



## **COLLEGE OF ENGINEERING & TECHNOLOGY**

**Department** : Computer Engineering  
**Lecturer** : Dr. Mohamed Waleed Fakhri  
**Assoc.** : Eng. Nourhan Tarek  
**Teacher** : Computer Networks  
**Course Title** : CC431  
**Course Code** :2022

### **CC431: Computer Networks Document**

#### **Final project**

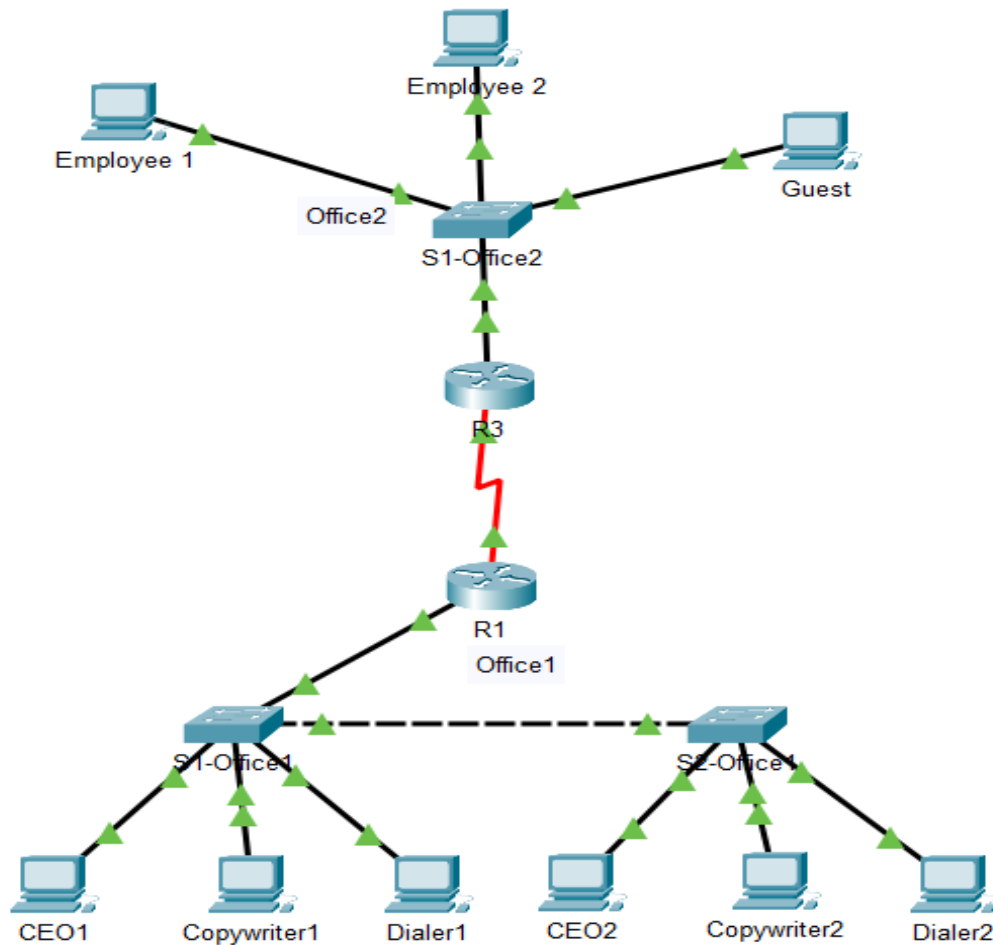
**Subscribed and Presented by:**

**Shady Hisham**

**Mostafa Ayman**

**Youssef Mohamed Barrima**

## Topology



Create the preceding topology and configure the devices.

## Scenario

As a junior network administrator, you and your team were tasked with planning and configuring a corporate network for a new bank branch. It is your duty to set implement basic security settings on all systems.

## Lab Task 1: Design an IP Address Scheme

Devise a Network Topology plan for the amount of subnets you will need, and where you want to assign the IPv4 addresses within each subnet.

1. Divide the 172.16.10.0/24 network into five subnets.

*The old subnet mask was /24 (32-24 = 8 bits for each host) after dividing it into 5 subnets ( $2^8/5 = 51.2 \gg \log_2(51.2) = 5.67$  then approximately 5 bits for each host in each subnet  $\gg 8 - 5 = 3$  bits for identifying each subnet), then the subnet mask for each subnet is 24+3 bits = /27*

2. What is the value of the new subnet mask?

*Then the new subnet mask is /27 for each new subnet*

3. How many usable host addresses exist per subnet?

*Number of IP addresses in each subnet =  $2^5$*

*Number of hosts in each subnet =  $2^5 - 2 = 30$  hosts*

4. Fill in the following table with the resulting subnets (from step 1 above):

Subnet Number	Network Address	Usable Host Address Range	Broadcast Address
1	172.16.10.0/27	172.16.10.1 -- 172.16.10.30	172.16.10.31
2	172.16.10.32/27	172.16.10.33 -- 172.16.10.62	172.16.10.63
3	172.16.10.64/27	172.16.10.65 -- 172.16.10.94	172.16.10.95
4	172.16.10.96/27	172.16.10.97 -- 172.16.10.126	172.16.10.127
5	172.16.10.128/27	172.16.10.129 -- 172.16.10.158	172.16.10.159

## Lab Task 2: Implement VLANs and Trunk

Configure VLANs and set trunks on the appropriate network and its associated devices.

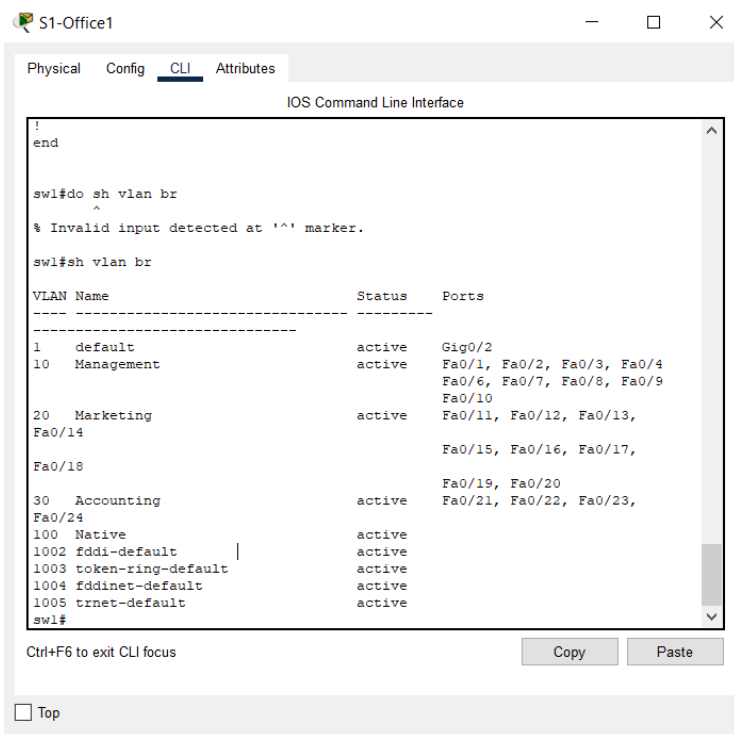
**Note:** Perform steps 1-4 on S1-Office1 and S2-Office1.

1. Create and name VLANs as follows:

- a. VLAN 10 – Management
- b. VLAN 20 – Marketing
- c. VLAN 30 – Accounting
- d. VLAN 100 – Native

2. On S1-Office1 and S2Office1 configure the interfaces as "Access" mode, and assign VLANs as follows:

- a. VLAN 10: FastEthernet0/1-10
- b. VLAN 20: FastEthernet0/11-20
- c. VLAN 30: FastEthernet0/21-24



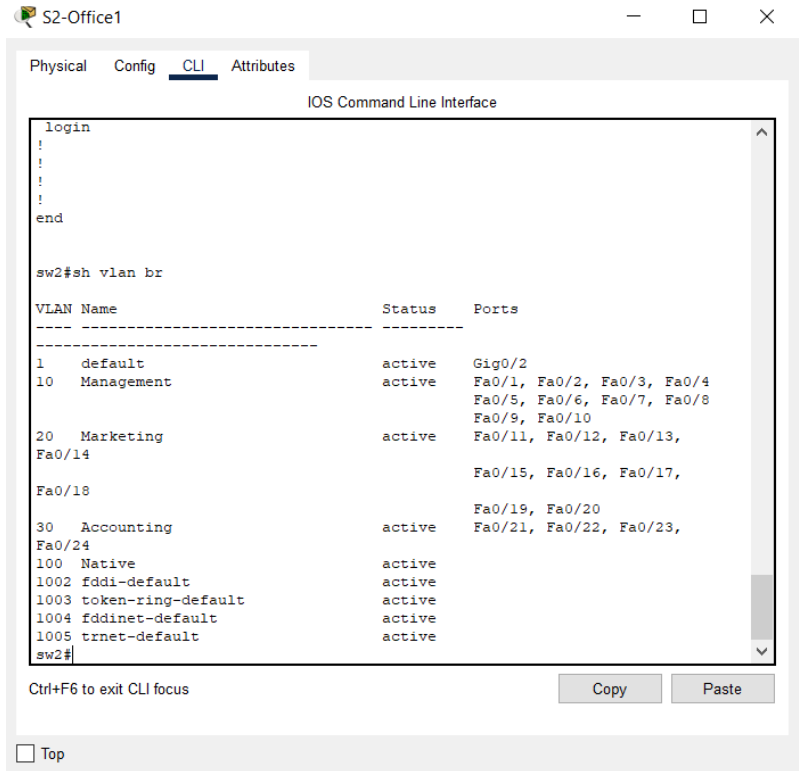
The screenshot shows the CLI of S1-Office1. The user has entered the command 'sw1#do sh vlan br' to display the current VLAN configuration. The output shows several VLANs, including the ones specified in the task: VLAN 10 (Management), VLAN 20 (Marketing), and VLAN 30 (Accounting). The status of each VLAN is 'active', and the associated ports are listed.

```
!
end

sw1#do sh vlan br
% Invalid input detected at '^' marker.

sw1#sh vlan br

VLAN Name                Status    Ports
-----
1    default                active    Gig0/2
10   Management              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                           Fa0/10
20   Marketing              active    Fa0/11, Fa0/12, Fa0/13,
                                           Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17,
                                           Fa0/18
30   Accounting              active    Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23,
                                           Fa0/24
100  Native                  active
1002 fddi-default            active
1003 token-ring-default     active
1004 fddinet-default         active
1005 trnet-default           active
sw1#
```



The screenshot shows the CLI of S2-Office1. The user has entered the command 'sw2#sh vlan br' to display the current VLAN configuration. The output shows several VLANs, including the ones specified in the task: VLAN 10 (Management), VLAN 20 (Marketing), and VLAN 30 (Accounting). The status of each VLAN is 'active', and the associated ports are listed.

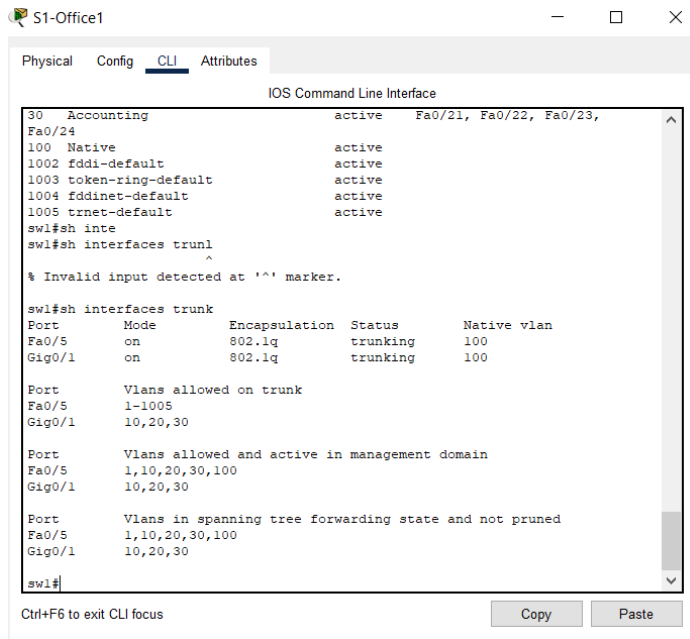
```
login
!
!
!
!
!
!
end

sw2#sh vlan br

VLAN Name                Status    Ports
-----
1    default                active    Gig0/2
10   Management              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10
20   Marketing              active    Fa0/11, Fa0/12, Fa0/13,
                                           Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17,
                                           Fa0/18
30   Accounting              active    Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23,
                                           Fa0/24
100  Native                  active
1002 fddi-default            active
1003 token-ring-default     active
1004 fddinet-default         active
1005 trnet-default           active
sw2#
```

3. Configure the S1-Office1 to S2-Office1 interconnecting link as "Trunk" on both.

**Note:** To simplify the identification of the ports, click “Options...”, click “Preferences...” and select “Always Show Port Labels in Logical Workspace”.



```
IOS Command Line Interface
30 Accounting active Fa0/21, Fa0/22, Fa0/23,
Fa0/24
100 Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
sw1#sh inte
sw1#sh interfaces trunl
^
% Invalid input detected at '^' marker.

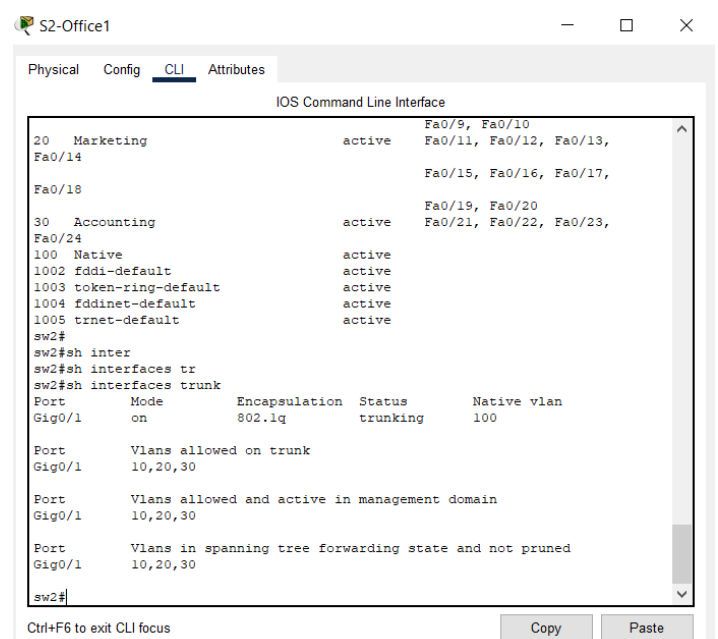
sw1#sh interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/5     on        802.1q         trunking    100
Gig0/1    on        802.1q         trunking    100

Port      Vlans allowed on trunk
Fa0/5     1-1005
Gig0/1    10,20,30

Port      Vlans allowed and active in management domain
Fa0/5     1,10,20,30,100
Gig0/1    10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/5     1,10,20,30,100
Gig0/1    10,20,30

sw1#
```



```
IOS Command Line Interface
20 Marketing active Fa0/9, Fa0/10
Fa0/11, Fa0/12, Fa0/13,
Fa0/14
Fa0/15, Fa0/16, Fa0/17,
Fa0/18
30 Accounting active Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23,
Fa0/24
100 Native active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
sw2#
sw2#sh inter
sw2#sh interfaces tr
sw2#sh interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Gig0/1    on        802.1q         trunking    100

Port      Vlans allowed on trunk
Gig0/1    10,20,30

Port      Vlans allowed and active in management domain
Gig0/1    10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Gig0/1    10,20,30

sw2#
```

4. Verify the VLAN and trunk configurations using the appropriate **Show** commands, and save the configuration.

Verification is shown above using command: **#show interfaces trunk**

And **# show vlan brief**

5. On both switches, disable DTP **only** on the access port

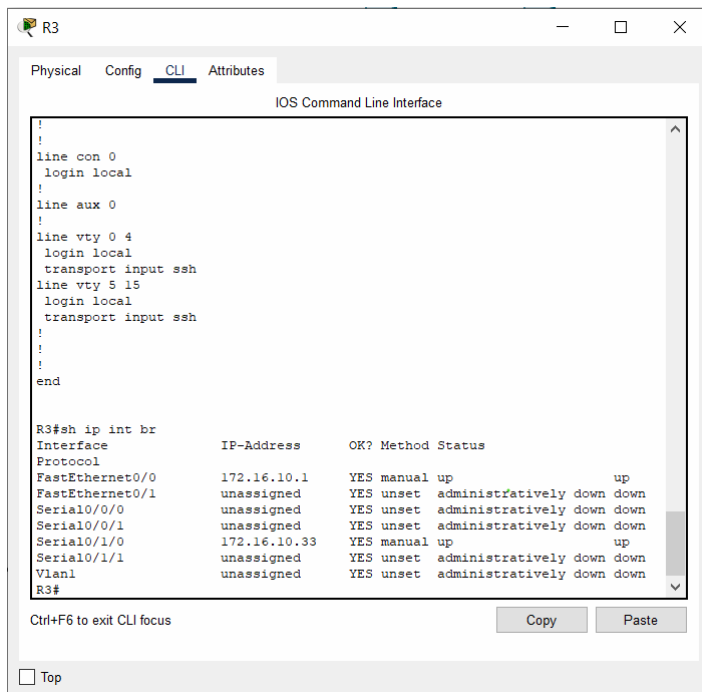
(automatic) through command **#switchport mode access**

## Lab Task 3: Assign IP Addresses

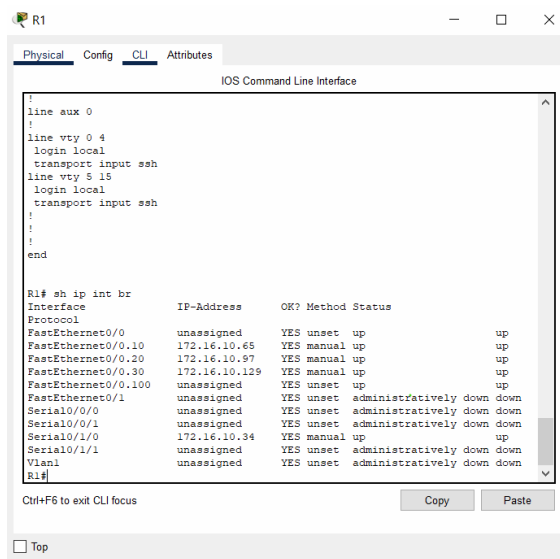
Using the table you made in Task 2, assign subnets to the topology.

**Note:** Make sure to document the assignment of the IP addresses in a separate file, to keep track of them.

1. Assign an IP address to subnet 1 to the R3 interface connected to the Office2 network. R1's LAN interface will be configured in Task 4.



2. Assign the first IPs in subnet 2 to the R1<->R3 WAN link.



3. Assign the last usable addresses of Subnet 3 to VLAN 10 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).

**Note:** Layer 3 connectivity with VLANs requires Router-on-a-Stick setup.

CEO1

Physical Config Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 000C.85B5.8D72

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.94

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address FE80::20C:85FF:FEB5:8D72

☐ Top

CEO2

Physical Config Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.2F68.9BB1

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.93

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address FE80::260:2FFF:FE68:9BB1

☐ Top

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.10.65 255.255.255.224
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.16.10.97 255.255.255.224
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.10.129 255.255.255.224
!
interface FastEthernet0/0.100
encapsulation dot1Q 100 native
no ip address
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

4. Assign the last usable addresses of Subnet 4 to VLAN 20 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).

CopyWriter1

Physical Config Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0003.E4D6.0554

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.126

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address FE80::203:E4FF:FED6:554

☐ Top

CopyWriter2

Physical Config Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0007.ECE5.285C

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.125

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address FE80::207:ECFF:FEE5:285C

☐ Top

R1

Physical Config CLI Attributes

IOS Command Line Interface

```
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.10.65 255.255.255.224
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.16.10.97 255.255.255.224
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.10.129 255.255.255.224
!
interface FastEthernet0/0.100
encapsulation dot1Q 100 native
no ip address
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



5. Assign the last usable addresses of Subnet 5 to VLAN 30 on the Office 1 network end devices. Also, assign the default gateway (first address in the subnet).

The image displays three network configuration windows. The top-left window, titled 'Dailer1', shows the 'Config' tab with 'Global Settings' for 'Dailer1' and 'FastEthernet0'. It is configured with a static IP of 172.16.10.129 and a default gateway of 172.16.10.129. The top-right window, titled 'Dialer2', shows the 'Config' tab for 'FastEthernet0'. It is configured with a static IP of 172.16.10.157, a subnet mask of 255.255.255.224, and a MAC address of 0001.4396.E4A9. The bottom window, titled 'R1', shows the 'CLI' tab with the 'IOS Command Line Interface'. It contains the following configuration commands:

```
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.16.10.65 255.255.255.224
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.16.10.97 255.255.255.224
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.16.10.129 255.255.255.224
!
interface FastEthernet0/0.100
encapsulation dot1Q 100 native
no ip address
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
```

At the bottom of the R1 CLI window, there are buttons for 'Copy' and 'Paste', and a 'Top' button.

- Assign the last useable IP addresses of Subnet 1 (Office 2) to the endpoints in each network or VLAN.

Employee 1

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex ☒ Auto

MAC Address 0090.2BD3.AA78

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.30

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::290:2BFF:FE03:AA78

☐ Top

Employee 2

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.9738.944B

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.29

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::201:97FF:FE38:944B

☐ Top

Guest

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

FastEthernet0

Port Status ☒ On

Bandwidth ☒ Auto

Duplex ☒ Full Duplex ☒ Auto

MAC Address 0060.3E47.3D15

IP Configuration

☐ DHCP

☒ Static

IPv4 Address 172.16.10.28

Subnet Mask 255.255.255.224

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address

Link Local Address: FE80::260:3EFF:FE47:3D15

☐ Top

## Lab Task 4: Configure R1 for Inter-VLAN Routing

Configure the router on the Office1 network to allow multiple VLANs to communicate on the network.

### Perform steps 1-4 on R1.

1. Enable GigabitEthernet 0/0
2. Create three sub-interfaces on GigabitEthernet 0/0 (use any sub-interface IDs you want).
3. Set the correct encapsulation type and VLAN ID for each sub-interface.
4. Configure the appropriate IP address and subnet mask (corresponding to VLAN). Use the first usable address of each subnet.  
(shown above)
5. Check the settings on the router using the appropriate show command.  
(above shown by #show run)
6. On S1-Office1, set GigabitEthernet 0/1 as Trunk, with appropriate Native

The image displays two side-by-side screenshots of the S1-Office1 CLI interface, showing the configuration and verification of a trunk interface.

**Left Screenshot (Configuration):**

```
SW1>en
Password:
Password:
sw1#sh
% Unknown command or computer name, or unable to find computer address

sw1#sh int g0/1 sw
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 100 (Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
--More--
```

**Right Screenshot (Verification):**

```
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

sw1#sh interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/5     on        802.1q         trunking    100
Gig0/1     on        802.1q         trunking    100

Port      Vlans allowed on trunk
Fa0/5     1-1005
Gig0/1     10,20,30

Port      Vlans allowed and active in management domain
Fa0/5     1,10,20,30,100
Gig0/1     10,20,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/5     1,10,20,30,100
Gig0/1     10,20,30

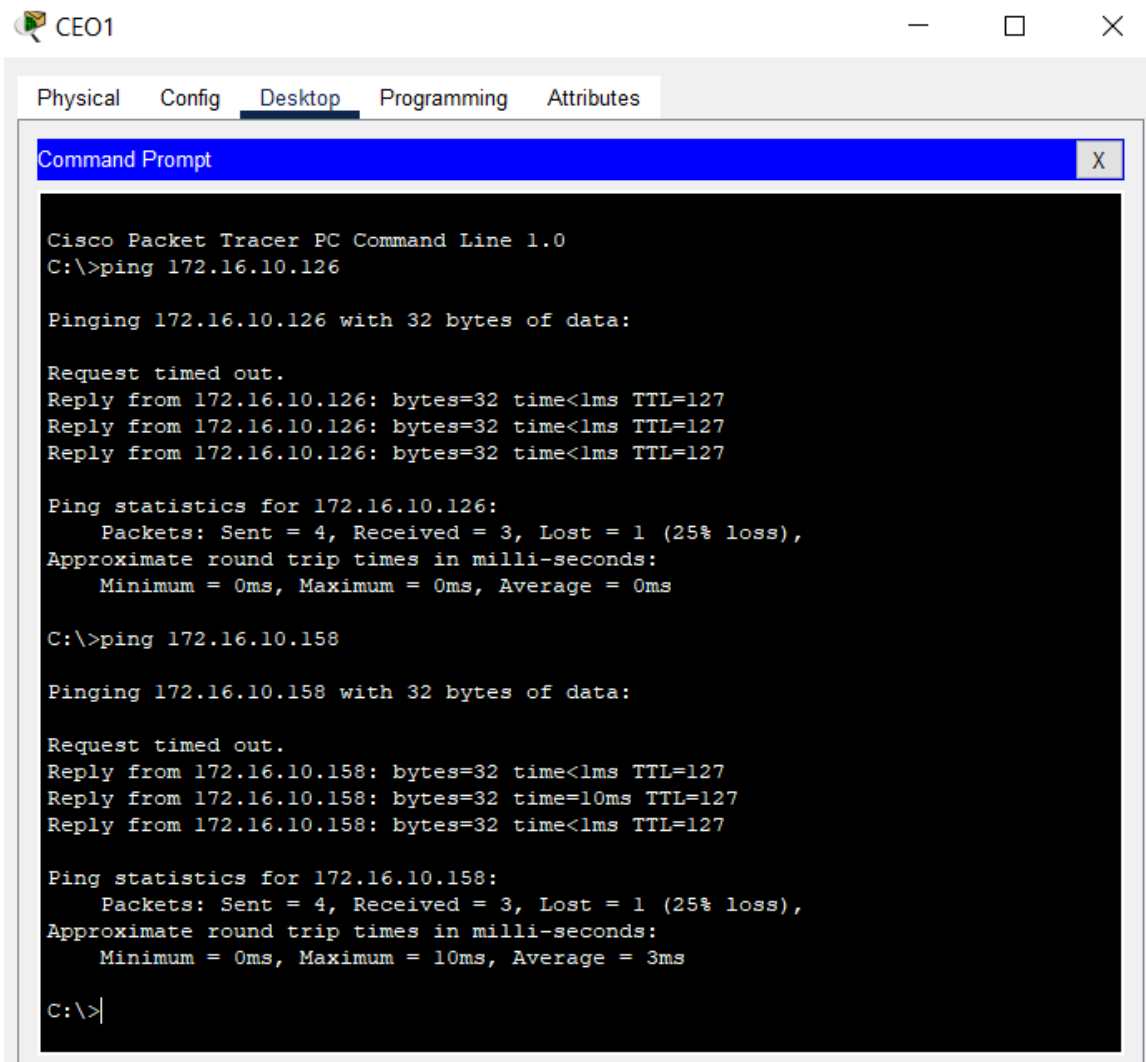
sw1#
```

VLAN.

7. Verify this part of the configuration using the appropriate show commands and save the configuration.

Shown above by #show interfaces trunk

8. Test the inter-VLAN routing by pinging Copyrigher1 and Dialer1 from the CEO1 PC.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.10.126

Pinging 172.16.10.126 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.126: bytes=32 time<1ms TTL=127
Reply from 172.16.10.126: bytes=32 time<1ms TTL=127
Reply from 172.16.10.126: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.126:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.10.158

Pinging 172.16.10.158 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.158: bytes=32 time<1ms TTL=127
Reply from 172.16.10.158: bytes=32 time=10ms TTL=127
Reply from 172.16.10.158: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.158:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

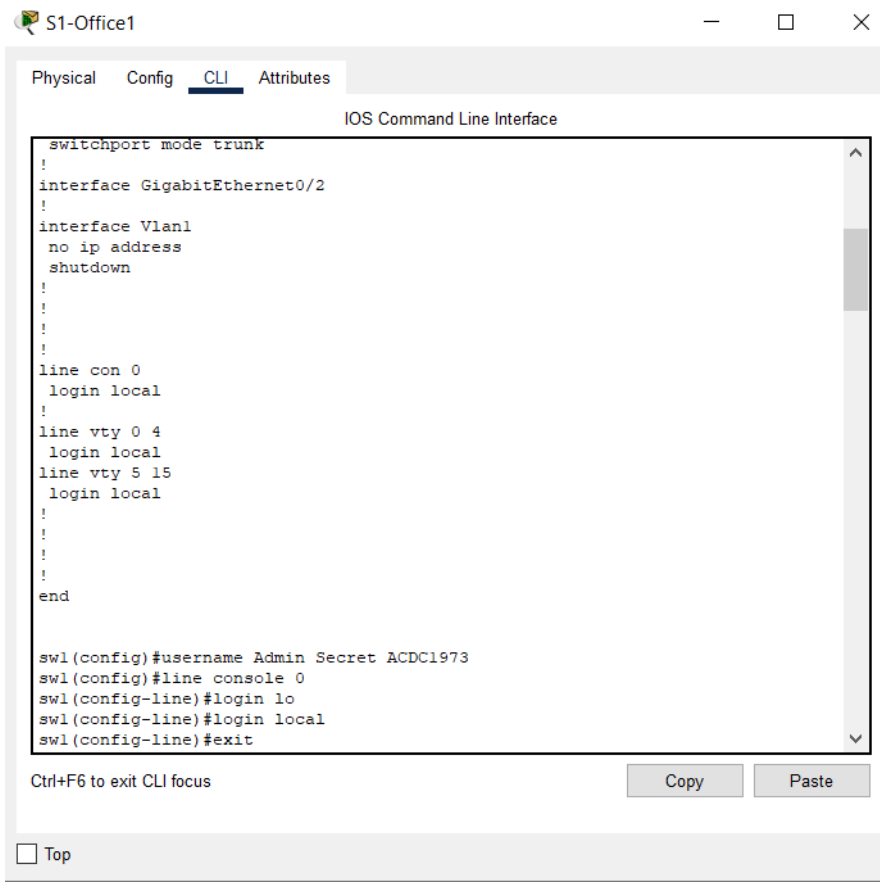
## Lab Task 5: Initial and Security Settings for Network Devices

Configure all network devices with basic security settings to prevent unauthorized access.

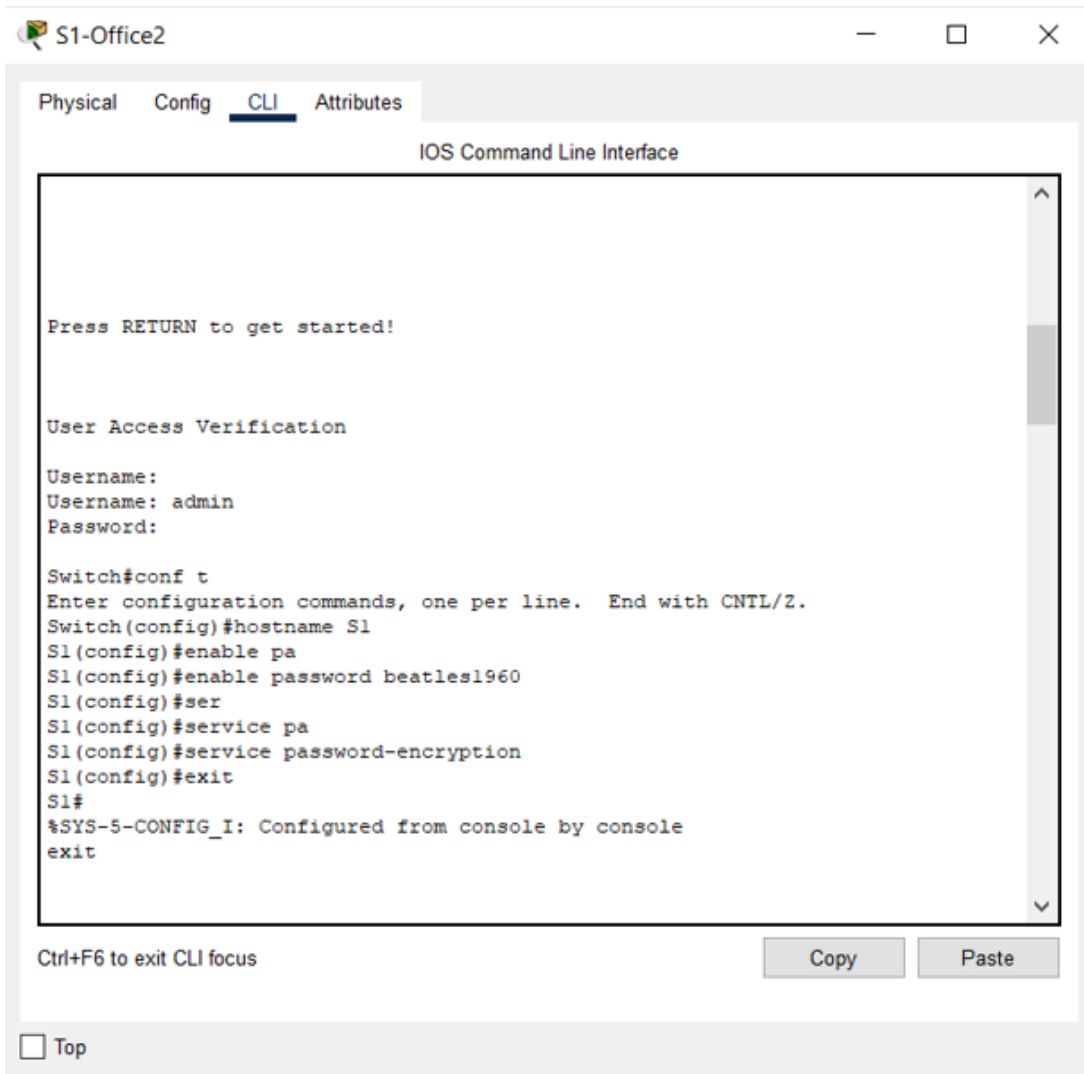
**Perform steps 1-5 on all routers and switches.**

1. Create a user account with the following login credentials:

- Username: Admin
- Password: ACDC1973



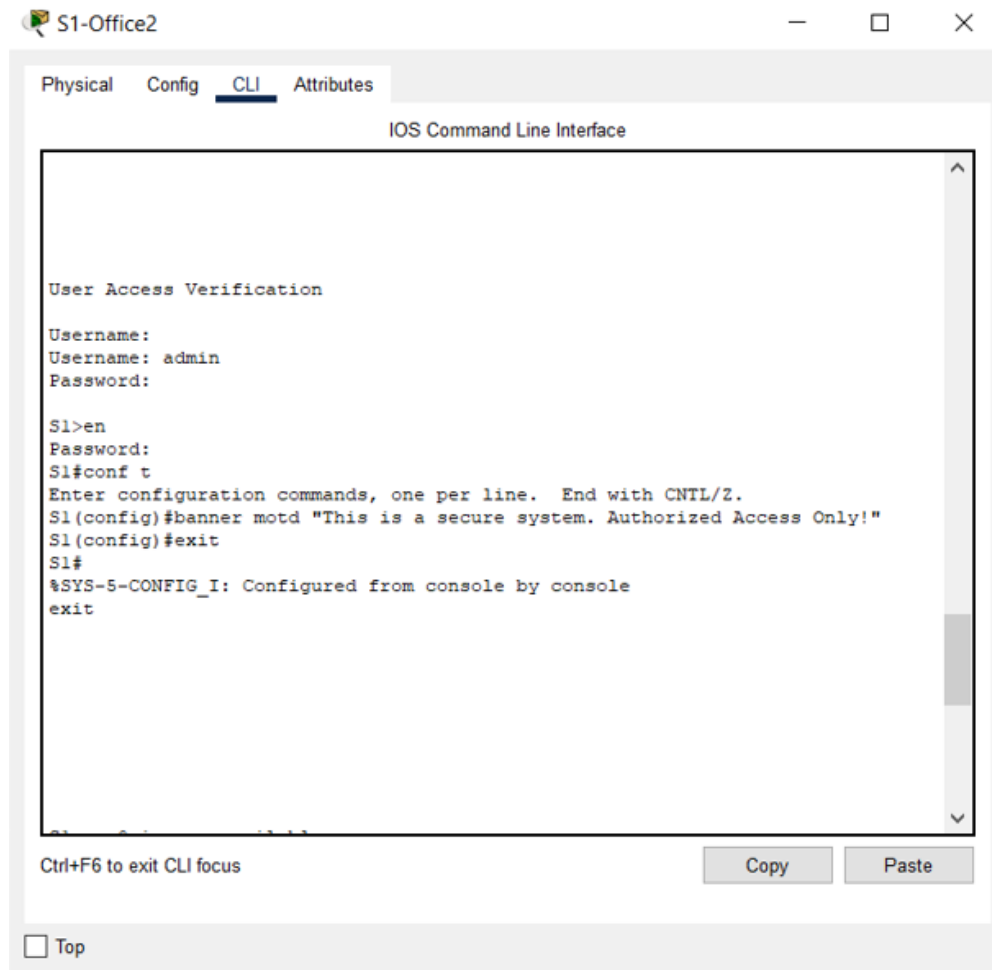
2. Secure access to the console line by checking local login credentials.
3. Shown above
4. Secure privileged mode access (password: beatles1960).



5. Encrypt all passwords on the device.

Shown above

6. Configure a suitable security message (hint: MOTD Banner).



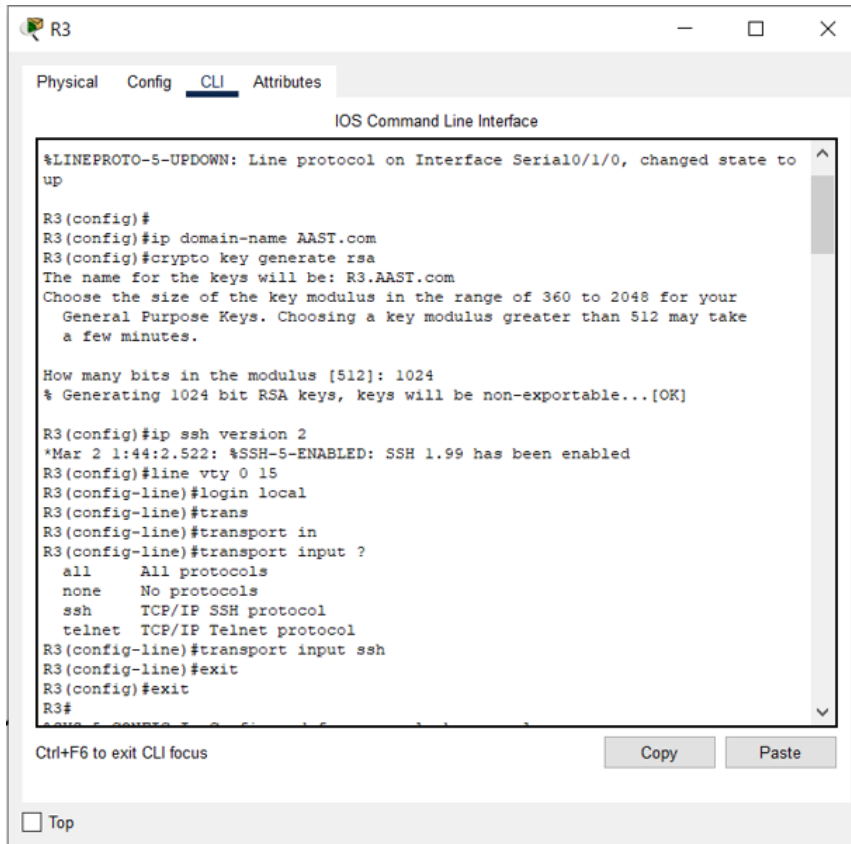
## Lab Task 6: Secure Remote Access

Configure SSHv2 services on all routers to allow for remote administration.

**Perform steps 1-4 on R1 and R3.**

1. Set the IP domain name to AAST.com.
2. Generate secure keys (minimum key length is 1024 bits).
3. Set SSH version 2.
4. Configure VTY lines to check for local login credentials, and allow only incoming SSH sessions.
5. Verify this part of the configuration using the appropriate show commands, and save the configuration.

6. Configure the correct default gateway on the Admin PC and try to log in to routers from admin PCs, using SSH.



The screenshot shows the R3 router's CLI interface. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The main window displays the following commands and their outputs:

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

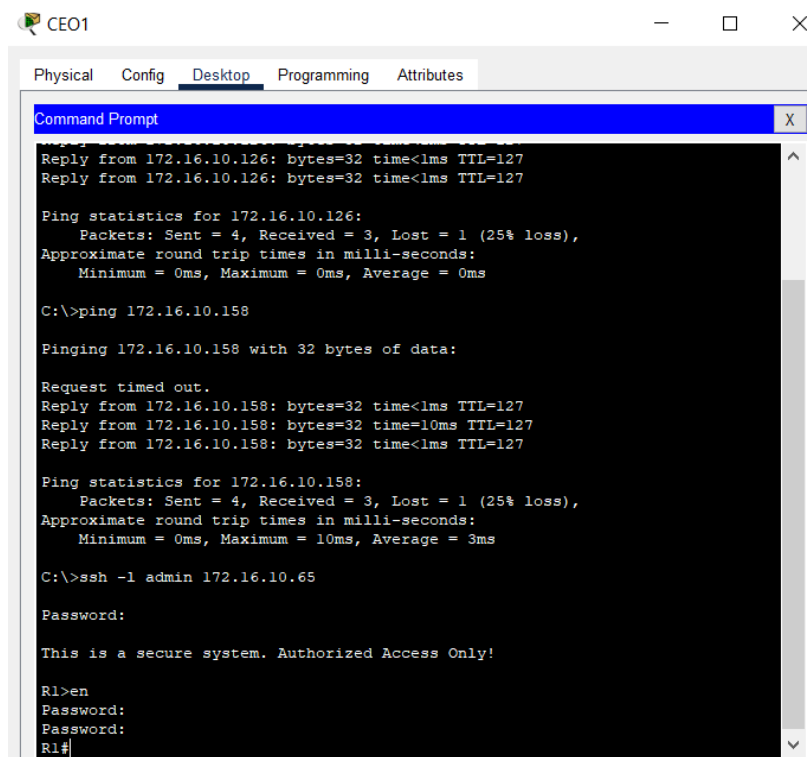
R3(config)#
R3(config)#ip domain-name AAST.com
R3(config)#crypto key generate rsa
The name for the keys will be: R3.AAST.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#ip ssh version 2
*Mar 2 1:44:2.522: %SSH-5-ENABLED: SSH 1.99 has been enabled
R3(config)#line vty 0 15
R3(config-line)#login local
R3(config-line)#trans
R3(config-line)#transport in
R3(config-line)#transport input ?
  all      All protocols
  none     No protocols
  ssh      TCP/IP SSH protocol
  telnet   TCP/IP Telnet protocol
R3(config-line)#transport input ssh
R3(config-line)#exit
R3(config)#exit
R3#
```

At the bottom, there is a button labeled "Copy" and a button labeled "Paste". A checkbox labeled "Top" is also visible.

Run the command: **ssh -l <username> <target-ip>**



The screenshot shows the Admin PC's Command Prompt window. The tabs at the top are Physical, Config, Desktop (selected), Programming, and Attributes. The main window displays the following commands and their outputs:

```
Reply from 172.16.10.126: bytes=32 time<1ms TTL=127
Reply from 172.16.10.126: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.126:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 172.16.10.158

Pinging 172.16.10.158 with 32 bytes of data:

Request timed out.
Reply from 172.16.10.158: bytes=32 time<1ms TTL=127
Reply from 172.16.10.158: bytes=32 time=10ms TTL=127
Reply from 172.16.10.158: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.158:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ssh -l admin 172.16.10.65

Password:
This is a secure system. Authorized Access Only!

R1>en
Password:
Password:
R1#
```



## **Perform steps 1-3 on all devices.**

1. Check the following parameters on all devices:
  - a. IP Address
  - b. Subnet Mask
  - c. Default Gateway
2. Make sure they are configured correctly and adjust them if necessary.
3. Go to the command prompt in the admin PC and try to ping CEO1 and Employee1.
4. Go to the command prompt in Employee2's PC and try to ping Copyrighter1 and Dialer1. The results should be successful.
5. If a connectivity test fails, perform troubleshooting.

**Note:** If this is your first time pinging the Dialer1 or Copyrighter1 PC from Employee 2's PC, the first ping may fail since the ARP tables are not populated.

The first ping will aid in populating the ARP tables in the network devices, and future pings should then work.