

Practical 4

Aim: Demonstrate the Dynamic routing configuration using RIP and OSPF protocol using cisco packet tracer

Theory:

Dynamic routing:

- It is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes.
- Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
- Dynamic routing protocols allow routers to share information about the network with other routers to allow them to select the best path to reach a destination.

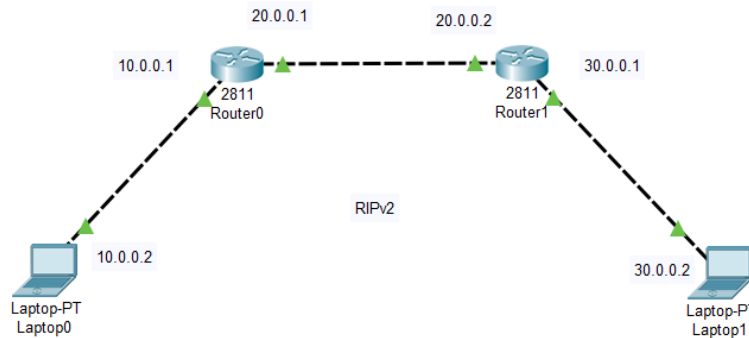
- RIP:
 1. Routing Information Protocol version 2 (RIPv2) is an old routing protocol.
 2. RIPv2 suffers from scalability issues due to a relatively low maximum hop count of 15 routing devices.

- OSPF:
 1. OSPF is the dynamic routing protocol used in large to very large IP networks.
 2. The protocol uses a link-state database and link-state advertisements to map the network topology.

- Advantages of Dynamic Routing:
 1. Allows the exchange of routing information whenever the network experiences a change in topology.
 2. Since the routes do not have to be configured manually, there is less administrative overhead.
 3. Less error-prone than static routing.
 4. Allows scalability since there is less administrative overhead involved.

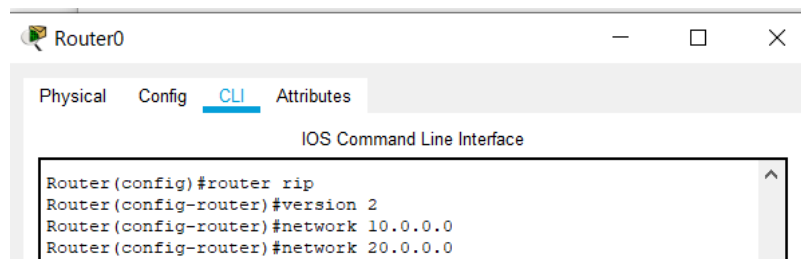
Configuration Using RIPv2:

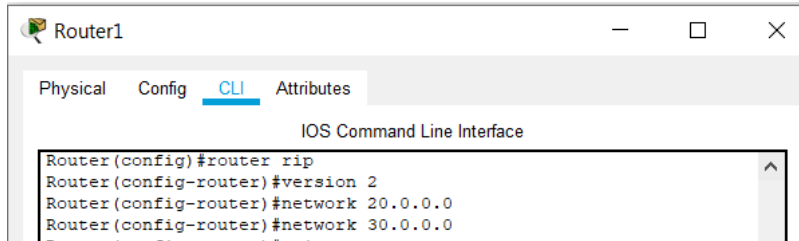
Topology:



Steps of Configurations:

- First of all to create a topology, click on the device and drop on workplace and connect all the devices with the necessary cables.
- Then configure all the router using CLI and give the ip address as mention in the topology diagram.
 1. Router 1: fa0/0 10.0.0.1
 fa0/1 20.0.0.1
 2. Router 2: fa0/0 20.0.0.2
 fa0/1 30.0.0.1
- Provide ip address and default gateway to the laptops.
 1. Laptop 1: ip address is 10.0.0.2
 default gateway is 10.0.0.1
 2. Laptop 2: ip address is 30.0.0.2
 default gateway is 30.0.0.1
- Configuration of RIPv2 on router 0 and router 1 are respectively,



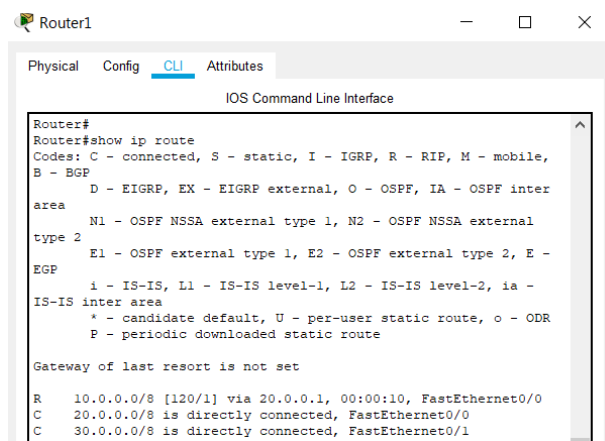


```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 20.0.0.0
Router(config-router)#network 30.0.0.0

```

- Verify RIP configuration.



```

Router1
Physical Config CLI Attributes
IOS Command Line Interface
Router#
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
       area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
       type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
       EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set

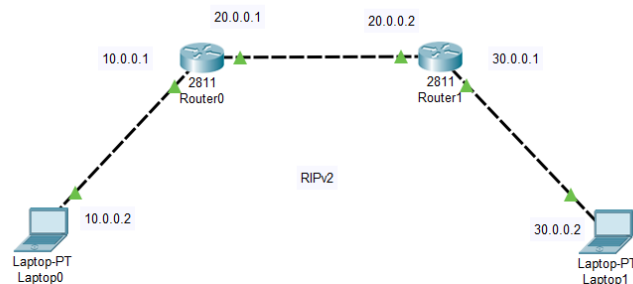
R    10.0.0.0/8 [120/1] via 20.0.0.1, 00:00:10, FastEthernet0/0
C    20.0.0.0/8 is directly connected, FastEthernet0/0
C    30.0.0.0/8 is directly connected, FastEthernet0/1

```

Checking Network Topology:

1. Message passing:

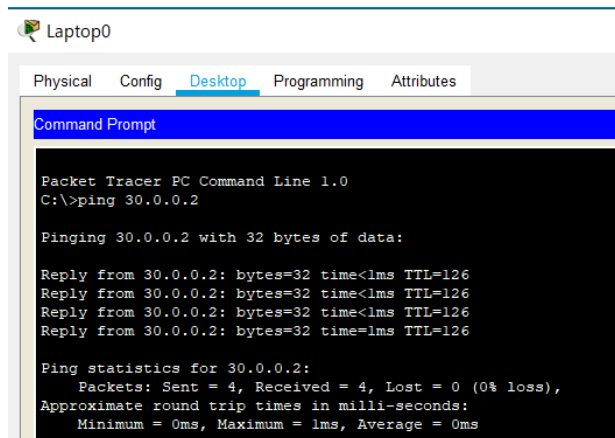
To check the connections are working properly or not drop one package on a Laptop 0 and receive it from the Laptop 1.



0	Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
		Successful	Laptop0	Laptop1	ICMP		0.000	N	0	(edit)	
		Successful	Laptop1	Laptop0	ICMP		0.000	N	1	(edit)	

2. Using ping:

Write a command ping 10.0.0.2 (ip address of the destination Laptop) from the command prompt of Laptop having ip address 30.0.0.2 (the source Laptop).



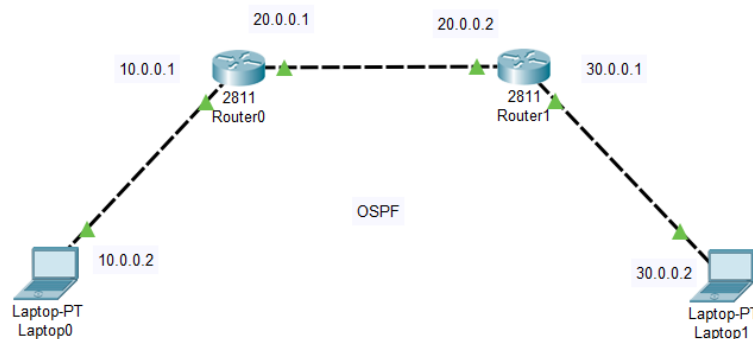
```

Laptop0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 30.0.0.2

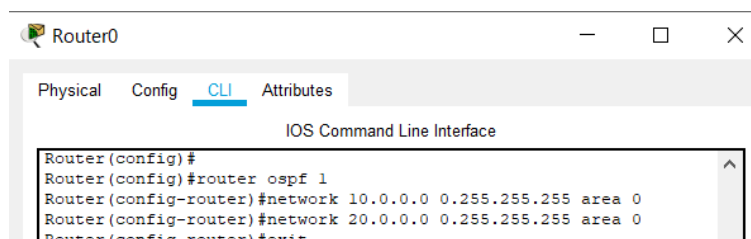
Pinging 30.0.0.2 with 32 bytes of data:

Reply from 30.0.0.2: bytes=32 time<1ms TTL=126
Reply from 30.0.0.2: bytes=32 time<1ms TTL=126
Reply from 30.0.0.2: bytes=32 time<1ms TTL=126
Reply from 30.0.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 30.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
  
```

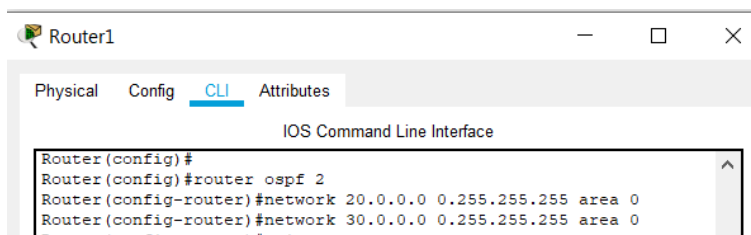
Configuration Using RIPv2:**Topology:****Steps of Configurations:**

- Configuration of OSPF on router 0 and router 1 are respectively,

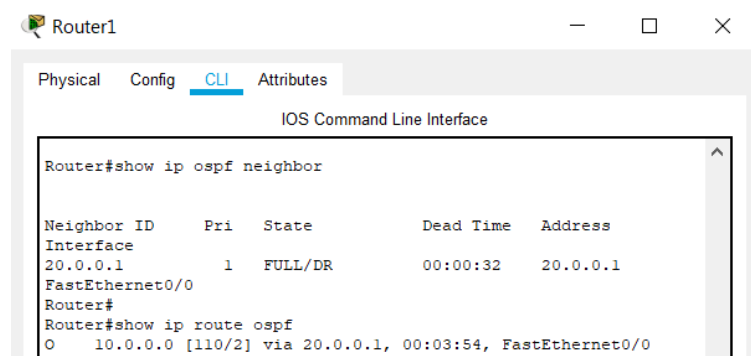


```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 0.255.255.255 area 0
Router(config-router)#network 20.0.0.0 0.255.255.255 area 0
Router(config-router)#exit
  
```



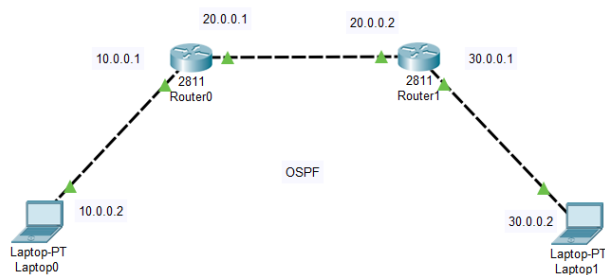
- Verify OSPF configuration.



Checking Network Topology:

1. Message passing:

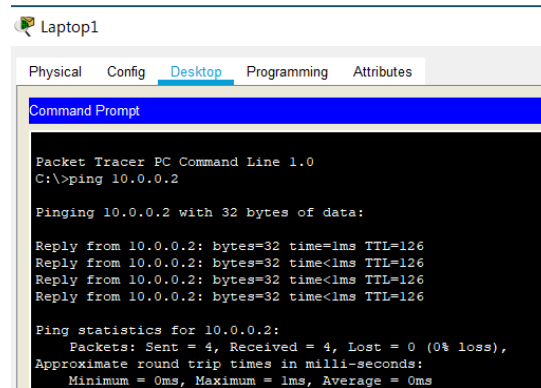
To check the connections are working properly or not drop one package on a Laptop 1 and receive it from the Laptop 0.



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop0	Laptop1	ICMP		0.000	N	0	(edit)	
	Successful	Laptop1	Laptop0	ICMP		0.000	N	1	(edit)	

2. Using ping:

Write a command ping 30.0.0.2 (ip address of the destination Laptop) from the command prompt of Laptop having ip address 10.0.0.2 (the source Laptop).



```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126
Reply from 10.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Conclusion:

Through this practical I learned about how to configure dynamic routing of routers using RIPv2 and OSPF protocol in different networks.

Practical 5

Aim: Demonstrate the EIGRP and BGP protocol configuration using cisco packet tracer.

Theory:

BGP Protocol:

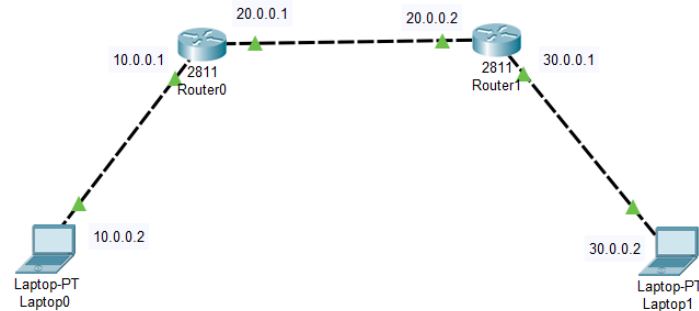
- Border Gateway Protocol (BGP) is an Internet Engineering Task Force (IETF) standard, and the most scalable of all routing protocols.
- BGP is the routing protocol of the global Internet, as well as for Service Provider private networks.
- BGP has expanded upon its original purpose of carrying Internet reachability information, and can now carry routes for Multicast, IPv6, VPNs, and a variety of other data.
- Cisco supports all IETF BGP standards, as well as most or all Internet Drafts for BGP. In addition, Cisco is an active participant in the BGP working groups at the IETF and a frequent contributor of new BGP extensions.

EIGRP Protocol:

- Enhanced Interior Gateway Routing Protocol (EIGRP) is an interior gateway protocol suited for many different topologies and media.
- In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic.
- Very low usage of network resources during normal operation; only hello packets are transmitted on a stable network
- When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load the routing protocol itself places on the network
- Rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous)
- EIGRP is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

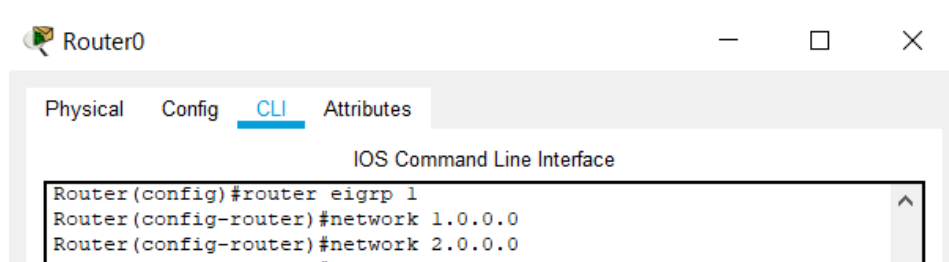
EIGRP protocol configuration:

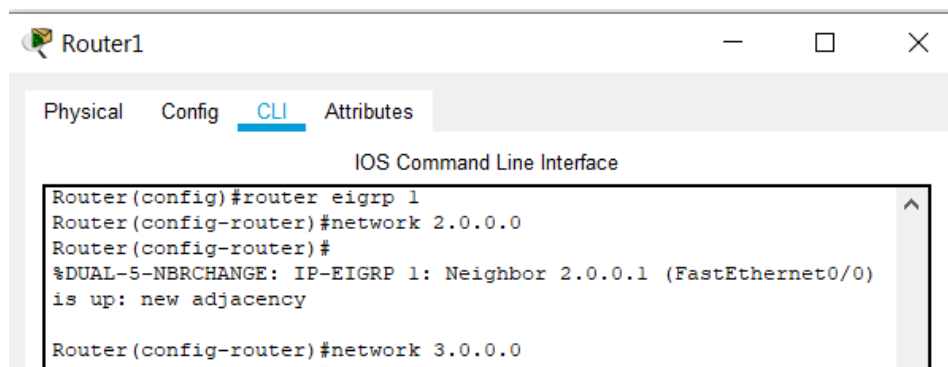
Topology:



Steps of Configurations:

- First of all to create a topology, click on the device and drop on workplace and connect all the devices with the necessary cables.
- Then configure all the router using CLI and give the ip address as mention in the topology diagram.
 - Router 1: fa0/0 1.0.0.1
 fa0/1 2.0.0.1
 - Router 2: fa0/0 2.0.0.2
 fa0/1 3.0.0.1
- Provide ip address and default gateway to the laptops.
 - Laptop 1: ip address is 1.0.0.2
 default gateway is 1.0.0.1
 - Laptop 2: ip address is 3.0.0.2
 default gateway is 3.0.0.1
- Configuration of EIGRP on router 0 and router 1 are respectively,





Router1

Physical Config **CLI** Attributes

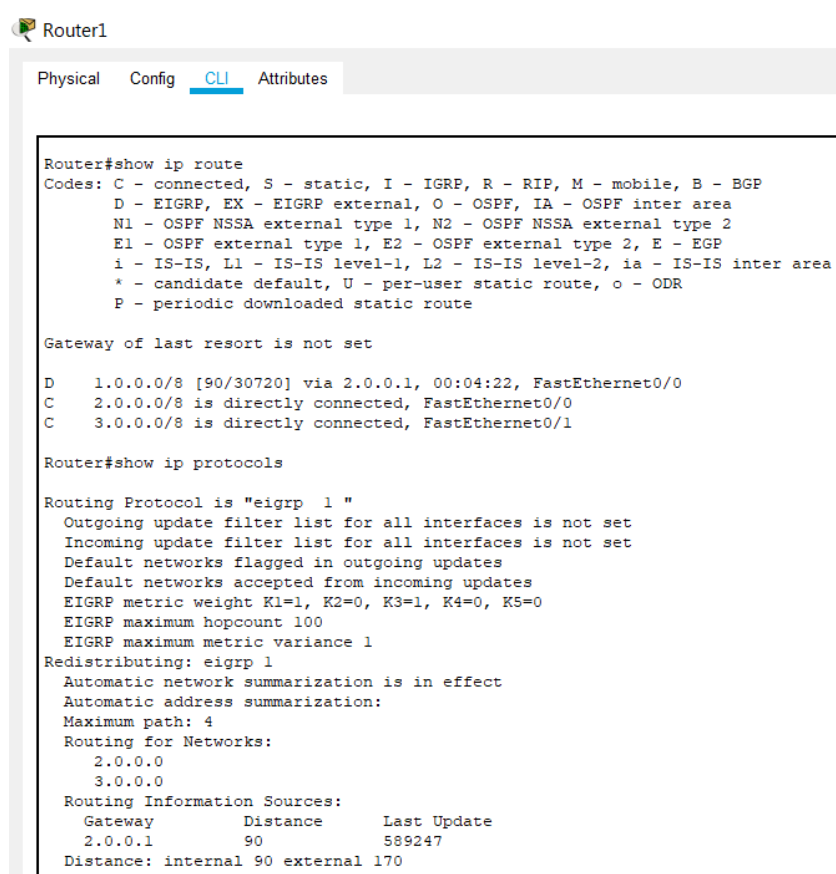
IOS Command Line Interface

```

Router(config)#router eigrp 1
Router(config-router)#network 2.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 2.0.0.1 (FastEthernet0/0)
is up: new adjacency
Router(config-router)#network 3.0.0.0

```

- Verify EIGRP configuration.



Router1

Physical Config **CLI** Attributes

```

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    1.0.0.0/8 [90/30720] via 2.0.0.1, 00:04:22, FastEthernet0/0
C    2.0.0.0/8 is directly connected, FastEthernet0/0
C    3.0.0.0/8 is directly connected, FastEthernet0/1

Router#show ip protocols

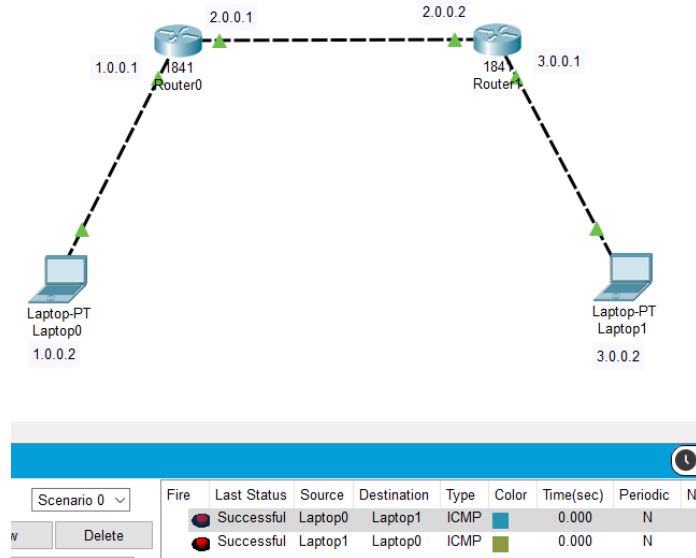
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
    Automatic network summarization is in effect
    Automatic address summarization:
      Maximum path: 4
  Routing for Networks:
    2.0.0.0
    3.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    2.0.0.1          90           589247
  Distance: internal 90 external 170

```

Checking Network Topology:

3. Message passing:

To check the connections are working properly or not drop one package on a Laptop 0 and receive it from the Laptop 1.



4. Using ping:

Write a command ping 1.0.0.2 (ip address of the destination Laptop) from the command prompt of Laptop having ip address 3.0.0.2 (the source Laptop).

Laptop1

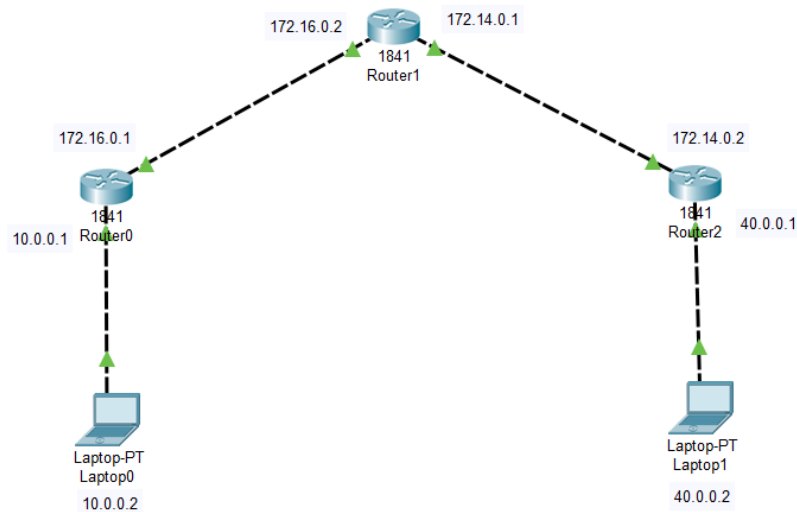
```

Packet Tracer PC Command Line 1.0
C:\>ping 1.0.0.2

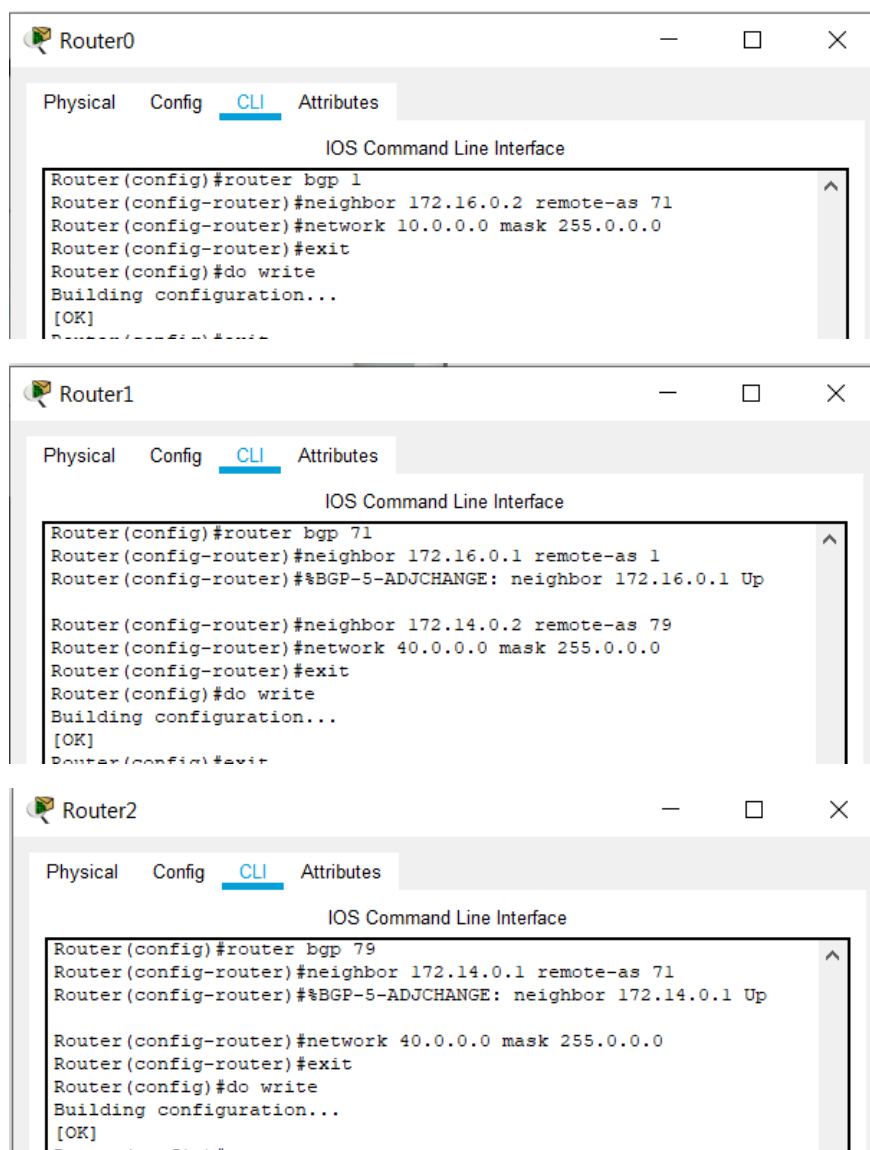
Pinging 1.0.0.2 with 32 bytes of data:

Reply from 1.0.0.2: bytes=32 time<1ms TTL=126
Reply from 1.0.0.2: bytes=32 time<1ms TTL=126
Reply from 1.0.0.2: bytes=32 time<1ms TTL=126
Reply from 1.0.0.2: bytes=32 time<1ms TTL=126

Ping statistics for 1.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
  
```

BGP protocol configuration:**Topology:****Steps of Configurations:**

- First of all to create a topology, click on the device and drop on workplace and connect all the devices with the necessary cables.
- Then configure all the router using CLI and give the ip address as mention in the topology diagram.
 - Router 1: fa0/0 10.0.0.1
fa0/1 172.16.0.1
 - Router 2: fa0/0 172.16.0.2
fa0/1 172.14.0.1
 - Router 2: fa0/0 172.14.0.2
fa0/1 40.0.0.1
- Provide ip address and default gateway to the laptops.
 - Laptop 1: ip address is 10.0.0.2
default gateway is 10.0.0.1
 - Laptop 2: ip address is 40.0.0.2
default gateway is 40.0.0.1
- Configuration of BGP on router 0, router 1 and router 2 are respectively,



- Verify BGP configuration.

```

Router2
Physical Config CLI Attributes
IOS Command Line Interface

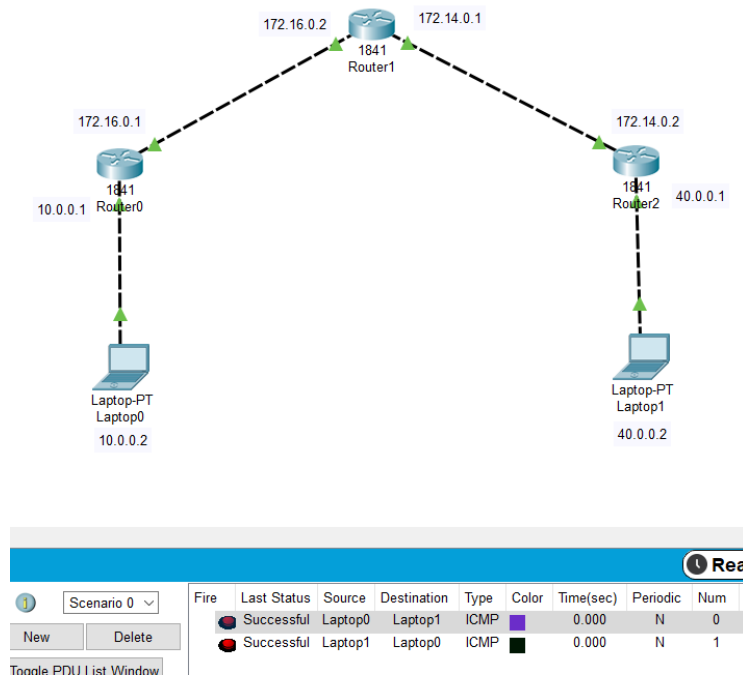
Router#show ip bgp summary
BGP router identifier 172.14.0.2, local AS number 79
BGP table version is 4, main routing table version 6
3 network entries using 396 bytes of memory
3 path entries using 156 bytes of memory
2/1 BGP path/bestpath attribute entries using 276 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 932 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor      V   AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/
Down State/PfxRcd
172.14.0.1    4   71      7      5      4   0   0
00:03:24      4
  
```

Checking Network Topology:

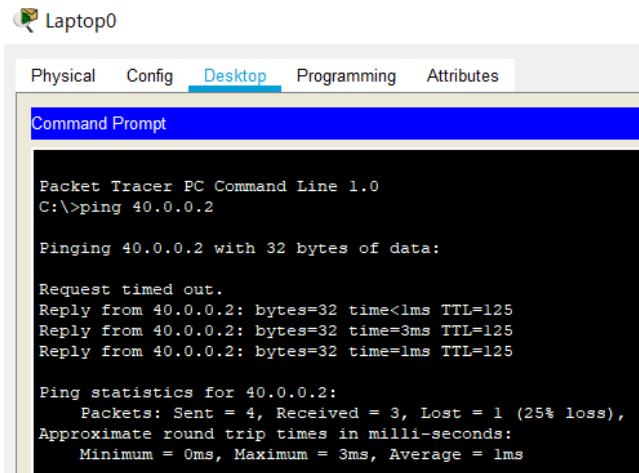
1. Message passing:

To check the connections are working properly or not drop one package on a Laptop 1 and receive it from the Laptop 0.



2. Using ping:

Write a command ping 40.0.0.2 (ip address of the destination Laptop) from the command prompt of Laptop having ip address 10.0.0.2 (the source Laptop).



```
Laptop0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 40.0.0.2

Pinging 40.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 40.0.0.2: bytes=32 time<1ms TTL=125
Reply from 40.0.0.2: bytes=32 time=3ms TTL=125
Reply from 40.0.0.2: bytes=32 time=1ms TTL=125

Ping statistics for 40.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Conclusion:

Through this practical I learned about how to configure BGP and EIGRP protocols in different networks.

Practical 6

Aim: Demonstrate the static and dynamic configuration of NAT using cisco packet tracer

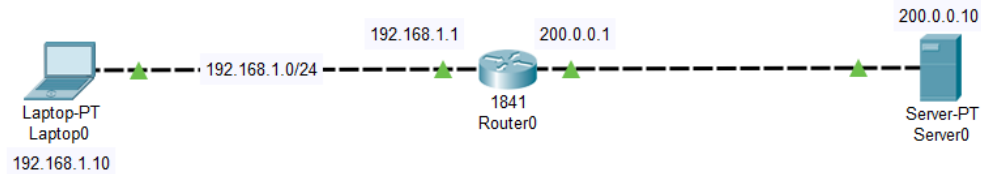
Theory:

❖ NAT:

- What is Network Address Translation (NAT)?
 - NAT (Network Address Translation) is a process of changing the source and destination IP addresses and ports.
 - Address translation reduces the need for IPv4 public addresses and hides private network address ranges.
 - The process is usually done by routers or firewalls.
- How does it work?
 - NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.
- There are three types of address translation.
 - Static NAT – translates one private IP address to a public one. The public IP address is always the same.
 - Dynamic NAT – private IP addresses are mapped to the pool of public IP addresses.
 - Port Address Translation (PAT)– one public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.

Static configuration of NAT:

Topology:



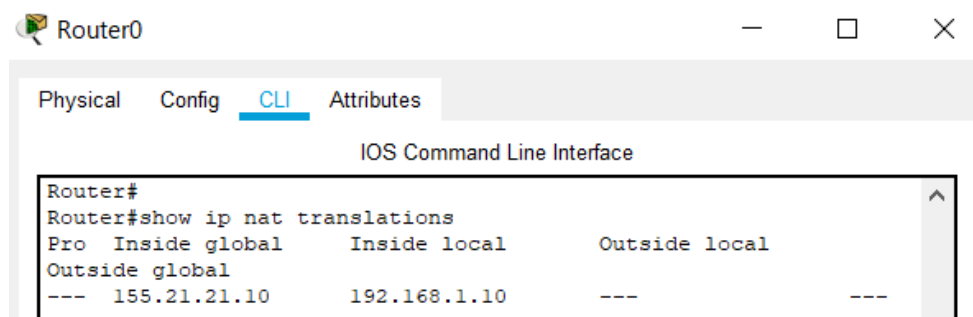
Steps of Configurations:

- First of all to create a topology, click on the device and drop on workplace and connect all the devices with the necessary cables.
- Then configure router using CLI and give the ip address as mention in the topology diagram.
 5. Router: fa0/0 192.168.1.1
 fa0/1 200.0.0.1
- Provide ip address and default gateway to the laptop.
 1. Laptop: ip address is 192.168.1.10
 default gateway is 200.0.0.1
- Provide ip address and default gateway to the server.
 1. Server: ip address is 200.0.0.10
 default gateway is 200.0.0.1
- Configuration of Static NAT on router 0,

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config)#
Router(config)#ip nat inside source static 192.168.1.10
155.21.21.10
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
  
```

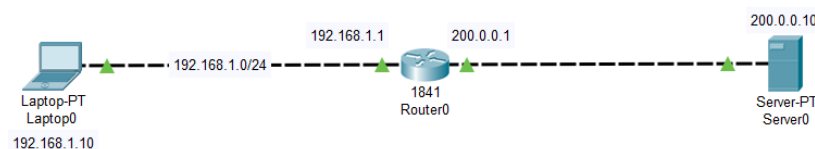
- Verify Static NAT configuration.



Checking Network Topology:

5. Message passing:

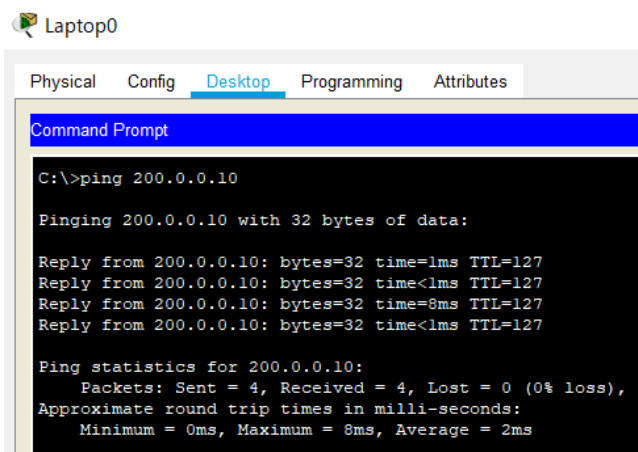
To check the connections are working properly or not drop one package on a Laptop and receive it from the Server.



Realtin									
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
Successful		Laptop0	Server0	ICMP	Blue	0.000	N	0	(edit)
Successful		Server0	Laptop0	ICMP	Red	0.000	N	1	(edit)

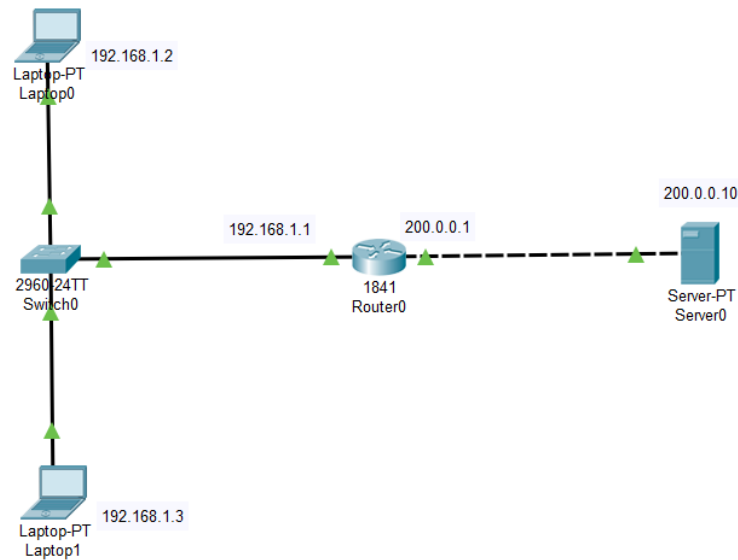
6. Using ping:

Write a command ping 200.0.0.10 (ip address of the Server) from the command prompt of Laptop having ip address 192.168.1.10 (the source Laptop).



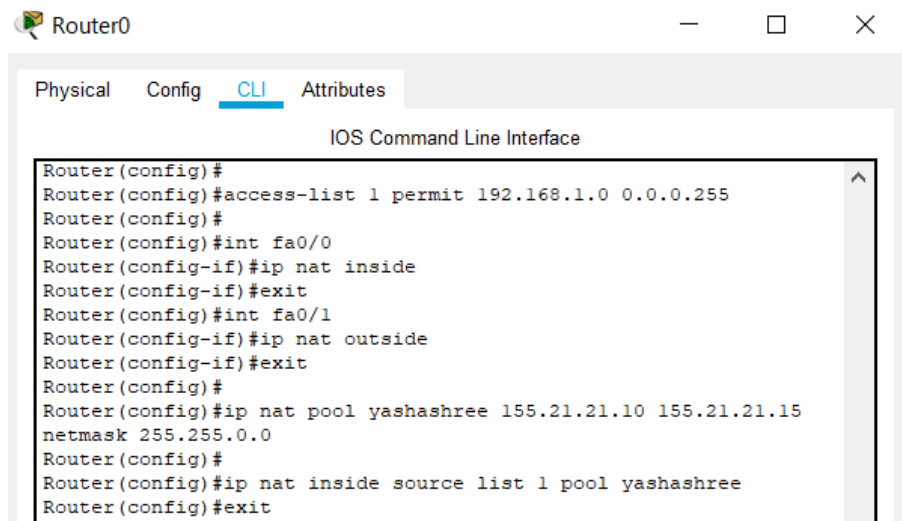
Dynamic configuration of NAT:

Topology:



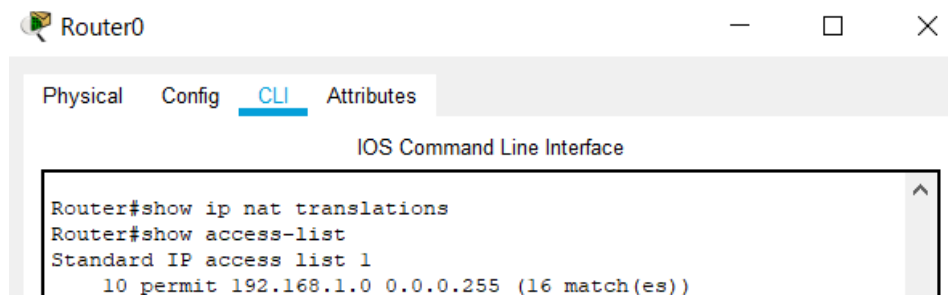
Steps of Configurations:

- First of all to create a topology, click on the device and drop on workplace and connect all the devices with the necessary cables.
- Then configure router using CLI and give the ip address as mention in the topology diagram.
 1. Router: fa0/0 192.168.1.1
 fa0/1 200.0.0.1
- Provide ip address and default gateway to the laptop.
 1. Laptop 1: ip address is 192.168.1.2
 default gateway is 200.0.0.1
 2. Laptop 2: ip address is 192.168.1.3
 default gateway is 200.0.0.1
- Provide ip address and default gateway to the server.
 1. Server: ip address is 200.0.0.10
 default gateway is 200.0.0.1
- Configuration of Dynamic NAT on router 0,

A screenshot of a network simulator window titled 'Router0'. It has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area is titled 'IOS Command Line Interface' and shows a series of configuration commands entered in a terminal-like font. The commands configure an access list, interfaces fa0/0 and fa0/1 with NAT, a NAT pool named 'yashashree', and a NAT rule mapping the access list to the pool.

```
Router(config)#
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#ip nat pool yashashree 155.21.21.10 155.21.21.15
netmask 255.255.0.0
Router(config)#
Router(config)#ip nat inside source list 1 pool yashashree
Router(config)#exit
```

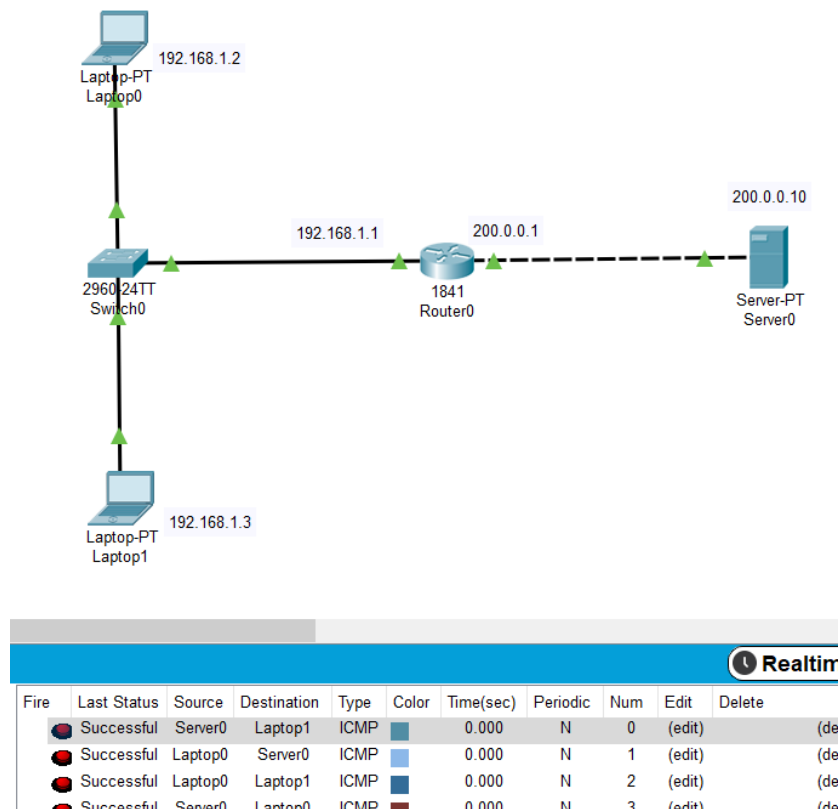
- Verify Dynamic NAT configuration.

A screenshot of the same 'Router0' window, now showing verification commands. The 'CLI' tab is still selected. The terminal shows the output of 'show ip nat translations' and 'show access-list', confirming that the NAT pool is active and the access list is correctly configured.

```
Router#show ip nat translations
Router#show access-list
Standard IP access list 1
 10 permit 192.168.1.0 0.0.0.255 (16 match(es))
```

Checking Network Topology:

1. Message passing:
To check the connections are working properly or not drop the packets from laptop to server.



2. Using ping:

Write a command ping 200.0.0.10 (ip address of the Server) from the command prompt of Laptop having ip address 192.168.1.2 (the source Laptop 0).

Laptop0

```

Physical  Config  Desktop  Programming  Attributes
Command Prompt

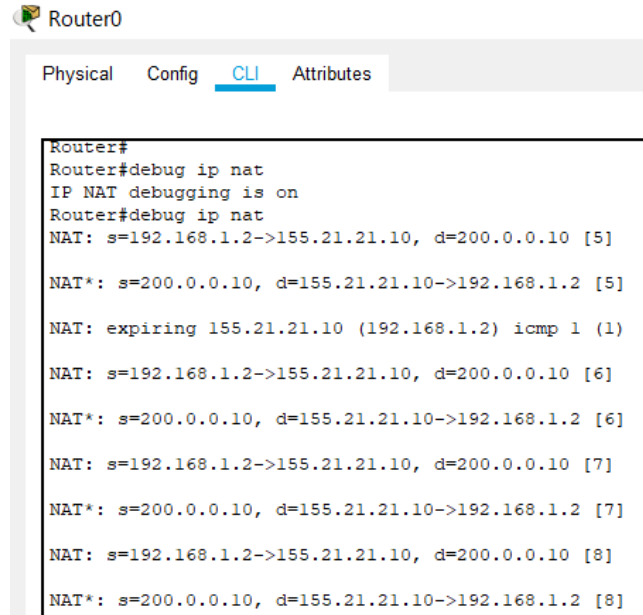
C:\>ping 200.0.0.10

Pinging 200.0.0.10 with 32 bytes of data:

Reply from 200.0.0.10: bytes=32 time=1ms TTL=127
Reply from 200.0.0.10: bytes=32 time<1ms TTL=127
Reply from 200.0.0.10: bytes=32 time<1ms TTL=127
Reply from 200.0.0.10: bytes=32 time=5ms TTL=127

Ping statistics for 200.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 5ms, Average = 1ms
  
```

Just when ping run `<debug ip nat>` command on router:



The image shows a screenshot of the Cisco Packet Tracer interface for a router named Router0. The 'CLI' tab is selected, displaying the following commands and output:

```
Router#
Router#debug ip nat
IP NAT debugging is on
Router#debug ip nat
NAT: s=192.168.1.2->155.21.21.10, d=200.0.0.10 [5]
NAT*: s=200.0.0.10, d=155.21.21.10->192.168.1.2 [5]
NAT: expiring 155.21.21.10 (192.168.1.2) icmp 1 (1)
NAT: s=192.168.1.2->155.21.21.10, d=200.0.0.10 [6]
NAT*: s=200.0.0.10, d=155.21.21.10->192.168.1.2 [6]
NAT: s=192.168.1.2->155.21.21.10, d=200.0.0.10 [7]
NAT*: s=200.0.0.10, d=155.21.21.10->192.168.1.2 [7]
NAT: s=192.168.1.2->155.21.21.10, d=200.0.0.10 [8]
NAT*: s=200.0.0.10, d=155.21.21.10->192.168.1.2 [8]
```

Conclusion:

Through this practical I learned about how to configure Dynamic and Static NAT (Network Address Translation) in cisco packet tracer.