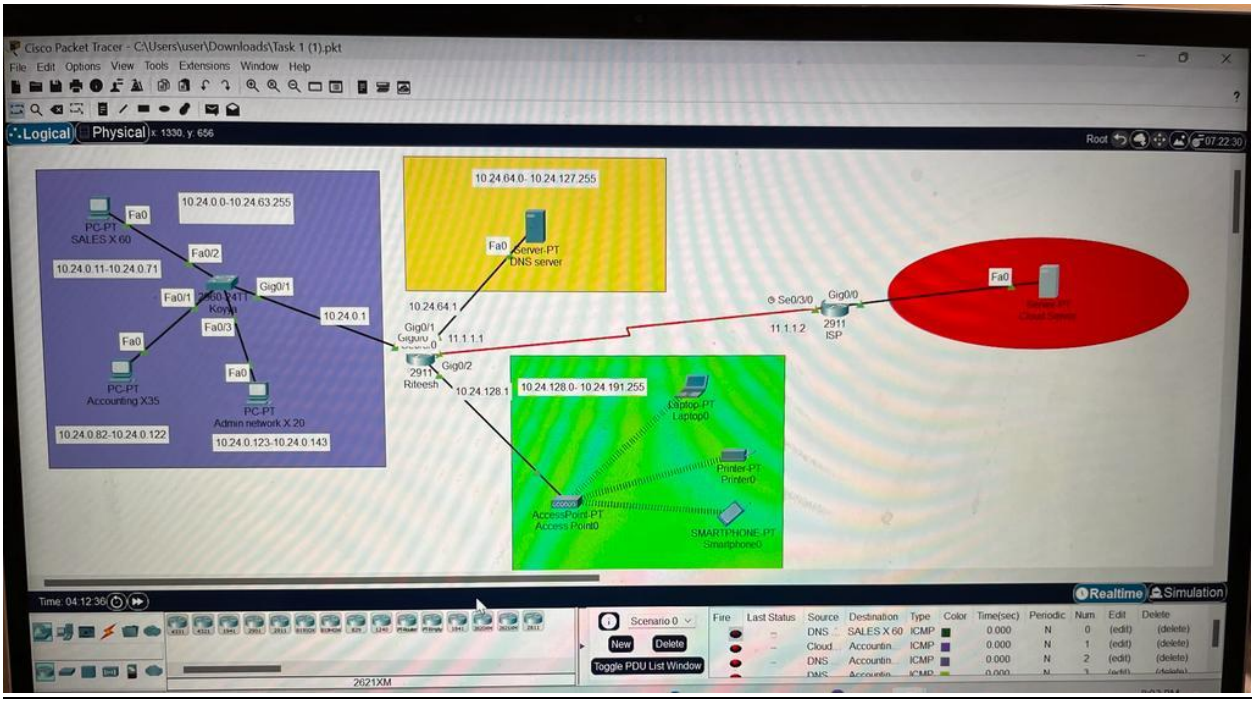
Coursework (**TA Finance Network Design)**

Introduction:

In this Coursework As a junior network engineer, I have been tasked with implementing and configuring a small computer network for TAK Finance's new branch in Hatfield, UK. The network must support IPv4 and provide full connectivity of all devices to their head office via the internet. Using Packet Tracer, I will need to build the physical topology shown in Assignment Brief , using the recommended devices and cables. I must also allocate IP addresses to the network using subnetting and configure the network for full connectivity using basic configuration and routing protocols. Finally, I will need to test the network's full connectivity and provide screenshots and explanations of the results in this report.

Image of Topology:



List of Cables:

Cable name	Connections	Specification
Copper Straight-Through	Used to connect Admin, Accounting, Sales to switch, Switch (Koyya) to Router (Riteesh), Router (Riteesh)to	A copper straight-through cable is used to connect two devices of different types in a network, such as a computer to a switch

	DNS server, Router (Riteesh) to Wireless, Router (ISP) to Cloud Server	or a router to a switch. In Cisco Packet Tracer, this type of cable can be used to establish a wired connection between devices in a simulated network.
Serial DCE	Used to connect Router (Riteesh) to Router (ISP)	A Serial DCE (Data Communications Equipment) is a type of interface used to connect networking devices via a serial cable

Addressing Table:

Name of device	IP address(range)	Subnet mask	Default Gateway
PC (Admin)	10.24.0.123 - 10.24.0.143	255.255.192.0	10.24.0.1
PC (Accounting)	10.24.0.82 - 10.24.0.122	255.255.192.0	10.24.0.1
PC (Sales)	10.24.0.11 - 10.24.0.71	255.255.192.0	10.24.0.1
Router (Riteesh) interfaces	10.24.0.1 10.24.64.1 10.24.128.1 11.1.1.1	255.255.192.0 255.255.192.0 255.255.192.0 255.255.255.252	
Switch	10.24.0.2	255.255.192.0	10.24.0.1
DNS Server	10.24.64.2	255.255.192.0	
ISP Router	88.44.22.1 11.1.1.2	255.255.255.252 255.255.255.252	
Wireless laptop	10.24.128.23	255.255.192.0	10.24.128.1
Mobile	10.24.128.30	255.255.192.0	10.24.128.1

Subnetting:

An IP address is a unique numerical identifier assigned to every device connected to a computer network. It consists of two parts: the network portion and the host portion. The network portion identifies the network to which the device belongs, while the host portion identifies the specific device within that network.

In binary notation, an IP address consists of 32 bits, divided into four octets, each containing 8 bits. For example, the IP address 10.24.0.0 can be represented in binary as:

00001010 00011000 00000000 00000000

The subnet mask is used to divide an IP address into its network and host portions. It is a 32-bit number that has a contiguous sequence of 1's followed by a contiguous sequence of 0's. The

number of 1's in the subnet mask determines the size of the network portion and the number of 0's determines the size of the host portion.

To determine the subnet mask for an IP address, we need to know how many bits are used to represent the network portion and the host portion. This information is provided by the IP address's class and the subnet prefix length.

In the case of the IP address 10.24.0.0/16, the /16 indicates that the first 16 bits of the IP address are used to represent the network portion, and the remaining 16 bits are used to represent the host portion.

To convert this prefix length to a subnet mask, we need to fill the first 16 bits with 1's and the remaining 16 bits with 0's. This gives us:

11111111 11111111 00000000 00000000

In decimal notation, this is equivalent to 255.255.0.0. However, since we need to further subnet this network, we need to borrow more bits from the host portion to create smaller subnets.

To create subnets with a /18 prefix length, we need to borrow 2 bits from the host portion. This gives us a subnet mask with the first 18 bits set to 1 and the remaining 14 bits set to 0:11111111

11111111 11000000 00000000

In decimal notation, this is equivalent to 255.255.192.0.

Therefore, the subnet mask 255.255.192.0 is derived by borrowing 2 bits from the host portion of the IP address 10.24.0.0/16 to create subnets with a /18 prefix length.

To create subnets from a given IP address and subnet mask, we use a process called subnetting. Subnetting allows us to divide a larger network into smaller subnetworks, each with its own unique network address and range of host addresses.

To create subnets for the IP address 10.24.0.0/18 (with subnet mask 255.255.192.0), we need to borrow 2 bits from the host portion of the IP address to create smaller subnets. This means that the first 18 bits of the IP address are used to represent the network portion, leaving 14 bits to represent the host portion.

The two bits that we borrow are represented by the last two bits of the third octet of the subnet mask (11000000). The value of these bits is 64+32=96. This means that each subnet has a block size of 96 (i.e., we can have up to 96 hosts in each subnet).

To calculate the number of subnets we can create, we need to determine how many times we can divide the network address space by the block size. This is done by taking 2 to the power of the number of bits we borrowed. In this case, we borrowed 2 bits, so we have:

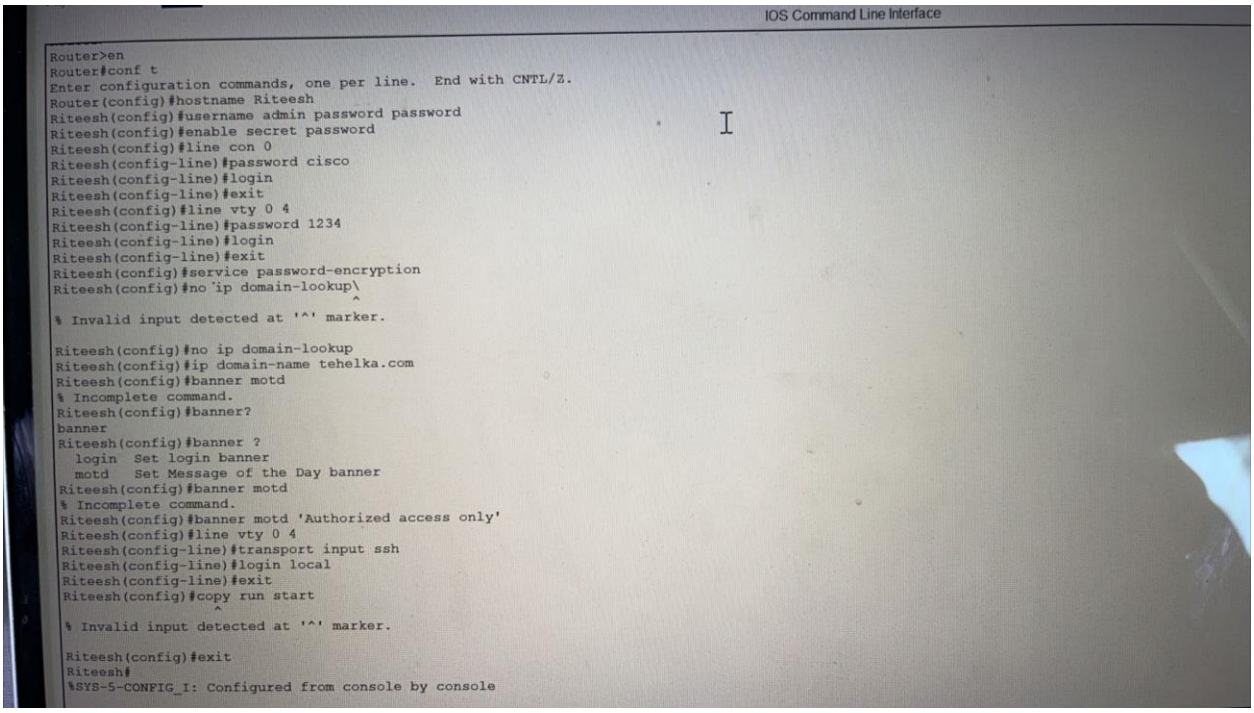
2^2 = 4 subnets

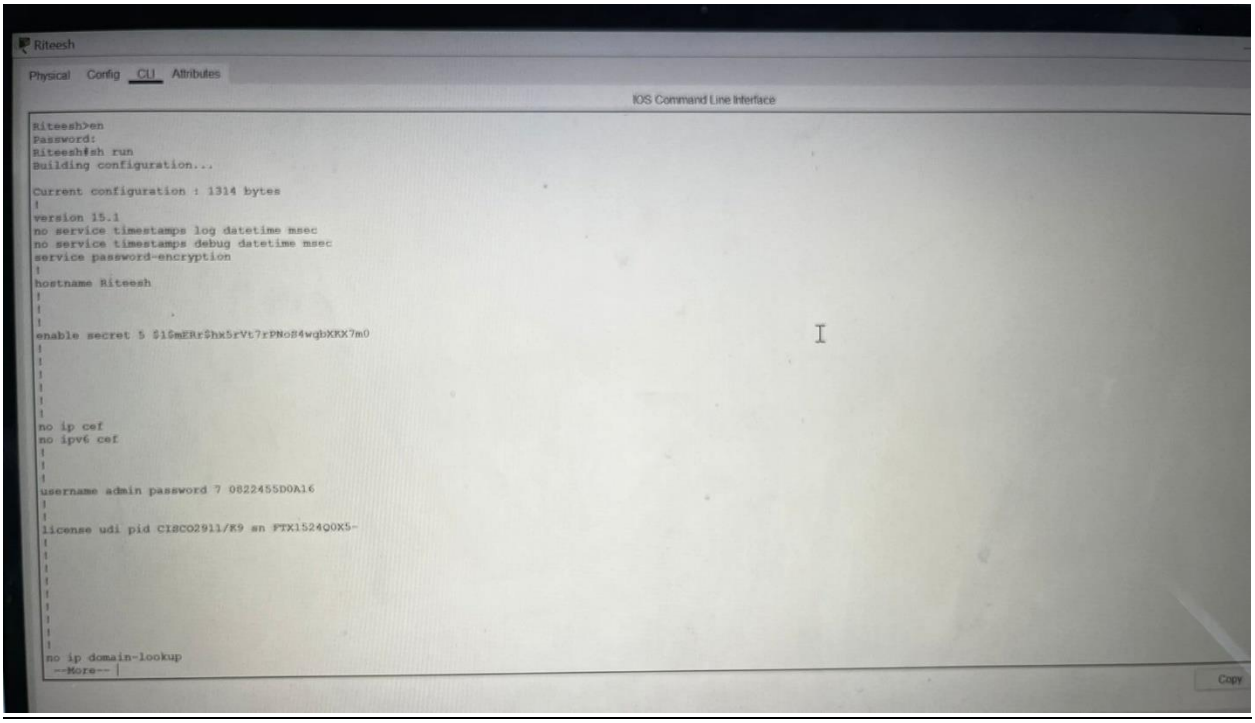
To determine the network addresses for each subnet, we increment the third octet of the IP address by the block size. The first subnet will have a network address of 10.24.0.0, the second subnet will have a network address of 10.24.64.0, the third subnet will have a network address of 10.24.128.0, and the fourth subnet will have a network address of 10.24.192.0.

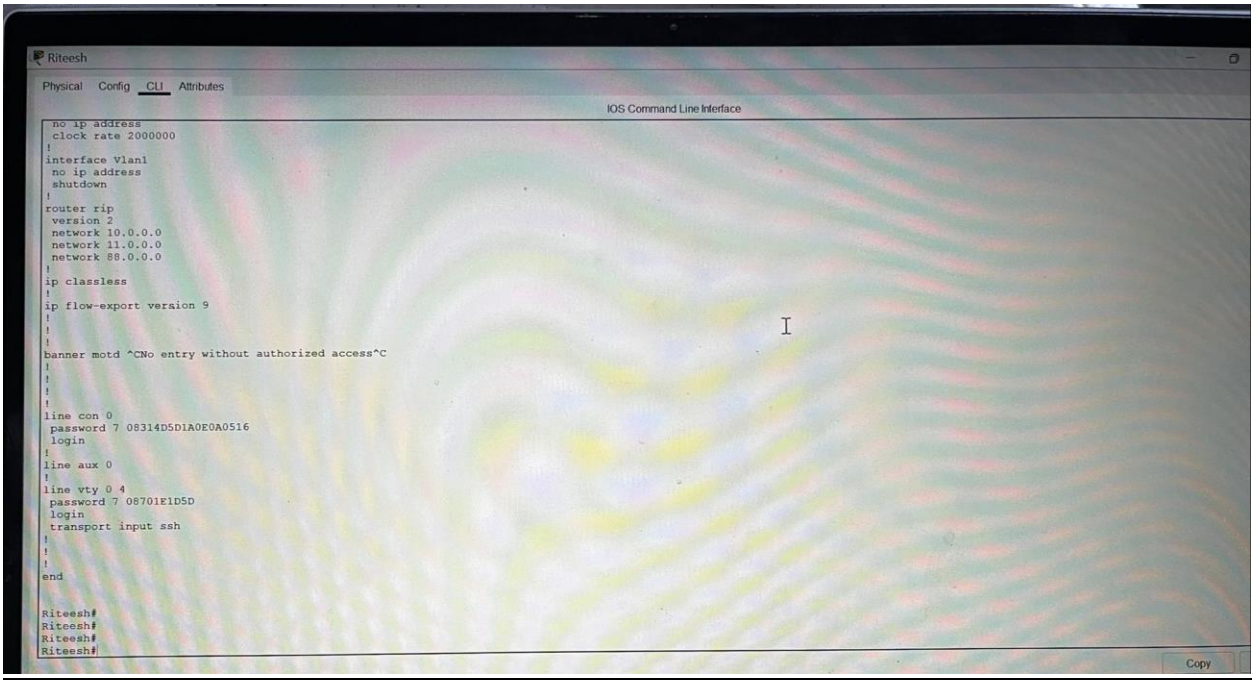
Each subnet has its own range of host addresses. For example, the first subnet has a host address range of 10.24.0.1 to 10.24.63.254, the second subnet has a host address range of 10.24.64.1 to 10.24.127.254, and so on.

Overall, subnetting allows us to create smaller, more efficient networks that can be managed more easily. By dividing a larger network into smaller subnets, we can also improve network security and reduce the amount of traffic on each network segment.

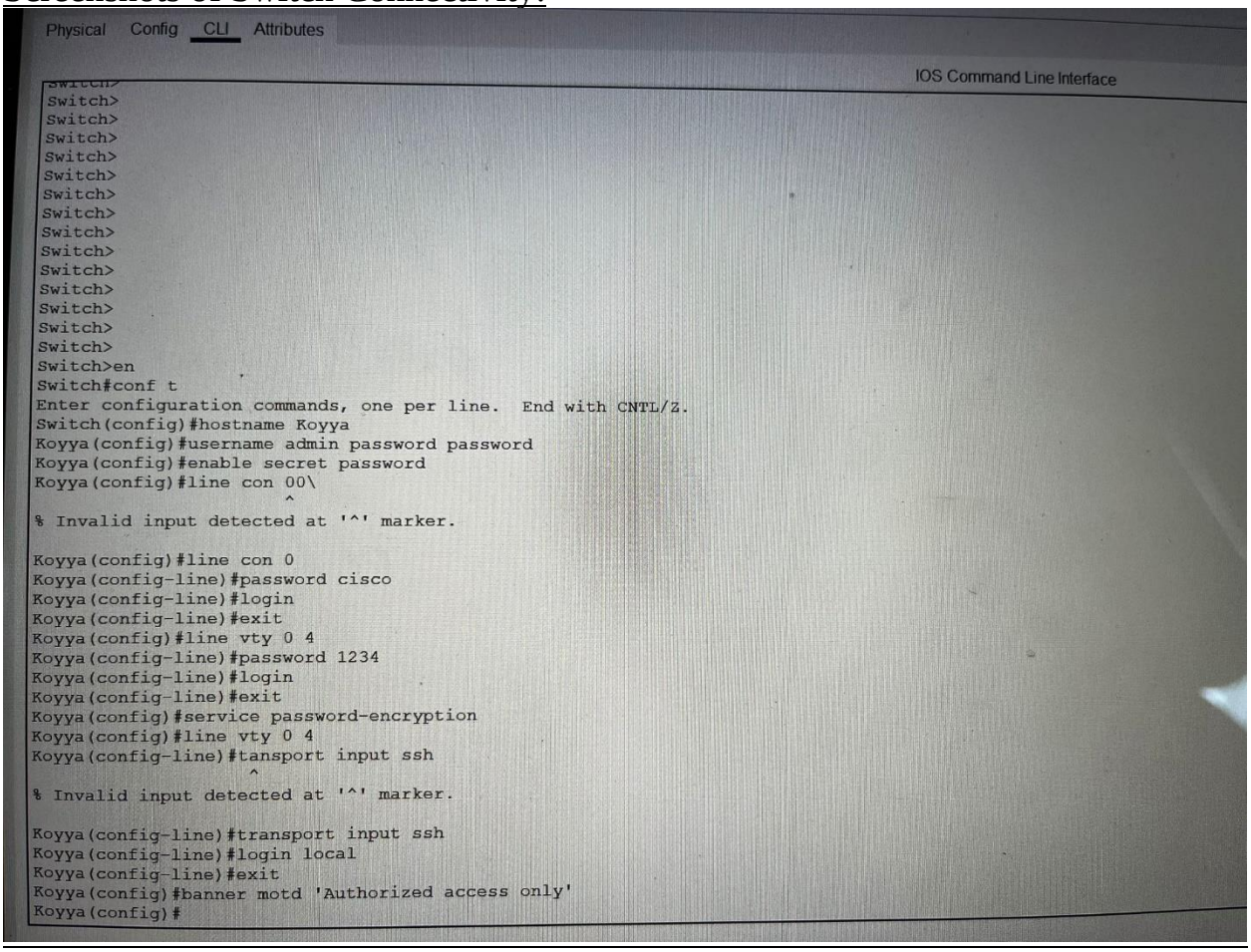
Screenshots of Router connectivity:

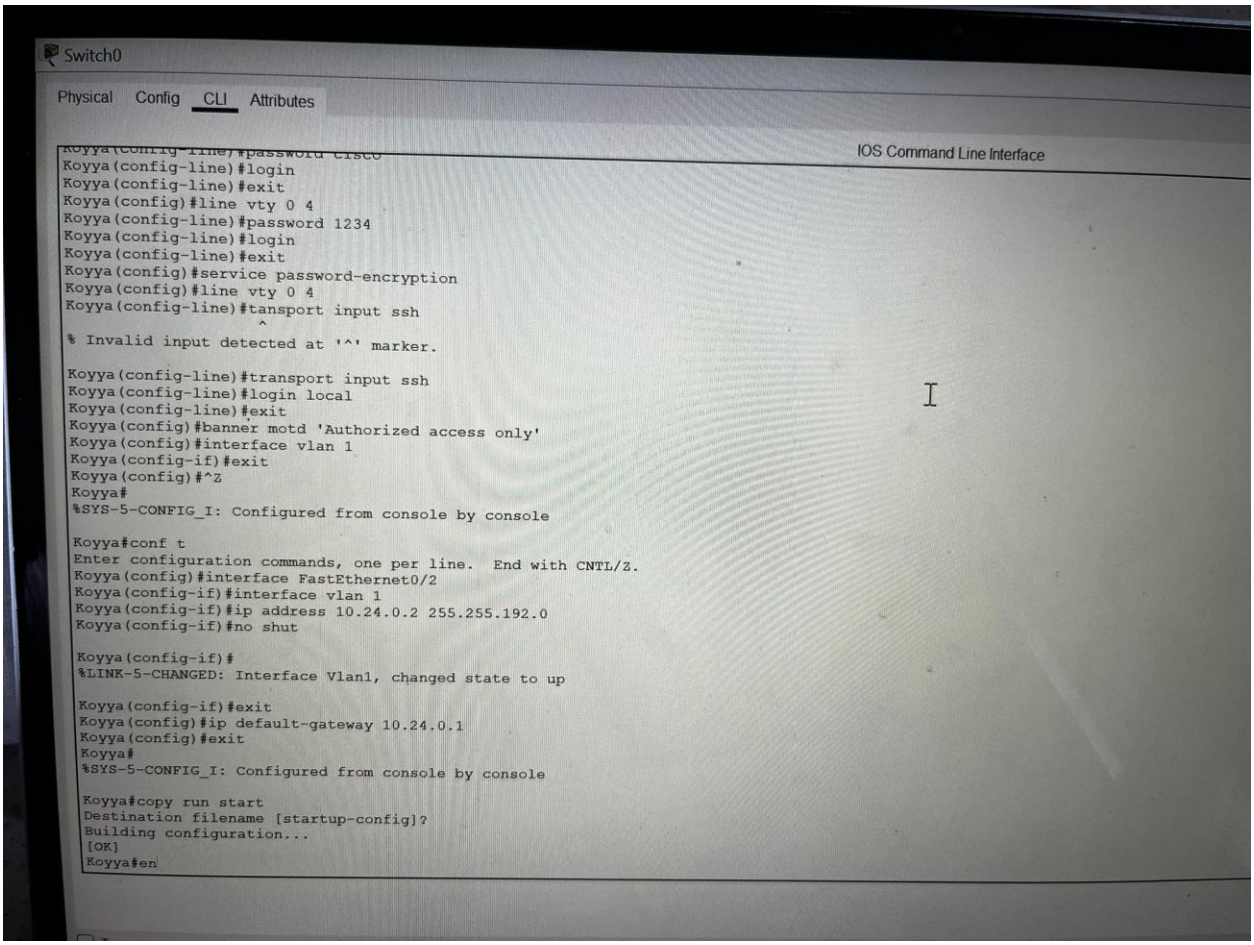


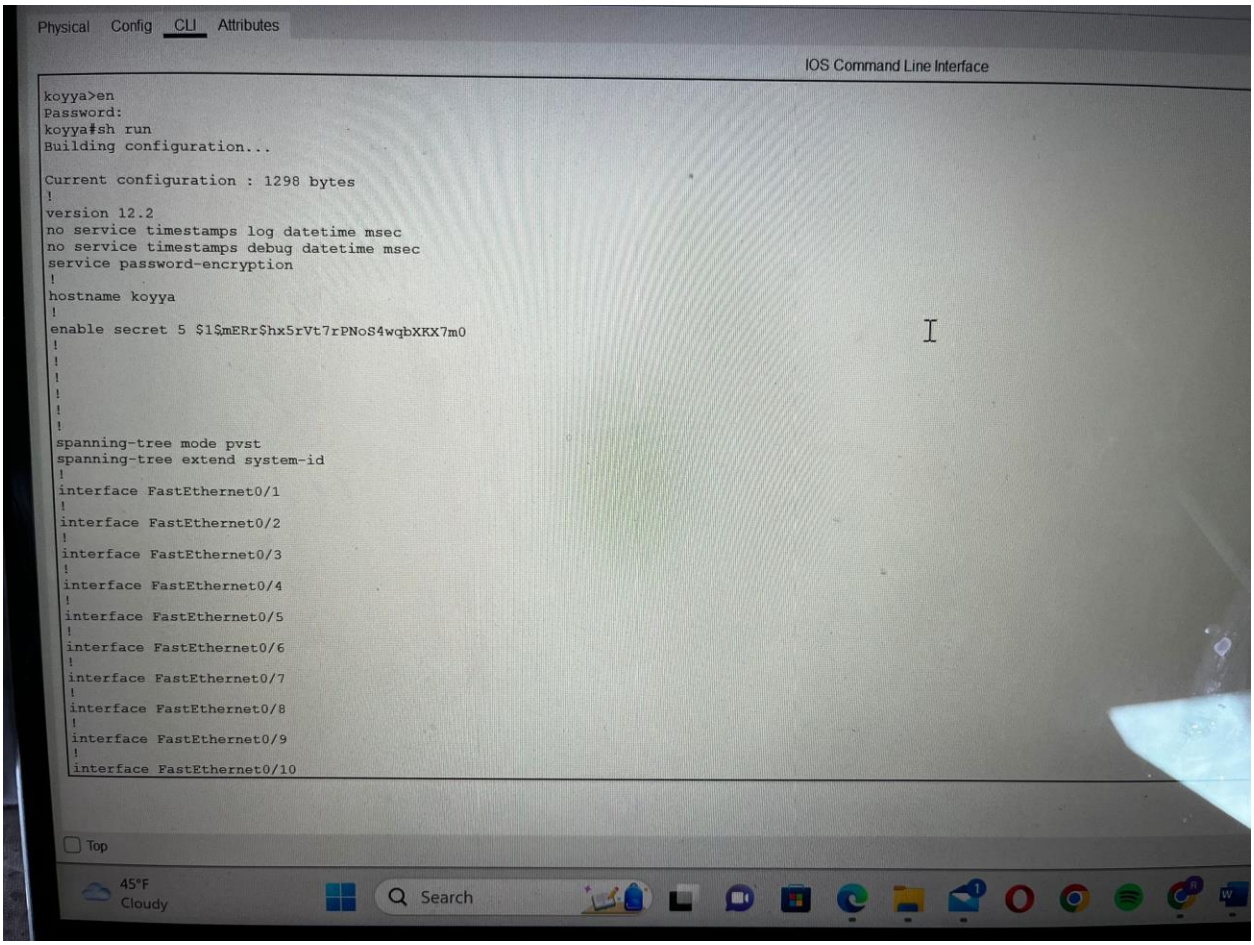

Riteesh
Physical Config CLI Attributes
IOS Command Line Interface
Riteesh>en
Password:
Riteesh#sh run
Building configuration...
Current configuration : 1314 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Riteesh
!
!
!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524Q0X5-
!
!
!
!
!
!
!
!
!
no ip domain-lookup
--More--
Copy

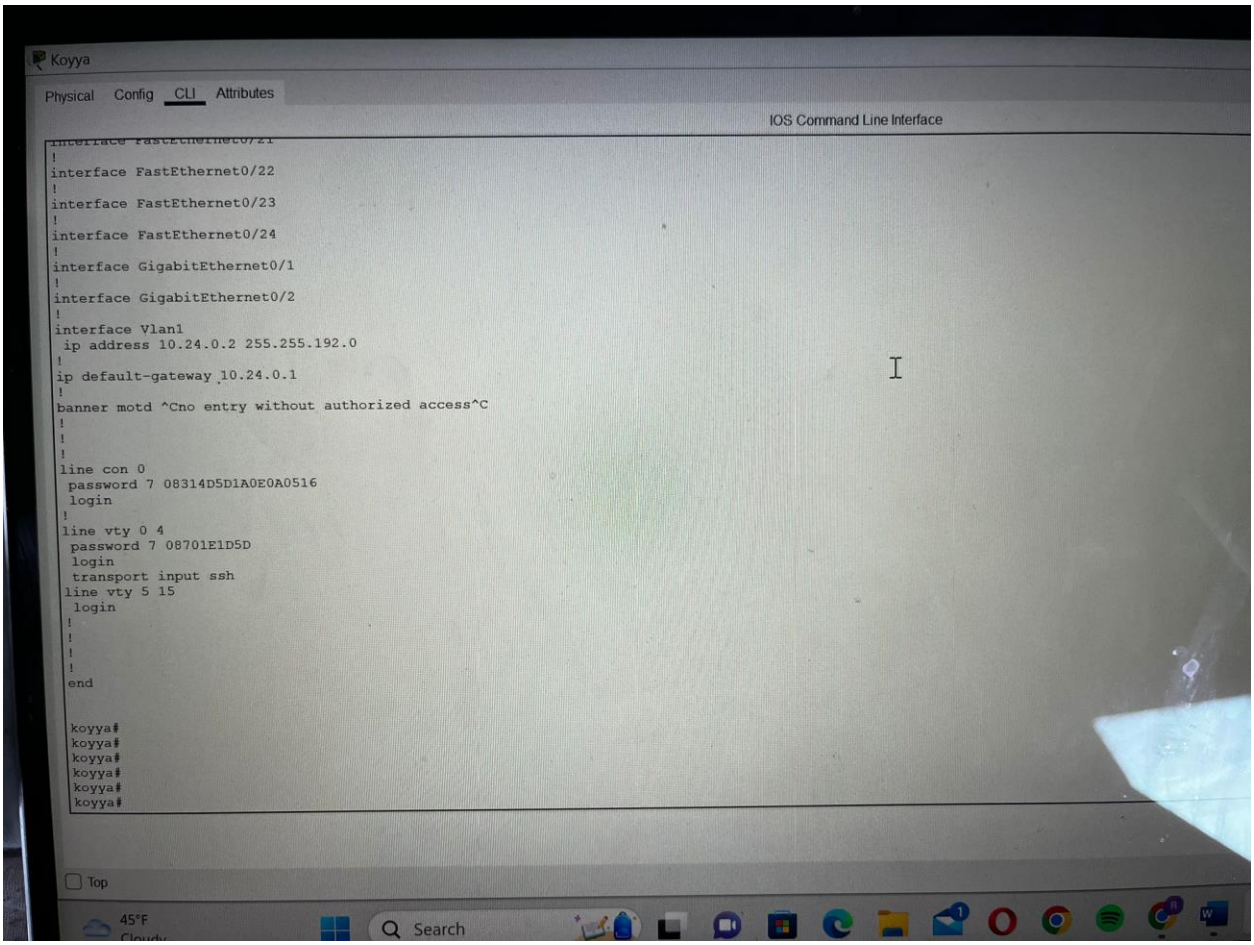

Riteesh
Physical Config CLI Attributes
IOS Command Line Interface
no ip address
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 10.0.0.0
network 11.0.0.0
network 88.0.0.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CNo entry without authorized access^C
!
!
!
!
line con 0
password 7 08314D5D1A0E0A0516
login
!
line aux 0
!
line vty 0 4
password 7 08701E1D5D
login
transport input ssh
!
!
!
end
Riteesh#
Riteesh#
Riteesh#
Riteesh#
Copy

Screenshots of Switch Connectivity:

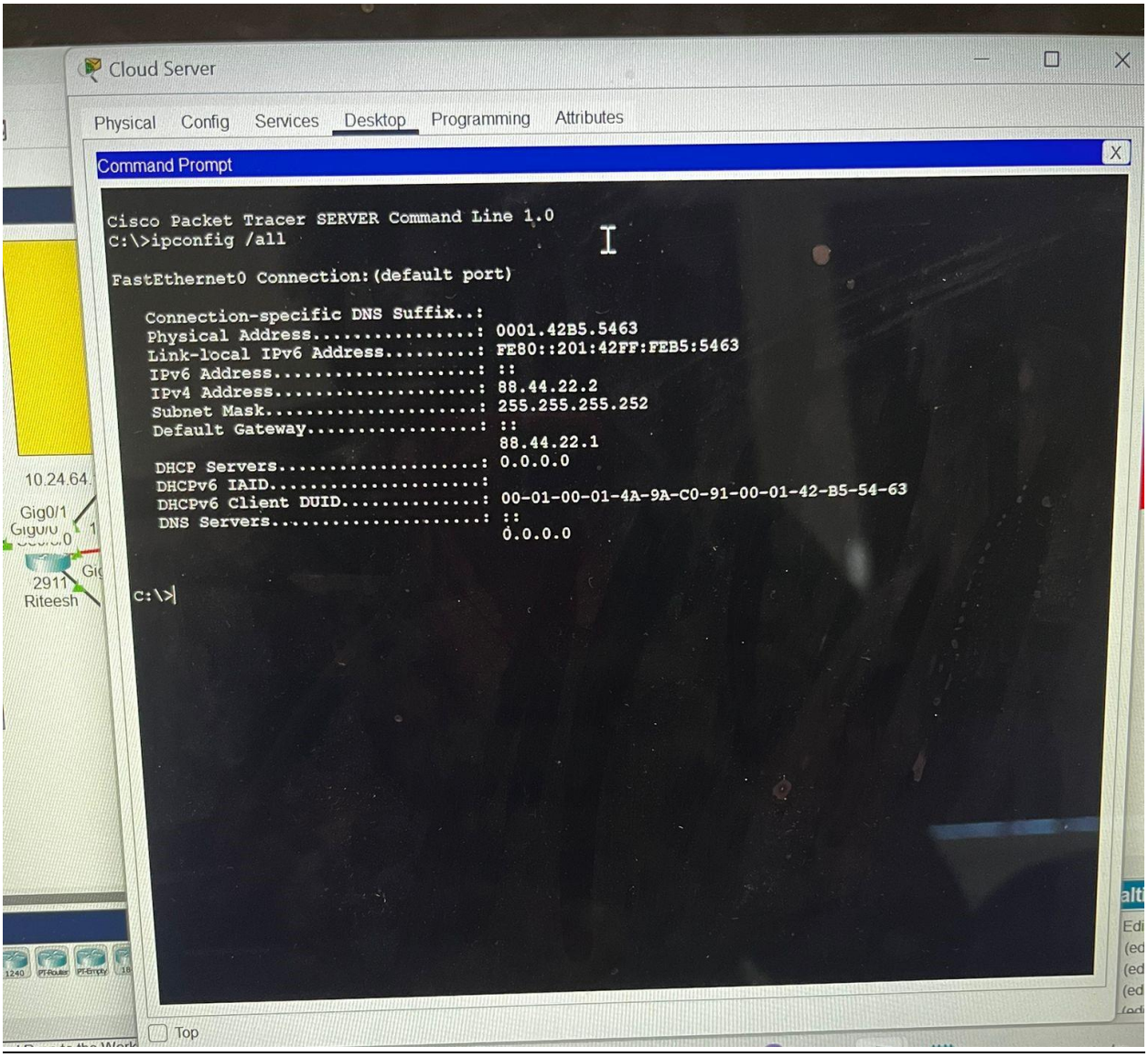


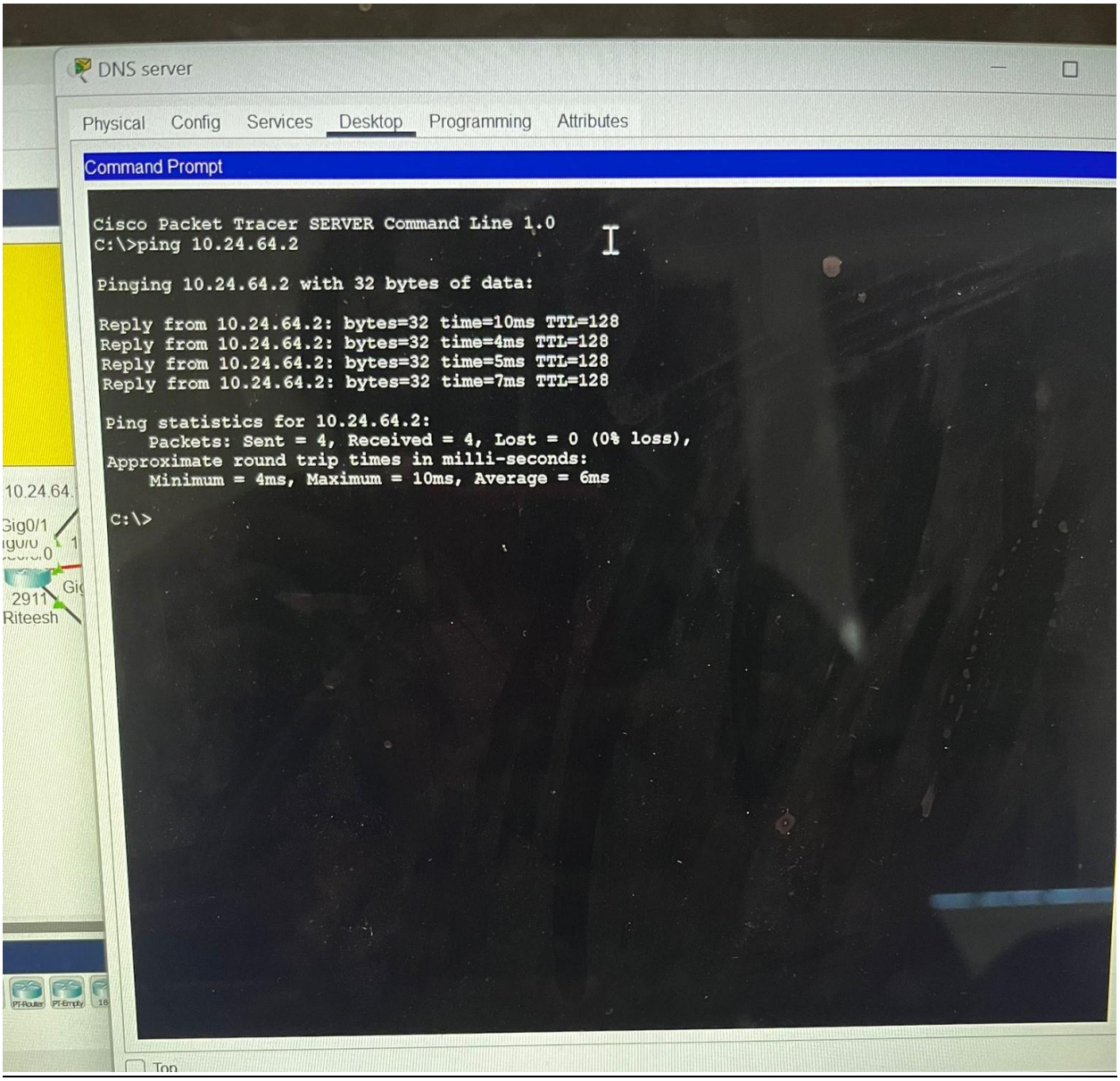

Switch0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Koyya(config-line)#password cisco
Koyya(config-line)#login
Koyya(config-line)#exit
Koyya(config)#line vty 0 4
Koyya(config-line)#password 1234
Koyya(config-line)#login
Koyya(config-line)#exit
Koyya(config)#service password-encryption
Koyya(config)#line vty 0 4
Koyya(config-line)#tansport input ssh
^
% Invalid input detected at '^' marker.
Koyya(config-line)#transport input ssh
Koyya(config-line)#login local
Koyya(config-line)#exit
Koyya(config)#banner motd 'Authorized access only'
Koyya(config)#interface vlan 1
Koyya(config-if)#exit
Koyya(config)#^Z
Koyya#
%SYS-5-CONFIG_I: Configured from console by console
Koyya#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Koyya(config)#interface FastEthernet0/2
Koyya(config-if)#interface vlan 1
Koyya(config-if)#ip address 10.24.0.2 255.255.192.0
Koyya(config-if)#no shut
Koyya(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
Koyya(config-if)#exit
Koyya(config)#ip default-gateway 10.24.0.1
Koyya(config)#exit
Koyya#
%SYS-5-CONFIG_I: Configured from console by console
Koyya#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Koyya#en

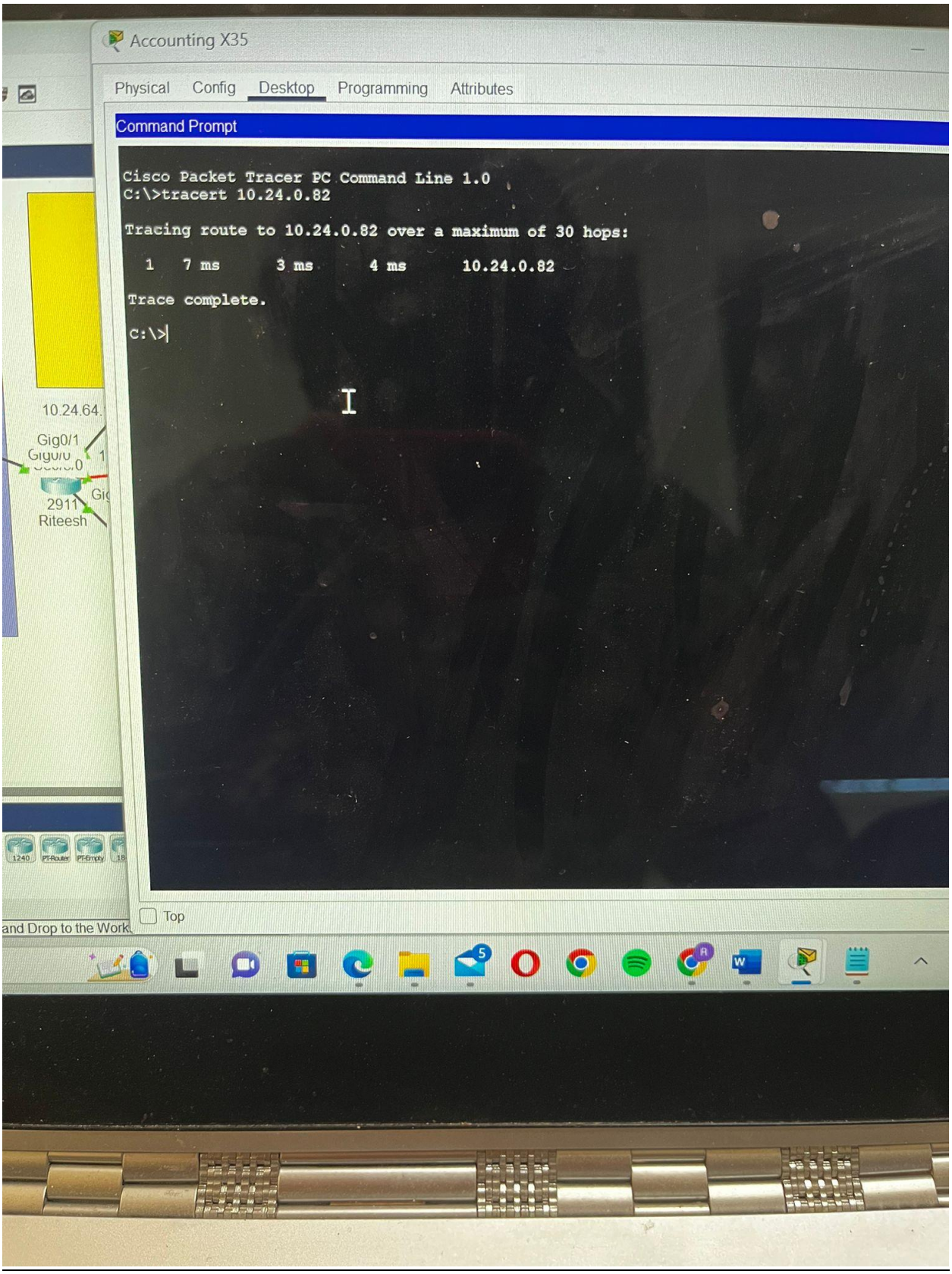

Physical
Config
CLI
Attributes
IOS Command Line Interface
koyya>en
Password:
koyya#sh run
Building configuration...
Current configuration : 1298 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname koyya
!
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
Top
45°F
Cloudy
Search

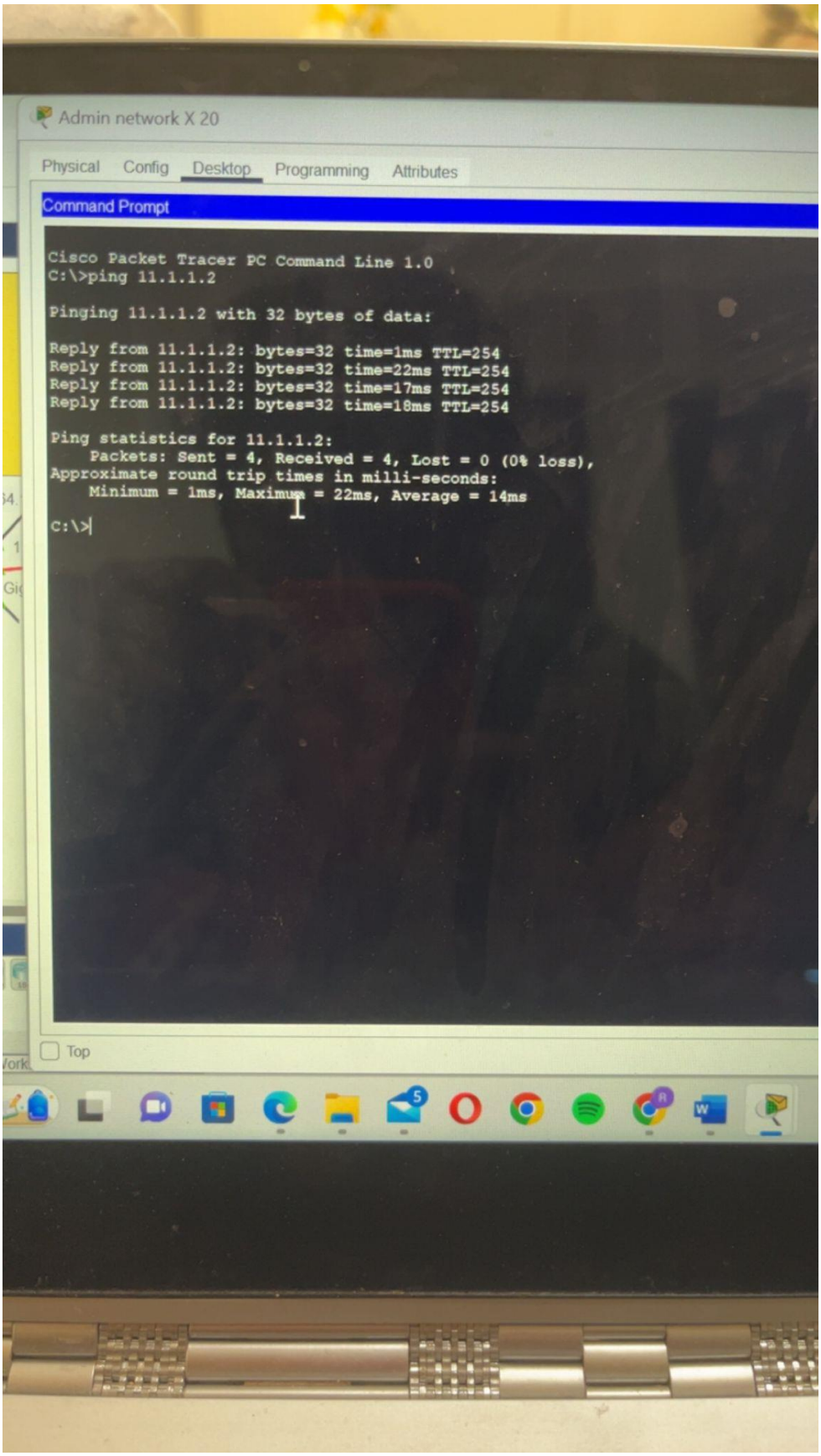

Koyya
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 10.24.0.2 255.255.192.0
!
ip default-gateway 10.24.0.1
!
banner motd ^Cno entry without authorized access^C
!
!
!
line con 0
password 7 08314D5D1A0E0A0516
login
!
line vty 0 4
password 7 08701E1D5D
login
transport input ssh
line vty 5 15
login
!
!
!
!
end
koyya#
koyya#
koyya#
koyya#
koyya#
koyya#
Top
45°F
Search

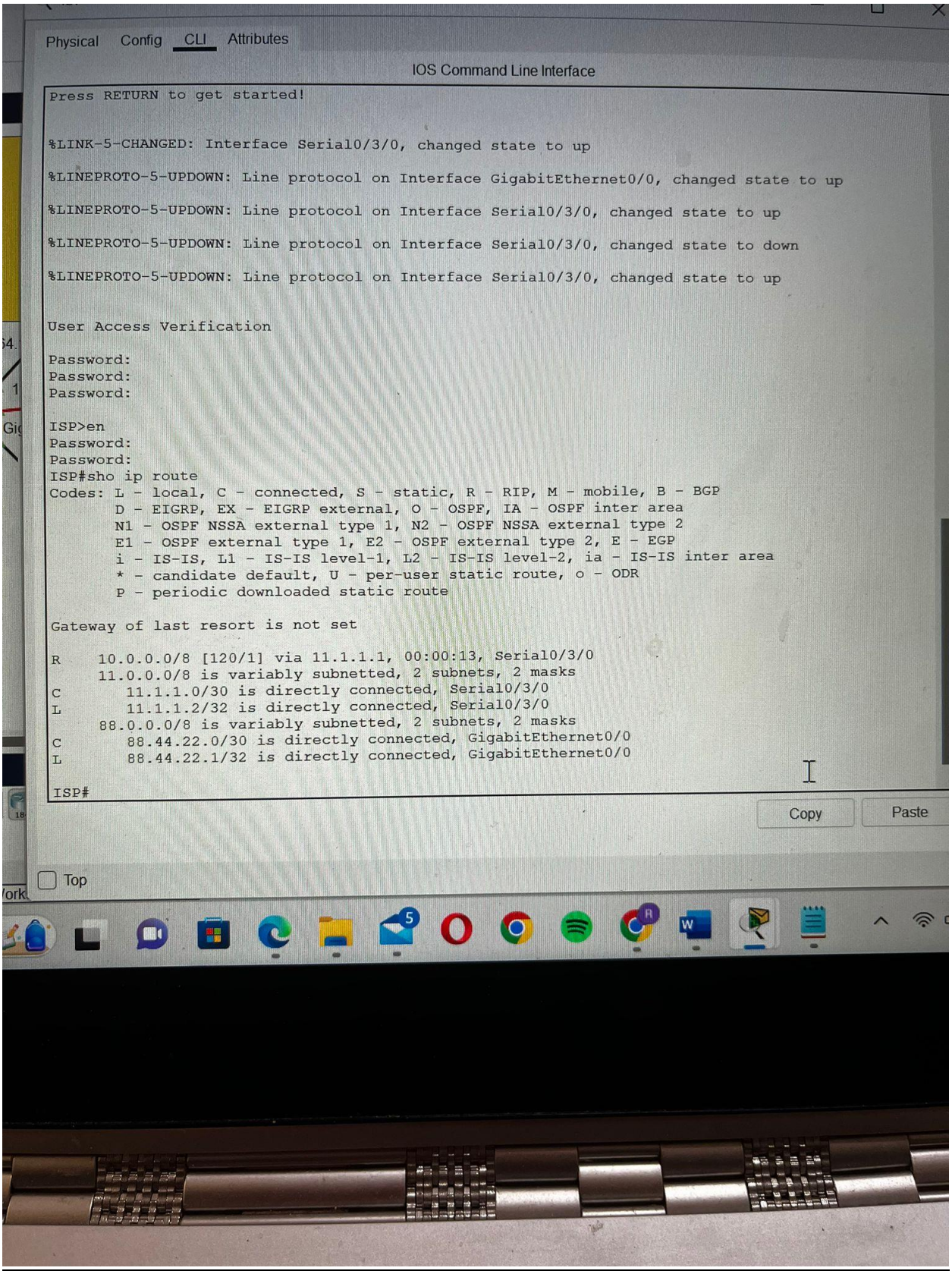
Screenshots Of Full Connectivity:

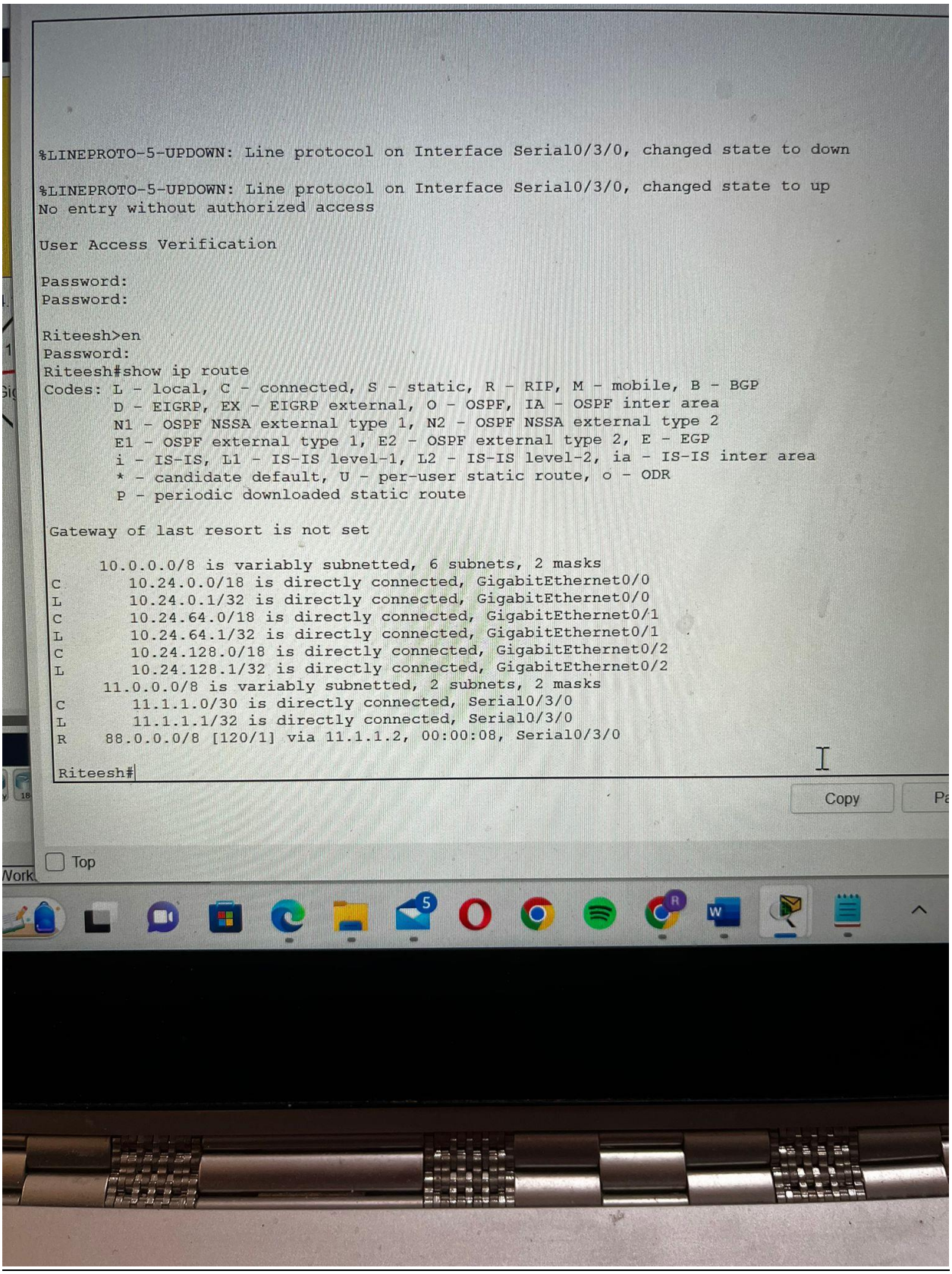


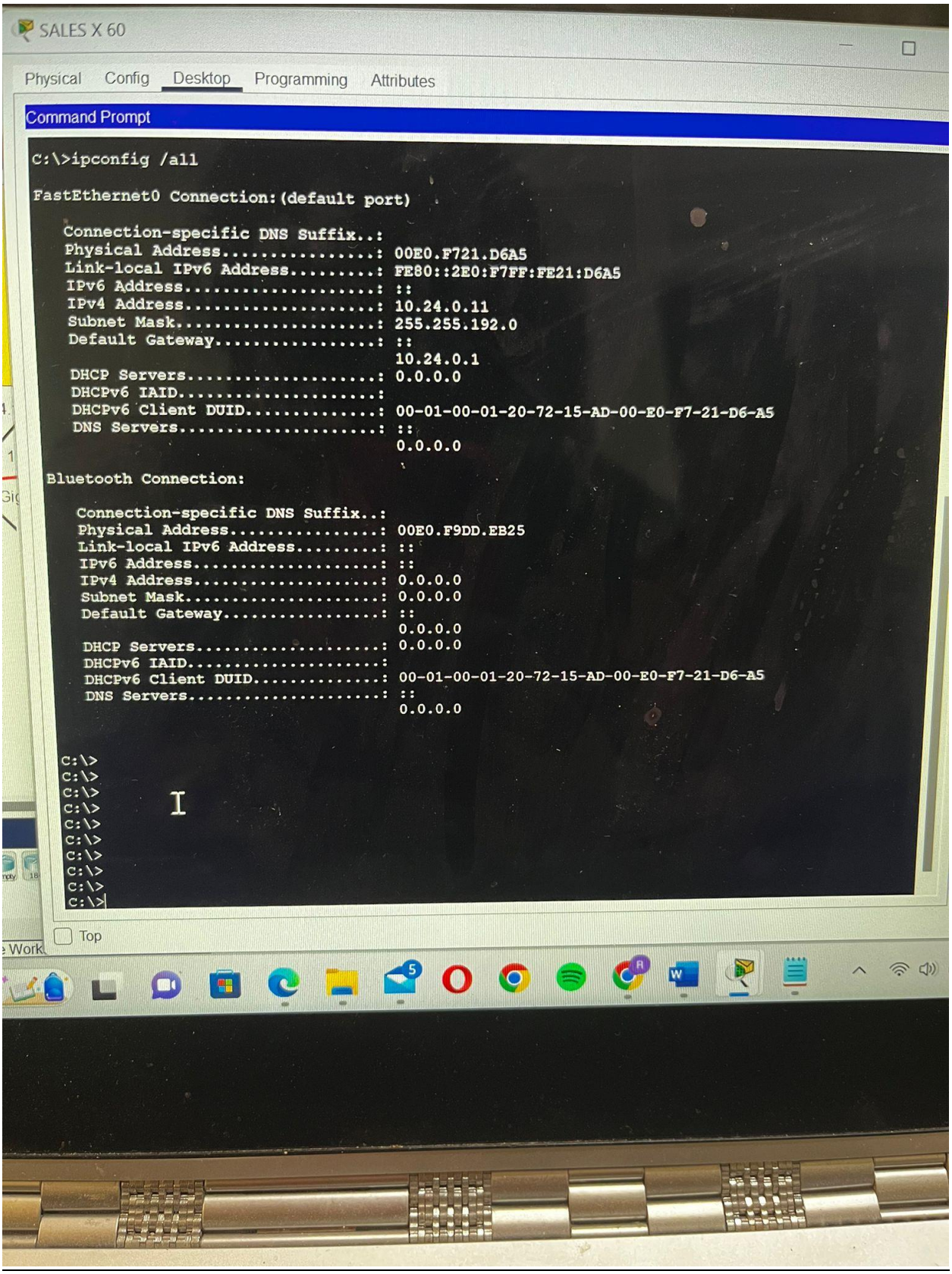

DNS server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 10.24.64.2
Pinging 10.24.64.2 with 32 bytes of data:
Reply from 10.24.64.2: bytes=32 time=10ms TTL=128
Reply from 10.24.64.2: bytes=32 time=4ms TTL=128
Reply from 10.24.64.2: bytes=32 time=5ms TTL=128
Reply from 10.24.64.2: bytes=32 time=7ms TTL=128
Ping statistics for 10.24.64.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 10ms, Average = 6ms
C:\>
2911
Riteesh
Top

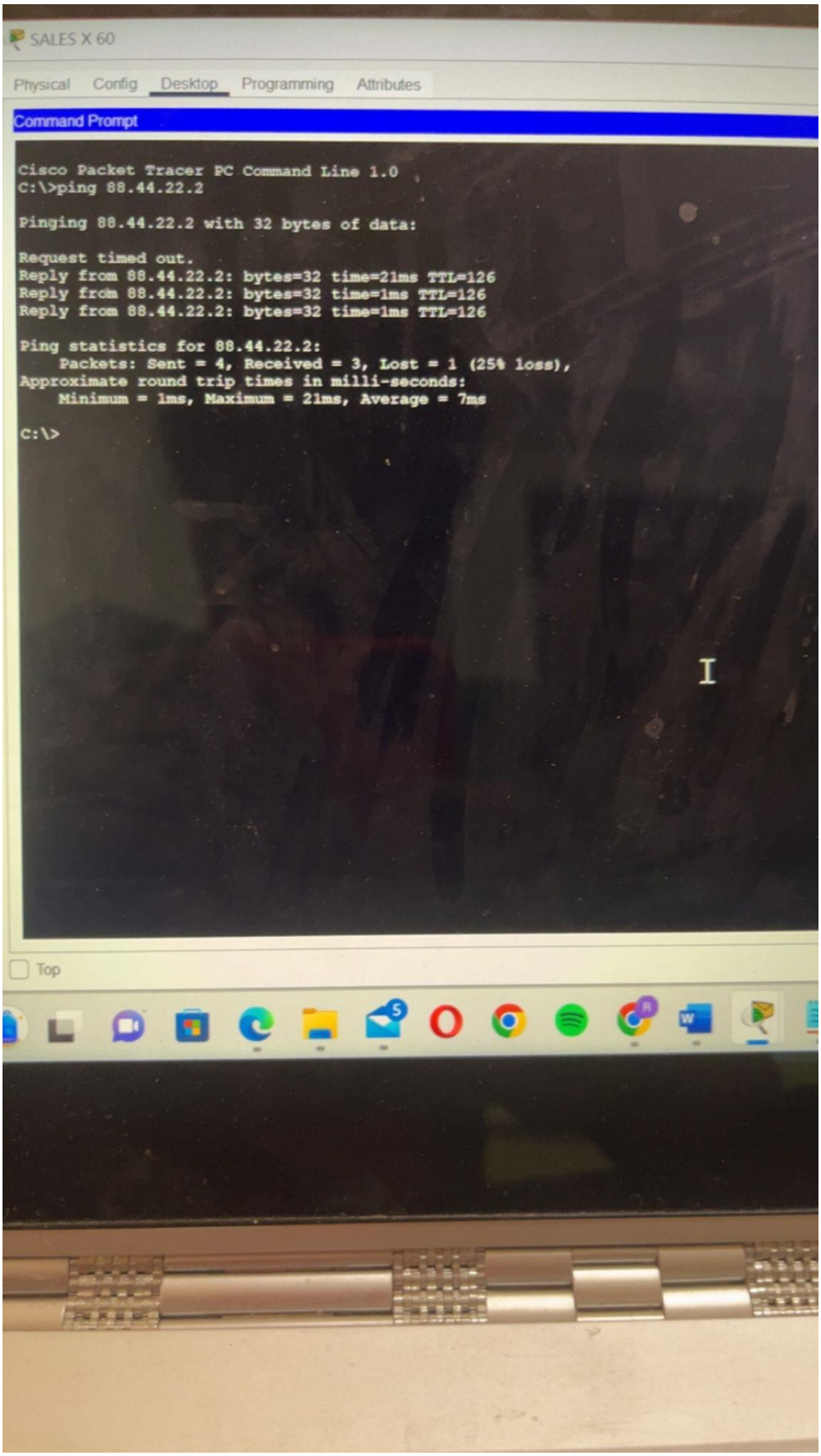

Accounting X35
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 10.24.0.82
Tracing route to 10.24.0.82 over a maximum of 30 hops:
1 7 ms 3 ms 4 ms 10.24.0.82
Trace complete.
C:\>
10.24.64.
Gig0/1
2911
Riteesh
Top


Admin network X 20
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 11.1.1.2
Pinging 11.1.1.2 with 32 bytes of data:
Reply from 11.1.1.2: bytes=32 time=1ms TTL=254
Reply from 11.1.1.2: bytes=32 time=22ms TTL=254
Reply from 11.1.1.2: bytes=32 time=17ms TTL=254
Reply from 11.1.1.2: bytes=32 time=18ms TTL=254
Ping statistics for 11.1.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 22ms, Average = 14ms
C:\>
Top


Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
User Access Verification
Password:
Password:
Password:
ISP>en
Password:
Password:
ISP#sho 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 10.0.0.0/8 [120/1] via 11.1.1.1, 00:00:13, Serial0/3/0
11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 11.1.1.0/30 is directly connected, Serial0/3/0
L 11.1.1.2/32 is directly connected, Serial0/3/0
88.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 88.44.22.0/30 is directly connected, GigabitEthernet0/0
L 88.44.22.1/32 is directly connected, GigabitEthernet0/0
ISP#
Copy
Paste
Top


%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up
No entry without authorized access
User Access Verification
Password:
Password:
Riteesh>en
Password:
Riteesh#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, 6 subnets, 2 masks
C 10.24.0.0/18 is directly connected, GigabitEthernet0/0
L 10.24.0.1/32 is directly connected, GigabitEthernet0/0
C 10.24.64.0/18 is directly connected, GigabitEthernet0/1
L 10.24.64.1/32 is directly connected, GigabitEthernet0/1
C 10.24.128.0/18 is directly connected, GigabitEthernet0/2
L 10.24.128.1/32 is directly connected, GigabitEthernet0/2
11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 11.1.1.0/30 is directly connected, Serial0/3/0
L 11.1.1.1/32 is directly connected, Serial0/3/0
R 88.0.0.0/8 [120/1] via 11.1.1.2, 00:00:08, Serial0/3/0
Riteesh#
Copy
Top


SALES X 60
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ipconfig /all
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 00E0.F721.D6A5
Link-local IPv6 Address.....: FE80::2E0:F7FF:FE21:D6A5
IPv6 Address.....: ::
IPv4 Address.....: 10.24.0.11
Subnet Mask.....: 255.255.192.0
Default Gateway.....: ::
10.24.0.1
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-20-72-15-AD-00-E0-F7-21-D6-A5
DNS Servers.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 00E0.F9DD.EB25
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-20-72-15-AD-00-E0-F7-21-D6-A5
DNS Servers.....: ::
0.0.0.0
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
Top


SALES X 60
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 88.44.22.2
Pinging 88.44.22.2 with 32 bytes of data:
Request timed out.
Reply from 88.44.22.2: bytes=32 time=21ms TTL=126
Reply from 88.44.22.2: bytes=32 time=1ms TTL=126
Reply from 88.44.22.2: bytes=32 time=1ms TTL=126
Ping statistics for 88.44.22.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 21ms, Average = 7ms
C:\>
Top

Uses of DHCP beneficial in the network IP address allocation:

The use of DHCP (Dynamic Host Configuration Protocol) can be beneficial in the network IP address allocation for several reasons:

1. Simplifies network administration: DHCP allows for centralized management of IP address assignment, reducing the need for manual configuration of individual devices. This makes it easier to manage the network and reduces the potential for human error.
2. Efficient use of IP addresses: DHCP ensures that IP addresses are allocated only when they are needed and released when they are no longer in use. This helps to conserve IP addresses and reduces the risk of address conflicts.
3. Automated IP configuration: DHCP automatically configures IP addresses and other network settings for devices on the network. This saves time and effort that would otherwise be spent on manual configuration.
4. Flexibility: DHCP allows for the dynamic allocation of IP addresses, meaning that devices can be easily moved or added to the network without requiring manual reconfiguration.

VLANs (Virtual Local Area Networks):

VLANs, or Virtual Local Area Networks, are a way of logically segmenting a physical network into multiple virtual networks. Each VLAN is treated as its own independent network with its own broadcast domain, allowing for more efficient use of network resources, improved security, and better management of network traffic. Some of the benefits and limitations of VLANs are:

Benefits:

1. Enhanced Security: VLANs can help improve network security by separating sensitive data traffic from other network traffic. By segregating different user groups, departments, and applications into different VLANs, network administrators can more effectively control access to network resources and reduce the risk of security breaches.
2. Improved Network Performance: VLANs can help improve network performance by reducing unnecessary network traffic. Broadcast and multicast traffic can be confined within a VLAN, reducing the amount of traffic on the network and improving overall network performance.
3. Better Network Management: VLANs can simplify network management by allowing network administrators to manage network traffic and devices at the VLAN level, rather than managing individual devices. VLANs can also help reduce network maintenance costs and downtime by making it easier to isolate and troubleshoot network issues.

Limitations:

1. Complexity: Setting up and configuring VLANs can be complex, especially in large networks. VLANs require specialized hardware and software, and network administrators

must have a good understanding of VLAN technology to effectively implement and manage VLANs.
2. Increased Network Overhead: VLANs can increase network overhead due to the additional processing required to handle VLAN traffic. This can lead to reduced network performance if the network infrastructure is not properly designed and configured to handle the additional traffic.
3. Limited Scalability: VLANs may not be scalable for very large networks or for networks with highly dynamic traffic patterns. In such cases, other network segmentation technologies such as Software-Defined Networking (SDN) may be more appropriate.

Virtual LANs can improve network performance by allowing network administrators to segment the network into smaller logical networks that can be managed independently. VLANs can also improve network security by isolating sensitive data traffic from other network traffic. By using VLANs, network administrators can more effectively manage network resources and reduce the risk of security breaches.

DHCP and VLAN's configuration process:

Here are the steps to configure DHCP and VLANs in Cisco Packet Tracer:

1. Create VLANs: In Cisco Packet Tracer, select the switch where the VLANs will be created. Go to the VLAN tab in the switch configuration, and click on the "+" button to create a new VLAN. Assign a VLAN ID and a name to the VLAN. Repeat the process to create additional VLANs.
2. Assign Ports to VLANs: In the switch configuration, select the port that will be assigned to a VLAN. Click on the port, and select the VLAN ID that the port will belong to. Repeat the process to assign ports to other VLANs.
3. Configure DHCP: In Cisco Packet Tracer, select a server device where the DHCP server will be configured. Go to the Services tab, and click on DHCP to open the DHCP configuration. Click on the "+" button to create a new DHCP pool. Assign a pool name, and specify the network address and subnet mask for the VLAN. Configure other DHCP settings, such as default gateway and DNS server. Repeat the process to create additional DHCP pools for other VLANs.
4. Configure DHCP Relay: If the DHCP server is not on the same VLAN as the client, enable DHCP relay on the network switches. In the switch configuration, select the interface that connects to the VLAN without the DHCP server. Configure the IP address of the DHCP server and enable DHCP relay.
5. Test the Configuration: Verify that clients on each VLAN are receiving IP addresses and can communicate with other devices on their VLAN and other VLANs.

It's important to note that the specific steps for configuring DHCP and VLANs may vary depending on the network equipment being used in Cisco Packet Tracer. It's also important to thoroughly test the configuration to ensure that it is working as expected.

References:

1. Cisco. "Introduction to VLANs." Cisco Systems, Inc. https://www.cisco.com/c/en/us/support/docs/lan-switching/virtual-lans-vlan-trunking-protocol-vlans-vtp/98169-vlan-design-ccda.html
2. Kurose, James F. and Keith W. Ross. Computer Networking: A Top-Down Approach. 7th ed., Pearson Education, Inc., 2016.
3. Mankin, Allison, et al. "Segmenting the Network with VLANs." Internet Engineering Task Force, RFC 5517, 2009. https://tools.ietf.org/html/rfc5517
4. Cisco Packet Tracer: "Configuring VLANs": https://www.netacad.com/courses/packet-tracer-tutorials/configuring-vlans-in-cisco-packet-tracer
5. Cisco Packet Tracer: "Configuring DHCP": https://www.netacad.com/courses/packet-tracer-tutorials/configuring-dhcp-in-cisco-packet-tracer
6. Cisco Packet Tracer: "Configuring DHCP Relay": https://www.netacad.com/courses/packet-tracer-tutorials/configuring-dhcp-relay-in-cisco-packet-tracer