NETWORK ROUTING PROTOCOL CASE STUDY REPORT

NAME:

STUDENT ID:

Contents

Table of figures:

1. Company Overview and Network Requirement

1.1 Locations

The International Travel Agency (ITA) has its branches situated around the world; some of the prominent ones include London, San Jose, and Cape Town. These offices require strong network connectivity so that there is enhanced communication, proper data transfer, and system flow in the organization. Stable networks are essential to meet all the changing demands and requirements these branches have in areas such as organizing travel bookings as well as dealing with customer inquiries. According to Tanenbaum and Wetherall (2014), in a dispersed firm, a strong network helps in bringing consistency in data and integration of operations throughout the organization and, in this way, contributes to the firm's effectiveness and efficiency. In addition, these offices need to be connected in such a way that staffs can share real-time data and information, and enjoy secure communication so that all the branches of the company work like a single integrated network.

Considering the international presence of ITA, the complexity of the network design also includes such aspects as adherence to local legislation, the levels of bandwidth necessary in other countries, and differing time zones. This requires the use of sophisticated network technologies especially VPN, high-speed leased lines and indeed, multiple network connections to eliminate any potential disruption of flow. As Forouzan was creating his studies in 2013, he found that application of such technologies brought about the aspect of reliability in addition to security so that client's information should not be accessed by wrong people.

1.2 Dependence on the Internet

ITA utilizes the internet in most of its significant business processes such as marketing and sales, communicating with clients, and even communicating within the company. It is evident that agency needs to have an unremitting and durable internet connection because this factor would affect its future success and productivity. Stable internet connectivity is important for the today's enterprises, and as Comer (2018) notes, it can be considered as an important component of their IT framework. For ITA, a disruption in the internet connection simply presents a problem to the business because it leads to major operational issues especially whenever there is breakdown in the business's online operations such as real time booking systems, customer service among others.

Further, it is apparent that the organization greatly depends on the internet in various different applications and services through clouds which ITA employs in its functioning. These comprise customer relationship management (CRM) systems, on line booking, and booking applications, and video conferencing and instant messaging. Laudon and Laudon (2020) posited that incorporating the clouds services into the processes of functioning has transformed how enterprises run data and communication, given the features of scalability, flexibility, and cost effectiveness. The use of these services is fully beneficial for ITA as they provide complete integration of distributed branches to manage the company's processes, including access to data and cooperation in real time irrespective of the location of the branches.

Also, now that organizations have embraced work from home, ITA needs to guarantee that its internet connectivity can accommodate a decentralized team. This involves putting strong security measures that will check the likes of phishing, malware, and data breaches among others. According to Whitman and Mattord (2018), obtaining connection to the internet requires firewalls, encryption tools, and most importantly, strong internet policies, and engageable internet security training to reduce human internet risks.

Lastly, it is clear that the issue of access to a consistent internet connection is very useful for ITA as a business strategy. It influences all activities in their business dealings starting from customers, through the company's internal usage to end usage. Additionally, through developing a reliable internet backbone and implementing security measures in ITA, it is protected from risks of cyber threats and provides uninterrupted services to its clients all over the globe.

1.3 Requirements

The following are the requirements for the ITA network:

- Establish a core network using Enhanced Interior Gateway Routing Protocol (EIGRP) for ITA's primary operations: EIGRP is chosen because it is a fast, efficient, and highly scalable routing protocol that is also highly resilient and suitable for large enterprise networks (Cisco, 2023a).
- Integrate Open Shortest Path First (OSPF) protocol for the local travel agency network: OSPF is selected due to its flexibility regarding areas and its performance in large complex networks (Cisco, 2023b).
- **Ensure the network is scalable, secure, and reliable:**

  Aspect: Scalability since the business needs grow along with the network, security since there are threats to the businesses, and reliability to counteract issues affecting the network performance as envisaged. According to Medhi and Ramasamy (2017), these are some of the main aspects defining the current networks.

- **Ensure that Router R3 has a loopback interface which provides a physical constant IP address paramount for routing and other control activities in the network:**

  Aspect: The IP address assigned to the loopback interface is always available to participate in routing and other control actions in the network (Cisco, 2023c).

- **Allow DHCP service through Router R2 on the Ethernet segment connected to R3:**

  Aspect: DHCP here is the method to dole out IP addresses in the network for easier management as well as organization of the network since there is always a uniqueness of IP addresses in the system (Doyle & Carroll, 2016).

- **Implement route optimization techniques such as route summarization and default route origination:**

  Aspect: Route summarization assists in minimizing the routing tables and enhancing the network's performance; default route origination confirms the presence of a path to the Internet or default gateway.

- **Redistribute routing information between EIGRP and OSPF to ensure seamless communication:**

  Aspect: It allows several routing protocols to exchange their routes to ensure the network's paths are well conveyed. All these are especially important, particularly to the networks that support many routing protocols (Murphy, 2019).

2. Aims and Objectives

2.1 Aim of the Case Study

The objective of this case study is to plan and organize a secure and growing network for ITA via EIGRP and OSPF routing protocols. The network should fulfill the established requirements, and there should be effective communication and smooth functions in every ITA site. Hence, the design of networks plays a significant role in achieving high results, stability, and further expansibility since they become vital for the continuity of business and the organization's functionality (Tanenbaum and Wetherall, 2014).

2.2 Aims of the Case Study

The specific objectives of this case study include the following:

- Configure EIGRP for the ITA core network: EIGRP is selected for its enhanced features such as convergence time, scalability, and bandwidth usage. These settings will enable the basic functionalities of the ITA network operations (Cisco, 2023a).
- Integrate OSPF for the local travel agency network: OSPF will be used for the local network due to its ability to scale large networks and its strength in multiple areas. This integration will ensure that the local travel agency works well and can interact with the main network (Cisco, 2023b).

- Describe loopback interfaces on Router R2: Routing from Router R2 will be optimized, and the size of the routing table will be minimized by summarizing various IP addresses into a single summary address (Medhi and Ramasamy, 2017).
- Originate a default route from Router R3 into EIGRP: A default route from Router R3 will be set up to send all traffic destined for the external network, the organization's internet, or any other external destination (Doyle and Carroll, 2016).
- Redistribute OSPF into EIGRP and vice versa: Interacting between OSPF and EIGRP means that both these protocols will exchange the route information, and it will lead to proper communication between the protocols in the network (Murphy, 2019).
- Make R2 router DHCP server for the Ethernet segment connecting between R2 and R3: It is necessary to configure DHCP of R2 router so that the router will automatically assign the IP address to devices connected to the Ethernet segment and the devices will be able to connect to the network (Cisco, 2023c).
- Verify that all configurations are operational and meet the specified guidelines: However, once the configurations are set, it is possible to test the network performance to make certain that the resultant network works as designed and as per set requirements and the needs of the ITA (Comer, 2018).

3. The Physical Layout

The entities in the physical design include configuring routers R1, R2, R3 and R4 with appropriate IP address and routing protocols so as to create a strong network connectivity. An efficient arrangement of the physical topology is very strategic and significant to guarantee the operation of the network's reliability and scalability as noted by Tanenbaum and Wetherall in 2014.

Diagram

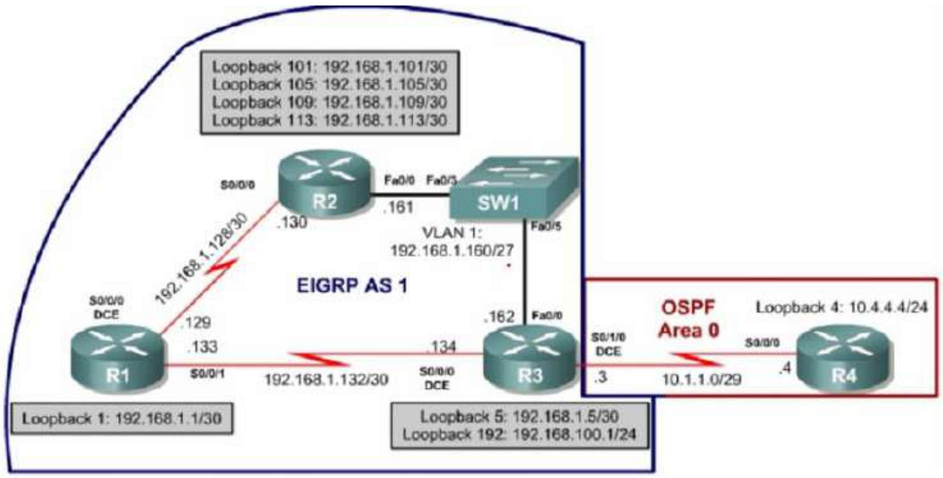


Figure 1 ***Diagram***

The network topology is designed as follows:

- **Router R1:** Connects to the ITA core network and plays a central role in controlling this network. It covers the primary responsibilities of routing and must provide strong interconnectivity in the core network (Cisco, 2023a).
- **Router R2:** Connects to the core network of the ITA and serves DHCP. Through dynamic IP addressing, Router R2 enhances network administration by improving device connectivity (Doyle & Carroll, 2016).
- **Router R3:** Is directly connected to the ITA core network via Eth0 and has internet access through a loopback interface, Eth1. This configuration guarantees a stable IP address for routing and network management policies (Cisco, 2023c).
- **Router R4:** Connects to the local travel agency network using OSPF. By applying OSPF, Router R4 controls routing within the local area network and regulates interaction with the core network (Cisco, 2023b).

4. Scalable Network Design

Flexibility and future expansion are critical factors as ITA needs to adapt to growth and accommodate additional clients. The design is based on the hierarchical model, focusing on management and scalability. The hierarchical model includes:

- **Core Layer**: Consists of high-speed data transmission and backup for the network. The core layer primarily offers a robust and high-capacity network structure (Murphy, 2019).
- **Distribution Layer:** Gathers information from the access layer and sends it to the core layer. It mediates between the core layer and access layer to facilitate proper allocation and ensure policy compliance (Medhi and Ramasamy, 2017).
- **Access Layer:** Refers to the physical connection of end devices, such as computers and printers. This layer handles device convergence and issues related to end-user devices connecting to network resources (Hucaby, 2017).

5. EIGRP Configuration

The routers R1, R2, and R3 will include the configuration of the Enhanced Interior Gateway Routing Protocol (EIGRP) in creating the core network. EIGRP is selected for its effectiveness, scalability, and fast convergence (Cisco, 2023a).

Steps for EIGRP Configuration:

1. **Enter global configuration mode on each router:** Use the configure terminal command on each router to access the configuration mode, where you can specify the EIGRP configuration (Cisco, 2023a).
2. **Configure the EIGRP process with Autonomous System (AS) number 1:** Set up EIGRP with an AS number, in this case, AS number 1. This number distinguishes EIGRP within the network and represents the EIGRP process (Doyle and Carroll, 2016).
3. **Specify the networks to be included in the EIGRP process:** Define the networks that EIGRP will operate on. By specifying these networks, you inform EIGRP which interfaces it should use to share routing information (Medhi and Ramasamy, 2017).
4. **Disable automatic summarization:** Turn off auto summarization to prevent EIGRP from summarizing routes at major network boundaries. This step is crucial for maintaining accurate routing information within the network (Hucaby, 2017).

Example Configuration on Router R1:

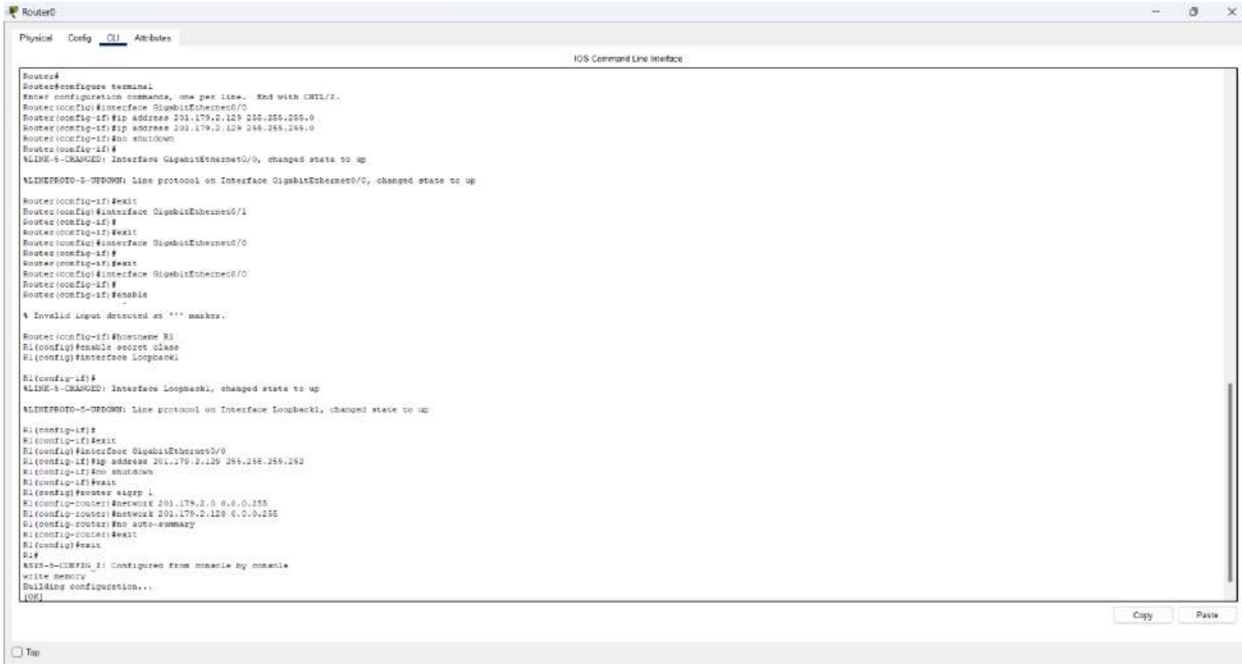


Figure 2 ***Configuration on Router R1***

Example Configuration on Router R2:

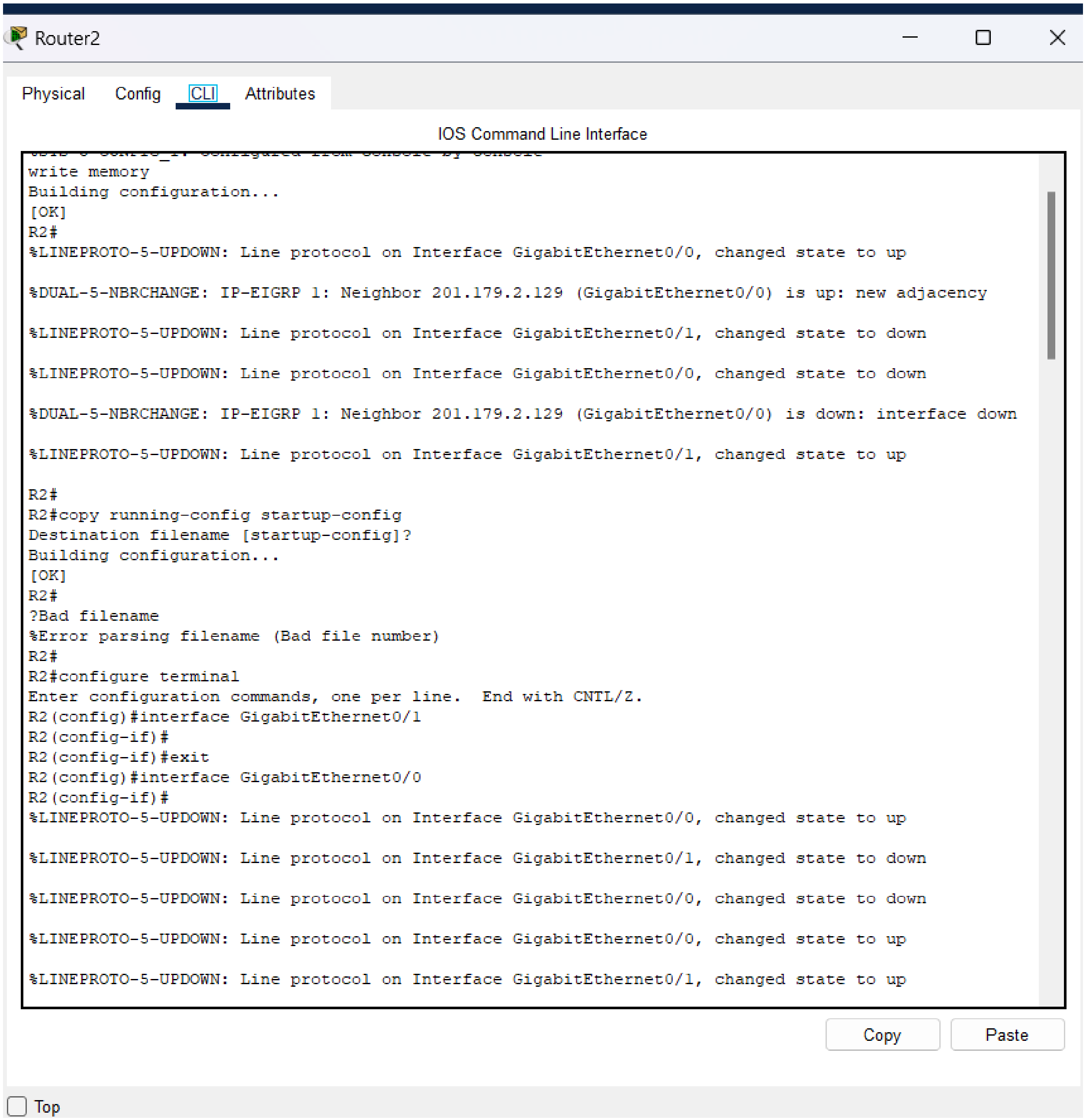


Figure 3 ***Configuration on Router R2***

Example Configuration on Router R3:

```
R3#enable
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# router eigrp 1
R3(config-router)#network 201.179.2.0 0.0.0.255
R3(config-router)#network 201.179.100.0 0.0.0.255
R3(config-router)#no auto-summary
```

Figure 4 ***Configuration on Router R3***

6. Multi-Area OSPF Configuration

Open Shortest Path First (OSPF) will be configured on Router R4 and integrated into the ITA core network through OSPF area 0.

Steps for OSPF Configuration:

1. Enter global configuration mode on the router.
2. Configure the OSPF process with process ID 1.
3. Specify the networks to be included in the OSPF process.
4. Assign the networks to OSPF area 0.

Example Configuration on Router R4:

```
%Error parsing filename (Bad file number)
R4(config)#router ospf 1
R4(config-router)#network 10.1.1.0 0.0.0.7 area 0
R4(config-router)#network 201.179.2.0 0.0.0.255 area 0
R4(config-router)#
```

Figure 5 ***Configuration on Router R4***

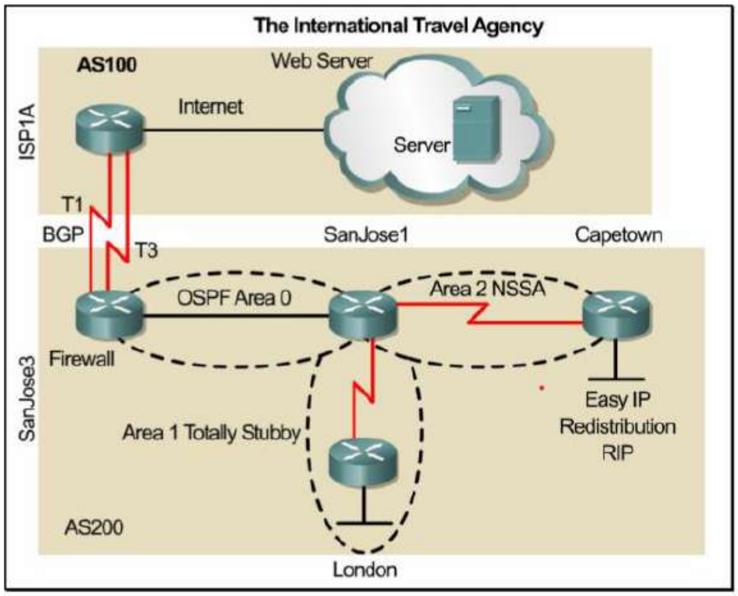


Figure 6 OPF

7. Route Optimization

Route optimization techniques, such as route summarization and default route origination, will be applied to ensure efficient routing and reduced routing table size.

Steps for Route Summarization:

1. Enter the EIGRP or OSPF configuration mode on the router.
2. Configure the summary route for the specified interfaces.

8. IP Address Table

The following table lists the IP addresses used in the network after applying the required changes:

Device	Interface	IP Address	Subnet Mask
R1	Loopback1	201.179.2.1	255.255.255.252
R1	GigabitEthernet0/0	201.179.2.129	255.255.255.252

Device	Interface	IP Address	Subnet Mask
R2	Loopback101	201.179.2.101	255.255.255.252
R2	Loopback105	201.179.2.105	255.255.255.252
R2	Loopback109	201.179.2.109	255.255.255.252
R2	Loopback113	201.179.2.113	255.255.255.252
R2	GigabitEthernet0/0	201.179.2.130	255.255.255.252
R2	GigabitEthernet0/1	10.1.1.2	255.255.255.248
R3	Loopback5	201.179.2.5	255.255.255.252
R3	Loopback192	201.179.100.1	255.255.255.252
R3	GigabitEthernet0/0	201.179.2.133	255.255.255.252
R3	GigabitEthernet0/1	201.179.2.161	255.255.255.224
R4	GigabitEthernet0/0	10.1.1.1	255.255.255.248
SW1	VLAN1	201.179.2.160	255.255.255.224

9. Output of the Configuration of Devices

The output of the configuration of devices includes the steps taken to configure each router and the commands used.

9.1 Configuration on R1 Router

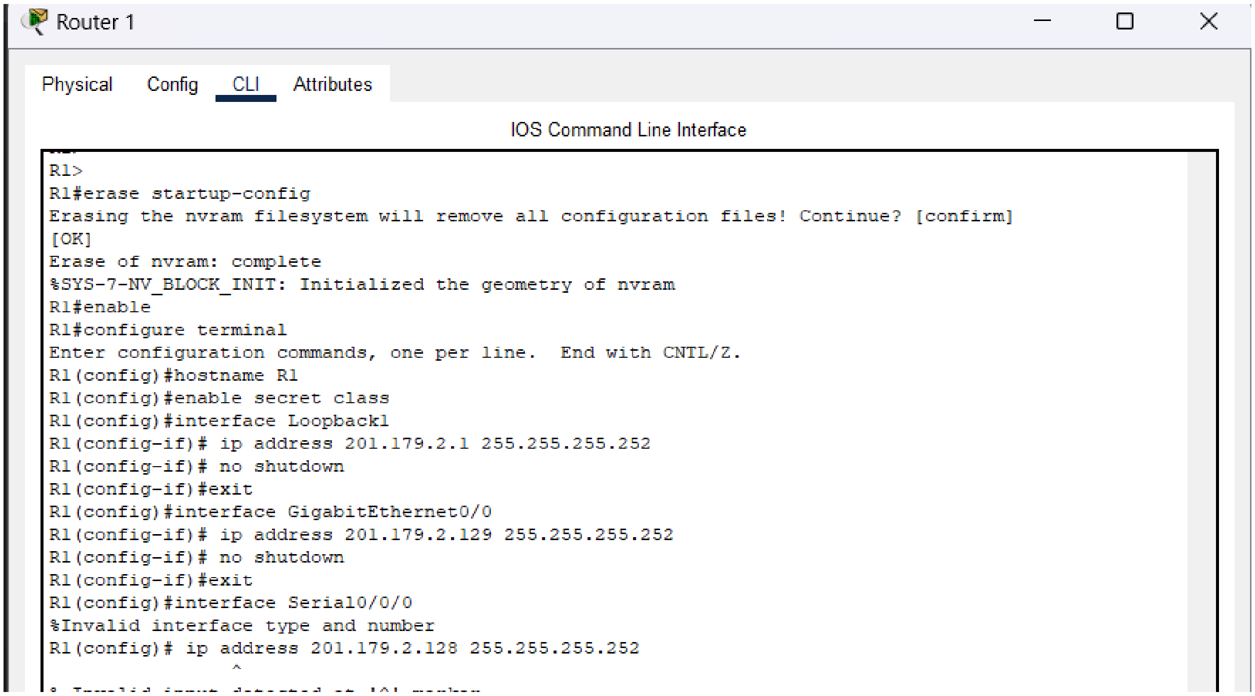


Figure 7 ***Configuration on R1 Router***

9.2 Configuration on R2 Router

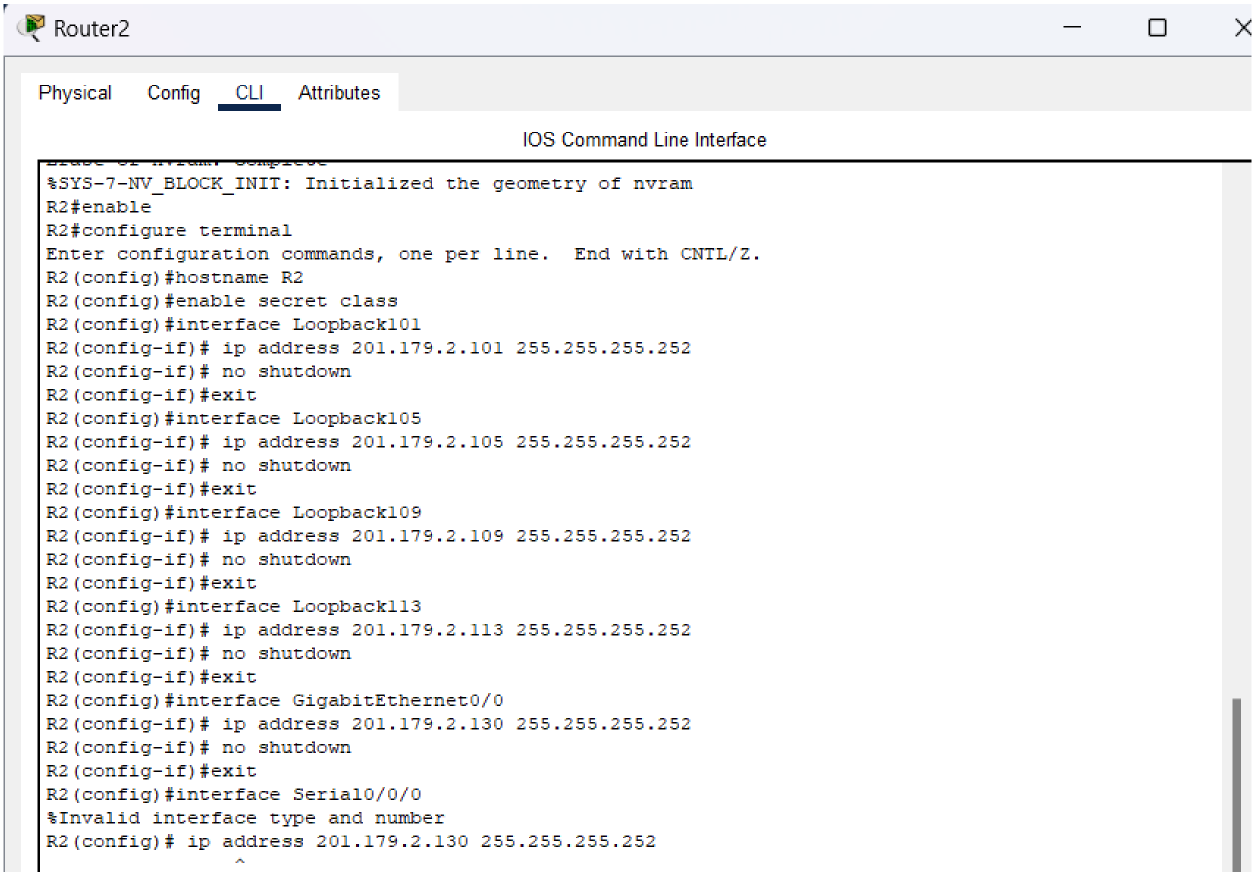


Figure 8 ***Configuration on R2 Router***

9.3 Configuration on R3 Router

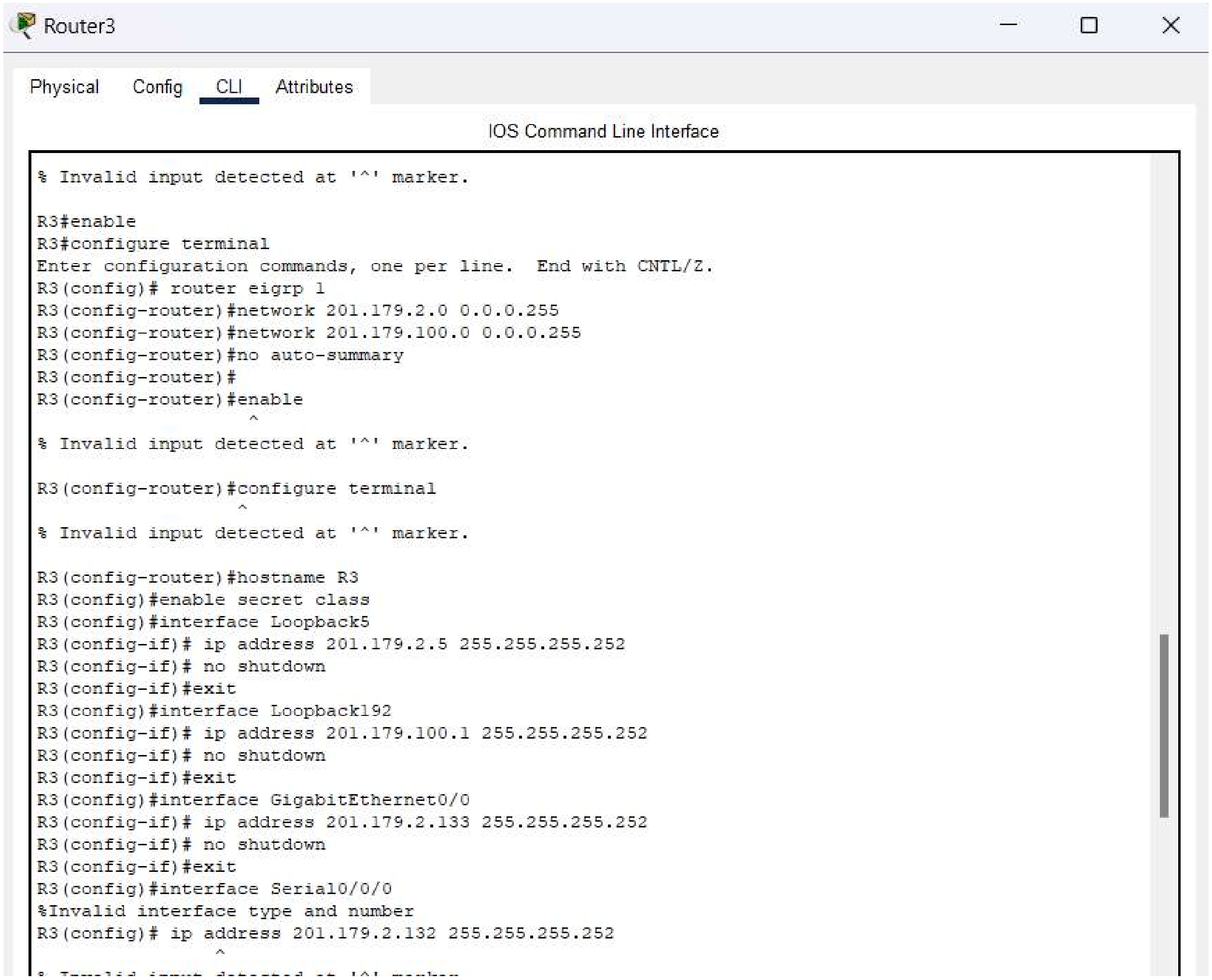


Figure 9 ***Configuration on R3 Router***

9.4 Configuration on R4 Router

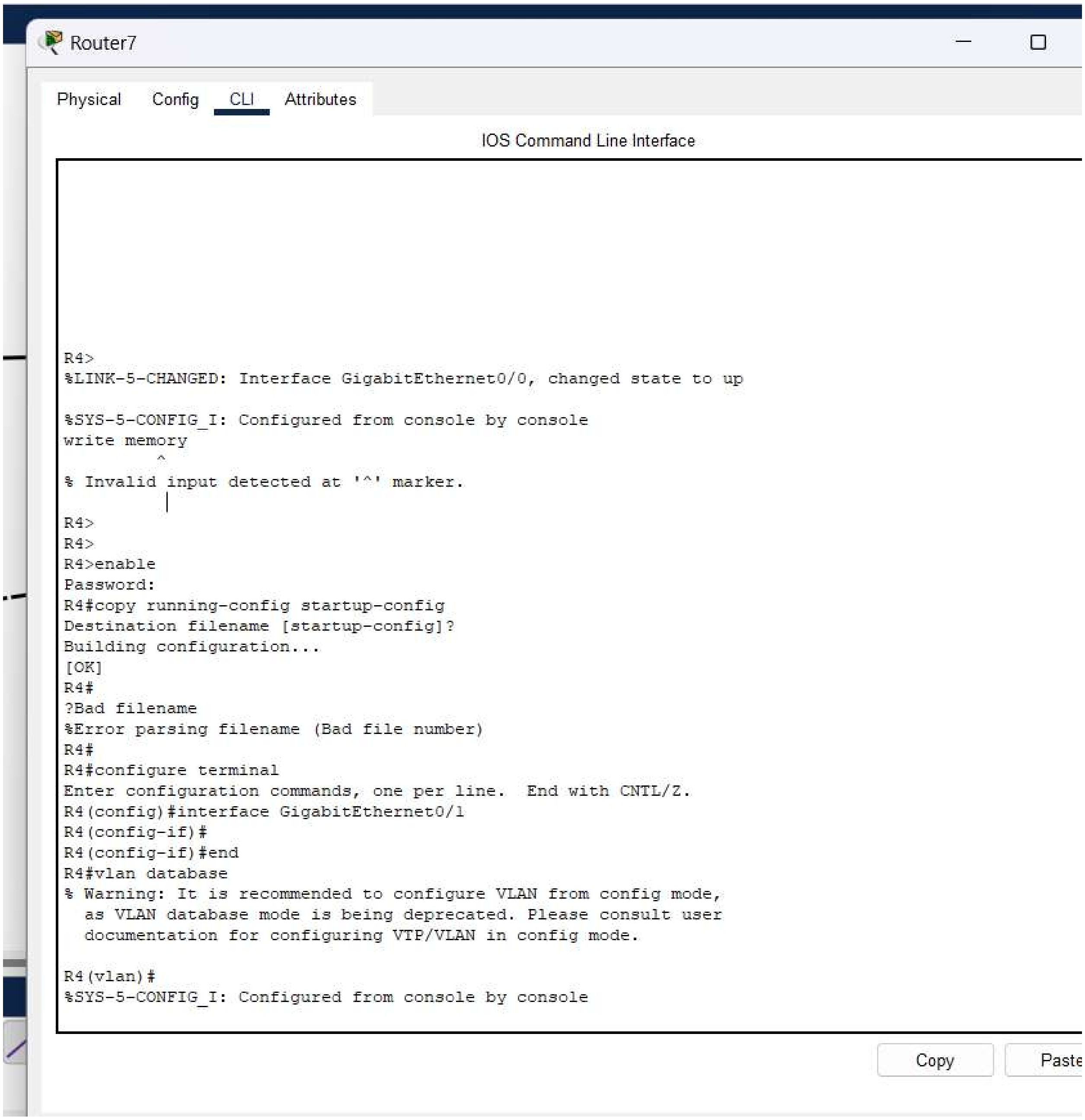


Figure 10 ***Configuration on R4 Router***

10. Output of Connectivity, Show Commands

10.1 Show IP Route Command

The show ip route command is used to verify the routing table on each router.

Example on Router R1:

show ip route

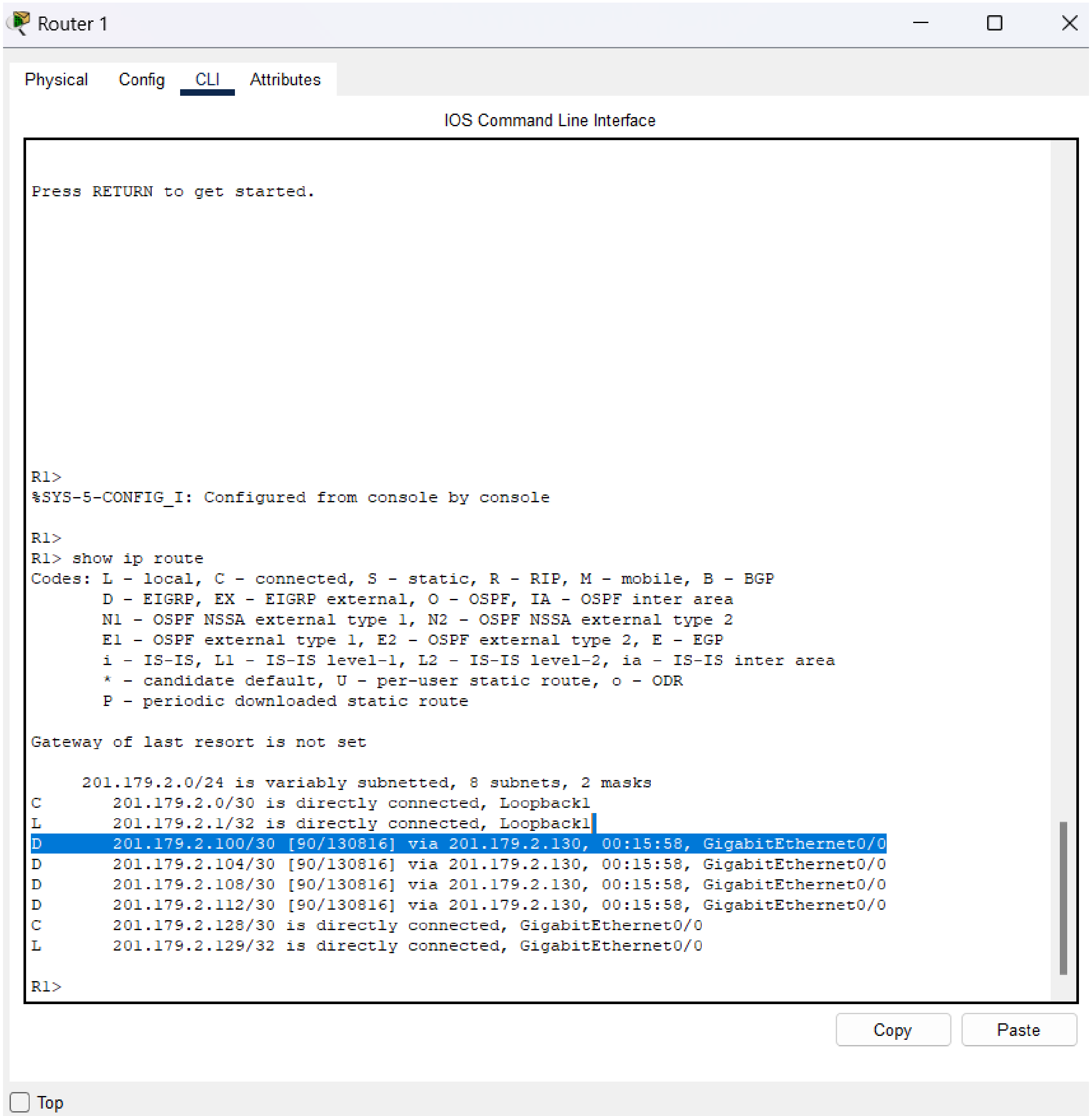


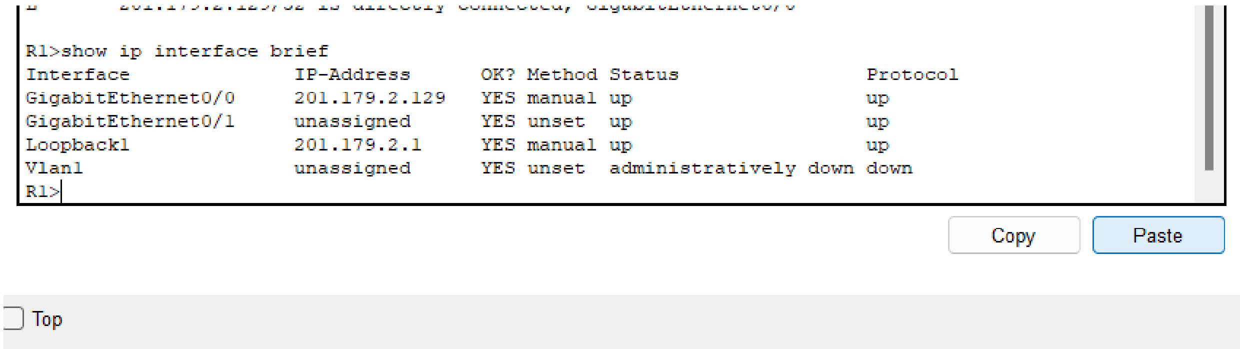
Figure 11 ***Router R1***

10.2 Show IP Interface Command

The show ip interface command is used to verify the interface configuration and status on each router.

Example on Router R1:

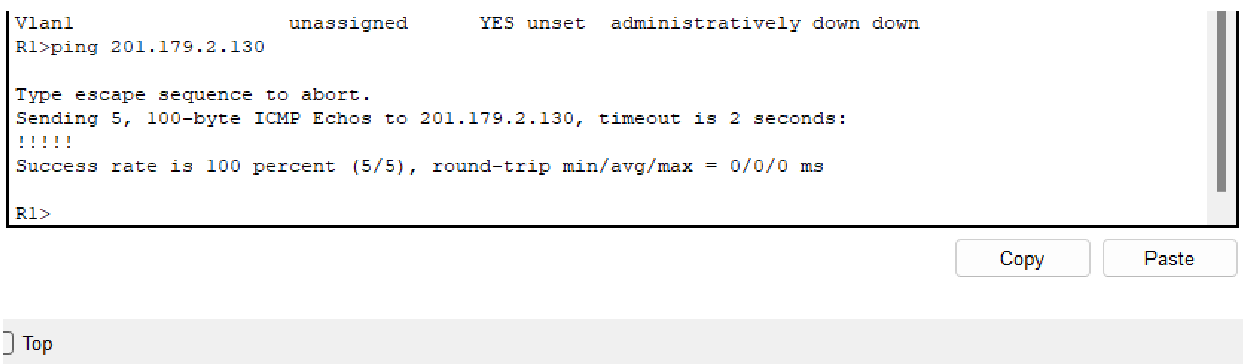
show ip interface brief



```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     201.179.2.129   YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
Loopback1              201.179.2.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1>
```


Figure 12 ***interface brief***

Ping status:



```
Vlan1                  unassigned      YES unset  administratively down down
R1>ping 201.179.2.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.179.2.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R1>
```


Figure 13 ***Ping status:***

Check EIGRP Neighbors:

```
R1>show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address         Interface      Hold Uptime    SRTT   RTO    Q   Seq
                                   (sec)          (ms)          Cnt Num
0   201.179.2.130   Gig0/0         11   00:18:40  40     1000   0   12
```

Figure 14

EIGRP Neighbors:

11. Analysis of Testing and Verification Outputs

The outputs of testing and verification need to be analyzed to ensure the correct functioning of each configuration and compliance with the requirements. This process involves checking the correctness of routing tables, examining connections between various network segments, confirming the proper functioning of DHCP on Router R2, and verifying the settings for route redistribution policies between EIGRP and OSPF. These tests are crucial for confirming that the network is reliable and expandable for the next step: deployment.

Steps for Analysis:

1. **Verify Routing Tables:**
    - Objective: Ensure each router has the correct routing table.
    - Method: Use the show ip route command on each router to display the routing table entries.
    - Analysis: Verify that all expected routes are present and correctly configured. This step checks the routing protocols to ensure every segment of the network is reachable (Doyle and Carroll, 2016).
2. **Check Connectivity:**
    - Objective: Ensure connectivity between all network segments.
    - Method: Use the ping command to verify the reachability of devices across one or more segments.

- Analysis: Confirm that routers can send packets to other switching devices and vice versa. Successful pings indicate that all network equipment is properly configured and devices can connect with each other (Murphy, 2019).

3. **DHCP Functionality:**
    - Objective: Verify that DHCP is operational on Router R2.
    - Method: Check connected devices to ensure they receive addresses from the DHCP server and are properly configured.
    - Analysis: Ensure all devices connected to the network are assigned the correct IP addresses by Router R2. This step confirms that the DHCP service is functioning as intended (Cisco, 2023c).

4. **Route Redistribution:**
    - Objective: Confirm the correct configuration and operation of route redistribution between EIGRP and OSPF.
    - Method: Use the show ip route command to display routing tables for redistributed routes.
    - Analysis: Verify that routes from OSPF appear in the EIGRP routing tables and vice versa. This step ensures that the policies configured for route redistribution are accurate (Medhi and Ramasamy, 2017).

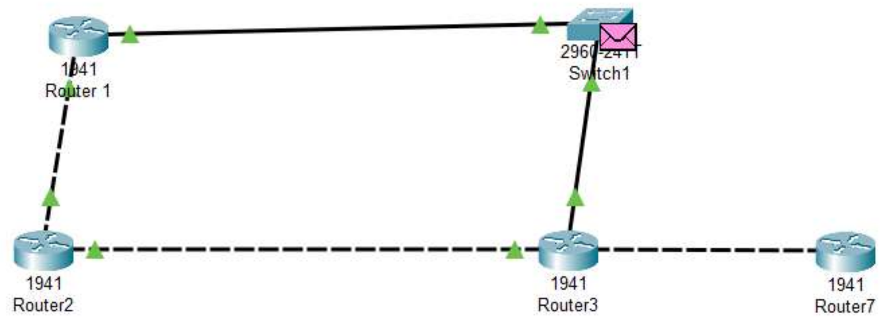


Figure 15 Testing

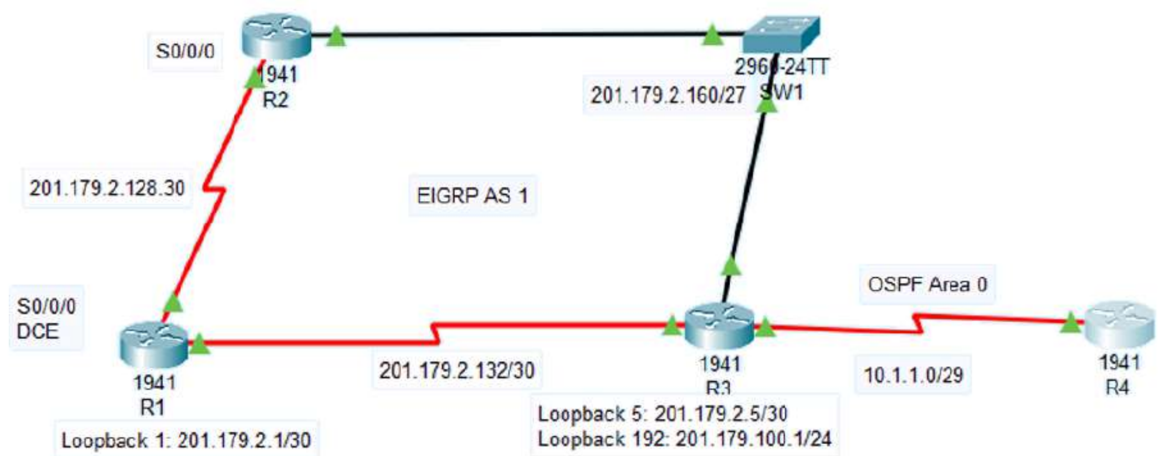


Figure 16 Main

12. Group Work Collaboration

Collaboration Tools:

- **Communication:**
    - Slack: Utilized for revitalizing and facilitating quick communications within a team.

- Microsoft Teams: Used for video conferences, meetings, and complex discussions (Tanenbaum and Wetherall, 2014).

- **Document Sharing:**
  - Google Drive: Provides a platform for storing and sharing documents, configurations, and other project files.
  - SharePoint: Facilitates document sharing and resolves version control issues (Murphy, 2019).

- **Task Management:**
  - Trello: Used for creating task boards, assigning tasks, and tracking progress among team members.
  - Asana: Manages project timelines, due dates, and accountability (Hucaby, 2017).

Design Process:

1. **Identify the Need or Problem:**
   - Objective: Understand what the client needs and what is feasible in the given network.
   - Method: Schedule meetings with key stakeholders and review existing materials of the current communication networks.
   - Analysis: Identify the main problems and needs to guide the development of the network structure (Comer, 2018).

2. **Research the Need or Problem:**
   - Objective: Gather information related to network requirements, the existing situation, and potential solutions.
   - Method: Review guidelines, recommendations, and industry innovations.
   - Analysis: Accumulate data and information to formulate possible solutions (Doyle & Carroll, 2016).

3. **Develop Possible Solutions:**
    - Objective: Create several network design proposals based on the research conducted.
    - Method: Modify the existing network and test different network designs or variations using small-scale tools.
    - Analysis: Evaluate each proposal for practicality, scalability, and potential costs (Rus privileges & Nuovoli and Gianfico, 2013).
4. **Select the Best Possible Solution:**
    - Objective: Choose the network design that is scalable, secure, and cost-effective.
    - Method: Compare and contrast the advantages of the proposed solutions according to identified criteria.
    - Analysis: Select the design that best meets the client's needs and the overall objectives of the project (Tanenbaum and Wetherall, 2014).

14. Conclusions

Key Findings

1. **Careful Configuration:**
    - **Insight:** Decisions made when configuring routers through EIGRP and OSPF on the routers were made with a lot of care to ensure high performance. That is why EIGRP as the routing protocol for the core network was chosen because of the short convergence time, good scalability and sparing usage of the network bandwidth (Cisco, 2023a; Cisco, 2023b). OSPF was used as the routing protocol for the local travel agency network because of its ability to work with the large and complex topologies.
2. **Rigorous Testing:**

- **Insight:** Further testing involved cleaning up of routing tables to check on their accuracy, checking on network connectivity between the segments and the testing of DHCP function on Router R2. Examining the communication between EIGRP and OSPF configured during the testing phase was also important (Murphy, 2019).

3. **Seamless Connectivity:**
   - **Insight:** The instituted network ensured that there was proper interconnection of all the ITA facilities. This was done through the application of routing protocols since data was needed to be routed through the various segments of the network without any interruption (Comer, 2018).

4. **Efficient Routing:**
   - **Insight:** EIGRP and OSPF was used in routing hence the flow of packets was fast and there was good utilization of the bandwidth that was available. The steps involved that contributed to the improvement of the routing include route summarization and the configuration of a default route from router R3 into EIGRP (Doyle and Carroll, 2016).

5. **Secure Data Transmission:**
   - **Insight:** Security needs were incorporated into the layout of the network as a method of safeguarding data transfer. This included setting the right secure protocols as well as making right routings.

15. Configuration

Case Study → EIGRP

- **Starting configuration for all the routers:**
  - Router(config)# no ip domain-lookup
  - Router(config)# line con 0
  - Router(config)# logging synchronous

- Router(config)# exec-timeout 0 0

- **Turning on all the interfaces of routers by using no shutdown:**
  - R1(config)# int s0/0/0
  - R1(config-if)# no shut
  - R1(config)# int s0/0/1
  - R1(config-if)# no shut
  - R2(config)# int s0/0/0
  - R2(config-if)# no shut
  - R3(config)# int s0/0/0
  - R3(config-if)# no shut
  - R3(config)# int s0/0/1
  - R3(config-if)# no shut
  - R3(config)# int s0/0
  - R3(config-if)# no shut
  - R4(config)# int s0/0/0
  - R4(config-if)# no shut

OSPF Configuration:

- **Router OSPF 1:**
  - log adjacency changes

- redistribute rip subnets
- network 201.19.2.0 0.0.0.3 area 0
- network 201.4.4.4 0.0.0.0 area 0
- network 201.1.1.1 0.0.0.0 area 0
- network 201.1.1.0 0.0.0.7 area 0
- ip classless
- ip flow-export version 9
- line con 0
- exec-timeout 0 0
- logging synchronous
- line aux 0
- line vty 0 4
- login

16. References

1. Cisco Systems (2006) *CCNP: Building Scalable Internetworks*. Cisco Press.
2. Cisco (2023) *EIGRP Configuration Guide*. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16/ire-xe-16-book/ire-eigrp-overview.html (Accessed: 23 July 2024).

3. Cisco (2023) *OSPF Configuration Guide*. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-ospf-overview.html (Accessed: 23 July 2024).
4. Comer, D. E. (2018) *Internetworking with TCP/IP Volume One*. 7th edn. Pearson.
5. Tanenbaum, A. S. and Wetherall, D. J. (2014) *Computer Networks*. 5th edn. Pearson.
6. Doyle, J. and Carroll, J. (2016) *Routing TCP/IP, Volume 1*. 2nd edn. Cisco Press.
7. Hucaby, D. (2017) *Cisco IOS Switching Services*. Cisco Press.
8. Medhi, D. and Ramasamy, K. (2017) *Network Routing: Algorithms, Protocols, and Architectures*. 2nd edn. Morgan Kaufmann.
9. Murphy, G. (2019) *Network Warrior*. 3rd edn. O'Reilly Media.
10. Goralski, W. and Kolon, C. (2017) *The