Eduvos
Your Education. Your Future.

Individual Assessment Coversheet

To be attached to the front of the assessment.

Campus: BEDFORDVIEW

Faculty: INFORMATION TECHNOLOGY

Module Code: ITENA2-44

Group: GROUP 1

Lecturer's Name: Idowu Aruleba

Student Full Name: Thapelo Masetla

Student Number: [redacted]

Indicate	Yes	No
Plagiarism report attached		

Declaration:

□ I declare that this assessment is my own original work except for source material explicitly acknowledged. I also declare that this assessment or any other of my original work related to it has not been previously, or is not being simultaneously, submitted for this or any other course. I am aware of the AI policy and acknowledge that I have not used any AI technology to generate or manipulate data, other than as permitted by the assessment instructions. I also declare that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations.

Signature	**Date** 7 November 2025

Lecturer's Comments:

Marks Awarded: %

Signature	**Date**

Eduvos (Pty) Ltd. (formerly Pearson Institute of Higher Education) is registered with the Department of Higher Education and Training as a private higher education institution under the Higher Education Act, 101, of 1997. Registration Certificate number: 2001/HE07/008

Table of Content

Section A

Question 1

1.1)

Zone	Hosts	Subnet Mask	Network Address	Range of assignable IP address	Broadcast Address	Routed Interface	VLAN ID
Corporate Wi-Fi	120	/25	10.20.0.0	10.20.0.1-10.20.0.126	10.20.0.127	10.20.0.1	VLAN 10/
Operations	100	/25	10.20.0.128	10.20.0.129-10.20.0.254	10.20.0.255	10.20.0.129	VLAN 20
Finance	80	/25	10.20.1.0	10.20.1.1-10.20.1.126	10.20.1.127	10.20.1.1	VLAN 30
Guest Wi-Fi	60	/26	10.20.1.128	10.20.1.129-10.20.1.190	10.20.1.191	10.20.1.129	VLAN 40
HR	50	/26	10.20.1.192	10.20.1.193-10.20.1.254	10.20.1.255	10.20.1.193	VLAN 50
IT	40	/26	10.20.2.0	10.20.2.1-10.20.2.62	10.20.2.63	10.20.2.1	VLAN 60
Server Farm	30	/27	10.20.2.64	10.20.2.65-10.20.2.94	10.20.2.95	10.20.2.65	VLAN 70
Network Management	20	/27	10.20.2.96	10.20.2.97-10.20.2.126	10.20.2.127	10.20.2.97	VLAN 80

Allocation Order

My table begins by allocating the largest subnets first , this is done because a large subnet requires a big, contiguous block of addresses .This is done so that we don't have issues such as:

- Fragmented address -Fragmented addresses makes it impossible to find a contiguous block large enough to support the large departments later on , even if the total number of free addresses was sufficient .Starting from the top going down ensures a efficient use of the Address space .
- Wastage of addresses -Small random allocation of addresses would force me to round up to the next power to often , this would place small fragments that cant be used for other needs .This means we will be left with unused slivers which is not efficient
- Break route summarisation-Continuous allocation gives us the ability to summarize routes , but random scattered subnets prevent summarisation and this leads to one having to advertise many specific prefixes or create awkward summarises that leak unrelated addresses

Efficient use of Space and Future Growth

Minimal Waste -All the subnet sizes were chosen as the next highest power of 2 that accompanies the total IPs needed , this is seen with the Operations subnet where we needed 100 addresses and /25 with 126 usable addresses fits this perfectly.

Preserved address Space – This allocation gives us a major, contiguous block of addresses free (10.20.2.128-10.20.3.255).This is a whole 128 address chuck that may be utilized for future use such as a new department without us having to re-address the whole network .

Route Summarisation

The design supports effective route summarisation. The whole Johannesburg HQ makes use of the 10.20.0.0/22 block. From the view of other sites a single route for 10.20.0.0/22 can be advertised , this helps keep routing tables small and simple .Internally the subnets are allocated on a hierarchical behaviour e.g :

- The first three departments all fall in the 10.20.0.0/23 supernet.
- The remaining subnets are nicely contained within 10.20.2.0/23

This grouping means that if ever the network is to grow and needs internal summarisation at distribution layers , it can be achieved efficiently and effectively, while reducing the load on core routers.

1.2)**HQ Network Topology and VLAN Deployment**

The Johannesburg HQ makes use of a simplified version of the access distribution model implemented through router on a stick configuration. While traditional access distribution models separate layer 2 access and layer 3 distribution functions across various/multiple switches this design consolidates inter vlan routing on one router due to the smaller network scale .The Layer 2 switch acts as the access layer device providing VLAN segmentation and trunking all VLANS to the router for inter VLAN communication

Each VLAN represents a functional department : VLAN 10,VLAN 20,VLAN 30, VLAN 40 ,VLAN 50, VLAN 60, VLAN 70 ,VLAN 80.

Topology Description

Layer 2 switch (Access Layer):

- All end user pcs , laptops and servers connect to this switch using access ports assigned to their respective VLANS.
- The switch manages VLAN segmentation but does not perform routing.
- VLANS are created on the switch and associated with the correct access ports
- The router will connect to the switch using a trunk link configured on one of the switches interfaces

Router (Inter VLAN Routing)

One physical interface will be divided into many sub interfaces, one per VLAN , and each with a unique IP address acting as the default gateway for that VLAN.

The router performs routing between VLAN's and enforces inter department access control using ACL.

Wireless Integration

The AP is connected to the same Layer 2 switch via a trunk port that carries multiple VLANS :

- Corporate Wi-Fi (VLAN 10)– authenticated staff
- Guest Wi-Fi (VLAN 40) -Visitors
- IT (VLAN 60)
- Operations (VLAN 20)

The AP tags each SSID's traffic with the corresponding VLAN ID and forwards it to the switch which then sends it to the router via trunk link.

Guest Wi-Fi Isolation

The Guest Wi-Fi VLAN will be separated from the internal corporate VLANs at layer 2

On the router ACLs will be applied to stop Guest VLAN users from reaching internal subnets .

Guest VLAN is only allowed internet access only through the routers outside or default route .

Inter VLAN routing Process

1. End devices send traffic to their default gateway
2. The router on a stick performs routing between VLANS using the configured sub interfaces
3. Return traffic is then sent back through the trunk to the switch then to the destination VLAN
4. ACLs on the router enforce departmental security

Reliability and Scalability

Reliability

- Even though one switch is used logical segmentation via VLANS isolates broadcast domains , improving stability.
- The router centralised inter VLAN routing which simplifies troubleshooting
- Making use of trunk for APs maintains VLAN consistency and reduces cabling

Scalability

- New VLANS/departments can be easily created through addition of more sub interfaces on the router and VLANS on the switch
- Access points have the ability to support more SSIDs mapped to new VLANS as the organization grows and wishes to add more departments
- This design fits the current size of the Johannesburg HQ and can later migrate/change to a layer 3 switch core if the volume of traffic increases over time

1.3)Two effective security measures that can be used are WPA3-Enterprise authentication and client isolation on guest networks.WPA3-Enterprise with 802.1X authentication makes the network stronger/more secure by requiring users to provide unique credentials before they can access the network this prevents unauthorized access and protects traffic against interception ,while client isolation on guest Wi-Fi stops guest devices from communicating with the main , other networks and other devices on the network, this stops lateral movement and it helps contain device based breaches .

WPA3-Enterprise with 802.1X risk reduction

Unauthorized access

This security protocol reduces unauthorized access by requiring unique credentials, such as username and password or digital certificate from user before they can gain access .Instead of a shared password every user or device is authenticated individually using 802.1X usually via a digital certificate or username and password through a RADIUS server. WPA3 makes use of Simultaneous Authentication of Equals so it can provide a properly secure handshake process, which protects against password cracking attacks that could bypass older WPA2 networks. Even if a attacker somehow manages to compromise a key , they wont be able to make use of it to decrypt previous or future sessions , this is because each connection generates unique, one time keys.

Interception of traffic

WPA3 Enterprise supports an optional 192 bit security mode that makes use of the commercial National Security Algorithm suite, offering a greater level of security for sensitive data , this protects data from attacks that can intercept traffic .

WPA3 uses a variety of robust encryption methods like GCMP-256 in the 192 bit mode which greatly enhances the strength of the encryption methods used and protection of wireless traffic

Client isolation on guest Wi-Fi risk reduction

This security measure prevents guests/wireless clients on the network from trying to communicate with one another. Devices on the network can only communicate with the internet and the assigned gateway and not other devices on the network.

Unauthorised access

This security measure limits guest user ability to access internal or other users devices , this is achieved by creating a secure sandbox for guest devices .While client isolation may not stop initial access to the network , it greatly reduces the risk impact/affect of unauthorized access to other network resources. If one of the guest devices are compromised an attacker is unable to leverage that to access sensitive files or services on other guest devices or the main corporate network.

Lateral Movement

Attackers cant scan , exploit or access other clients on the network , this helps prevent infected devices (devices with malware) from spreading malicious software to other devices that are on the network.

This security measure ensures that guest devices stay isolated , and it this ensures that sensitive data such as personal information isn't exposed to other devices on that same network

Question 2

2.1)Routing protocols are standardised rules the that determine/choose how data packets are sent from one network node to the next/another. Their importance is that they help in creating and miniating routing tables , which are utilised to make informed decisions on the best path for data transmission. The two routing protocols we will be focused on are OSPF and BGP.

Open Shortest Path (OSPF)

This is a link state routing protocol utilized for routing IP networks .It efficiently routes data in a Autonomous System by making use of Shortest Path First (SPF) algorithm to figure out/calculate the best path for forwarding packets. Its designed to determine the best/shortest path from one router to another in a LAN.

Scalability

OSPF is a very scalable routing protocol , this is because of its hierarchical multi layer design , which breaks large networks into smaller manageable areas. This decreases the size of routing tables and reduces the impact of local changes on the rest of the network.

Another factor that allows OSPF to be scalable is that it’s a link state protocol that only sends updates when there’s a change in the network , rather than on a fixed timer. This decreases bandwidth requirements and usage

Efficiency

OSPF is a very efficient protocol and this is because :

Fast Convergence- When there’s a change in the topology of the network , such as link failure or a new router joining OSPF can quickly recalculates new routes and routing tables are updated , this is usually done in seconds

Flexible path calculation-It makes use of the Dijkstra algorithm to find the best/most efficient path based on a cost metric set by the network admin rather than a basic hop count

Policy Control

OSPF is not best suited for policy control this is because it was designed for providing fast internal network convergence , and not granular traffic management. Its main/core function needs all routers in a area to have a full, identical view of the network , making it impossible to selectively filter or hide routes between them.

Behaviour over high latency satellite links

OSPF behaves poorly over high latency satellite links and this is because:

Latency is not accounted for, the factory/default OSPF cost metric is mainly based on bandwidth. This may lead to it choosing a high bandwidth but a high latency satellite link over a lower bandwidth , lower latency terrestrial link.

OSPF routers exchange Hello packets periodically , by default its 10 seconds on broadcast networks and 30 seconds on point to point networks, the dead interval , default 40 seconds defines when a neighbour is declared as down. If OSPF is used on high latency satellite links it may lead to missed hellos which possibly could lead to false adjacency resets.

Border Gateway Protocol (BGP)
This is an exterior gateway protocol utilized to connect autonomous systems in any topology. Each AS should have at least one BGP enabled router connected to another AS's BGP router. Its main purpose it to exchange network reachability information between BGP systems is a path vector routing protocol unlike distance vector or link state protocols.

Scalability

BGP is highly scalable and a few of the reasons for this is because of its decentralized architecture , and use of route aggregation and specialised technologies such as route reflectors . These features allow it to manage the large amounts of routes on the internet without a single point of failure or overwhelming any router, and it also has the ability to send only incremental updates , making routing changes efficient

Decentralized and hierarchical structure

Decentralised management -BGP distributes control across many autonomous systems rather than being dependant on one central authority

Hierarchical structure-The internet is organised hierarchically which helps manage complexity by breaking down

Route aggregation and Route reflectors

Route aggregation-BGP aggregates many smaller network prefixes into one large block , this greatly decreases the size of routing tables

Route reflectors-In a single AS , route reflectors decrease the need for every router to be fully meshed with every other router. Rather clients are connected to route reflectors, which share routes with other clients, making internal BGP deployment easier

Another thing about BGP is that it has the ability to manage large and diverse networks which makes it a ideal choice for scaling operations. It dynamically learns and adjusts to changes in the network topology, which in turn allows/enables efficient routing decisions in complex and always changing environments.

Efficiency

Path Selection

BGP provides advanced path selection mechanism. By considering many/multiple attributes like AS Path ,Multi Exit Discrimination , and local preference , BGP choses the best pat for traffic , this ensures efficient routing tables and redundancy.

Traffic Engineering and control

BGPs flexibility provides network administrators with precise control over the flow off traffic. Techniques such as AS Path prepending and route manipulation allows traffic engineering , pointing of traffic along preferred paths , and optimization of network performance

Global Reachability and Multihoming

For organisations that need global reachability or multihoming , BGP offers the means to advertise and manage diverse IP prefixes , allowing for seamless connectivity across various networks.

Policy control

BGP policy control makes use of rules and filters to manage how BGP routes are accepted and advertised between routers. This control is there to provide security , efficient network performance and managing traffic flow. Policies are outlined with conditions and actions , applied in ordered list and can filter routes based on different attributes such as AS number , community tags or prefix list.

Key aspects of BGP policy control

Route acceptance and advertisement-Policies dictate which routes are allowed in a routers routing table and which routes are advertised to neighbours.

Policy definition -Policies are set up/configured as a ordered list of terms. Every term has a condition and a action. A match in a earlier term stops the evaluation for that route

Behaviour over high latency satellite links

BGP doesn't perform great of high latency satellite links but it performs way better than OSPF, this is because it sends incremental updates and holds/maintains stable TCP sessions , though convergence may be slow. With BGP there are less frequent updates and its more centred on policy over speed , which makes it more stable over high latency links, updates are only sent when there are changes.

OSPF affect

Network performance

OSPF supports a hierarchical network design which enables/allows us to breakdown/divide our network into areas and decrease the amount of routing information that needs to be exchanged and processed. In OSPF if one link fails only the routers in that particular area have to quickly recalculate their routes , the rest of the network remains unaffected .Because of the features that OSPF comes with such as less routing information to process , lower bandwidth usage for updates and faster route recalculation it allows the network to operate more efficiently , with lower latency and better stability.

OSPF allows for improved network performance, this is because it supports load balancing to distribute traffic across various/multiple paths with equal cost , improving network utilization and ensuring reduced network congestion .

Fault tolerance

OSPF enabled routers on a network topology provide high availability and this is for many reasons mainly :

Fast convergence -When a link or a router fails OSPF quickly detects the failure using Hello packets and dead timers . Once a failure is detected the affected routers send Link state Advertisements to inform others of the change , each router then recalculates the best path using Dijkstra algorithm . This quick recalculation makes sure that traffic is rerouted through alternate paths almost immediately.

Multiple path support -OSPF supports multiple equal cost paths to destination . If one path fails ,OSPF can instantly forward traffic over another available equal cost route , this ensures continuous data delivery without disturbance.

Link State Database Synchronization -Each OSFP router maintains a LSDB that reflects the exact topology of the network .Now because every router has a full and consistent view it can rapidly find alternative routers in a situation where we have link or node failure.

Ability to grow WAN as the company expands

OSPF has the ability to grow the WAN as the company expands but it needs disciplined hierarchical planning. Adding a new regional office is not complicated if its designed as a new area, but a mesh of satellite links to remote warehouses can complicate the area design and may lead to scalability issues.

BGP affect

Network performance

BGP provides improved network performance it does this through route optimization. BGP allows networks to analyse multiple available paths for transmission of data and select the most efficient route based on :

- Network policies
- Path attributes
- Metrics like hope count and latency

Through route optimization, BGP decreases delay and allows for faster delivery of data.

Fault tolerance

The border gateway protocol provides good fault tolerance when issues between the networks are faced ,one of the most essential features of BGP is its ability to provide redundancy . By maintain many/multiple connections to upstream providers or peer networks ,BGP ensures :

Automatic Failover -If a single path fails ,BGP dynamically reroutes traffic to alternative routes

Load Balancing-Distributes traffic across many/multiple links to avoid congestion .

Ability to grow WAN as the company expands

BGP has the ability to grow the company WAN and this is because its built to scale across thousands of prefixes and many administrative domains. It supports route aggregation , policy controls and mechanism like route reflectors and confederations to manage very large deployments. BGP easily manages multihoming ,ISP failover and selective route advertisement which is very critical when adding new regions or ISPs.

2.2)The routing protocol id recommendation is implementation of OSPF for inter region routing the reason for this is because :

Routing Efficiency

OSPF supports a hierarchical network design which enables/allows us to breakdown/divide our network into areas and decrease the amount of routing information that needs to be exchanged and processed. In OSPF if one link fails only the routers in that particular area have to quickly recalculate their routes , the rest of the network remains unaffected .Because of the features that OSPF comes with such as less routing information to process , lower bandwidth usage for updates and faster route recalculation it allows the network to operate more efficiently , with lower latency and better stability.

OSPF allows for improved network performance, this is because it supports load balancing to distribute traffic across various/multiple paths with equal cost , improving network utilization and ensuring reduced network congestion .

Scalability

OSPF is a very scalable routing protocol , this is because of its hierarchical multi layer design , which breaks large networks into smaller manageable areas. This decreases the size of routing tables and reduces the impact of local changes on the rest of the network.

Another factor that allows OSPF to be scalable is that it’s a link state protocol that only sends updates when there’s a change in the network , rather than on a fixed timer. This decreases bandwidth requirements and usage

Resilience in a Mixed fibre satellite environment

OSPF is very resilient over mixed fibre satellite environments this is because :

OSPF has the ability to detect topology changes such as a link failure , when this is encountered it recalculates alternative paths , reducing downtime and packet loss .

In a multi area design , if there's failure in one non backbone area it wont trigger a recalculation of routes across the entire network , localizing the impact and improving overall network stability.

The SPF algorithm ensures/guarantees a loop free routing topology , which is required for network stability and reliability , especially with dynamic links.

How to integrate site level routing with inter region routing

The integration is achieved through running OSPF routing process across the entire WAN . Every router interface participating in the WAN routing will be placed in the OSPF Backbone area which is area 0 . This allows every router to have a complete view of all networks , enabling direct communication .

Hierarchy and OSPF Areas

While OSPF makes use of a flat area in this design a logical hierarchy exits in the IP addressing scheme which is essential for efficient routing.

Johannesburg HQ makes use of a router on a stick configuration with different VLAN's and subnets

Other branch offices/sites make use of a standard LAN topology with no VLAN's , devices are assigned IP addresses from a single network range.

All the routers in the topology have their WAN and LAN interfaces configured as part of OSPF area 0.

Configure Routing on the Router

The main routing protocol for the entire network is OSPF

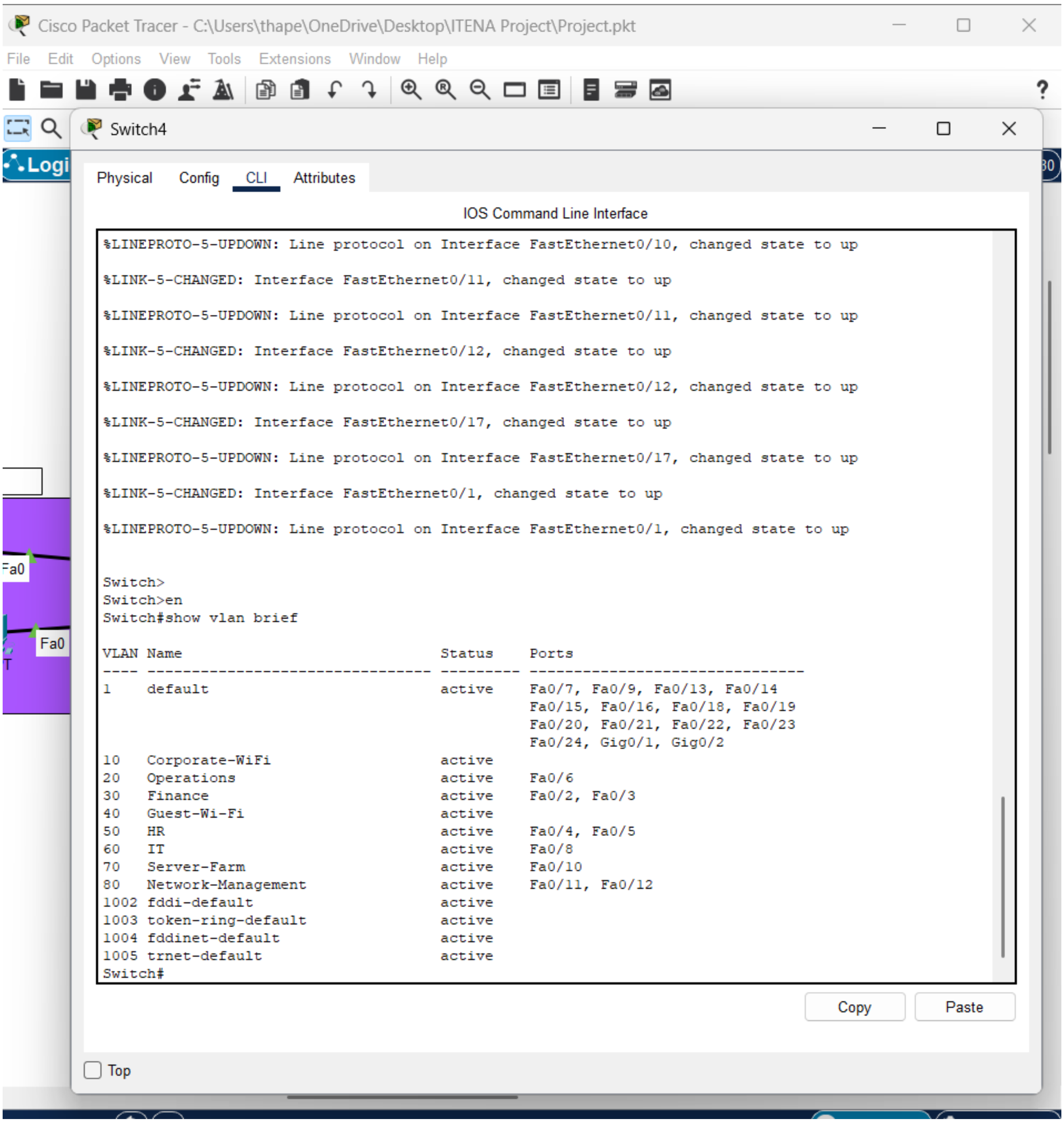
1)A single OSPF process is enabled on all routers

2 All directly connected networks that need to be reachable across the WAN are advertised into OSPF area 0 this includes :

- The point to point WAN links between routers
- The LAN subnets at each branch office
- The individual VLAN subnets on the HQ router

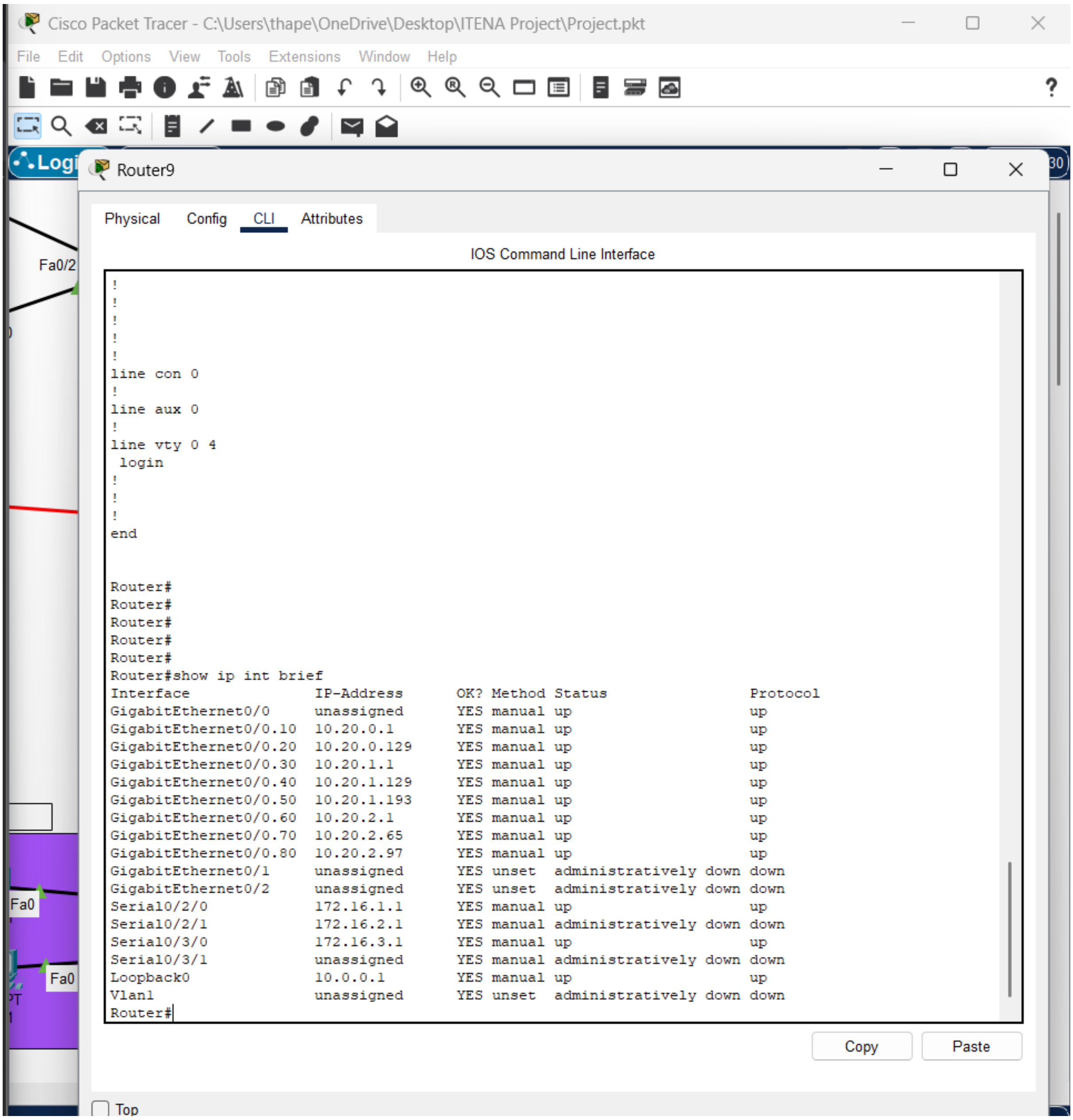
Question 3

3.1)Creation of VLANS on Switch and assignment of ports


Cisco Packet Tracer - C:\Users\thape\OneDrive\Desktop\ITENA Project\Project.pkt
File Edit Options View Tools Extensions Window Help
Switch4
Physical Config CLI Attributes
IOS Command Line Interface
Copy
Paste
Top

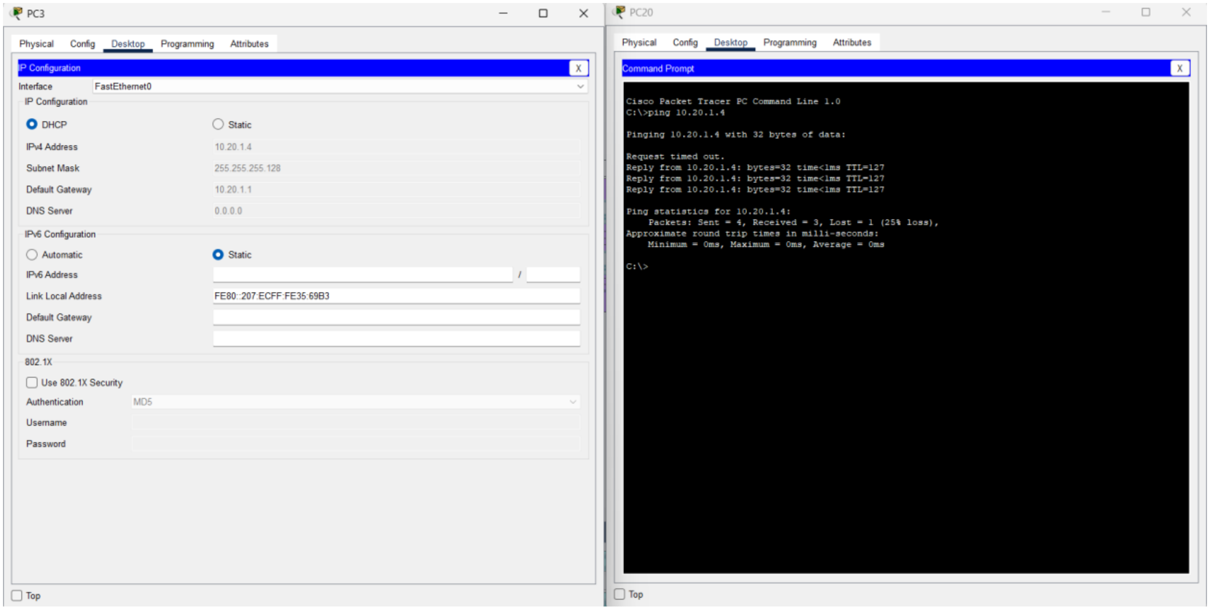
```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/17, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>
Switch>en
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/9, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
10   Corporate-WiFi                   active
20   Operations                       active    Fa0/6
30   Finance                          active    Fa0/2, Fa0/3
40   Guest-Wi-Fi                      active
50   HR                               active    Fa0/4, Fa0/5
60   IT                               active    Fa0/8
70   Server-Farm                      active    Fa0/10
80   Network-Management               active    Fa0/11, Fa0/12
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Verification of encapsulation configured on the router/ router on a stick configured and IP addresses assigned


Cisco Packet Tracer - C:\Users\thape\OneDrive\Desktop\ITENA Project\Project.pkt
File
Edit
Options
View
Tools
Extensions
Window
Help
Router9
Physical
Config
CLI
Attributes
IOS Command Line Interface
Copy
Paste
Top
Fa0/2
Fa0
Fa0

```
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end


Router#
Router#
Router#
Router#
Router#
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual up                    up
GigabitEthernet0/0.10  10.20.0.1       YES manual up                    up
GigabitEthernet0/0.20  10.20.0.129     YES manual up                    up
GigabitEthernet0/0.30  10.20.1.1       YES manual up                    up
GigabitEthernet0/0.40  10.20.1.129     YES manual up                    up
GigabitEthernet0/0.50  10.20.1.193     YES manual up                    up
GigabitEthernet0/0.60  10.20.2.1       YES manual up                    up
GigabitEthernet0/0.70  10.20.2.65      YES manual up                    up
GigabitEthernet0/0.80  10.20.2.97      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/2/0            172.16.1.1      YES manual up                    up
Serial0/2/1            172.16.2.1      YES manual administratively down down
Serial0/3/0            172.16.3.1      YES manual up                    up
Serial0/3/1            unassigned      YES manual administratively down down
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
```

Verification of inter VLAN routing



Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address	10.20.1.4
Subnet Mask	255.255.255.128
Default Gateway	10.20.1.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::207:ECFF:FE35:69B3
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

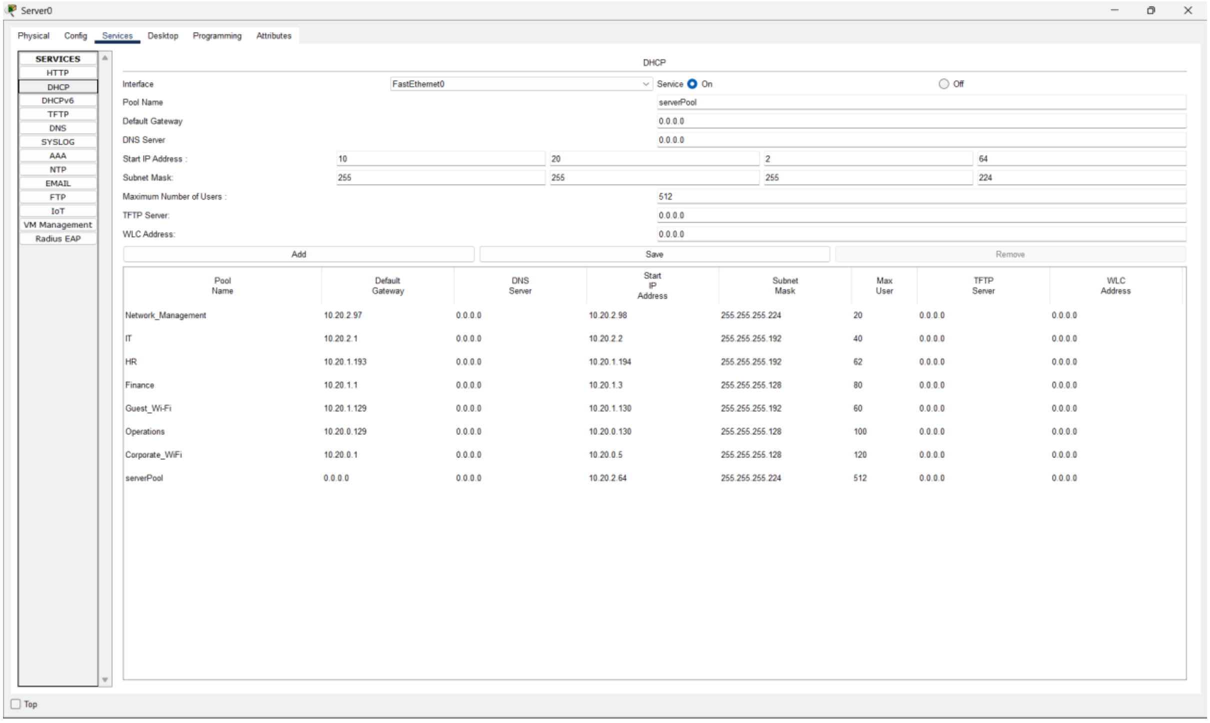
Authentication	MD5
Username	
Password	

□ Top

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.20.1.4

Pinging 10.20.1.4 with 32 bytes of data:

Request timed out.
Reply from 10.20.1.4: bytes=32 time<1ms TTL=127
Reply from 10.20.1.4: bytes=32 time<1ms TTL=127
Reply from 10.20.1.4: bytes=32 time<1ms TTL=127

Ping statistics for 10.20.1.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

□ Top

DHCP Scope configuration on server



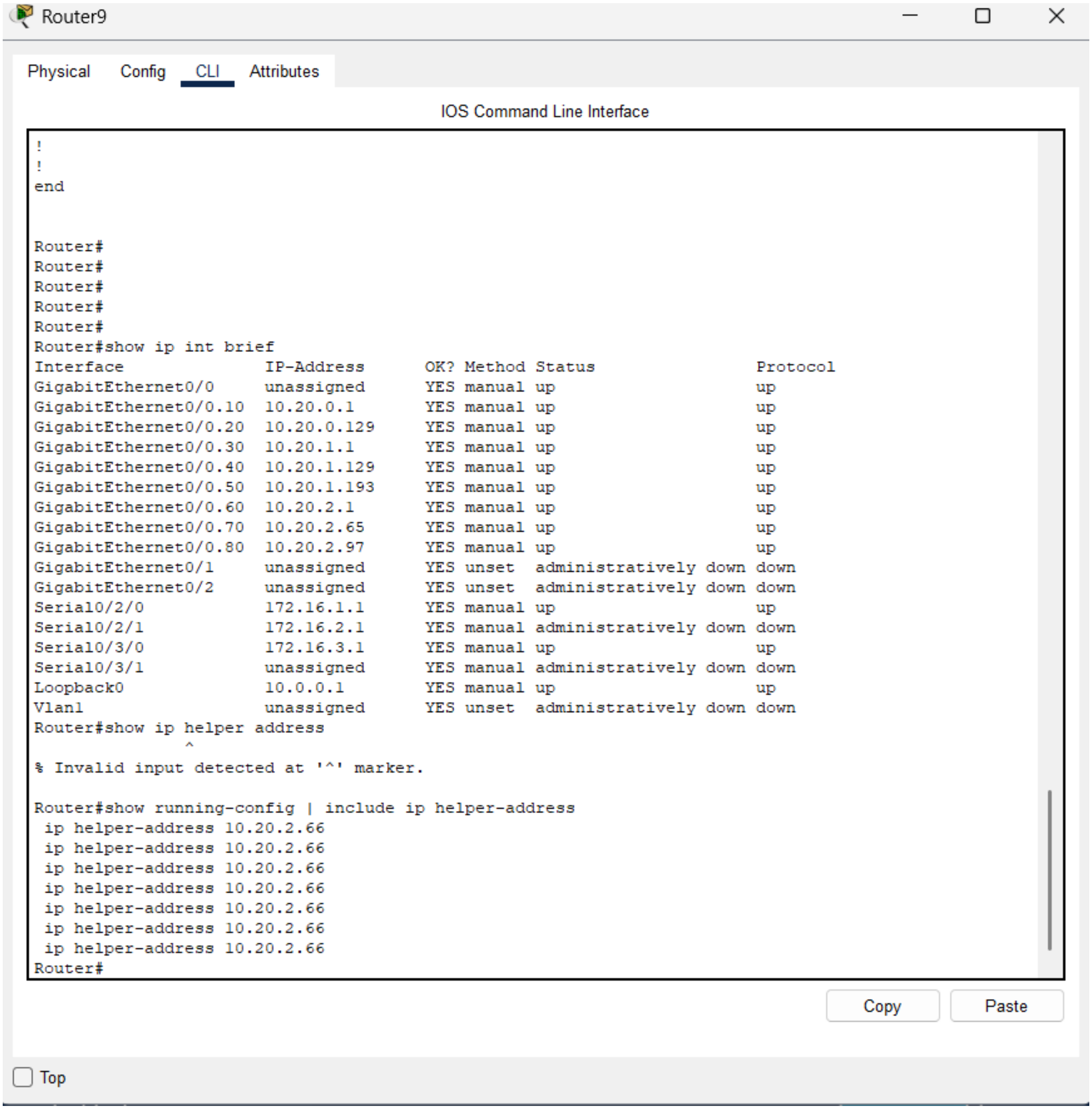
Interface: FastEthernet0 Service ● On ○ Off

Pool Name	serverPool			
Default Gateway	0.0.0.0			
DNS Server	0.0.0.0			
Start IP Address :	10	20	2	64
Subnet Mask:	255	255	255	224
Maximum Number of Users :	512			
TFTP Server:	0.0.0.0			
WLC Address:	0.0.0.0			

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
Network_Management	10.20.2.97	0.0.0.0	10.20.2.98	255.255.255.224	20	0.0.0.0	0.0.0.0
IT	10.20.2.1	0.0.0.0	10.20.2.2	255.255.255.192	40	0.0.0.0	0.0.0.0
HR	10.20.1.193	0.0.0.0	10.20.1.194	255.255.255.192	62	0.0.0.0	0.0.0.0
Finance	10.20.1.1	0.0.0.0	10.20.1.3	255.255.255.128	80	0.0.0.0	0.0.0.0
Guest_Wi-Fi	10.20.1.129	0.0.0.0	10.20.1.130	255.255.255.192	60	0.0.0.0	0.0.0.0
Operations	10.20.0.129	0.0.0.0	10.20.0.130	255.255.255.128	100	0.0.0.0	0.0.0.0
Corporate_WiFi	10.20.0.1	0.0.0.0	10.20.0.5	255.255.255.128	120	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	10.20.2.64	255.255.255.224	512	0.0.0.0	0.0.0.0

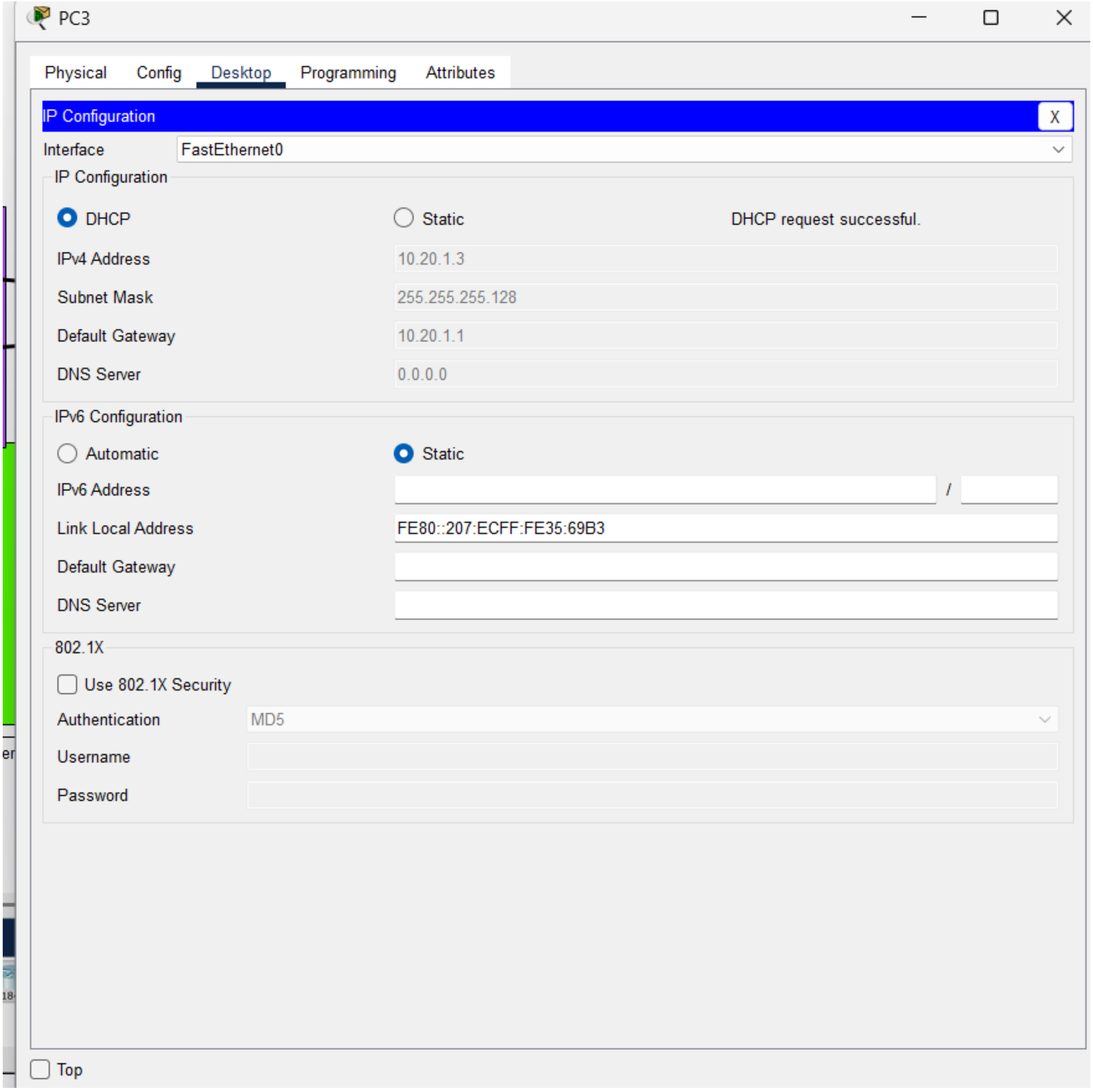
□ Top

IP helper configuration on the router so that all devices in different VLANS get their required IP address



```
!
!
end


Router#
Router#
Router#
Router#
Router#
Router#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     unassigned      YES manual up                    up
GigabitEthernet0/0.10  10.20.0.1       YES manual up                    up
GigabitEthernet0/0.20  10.20.0.129     YES manual up                    up
GigabitEthernet0/0.30  10.20.1.1       YES manual up                    up
GigabitEthernet0/0.40  10.20.1.129     YES manual up                    up
GigabitEthernet0/0.50  10.20.1.193     YES manual up                    up
GigabitEthernet0/0.60  10.20.2.1       YES manual up                    up
GigabitEthernet0/0.70  10.20.2.65      YES manual up                    up
GigabitEthernet0/0.80  10.20.2.97      YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/2/0            172.16.1.1      YES manual up                    up
Serial0/2/1            172.16.2.1      YES manual administratively down down
Serial0/3/0            172.16.3.1      YES manual up                    up
Serial0/3/1            unassigned      YES manual administratively down down
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#show ip helper address
               ^
% Invalid input detected at '^' marker.

Router#show running-config | include ip helper-address
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
 ip helper-address 10.20.2.66
Router#
```

Verification of devices getting the correct IP address from the DHCP server


PC3

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 10.20.1.3

Subnet Mask: 255.255.255.128

Default Gateway: 10.20.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::207:ECFF:FE35:69B3

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

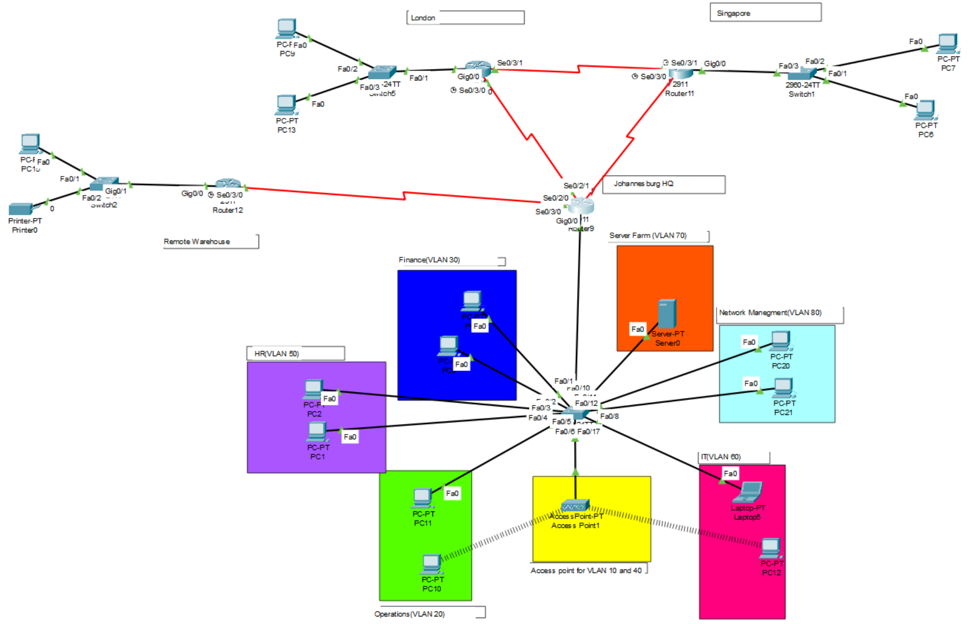
Authentication: MD5

Username:

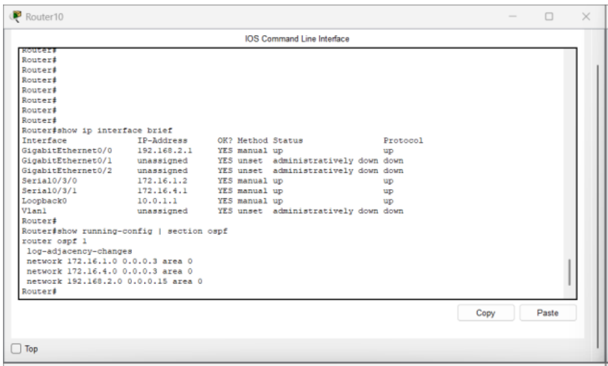
Password:

□ Top

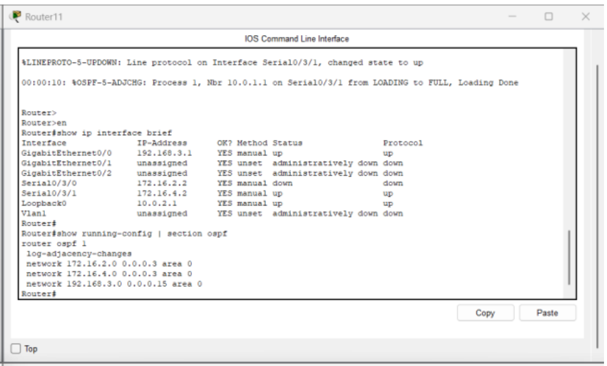
3.2)Topology , with the interconnected sites (London and Singapore) and a remote ware house attached to HQ via serial



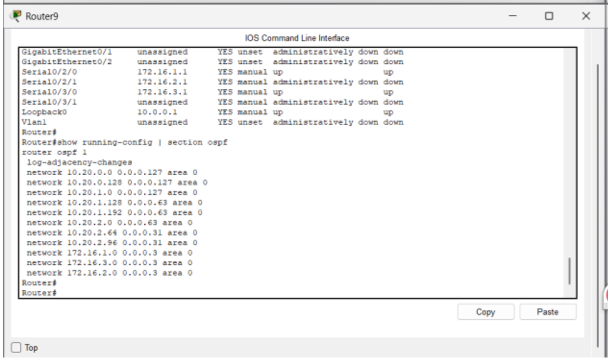
Addresses for Point to Point WAN links configured on routers , advertisement of a loopback address



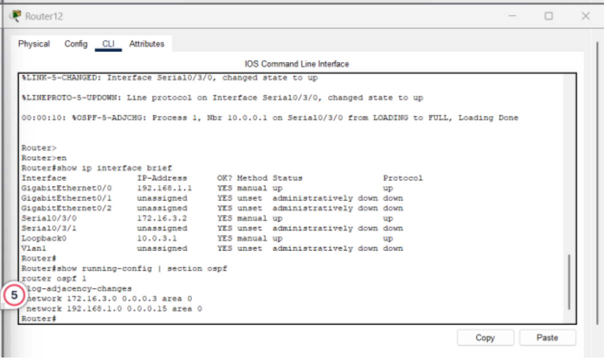
```
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.2.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            172.16.1.2      YES manual up                    up
Serial0/3/1            172.16.4.1      YES manual up                    up
Loopback0              10.0.1.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#show running-config | section ospf
router ospf 1
 log-adjacency-changes
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.4.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.15 area 0
Router#
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/1, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.1.1 on Serial0/3/1 from LOADING to FULL, Loading Done


Router>
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.3.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            172.16.2.2      YES manual down                  down
Serial0/3/1            172.16.4.2      YES manual up                    up
Loopback0              10.0.2.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#show running-config | section ospf
router ospf 1
 log-adjacency-changes
 network 172.16.2.0 0.0.0.3 area 0
 network 172.16.4.0 0.0.0.3 area 0
 network 192.168.3.0 0.0.0.15 area 0
Router#
```

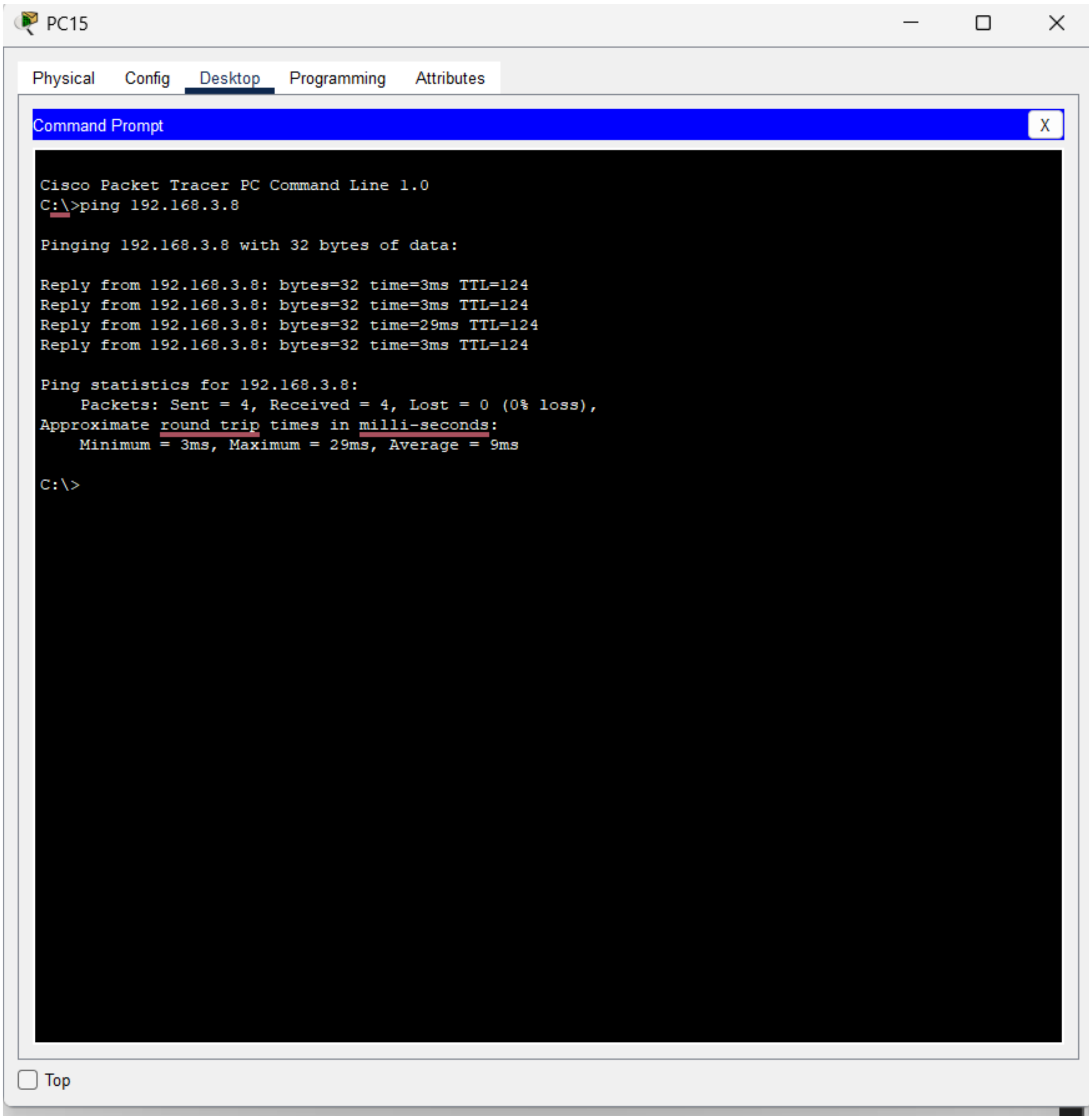


```
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/2/0            172.16.1.1      YES manual up                    up
Serial0/2/1            172.16.2.1      YES manual administratively down down
Serial0/3/0            172.16.3.1      YES manual up                    up
Serial0/3/1            unassigned      YES manual administratively down down
Loopback0              10.0.0.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#show running-config | section ospf
router ospf 1
 log-adjacency-changes
 network 10.20.0.0 0.0.0.127 area 0
 network 10.20.0.128 0.0.0.127 area 0
 network 10.20.1.0 0.0.0.127 area 0
 network 10.20.1.128 0.0.0.63 area 0
 network 10.20.1.192 0.0.0.63 area 0
 network 10.20.2.0 0.0.0.63 area 0
 network 10.20.2.64 0.0.0.31 area 0
 network 10.20.2.96 0.0.0.31 area 0
 network 172.16.1.0 0.0.0.3 area 0
 network 172.16.3.0 0.0.0.3 area 0
 network 172.16.2.0 0.0.0.3 area 0
Router#
Router#
```



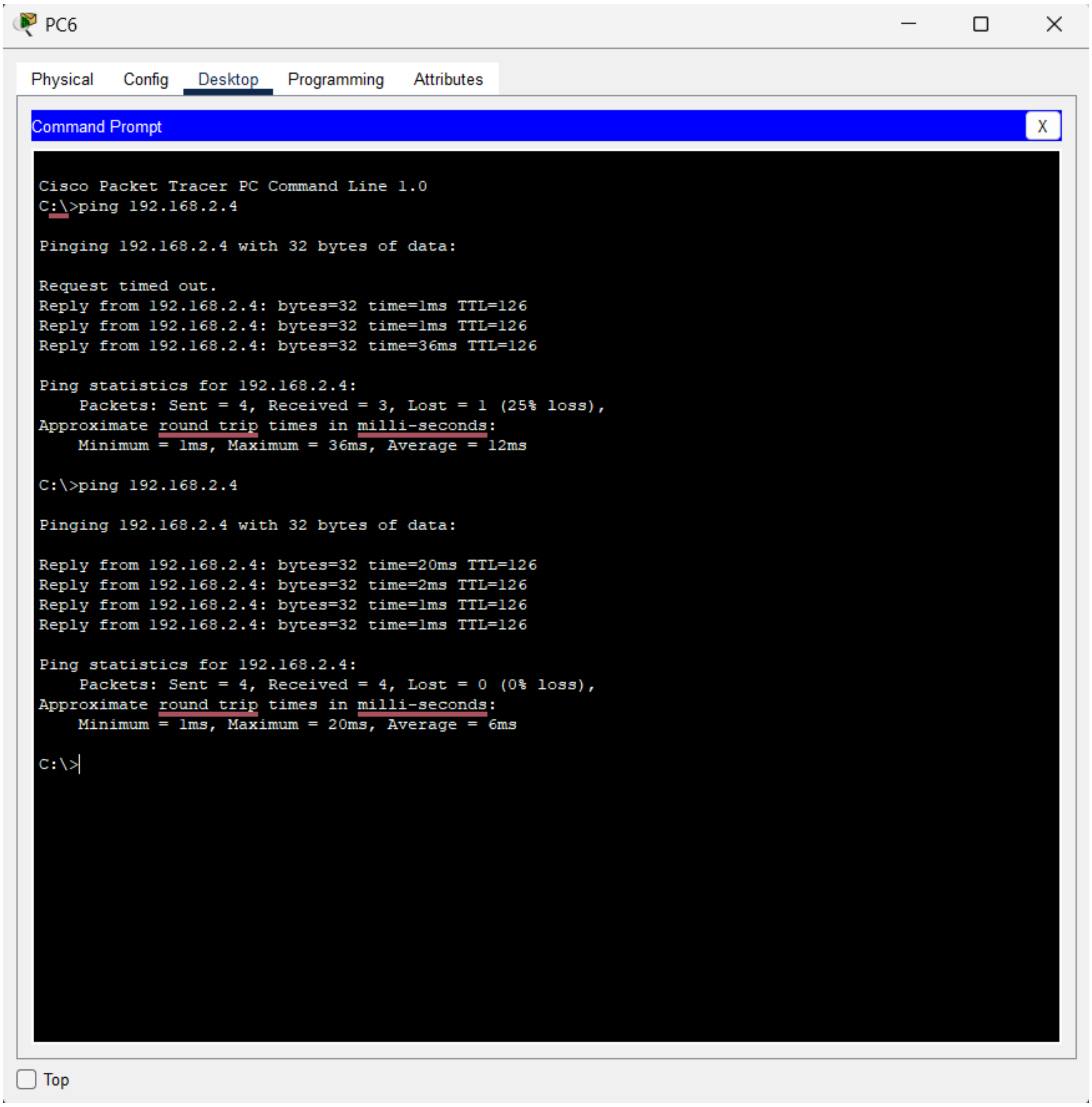
```
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Serial0/3/0 from LOADING to FULL, Loading Done


Router>
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/3/0            172.16.3.2      YES manual up                    up
Serial0/3/1            unassigned      YES unset  administratively down down
Loopback0              10.0.3.1        YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#show running-config | section ospf
router ospf 1
 log-adjacency-changes
 network 172.16.3.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.15 area 0
Router#
```

Remote Warehouse ping Singapore



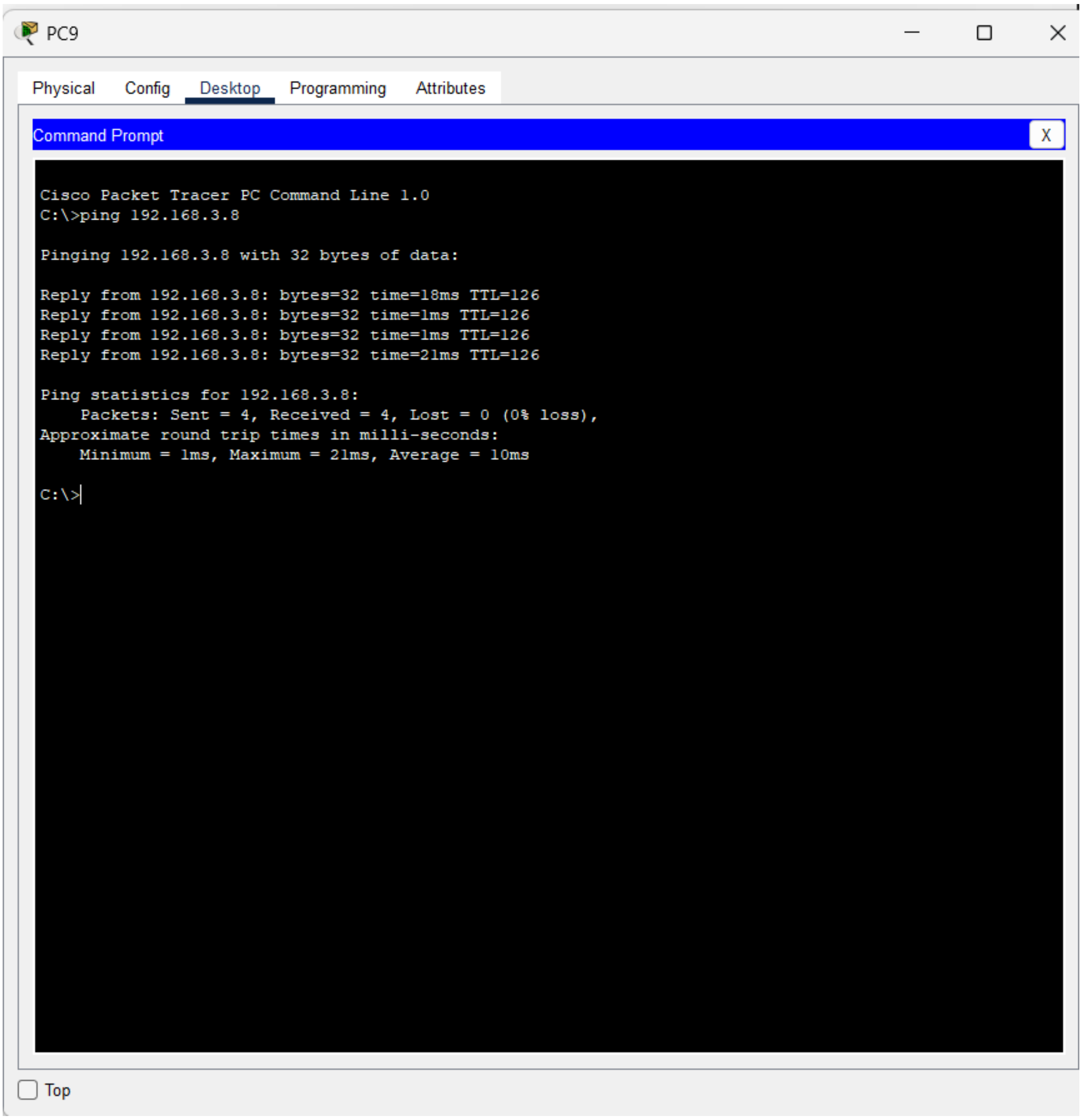
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.8

Pinging 192.168.3.8 with 32 bytes of data:

Reply from 192.168.3.8: bytes=32 time=3ms TTL=124
Reply from 192.168.3.8: bytes=32 time=3ms TTL=124
Reply from 192.168.3.8: bytes=32 time=29ms TTL=124
Reply from 192.168.3.8: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 29ms, Average = 9ms

C:\>
```

Singapore to London



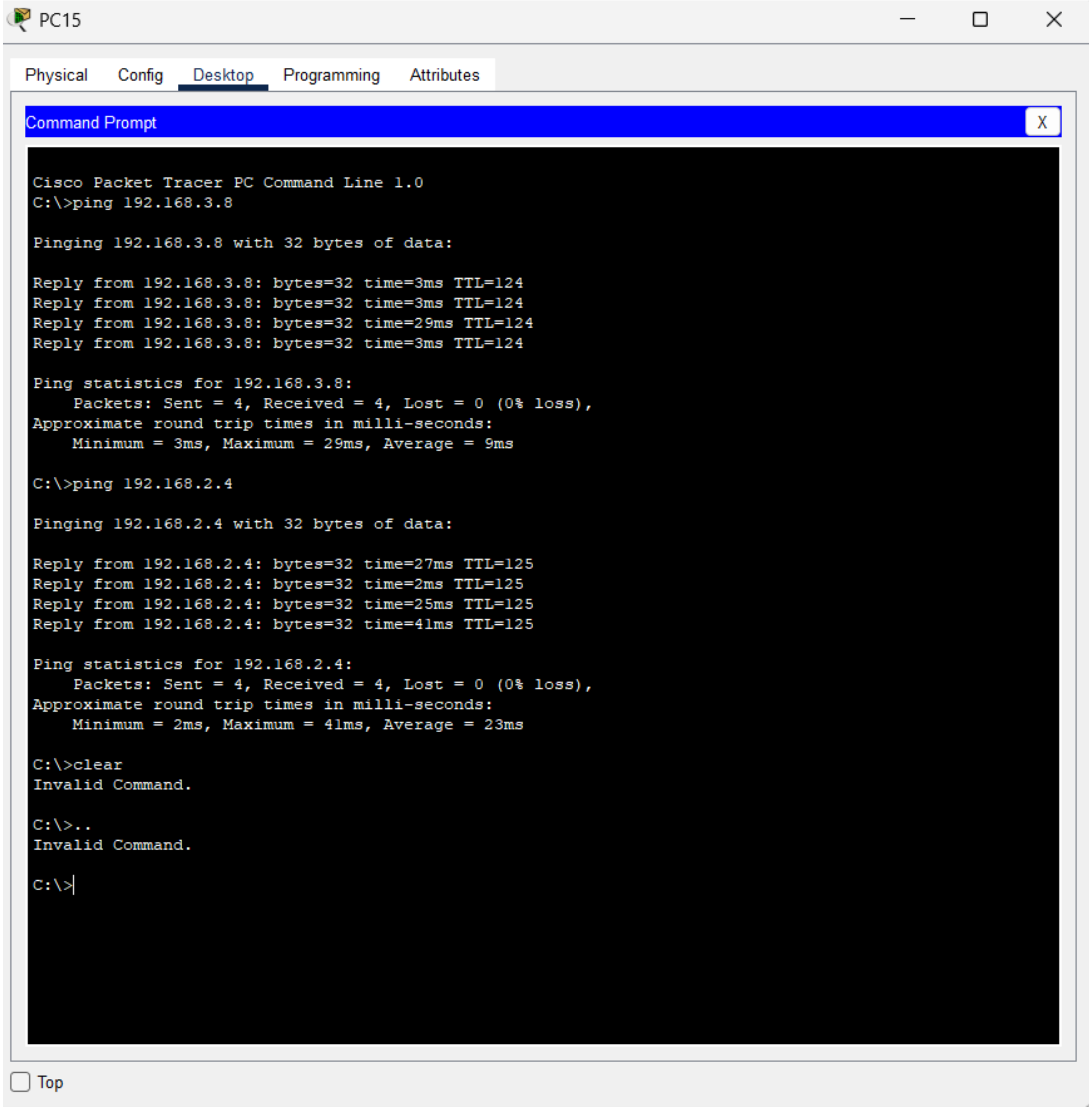
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=36ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 36ms, Average = 12ms

C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=20ms TTL=126
Reply from 192.168.2.4: bytes=32 time=2ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 6ms

C:\>
```

London to Singapore



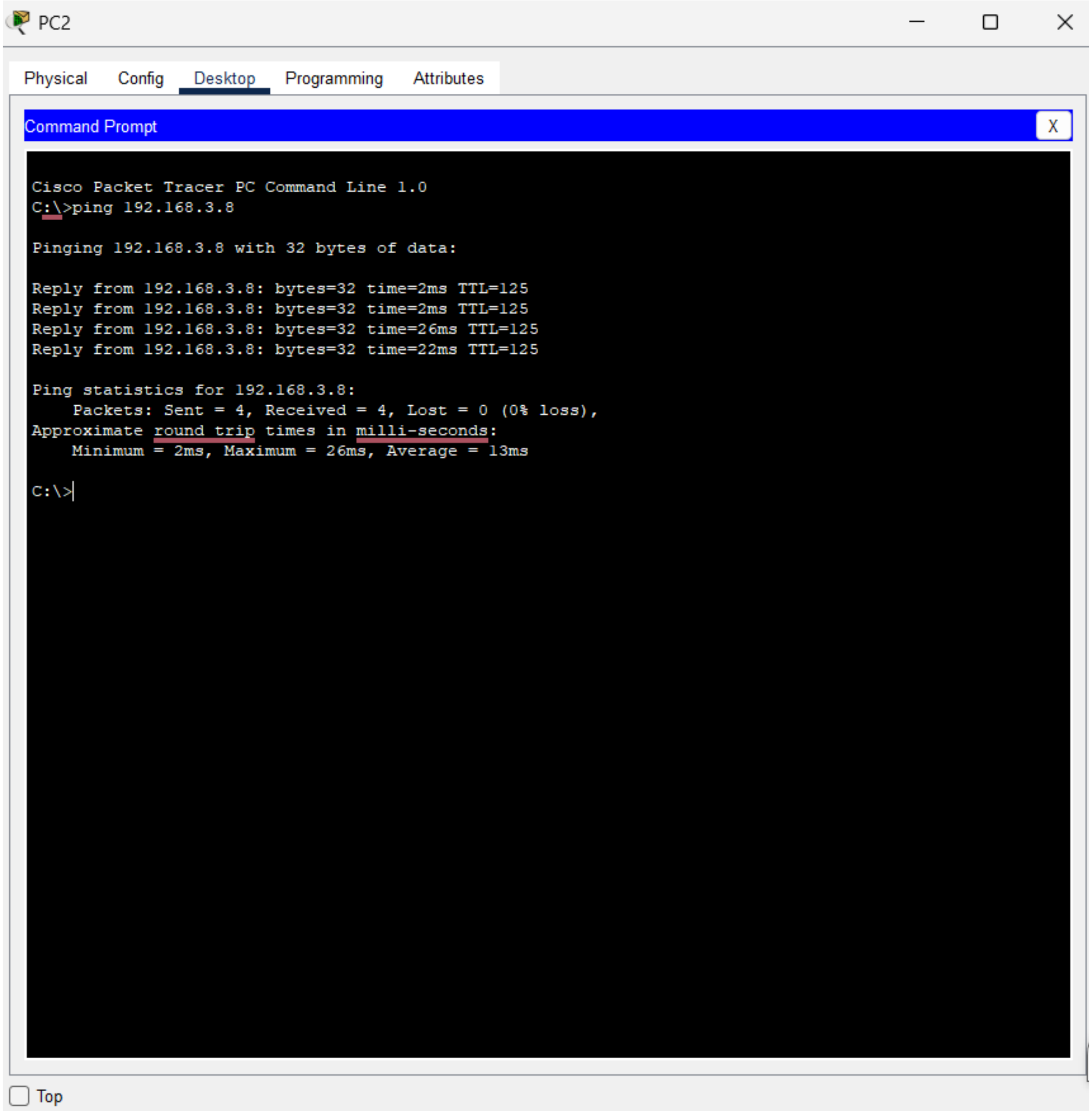
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.8

Pinging 192.168.3.8 with 32 bytes of data:

Reply from 192.168.3.8: bytes=32 time=18ms TTL=126
Reply from 192.168.3.8: bytes=32 time=1ms TTL=126
Reply from 192.168.3.8: bytes=32 time=1ms TTL=126
Reply from 192.168.3.8: bytes=32 time=21ms TTL=126

Ping statistics for 192.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 10ms

C:\>
```

Remote Warehouse to London



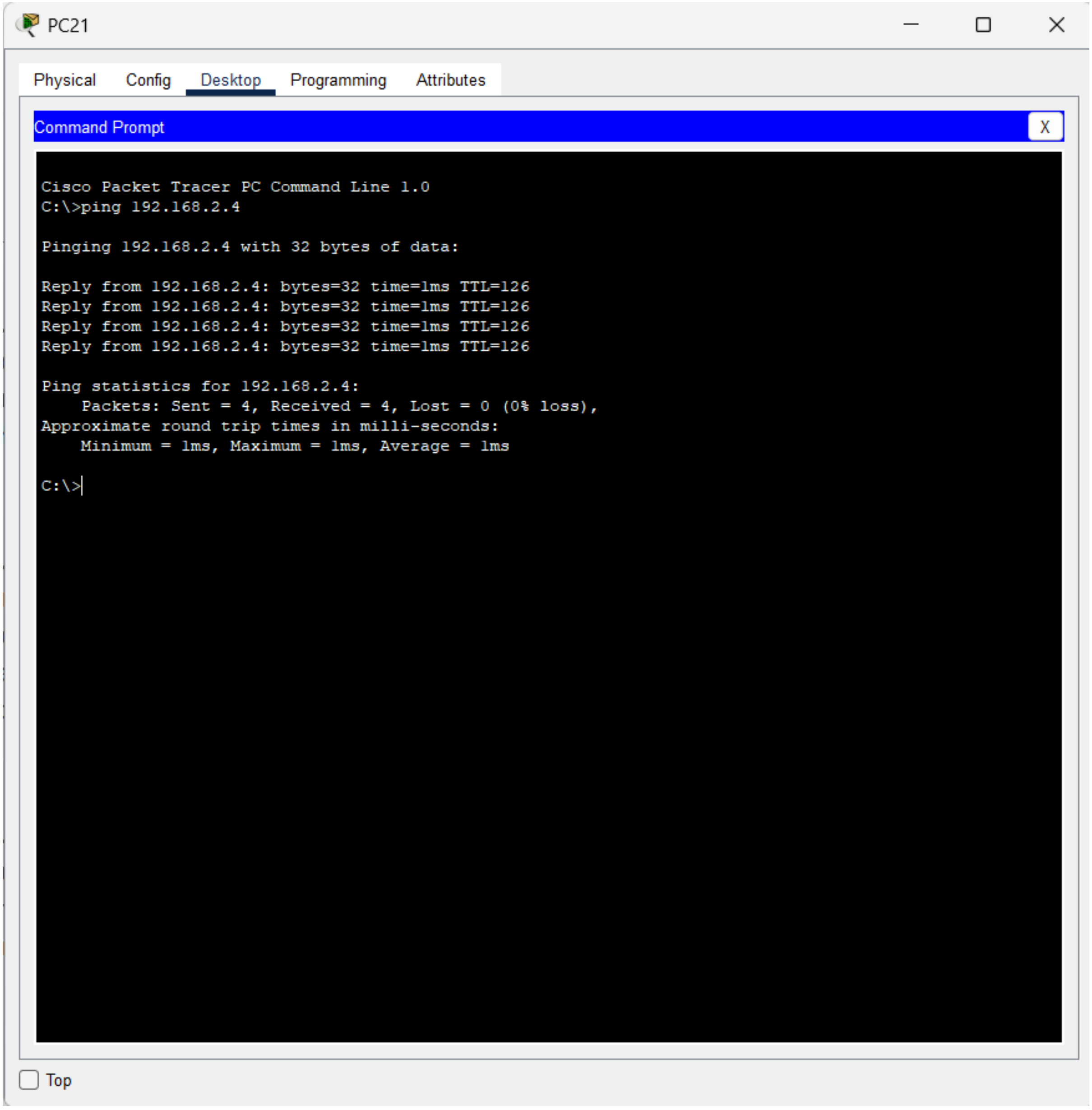
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.8

Pinging 192.168.3.8 with 32 bytes of data:

Reply from 192.168.3.8: bytes=32 time=3ms TTL=124
Reply from 192.168.3.8: bytes=32 time=3ms TTL=124
Reply from 192.168.3.8: bytes=32 time=29ms TTL=124
Reply from 192.168.3.8: bytes=32 time=3ms TTL=124

Ping statistics for 192.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 29ms, Average = 9ms

C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=27ms TTL=125
Reply from 192.168.2.4: bytes=32 time=2ms TTL=125
Reply from 192.168.2.4: bytes=32 time=25ms TTL=125
Reply from 192.168.2.4: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 41ms, Average = 23ms

C:\>clear
Invalid Command.

C:\>..
Invalid Command.

C:\>
```

HR pc to Singapore



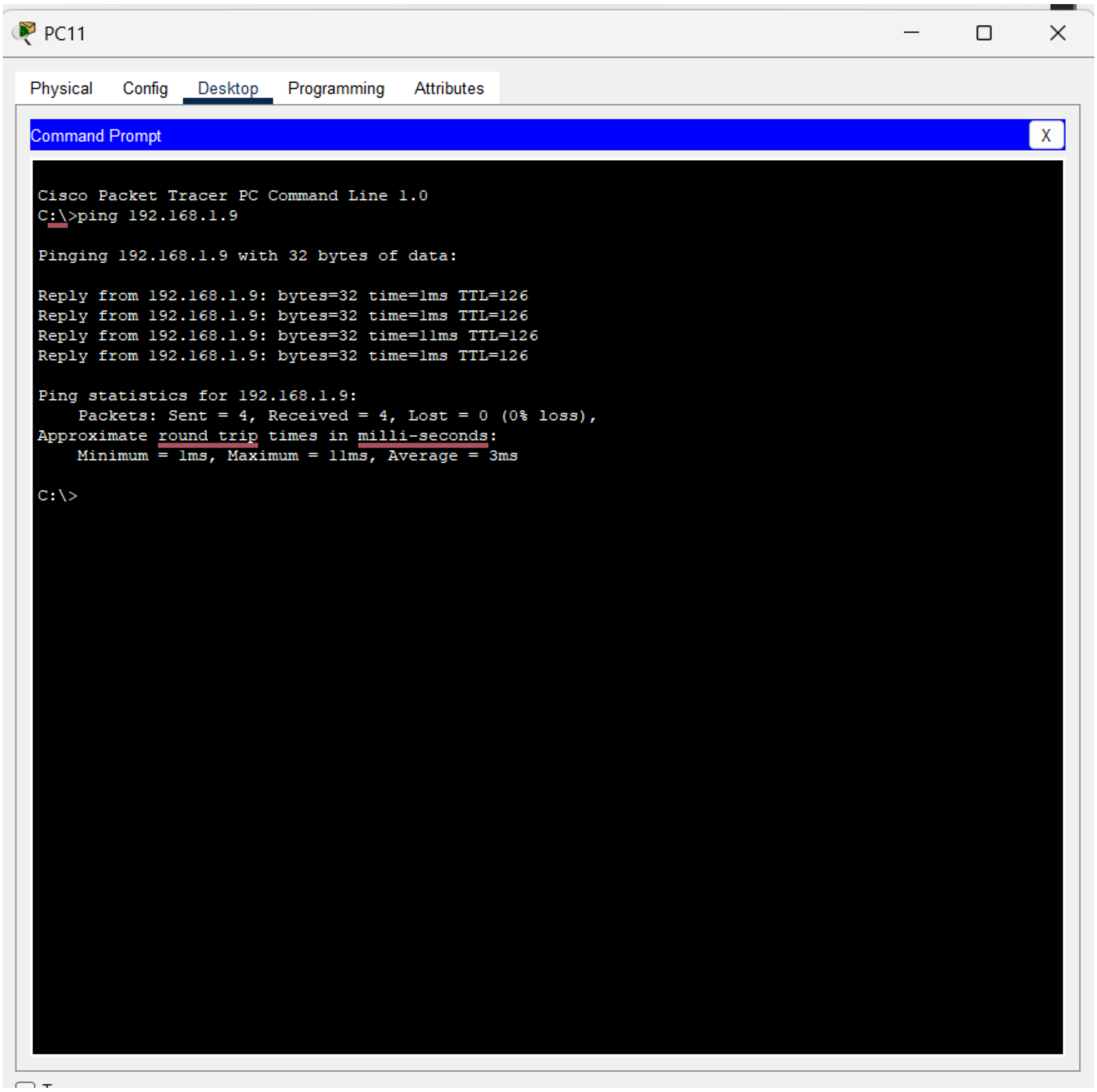
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.8

Pinging 192.168.3.8 with 32 bytes of data:

Reply from 192.168.3.8: bytes=32 time=2ms TTL=125
Reply from 192.168.3.8: bytes=32 time=2ms TTL=125
Reply from 192.168.3.8: bytes=32 time=26ms TTL=125
Reply from 192.168.3.8: bytes=32 time=22ms TTL=125

Ping statistics for 192.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 26ms, Average = 13ms

C:\>
```

Network Management to London



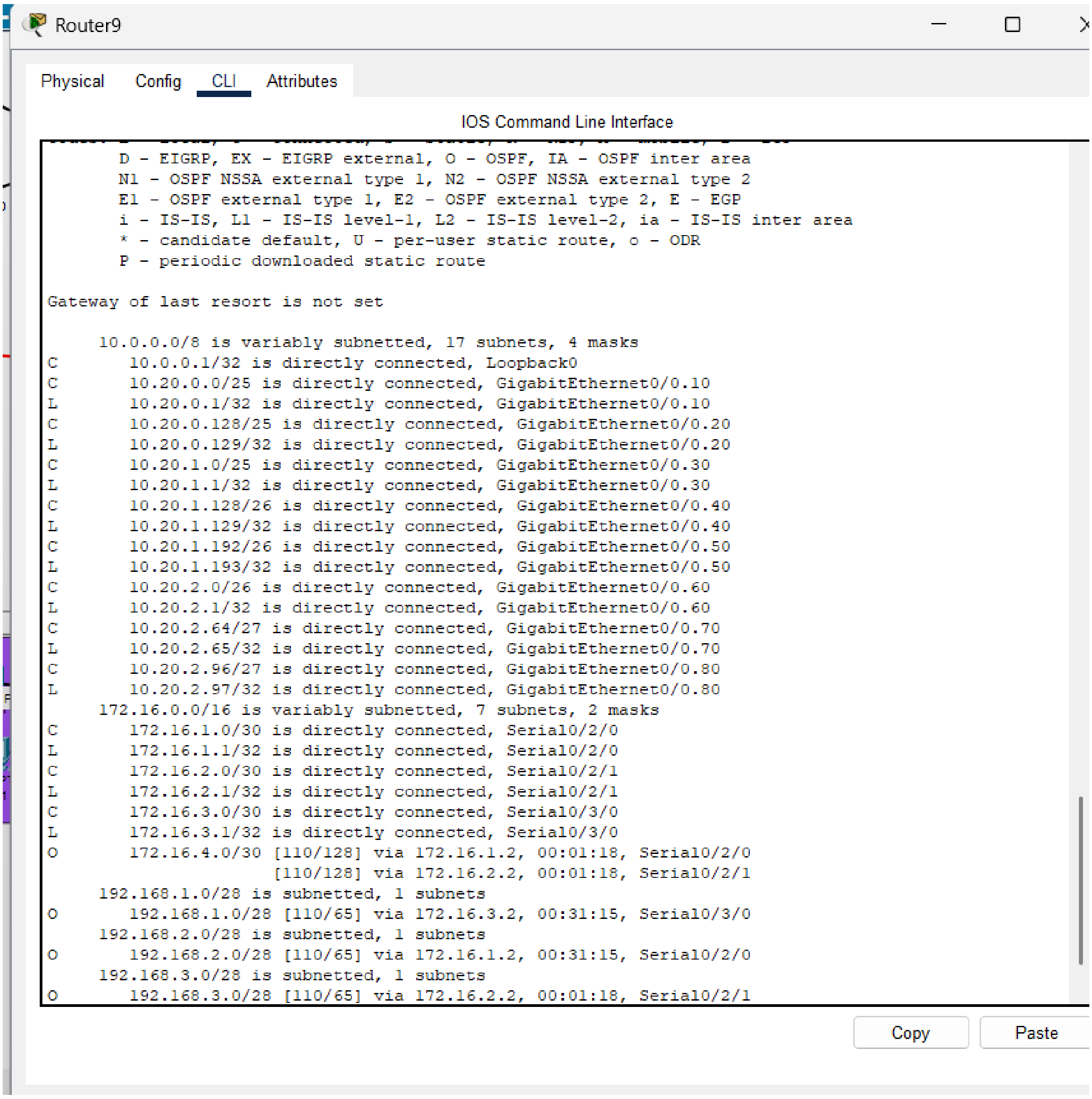
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126
Reply from 192.168.2.4: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Operations to remote warehouse pc



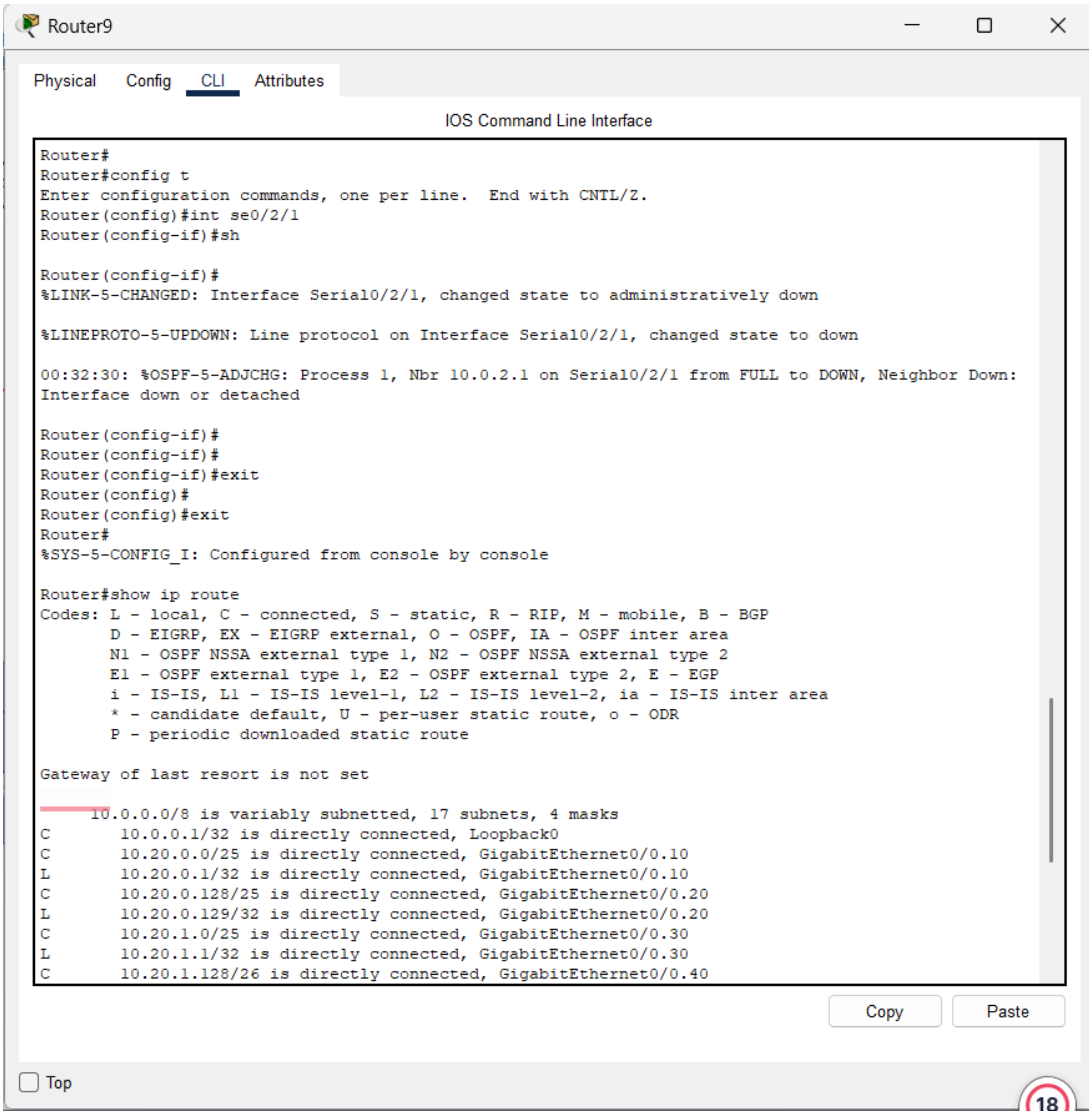
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.9

Pinging 192.168.1.9 with 32 bytes of data:

Reply from 192.168.1.9: bytes=32 time=1ms TTL=126
Reply from 192.168.1.9: bytes=32 time=1ms TTL=126
Reply from 192.168.1.9: bytes=32 time=11ms TTL=126
Reply from 192.168.1.9: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>
```

3.3)Routing Table before link failure



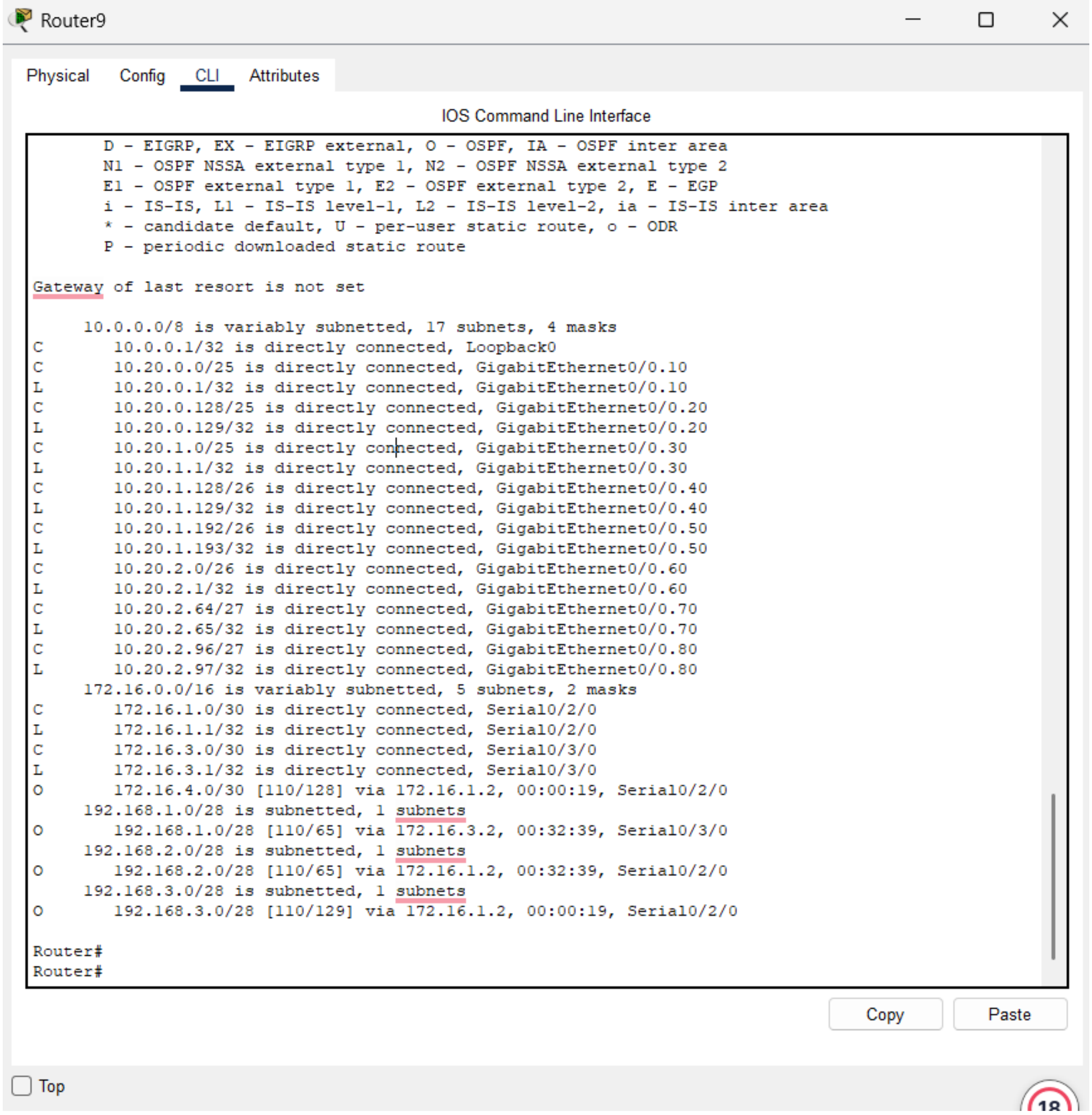
```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
C       10.0.0.1/32 is directly connected, Loopback0
C       10.20.0.0/25 is directly connected, GigabitEthernet0/0.10
L       10.20.0.1/32 is directly connected, GigabitEthernet0/0.10
C       10.20.0.128/25 is directly connected, GigabitEthernet0/0.20
L       10.20.0.129/32 is directly connected, GigabitEthernet0/0.20
C       10.20.1.0/25 is directly connected, GigabitEthernet0/0.30
L       10.20.1.1/32 is directly connected, GigabitEthernet0/0.30
C       10.20.1.128/26 is directly connected, GigabitEthernet0/0.40
L       10.20.1.129/32 is directly connected, GigabitEthernet0/0.40
C       10.20.1.192/26 is directly connected, GigabitEthernet0/0.50
L       10.20.1.193/32 is directly connected, GigabitEthernet0/0.50
C       10.20.2.0/26 is directly connected, GigabitEthernet0/0.60
L       10.20.2.1/32 is directly connected, GigabitEthernet0/0.60
C       10.20.2.64/27 is directly connected, GigabitEthernet0/0.70
L       10.20.2.65/32 is directly connected, GigabitEthernet0/0.70
C       10.20.2.96/27 is directly connected, GigabitEthernet0/0.80
L       10.20.2.97/32 is directly connected, GigabitEthernet0/0.80
     172.16.0.0/16 is variably subnetted, 7 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Serial0/2/0
L       172.16.1.1/32 is directly connected, Serial0/2/0
C       172.16.2.0/30 is directly connected, Serial0/2/1
L       172.16.2.1/32 is directly connected, Serial0/2/1
C       172.16.3.0/30 is directly connected, Serial0/3/0
L       172.16.3.1/32 is directly connected, Serial0/3/0
O       172.16.4.0/30 [110/128] via 172.16.1.2, 00:01:18, Serial0/2/0
                      [110/128] via 172.16.2.2, 00:01:18, Serial0/2/1
     192.168.1.0/28 is subnetted, 1 subnets
O       192.168.1.0/28 [110/65] via 172.16.3.2, 00:31:15, Serial0/3/0
     192.168.2.0/28 is subnetted, 1 subnets
O       192.168.2.0/28 [110/65] via 172.16.1.2, 00:31:15, Serial0/2/0
     192.168.3.0/28 is subnetted, 1 subnets
O       192.168.3.0/28 [110/65] via 172.16.2.2, 00:01:18, Serial0/2/1
```

Link Failure simulation



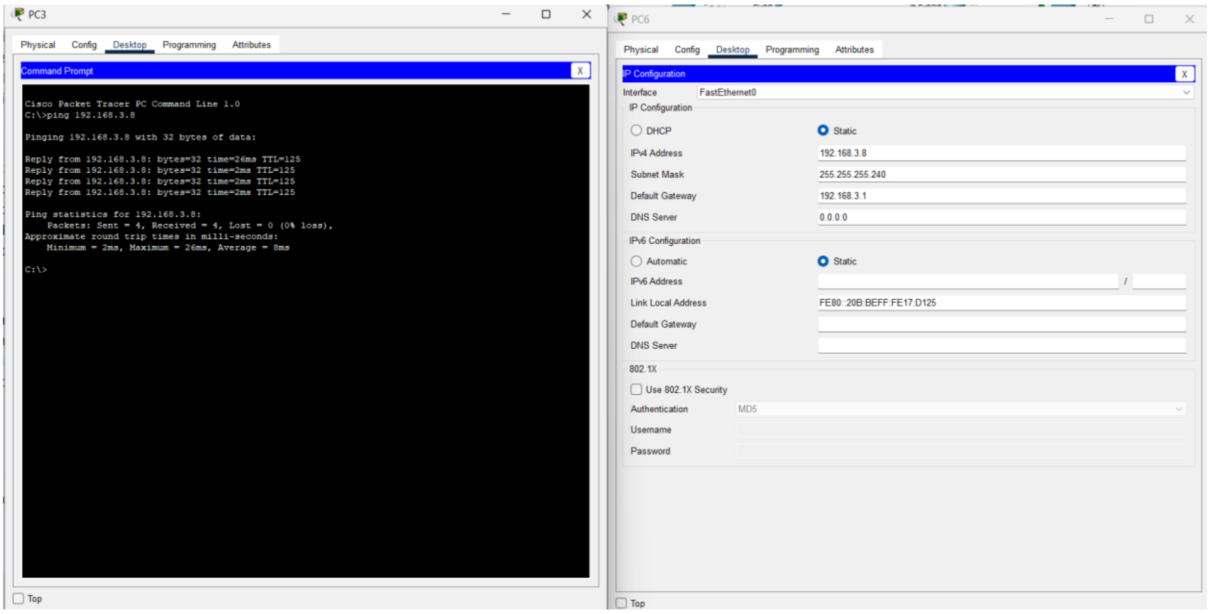
```
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int se0/2/1
Router(config-if)#sh

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/2/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2/1, changed state to down

00:32:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.2.1 on Serial0/2/1 from FULL to DOWN, Neighbor Down:
Interface down or detached

Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show ip route
Codes: L - local, C - connected, S - static, 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

     10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
C       10.0.0.1/32 is directly connected, Loopback0
C       10.20.0.0/25 is directly connected, GigabitEthernet0/0.10
L       10.20.0.1/32 is directly connected, GigabitEthernet0/0.10
C       10.20.0.128/25 is directly connected, GigabitEthernet0/0.20
L       10.20.0.129/32 is directly connected, GigabitEthernet0/0.20
C       10.20.1.0/25 is directly connected, GigabitEthernet0/0.30
L       10.20.1.1/32 is directly connected, GigabitEthernet0/0.30
C       10.20.1.128/26 is directly connected, GigabitEthernet0/0.40
```

Routing table after link failure



```
       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

     10.0.0.0/8 is variably subnetted, 17 subnets, 4 masks
C       10.0.0.1/32 is directly connected, Loopback0
C       10.20.0.0/25 is directly connected, GigabitEthernet0/0.10
L       10.20.0.1/32 is directly connected, GigabitEthernet0/0.10
C       10.20.0.128/25 is directly connected, GigabitEthernet0/0.20
L       10.20.0.129/32 is directly connected, GigabitEthernet0/0.20
C       10.20.1.0/25 is directly connected, GigabitEthernet0/0.30
L       10.20.1.1/32 is directly connected, GigabitEthernet0/0.30
C       10.20.1.128/26 is directly connected, GigabitEthernet0/0.40
L       10.20.1.129/32 is directly connected, GigabitEthernet0/0.40
C       10.20.1.192/26 is directly connected, GigabitEthernet0/0.50
L       10.20.1.193/32 is directly connected, GigabitEthernet0/0.50
C       10.20.2.0/26 is directly connected, GigabitEthernet0/0.60
L       10.20.2.1/32 is directly connected, GigabitEthernet0/0.60
C       10.20.2.64/27 is directly connected, GigabitEthernet0/0.70
L       10.20.2.65/32 is directly connected, GigabitEthernet0/0.70
C       10.20.2.96/27 is directly connected, GigabitEthernet0/0.80
L       10.20.2.97/32 is directly connected, GigabitEthernet0/0.80
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C       172.16.1.0/30 is directly connected, Serial0/2/0
L       172.16.1.1/32 is directly connected, Serial0/2/0
C       172.16.3.0/30 is directly connected, Serial0/3/0
L       172.16.3.1/32 is directly connected, Serial0/3/0
O       172.16.4.0/30 [110/128] via 172.16.1.2, 00:00:19, Serial0/2/0
     192.168.1.0/28 is subnetted, 1 subnets
O       192.168.1.0/28 [110/65] via 172.16.3.2, 00:32:39, Serial0/3/0
     192.168.2.0/28 is subnetted, 1 subnets
O       192.168.2.0/28 [110/65] via 172.16.1.2, 00:32:39, Serial0/2/0
     192.168.3.0/28 is subnetted, 1 subnets
O       192.168.3.0/28 [110/129] via 172.16.1.2, 00:00:19, Serial0/2/0

Router#
Router#
```

Finance pc being able to ping Singapore devices during link failure



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.8

Pinging 192.168.3.8 with 32 bytes of data:

Reply from 192.168.3.8: bytes=32 time=26ms TTL=125
Reply from 192.168.3.8: bytes=32 time=2ms TTL=125
Reply from 192.168.3.8: bytes=32 time=2ms TTL=125
Reply from 192.168.3.8: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 26ms, Average = 8ms

C:\>
```

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.3.8

Subnet Mask: 255.255.255.240

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::20B:BEFF:FE17:D125

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

How failover was achieved :

OSPF detected link failure between HQ and Singapore using Hello packets and the Dead timer .Once the link was declared down , OSPF recalculated the topology using SPF algorithm. The new best path to Singapore was via London so routing tables updated automatically . This made sure that traffic was rerouted seamlessly without the need of manual intervention .

Question 4

4.1)To address the issue of bandwidth congestion during peak hours TransGlobe should make use of a Quality of Service with Traffic Shaping and Local Content caching , the two techniques will help decrease jitter, delays for real time applications and it they will help improve network reliability.

Quality of Service

QoS refers to the techniques and mechanisms utilized to manage and prioritize network traffic to make sure that a certain level of performance, reliability and availability for certain applications or services .QoS manages/controls factors like bandwidth ,latency, jitter and packet loos to ensure the necessary requirements of critical applications are met and optimization of the network .QoS classifies and marks packets based on their importance and then makes sure that high priority traffic receives the necessary/required bandwidth and low latency across both LAN and WAN links.

How it improves performance

Reduced Congestion -Through higher prioritization to real time application quality of service ensures that critical/important services don't suffer delays during peak traffic periods.

Improves Reliability-Guarantees consistent performance for time sensitive applications regardless of if the network is under heavy load or not

Enhances User Experience-Decreases jitter and packet loss for essential applications such as shipment tracking dashboard , this leads to smoother real time updates.

Caching and Local Load Balancing

Caching refers to storing frequently accessed data to users on devices such as edge nodes or local servers within a LAN. Local load balancing distributes traffic /user requests evenly across multiple servers or network paths to prevent/avert overloading on a single link on device.

How it improves performance

Reduces WAN bandwidth Usage-Constant /repeated requests are provided from the local cache instead of being fetched across the WAN , this reduces network congestion greatly.

Enhanced User Experience-Users experience faster access to data as data is stored closer to them rather than remote servers , this drastically reduces latency and conserves bandwidth .

Enhances Reliability-Load balancing makes sure that no single server or link becomes or is a bottleneck , doing so it ensures the system provides continuous access even if one path or device were to fail

4.2)**Application Allow Listing**

Application allow listing is a security approach that dictates that only explicitly preapproved applications, executables, scripts and libraries are allowed to run on a system .Everything else is blocked by default , this is a nig shift from the traditional allow all , block known bad model of antivirus software .

How it reduces risk:

Malware infection -This is the most significant benefit that comes with application allow listing , the various type of malware need to execute payload to be effective. Allow listing stops the execution of any unapproved program , this leaves malware ineffective/cant carry out its goal. Even if a user is tricked into downloading malicious content it wont run.

Lateral Movement-Attacker usually make use of tools and custom backdoors to move laterally through a network after compromising one machine .With strict allow listing in place the common lateral movement tools are blocked on other protected hosts , this effectively creates a barrier that contains the breach

Unauthorised Software-It also stops/prevents the installation and use of unauthorised software if a machine(s) are compromised .

End point Detection and Response

EDR goes far beyond standard antivirus by constantly monitoring endpoint activity for suspicious behaviour and pattern. They collect large amounts of data and make use of advance analytics , machine learning and threat intelligence to detect threats that run away from other controls. They offer deep visibility and response capabilities.

How it reduces risks :

Advanced Malware and Zero day threats -EDR has been created to detect malicious behaviour rather than just known malicious signatures. If a application starts acting like ransomware(rapidly encrypting files) or PowerShell scripts show behaviour of typical file attack the EDR can detect this and block the activity in real time , even if that specific malware has never been seen before .

Lateral Movement -EDR offers unparalleled visibility into cross system activities .They have the ability to detect and alert on reconnaissance commands ,lateral movement tools and the creation of unexpected network connections between hosts .This allows the security team to see the attacker movement in real time and respond .

Unauthorised Access and Post Exploitation Activity -EDR has the ability to detect signs of credential misuse , such as one user logging in from two geographically impossible locations in a short time frame .It also check/monitors for post exploitation activities such as LSASS memory for credential or modifying scheduled tasks for persistence

Bibliography

Andrea Schauer . (2018). *Video Tutorial VLSM*. [online] Available at: https://www.youtube.com/watch?v=P5t2gN2l7ZI.

GeeksforGeeks (2018). *Supernetting in Network Layer*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/computer-networks/supernetting-in-network-layer/.

Wikipedia Contributors (2019). *IEEE 802.1X*. [online] Wikipedia. Available at: https://en.wikipedia.org/wiki/IEEE_802.1X.

Nile. (n.d.). *What Is Wi-Fi Security? WEP, WPA, WPA2 & WPA3 Differences*. [online] Available at: https://nilesecure.com/network-security/what-is-wi-fi-security-wep-wpa-wpa2-wpa3-differences.

Damon (2025). *WPA3 Explained: How to Set Up a More Secure Wi-Fi Network - VSOL*. [online] Vsolcn.com. Available at: https://www.vsolcn.com/blog/what-is-wpa3.html.

Hotel Online. (2023). *The Crucial Role of Client Isolation in Hotel Wi-Fi*. [online] Available at: https://www.hotel-online.com/news/the-crucial-role-of-client-isolation-in-hotel-wi-fi [Accessed 7 Nov. 2025].

Rsinc.com. (2025). *Setting Up a Guest WiFi Network: Security Benefits and How-To Guide 2025*. [online] Available at: https://www.rsinc.com/setting-up-a-guest-wifi-network-security-benefits-and-how-to-guide.php [Accessed 7 Nov. 2025].

Rao, D.A. (2024). *Understanding Routing Protocols: Key Insights for Networks*. [online] SciVast. Available at: https://scivast.com/articles/understanding-routing-protocols/.

Exam-Labs - Pass Your Certification Exam Easily. (2025). *Understanding OSPF Area Structure and LSA Types: Enhancing Network Performance and Scalability - Exam-Labs*. [online] Available at: https://www.exam-labs.com/blog/understanding-ospf-area-structure-and-lsa-types-enhancing-network-performance-and-scalability [Accessed 7 Nov. 2025].

www.learncisco.net. (n.d.). *Dijkstra's Shortest Path First (SPF) Algorithm | ICND2 200-105*. [online] Available at: https://www.learncisco.net/courses/icnd-2/an-overview-of-ospf/ospf-data-overview.html.

Ipspace.net. (2016). *Don't Run OSPF with Your Customers «ipSpace.net blog*. [online] Available at: https://blog.ipspace.net/2016/03/dont-run-ospf-with-your-customers/ [Accessed 7 Nov. 2025].

Vasilena Markova (2025). *Understanding BGP: A Comprehensive Guide for Beginners - ClouDNS Blog*. [online] ClouDNS Blog. Available at: https://www.cloudns.net/blog/understanding-bgp-a-comprehensive-guide-for-beginners/.

www.ciscopress.com. (2018.). *IBGP Scalability > BGP Fundamentals | Cisco Press*. [online] Available at: https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=9.

j2sw (2023). *The Benefits of Running Border Gateway Protocol (BGP) in Your Network*. [online] j2sw Blog. Available at: https://blog.j2sw.com/networking/bgp/the-benefits-of-running-border-gateway-protocol-bgp-in-your-network/.

Google Cloud. (2020). *BGP route policies overview*. [online] Available at: https://cloud.google.com/network-connectivity/docs/router/concepts/bgp-route-policies-overview.

Huawei.com. (2025). Available at: https://support.huawei.com/enterprise/en/doc/EDOC1100367121/e80160f/configuring-bgp-routing-policies [Accessed 7 Nov. 2025].

Linkedin.com. (2024). *Learn what OSPF is, why you should use it, how to configure it, what are the challenges of it, and how to troubleshoot it in this article.* [online] Available at: https://www.linkedin.com/advice/3/how-can-ospf-improve-large-scale-network-performance-sejhc [Accessed 7 Nov. 2025].

dedirock-admin (2025). *How BGP Improves Network Resilience in IP Transit - DediRock*. [online] DediRock. Available at: https://dedirock.com/blog/how-bgp-improves-network-resilience-in-ip-transit/.

GeeksforGeeks (2024). *Edge Caching System Design*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/system-design/edge-caching-system-design/.

Trainingcamp.com. (2025). *QoS*. [online] Available at: https://trainingcamp.com/glossary/qos/ [Accessed 7 Nov. 2025].

GeeksforGeeks (2024). *Global Load Balancing vs. Local Load Balancing*. [online] GeeksforGeeks. Available at: https://www.geeksforgeeks.org/system-design/global-load-balancing-vs-local-load-balancing/ [Accessed 7 Nov. 2025].

Exam-Labs - Pass Your Certification Exam Easily. (2025). *Understanding OSPF: The Backbone of Efficient Networking - Exam-Labs*. [online] Available at: https://www.exam-labs.com/blog/understanding-ospf-the-backbone-of-efficient-networking.