

Office Network Management

submitted by:

Sitanshu Pokalwar(RA2011026010147), Udit Gogia(RA2011026010145), Abhikanksh
Chand(RA2011026010146), Rigved Thorat(RA2011026010142), Harsh
Jain(RA2011026010141)

Under the Guidance of

Mr Prakash B

(Assistant Professor, Dept of Networking and Communications) in

partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY in

COMPUTER SCIENCE ENGINEERING

with specialization in INFORMATION TECHNOLOGY



**DEPARTMENT OF NETWORKING AND COMMUNICATIONS COLLEGE
OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE O F SCIENCE
AND TECHNOLOGY**

KATTANKULATHUR - 603 203

JUNE 2022



SRM INSTITUTE OF SCIENCE AND TECHNOLOGY KATTANKULATHUR - 603 203

BONAFIDE CERTIFICATE

Certified that 18CSP110L internship report titled “Office Network Management” is the bonafide work of Sitanshu Pokalwar, Udit Gogia, Abhikanksh Chand, Rigved Thorat, Harsh Jain who carried out the work under my supervision along with the company mentor.

Certified further, that to the best of my knowledge the work reported herein does not form any other internship report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

Project Scenario explanation:

Network management software is getting more expensive and complex, and at the same time network management challenges are becoming more demanding and complicated as well. In such a scenario, what the IT managers of small and mid-sized organizations should do is prioritize their network management needs and implement solutions that offer these basic functions exceptionally well.

Some of the basic network management functions that are critical for SMEs are

Network Visualization:

Auto-discovery and mapping of all critical network elements such as mail servers, WAN links, business applications, and entire LAN infrastructure including switches, printers, wireless routers, load balancers, and non-standard devices if any.

Proactive Monitoring: 24/7 network surveillance for detecting network faults.

Monitoring critical resources for availability, threshold violations, host resource (CPU, Disc space, Memory) utilization, service availability, service response times etc. Automated Response: Ability to send notifications and take automated remedial actions by executing custom scripts.

Flexible Reporting: Reports that help answer questions such as how many service outages occurred for all systems monitored that provide service to the Atlanta branch office? What's the percentage of free space on all file servers across the entire network? And so on.

Network Visualization To manage any network, first, you must be able to identify and group network elements into different views that represent your deployment.

For example, if you are the IT manager responsible for managing the network infrastructure of your organization, then you would want the following in your management tool Automated discovery and grouping of all elements across the offices, Grouping of devices into routers, wireless, switches, servers etc. Custom maps that show branch office status at -a- glance Network management refer to two related concepts. First is the process of configuring, monitoring, and managing the performance of a network. Second is the platform IT and NetOps teams use to complete these ongoing tasks.

Over the past 10 years, network management systems have evolved to help IT teams operate in more agile ways, incorporating advanced analytics, machine learning, and intelligent automation to continually optimize network performance. As organizations adapt to a more distributed workforce, these network management systems are increasingly deployed in the cloud and hosted environments.

Network management systems collect data from connected network devices such as switches, routers, access points, and client devices. They also give network administrators fine-grained control over how those devices operate and interact with one another.

The data captured from these devices is used to proactively identify performance issues, monitor security and segmentation, and accelerate troubleshooting. Many network management platforms started as a way to control LANs.

As enterprise networks increased in complexity and diversity, these management planes extended their capabilities into SD -WAN, security, and IoT. The most effective platforms

combine devices and sensors into a single view of network traffic, making it easy for IT not only to monitor but to protect and remediate performance issues .

Network management systems collect real -time data from network elements, such as switches, routers, and access points, as well as from endpoint devices, such as mobile phones, laptops, and desktops. This information is used to provide insights into the health of the network. Typically, the data is collected and sent to the system in one of two ways:

SNMP: The Simple Network Management Protocol is an open standard and has been widely supported by most manufacturers of network elements since the early 1990s. SNMP queries each element in the network and sends each response to the network management system.

Streaming telemetry: A software agent installed in a network element allows for the automatic transmission of key performance indicators in real -time. Streaming telemetry is rapidly replacing SNMP, because it is more efficient, can produce many more data points, and is more scalable. And telemetry standards, such as NETCONF/YANG, are gaining traction as ways to offer the same multivendor support as S NMP.

When it comes to managing a complex or highly distributed network, the three most critical capabilities of a network management tool are directly tied to how well that platform unifies sites and remote workers. First, ease of adoption and deployment directly affects the value that IT teams will get from the tool. There's an adage in software as a service (SaaS) — "Adoption is the new ROI" —and the

same is true for network management. If it's not easy to deploy and use on a daily basis, it will quickly fall by the wayside.

It's also key to find a platform that can manage the full scope of the network, from access to WAN to IoT. And finally, the security, control, and treatment of network data must have equal priority, no matter how you choose to deploy it.

Networks become more complicated as the number of devices and applications connected to them grows, but a complicated network doesn't require a complicated -touse network management system. Today's network management systems are open, extensible, and software-driven to help accelerate and simplify network operations while lowering costs and reducing risk.

Powered by deep intelligence and integrated security, these systems deliver automation and assurance across the entire network, whether big or small, resulting in better efficiency and cost savings while offering end -to-end visibility, automation, and insight. Open APIs and standards such as OpenConfig mean users can optimize their networks with solutions that best fit their business objectives.

In today's hybrid work environment, organizations face a variety of new challenges. The challenges include a highly distributed and mobile workforce, an inconsistent range of quality connectivity options, and the need to rapidly implement tools for coll aboration, support, and business continuity. In turn, network management systems need to be agile, with built -in intelligence and automation to facilitate decision -making and reduce errors. Security must be inherent and prioritized to help ensure that netw orks and the devices connected to them are secure from the core to the edge.

Whether you need to prepare your central campus for its new role as a hub of hybrid work or you're scaling out hundreds (or thousands) of branch sites, cloud-based network management systems are designed to give you the flexibility and reach you need. These platforms offer easy access and monitoring across highly distributed networks and make provisioning of remote sites simple. Cloud-based platforms also provide a high level of configurability and customization, through open APIs and robust application ecosystems.

These platforms also support advanced analytics, automation, and optimization use cases, through large data lakes and the power of cloud computing to support sophisticated machine learning applications. On-premises network management systems can be used for large campus networks that require greater performance and scalability. They also provide advanced features such as analytics, assurance, artificial intelligence (AI) and machine learning (ML).

Organizations that need sovereign operations can benefit from on-premises network management servers since all the data is stored onsite. In many cases, network management systems for larger networks can generate a lot of data that is collected from telemetry and SNMP. On-premises systems are usually larger servers that have enough power to process the data so that it can be used to provide the insights IT needs to manage the network. This is one reason an on-premises server is usually located at the core of the network. Although it can be accessed from the internet, remote access requires a VPN connection.

Concept-

1. VLSM -

Variable Length Subnet Mask (VLSM) is a subnet -- a segmented piece of a larger network -- design strategy where all subnet masks can have varying sizes. This process of "subnetting subnets" enables network engineers to use multiple masks for different subnets of a single class A, B or C network.

With VLSM, an IP address space can be divided into a well-defined hierarchy of subnets with different sizes. This helps enhance the usability of subnets because subnets can include masks of varying sizes.

A subnet mask helps define the size of the subnet and create subnets with very different host counts without wasting large numbers of addresses.

VLSM fundamentals

To fully understand VLSM, it's important to be familiar with several fundamental terms: subnet mask, subnetting and supernetting.

Subnet mask

Every device on a network has an IP address. A subnet mask splits this IP address into

the host and network addresses. This helps define which part of the IP address belongs to the network, and which part belongs to the device.

A subnet mask is a 32-bit number, where all the host bits are set to 0, and the network

bits are set to 1. So, the subnet mask consists of a sequence of 1s followed by a block of 0s, where the 1s represent the network prefix and the 0s mark the host identifier.

Subnetting

In subnetting (or sub networking), a large network is logically or physically divided into multiple small networks or "subnets." The reason for subnetting a large network is to address network congestion and its negative impact on speed and productivity.

Subnetting also improves efficiency due to the way an address space is utilized in a small network. Finally, the divisions between subnets allow organizations to enforce access controls, which improves network security and helps contain security incidents.

Supernetting

In supernetting, multiple contiguous networks are combined into a single large network known as a supernet (or supernetwork). Supernetting advertises many routes in one summarized advertisement or routing entry, instead of individually. This routing entry encompasses all the networks in the supernet and provides route

updates very efficiently.

Supernetting is especially useful in route aggregation to reduce the size of routing tables and to reduce the size of routing updates exchanged by routing protocols.

2. Routing

RIP Protocol

RIP stands for Routing Information Protocol. RIP is an intra-domain routing protocol used within an autonomous system. Here, intra-domain means routing the packets in a defined domain, for example, web browsing within an institutional area. To understand the RIP protocol, our main focus is to know the structure of the packet, how many fields it contains, and how these fields determine the routing table.

Before understanding the structure of the packet, we first look at the following points:

- RIP is based on the distance vector-based strategy, so we consider the entire structure as a graph where nodes are the routers, and the links are the networks.
- In a routing table, the first column is the destination, or we can say that it is a network address.
- The cost metric is the number of hops to reach the destination. The number of hops available in a network would be the cost. The hop count is the number of networks required to reach the destination.
- In RIP, infinity is defined as 16, which means that the RIP is useful for smaller networks or small autonomous systems. The maximum number of hops that RIP can contain is 15 hops, i.e., it should not have more than 15 hops as 16 is infinity.
- The next column contains the address of the router to which the packet is to be sent to reach the destination.

ADDRESSING TABLE:

- **CEO OFFICE**

DEVI CE	INTERF ACE	IP ADDRE SS	SUBNET MASK	GATEW AY
Lapto p0	Fa0/0	192.168. 10.5	255.255.2 55.0	192.168. 10.1
PC0	Fa0/0	192.168. 10.4	255.255.2 55.0	192.168. 10.1
PC1	Fa0/0	192.168. 10.2	255.255.2 55.0	192.168. 10.1
Switc h0	-	-	-	-
Printe r0	-	-	-	-

FINANCE ROOM

DEVI CE	INTERF ACE	IP ADDRE SS	SUBNET MASK	GATEW AY
PC2	Fa0/0	192.168. 20.2	255.255.2 55.0	192.168. 20.1
PC0	Fa0/0	192.168. 20.7	255.255.2 55.0	192.168. 20.1
PC1	Fa0/0	192.168. 20.3	255.255.2 55.0	192.168. 20.1

PC4	Fa0/0	192.168.20.4	255.255.255.0	192.168.20.1
-----	-------	--------------	---------------	--------------

Switch1	-	-	-	-
---------	---	---	---	---

Printer1	-	-	-	-
Printer2	-	-	-	-

EMPLOYEE ROOM 1

DEVI CE	INTERF ACE	IP ADDRE SS	SUBNET MASK	GATEW AY
PC2	Fa0/0	192.168.30.2	255.255.255.0	192.168.30.1
PC0	Fa0/0	192.168.30.4	255.255.255.0	192.168.30.1
PC1	Fa0/0	192.168.30.3	255.255.255.0	192.168.30.1
PC3	Fa0/0	192.168.30.6	255.255.255.0	192.168.30.1

Printe r0	-	-	-	-
-----------	---	---	---	---

EMPLOYEE ROOM 2

DEVI CE	INTERF ACE	IP ADDRE SS	SUBNET MASK	GATEW AY
PC2	Fa0/0	192.168.40.2	255.255.255.0	192.168.40.1
PC0	Fa0/0	192.168.40.8	255.255.255.0	192.168.40.1
PC1	Fa0/0	192.168.40.3	255.255.255.0	192.168.40.1
PC4	Fa0/0	192.168.40.4	255.255.255.0	192.168.40.1
Printe r2	-	-	-	-

IT DEPARTMENT

DEVI CE	INTERF ACE	IP ADDRE SS	SUBNET MASK	GATEW AY
PC2	Fa0/0	192.168.60.2	255.255.255.0	192.168.50.1
PC0	Fa0/0	192.168.50.6	255.255.255.0	192.168.50.1
PC1	Fa0/0	192.168.50.3	255.255.255.0	192.168.50.1
PC4	Fa0/0	192.168.50.4	255.255.255.0	192.168.50.1
Switc h4	-	-	-	-

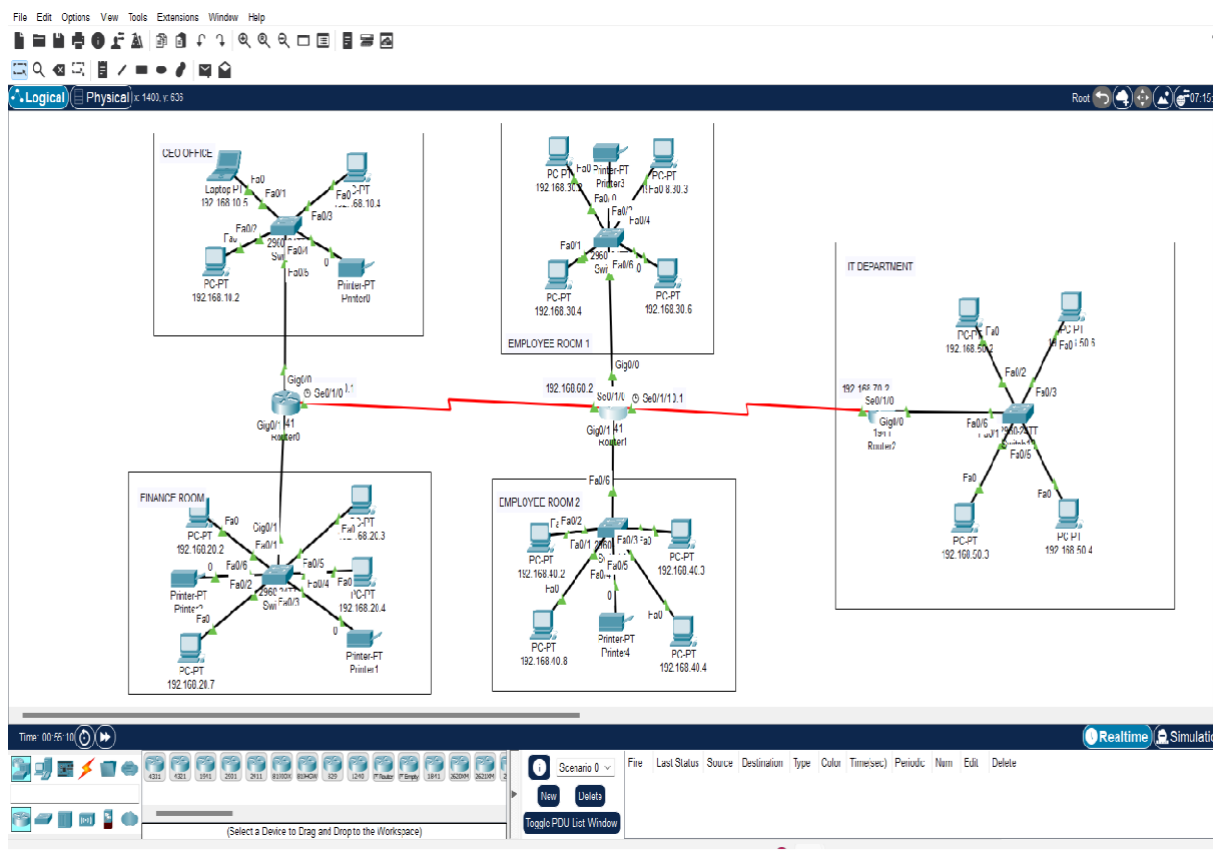
ROUTERS

DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK
ROUTER0	GIG0/0	192.168.10.1	255.255.255.0
ROUTER0	GIG0/1	192.168.20.1	255.255.255.0
ROUTER1	GIG0/0	192.168.30.1	255.255.255.0
ROUTER1	GIG0/1	192.168.40.1	255.255.255.0
ROUTER2	GIG0/0	192.168.50.1	255.255.255.0
ROUTER2	Se0/1/1	192.168.70.2	255.255.255.0
ROUTER1	Se0/1/1	192.168.70.1	255.255.255.0

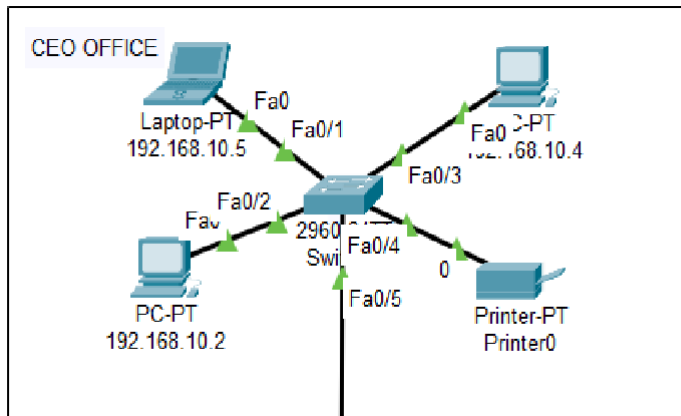
ROUTER1	Se0/1/0	192.168.60.2	255.255.255.0
ROUTER0	Se0/1/0	192.168.60.1	255.255.255.0

Project Photos

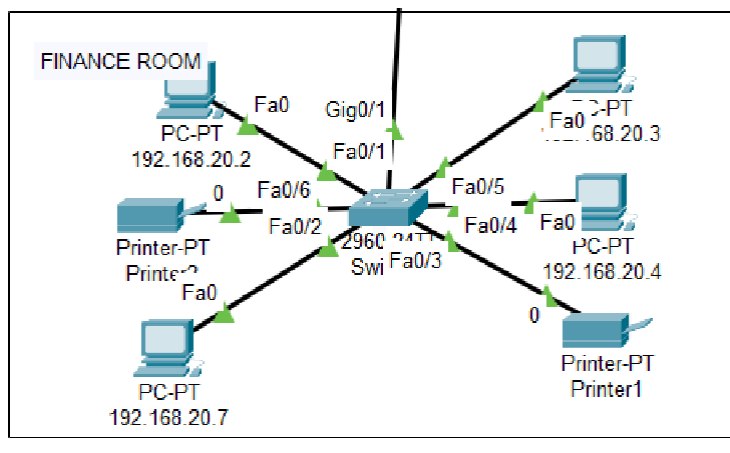
OFFICE MANAGEMENT IN CISCO PAKET TRACER



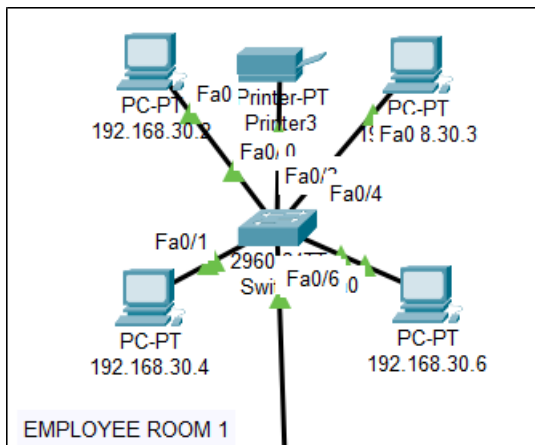
- CEO OFFICE



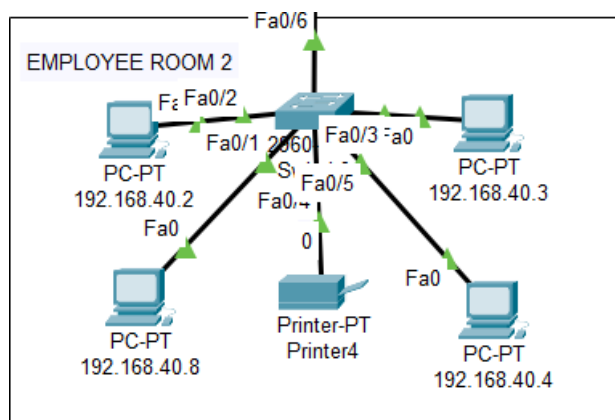
FINANCE ROOM



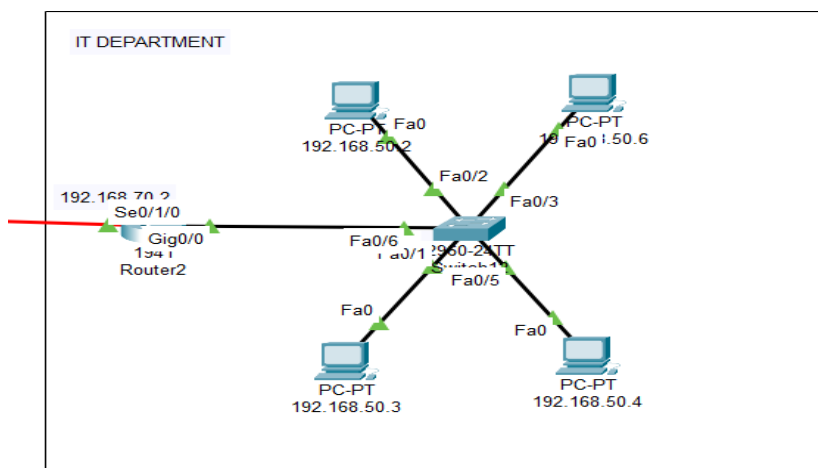
EMPLOYEE ROOM1



EMPLOYEE ROOM2



IT DEPARTMENT



ROUTER0 ROUTE:

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router(config-if)#EXIT
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


    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
    192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/1
L       192.168.20.1/32 is directly connected, GigabitEthernet0/1
R       192.168.30.0/24 [120/1] via 192.168.60.2, 00:00:01, Serial0/1/0
R       192.168.40.0/24 [120/1] via 192.168.60.2, 00:00:01, Serial0/1/0
R       192.168.50.0/24 [120/2] via 192.168.60.2, 00:00:01, Serial0/1/0
    192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.60.0/24 is directly connected, Serial0/1/0
L       192.168.60.1/32 is directly connected, Serial0/1/0
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

ROUTER1 ROUTE:

 Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Router>EN
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

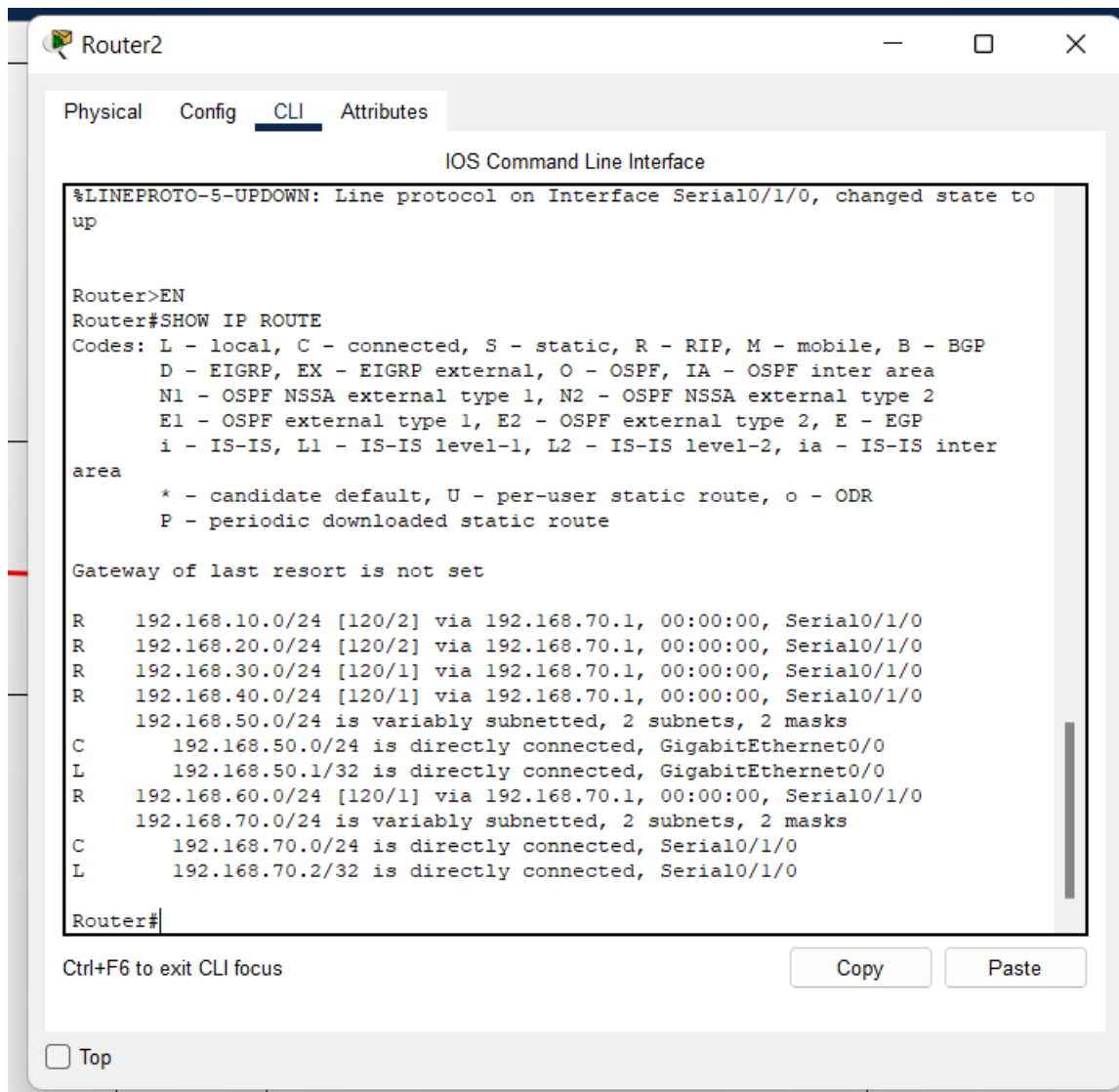
R    192.168.10.0/24 [120/1] via 192.168.60.1, 00:00:16, Serial0/1/0
R    192.168.20.0/24 [120/1] via 192.168.60.1, 00:00:16, Serial0/1/0
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
       C    192.168.30.0/24 is directly connected, GigabitEthernet0/0
       L    192.168.30.1/32 is directly connected, GigabitEthernet0/0
     192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
       C    192.168.40.0/24 is directly connected, GigabitEthernet0/1
       L    192.168.40.1/32 is directly connected, GigabitEthernet0/1
R    192.168.50.0/24 [120/1] via 192.168.70.2, 00:00:14, Serial0/1/1
     192.168.60.0/24 is variably subnetted, 2 subnets, 2 masks
       C    192.168.60.0/24 is directly connected, Serial0/1/0
       L    192.168.60.2/32 is directly connected, Serial0/1/0
--More--
```

Ctrl+F6 to exit CLI focus

Copy Paste

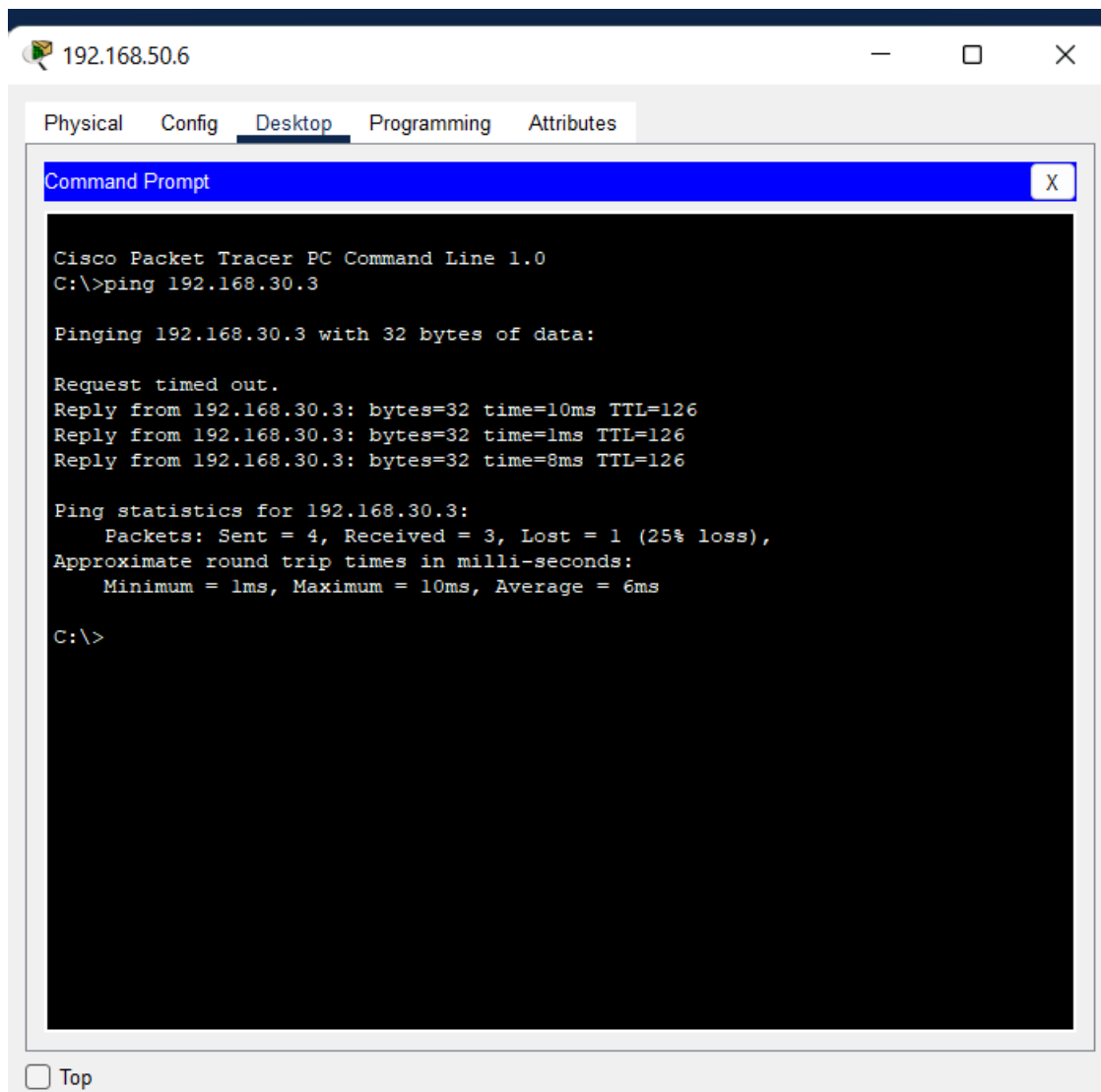
☐ Top

- ROUTER2 ROUTE:



VERIFICATION:

PINGING PC0 OF IT DEPARTMENT TO PC1 OF EMPLOYEE ROOM1.



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device with IP 192.168.50.6. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt window. The Command Prompt shows the execution of the command 'ping 192.168.30.3'. The output indicates that the ping was successful, with 3 out of 4 packets received and a 25% loss. The round trip times are 10ms, 1ms, and 8ms, with an average of 6ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.30.3: bytes=32 time=10ms TTL=126
Reply from 192.168.30.3: bytes=32 time=1ms TTL=126
Reply from 192.168.30.3: bytes=32 time=8ms TTL=126

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 6ms

C:\>
```

Result: Office network management has been successfully implemented

BIBLIOGRAPHY:

- <https://www.geeksforgeeks.org/introduction-of-variable-length-subnet-mask-vlsm/>

- eBook:
Data Communications and Networking (4th edition)
~B. A. Forouzan