google

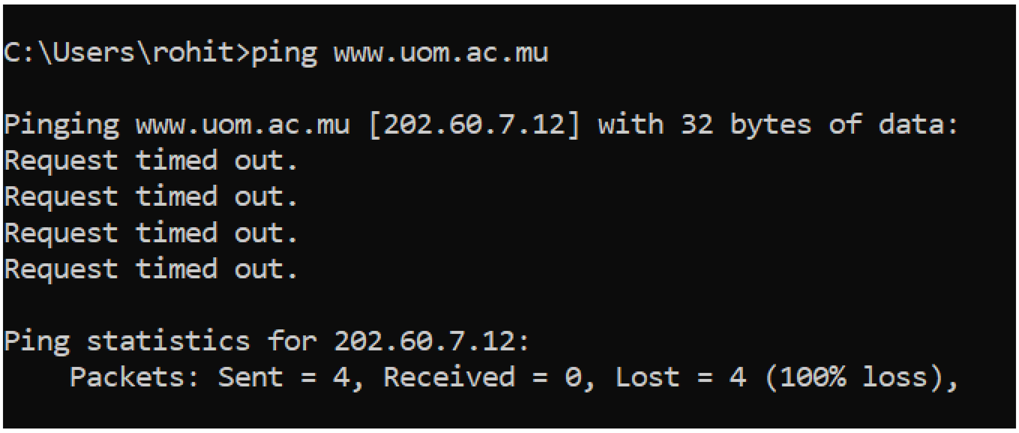
The same thing we can see it in wireshark as shown below figure with the ICMP message format.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.  Time       Source         Destination    Protocol Length Info
 878 47.429435  192.168.29.44  142.250.67.36  ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (reply in 890)
 890 47.616791  142.250.67.36  192.168.29.44  ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=114 (request in 878)
 899 48.443188  192.168.29.44  142.250.67.36  ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 901)
 901 48.635377  142.250.67.36  192.168.29.44  ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=114 (request in 899)
 905 49.462067  192.168.29.44  142.250.67.36  ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 907)
 907 49.644413  142.250.67.36  192.168.29.44  ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=114 (request in 905)
 909 50.479209  192.168.29.44  142.250.67.36  ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 910)
 910 50.646306  142.250.67.36  192.168.29.44  ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=114 (request in 909)

> Ethernet II, Src: AzureWav_5a:35:0b (c0:e4:34:5a:35:0b), Dst: Sercomm_04:60:b7 (18:fd:cb:a4:60:b7)
> Internet Protocol Version 4, Src: 192.168.29.44, Dst: 142.250.67.36
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 890]
  > Data (32 bytes)

0000  18 fd cb a4 60 b7 c0 e4  34 5a 35 0b 08 00 45 00   ····`··· 4Z5···E·
0010  00 3c fd 0a 00 00 80 01  8d c3 c0 a8 1d 2c 8e fa   ·<······ ·····,··
0020  43 24 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   C$··MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Figure 23: Wireshark- Pinging to google

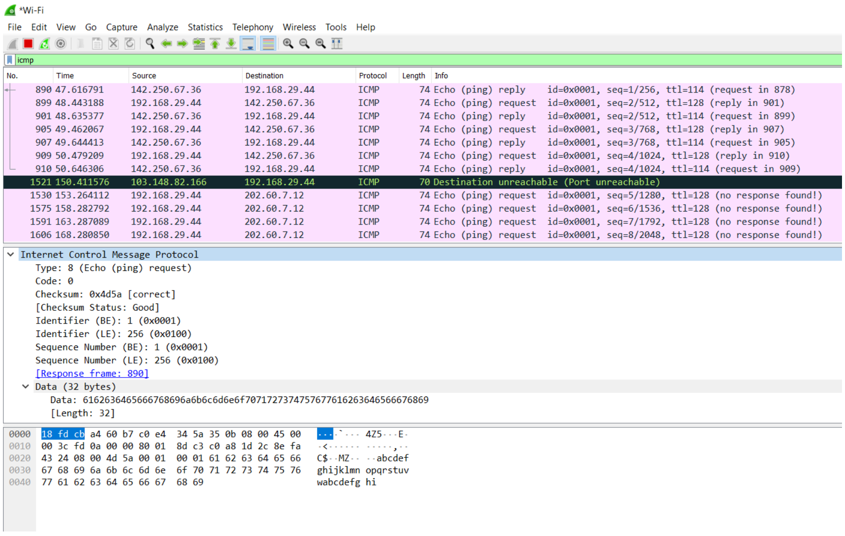
Now we again ping to www.uom.ac.wu and we didn't get the reply as shown in below figure.



```
C:\Users\rohit>ping www.uom.ac.mu

Pinging www.uom.ac.mu [202.60.7.12] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 202.60.7.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 24: Pinging to www.uom.ac.wu

The same thing we can see it in wireshark as shown below figure 25 with the ICMP message format.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.     Time        Source           Destination      Protocol  Length Info
    890 47.616791   142.250.67.36    192.168.29.44    ICMP      74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=114 (request in 878)
    899 48.443188   192.168.29.44    142.250.67.36    ICMP      74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 901)
    901 48.635377   142.250.67.36    192.168.29.44    ICMP      74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=114 (request in 899)
    905 49.462067   192.168.29.44    142.250.67.36    ICMP      74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 907)
    907 49.644413   142.250.67.36    192.168.29.44    ICMP      74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=114 (request in 905)
    909 50.479209   192.168.29.44    142.250.67.36    ICMP      74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 910)
    910 50.646306   142.250.67.36    192.168.29.44    ICMP      74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=114 (request in 909)
   1521 150.411576  103.148.82.166   192.168.29.44    ICMP      70 Destination unreachable (Port unreachable)
   1530 153.264112  192.168.29.44    202.60.7.12      ICMP      74 Echo (ping) request  id=0x0001, seq=5/1280, ttl=128 (no response found!)
   1575 158.282792  192.168.29.44    202.60.7.12      ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (no response found!)
   1591 163.287089  192.168.29.44    202.60.7.12      ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (no response found!)
   1606 168.280850  192.168.29.44    202.60.7.12      ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (no response found!)
```

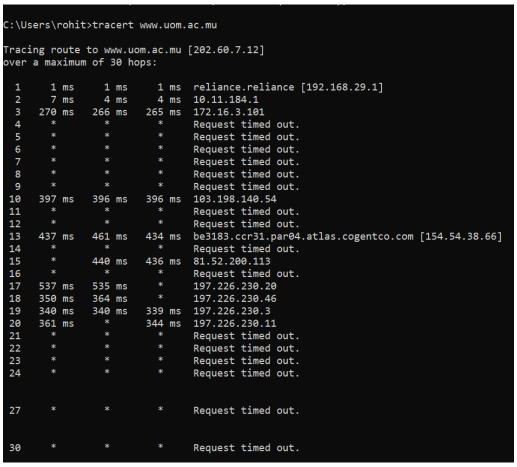
```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 890]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  18 fd cb a4 60 b7 c0 e4  34 5a 35 0b 08 00 45 00   ···`··· 4Z5···E·
0010  00 3c fd 0a 00 00 80 01  8d c3 c0 a8 1d 2c 8e fa   ·<······ ·····,··
0020  43 24 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   C$··MZ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Figure 25: Wireshark- Pinging to www.uom.ac.wu

This doesn't mean that the server is unreachable , this means that the ICMP message were block by the firewall o the destination address.

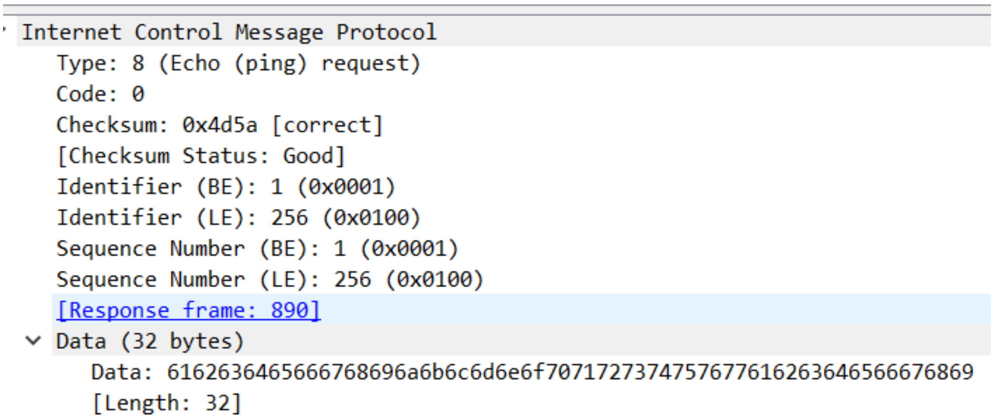
Now, Lets us look at the TRACEROUTE as shown in below figure.



```
C:\Users\rohit>tracert www.uom.ac.mu

Tracing route to www.uom.ac.mu [202.60.7.12]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  reliance.reliance [192.168.29.1]
  2     7 ms     4 ms     4 ms  10.11.184.1
  3   270 ms   266 ms   265 ms  172.16.3.101
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10   397 ms   396 ms   396 ms  103.198.140.54
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13   437 ms   461 ms   434 ms  be3183.ccr31.par04.atlas.cogentco.com [154.54.38.66]
 14     *        *        *     Request timed out.
 15     *      440 ms   436 ms  81.52.200.113
 16     *        *        *     Request timed out.
 17   537 ms   535 ms     *     197.226.230.20
 18   350 ms   364 ms     *     197.226.230.46
 19   340 ms   340 ms   339 ms  197.226.230.3
 20   361 ms     *      344 ms  197.226.230.11
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.


 27     *        *        *     Request timed out.


 30     *        *        *     Request timed out.
```

Figure 26: tracing to to www.uom.ac.wu

The same thing we can see it in wireshark as shown below figure with the ICMP message format.



```
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0x4d5a [correct]
   [Checksum Status: Good]
   Identifier (BE): 1 (0x0001)
   Identifier (LE): 256 (0x0100)
   Sequence Number (BE): 1 (0x0001)
   Sequence Number (LE): 256 (0x0100)
   [Response frame: 890]
 Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

Figure 27: ICMP message format using Wireshark

We can see from this the ICMP has been rerturn , It has been highlighted to show us that there as not been a response. Also it has been prove that it can be used a diagnosed network issues.

# 4 Conclusion

We have configured ICMP , connect 2 routers and verify ICMP, Use ICMP to test and correct network connectivity, Use wireshark to show the message formate of the ICMP by pinging and tracing. By performing the experiment, we get that ICMP plays an important role in IP protocol that its connection issued is solved and detect by ICMP protocol by using the ping and tracert command.

# 5 Reference

1. Introduction to Packet Tracer by NETACAD
2. The Internet and its protocols by Adrian Farrel
3. Internet Control Message Protocol (ICMP) by GeeksforGeeks
4. INTERNET CONTROL MESSAGE PROTOCOL by J. Postel September 1981