

CYBER SHUJAA CLOUD & NETWORK SECURITY

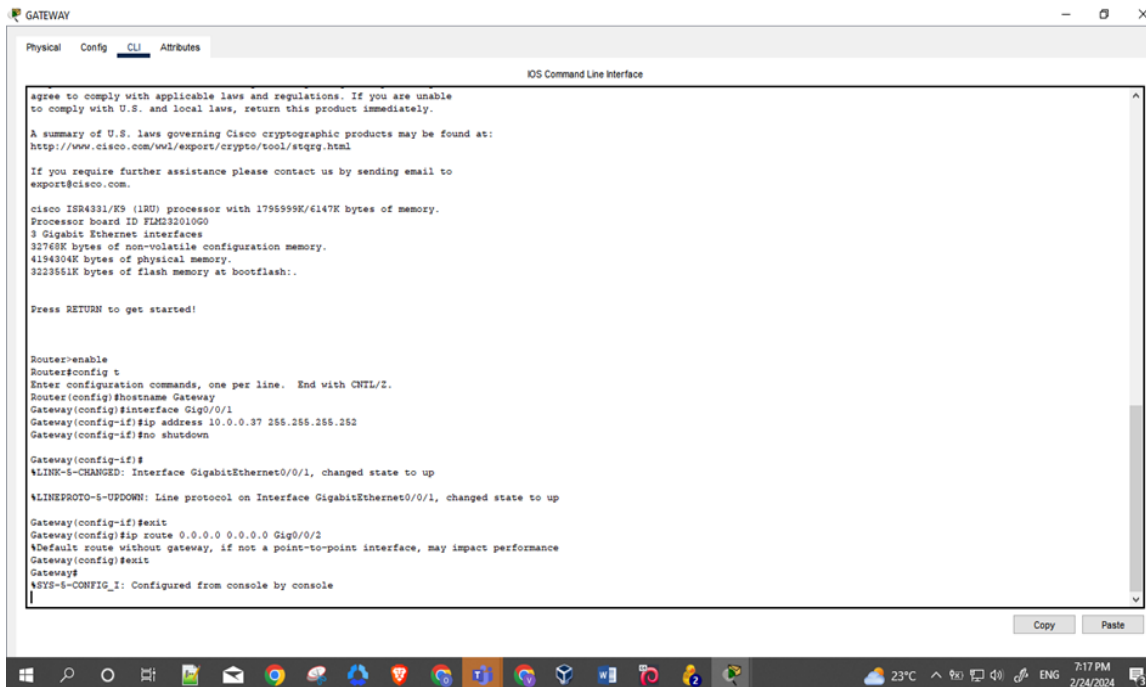
PACKET TRACER MID-EXAM

TIME ALLOWED: 2 HOURS

TOTAL: marks

Instructions:

- Answer **ALL** questions
- The exam should **NOT be** worked on in groups or with assistance from others.
- You **MUST** have your **camera on** throughout the session.
- Use this file as your write-up reporting template as you complete each task outlined and answer the questions.
- **Rename this file with your full names e.g Firstname_Lastname.docx**
- Once you have completed your work, save the file and upload it for marking.
- Before leaving the exam, **ensure you have uploaded the correct file** capturing all the work you have submitted for marking.
- Ensure you compile a **detailed report write-up** that outlines your approach to addressing the various exam challenges. Ensure that your write up is authentic. Show screenshots of the working for all answers showing how you got your answers.
- The screen shots should capture your full screen and display the command you ran to get the answer. Include a taskbar showing your machine taskbar and time stamp as shown below.



The screenshot shows a Windows desktop with a window titled "GATEWAY" containing a Cisco IOS Command Line Interface. The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The CLI text includes legal disclaimers, hardware specifications (Cisco ISR4331/K9), and a series of configuration commands: enabling the router, entering configuration mode, setting the hostname to "Gateway", configuring interface GigabitEthernet0/0/1 with IP address 10.0.0.37, and configuring interface GigabitEthernet0/0/2 with IP address 0.0.0.0. The output shows the interface state changes and the final configuration summary.

```
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco ISR4331/K9 (1NU) processor with 1795999K/6147K bytes of memory.
Processor board ID FIM23201000
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223561K bytes of flash memory at bootflash:.

Press RETURN to get started!

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Gateway
Gateway(config)#interface Gig0/0/1
Gateway(config-if)#ip address 10.0.0.37 255.255.255.252
Gateway(config-if)#no shutdown

Gateway(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

Gateway(config-if)#exit
Gateway(config)#ip route 0.0.0.0 0.0.0.0 Gig0/0/2
%Default route without gateway, if not a point-to-point interface, may impact performance
Gateway(config)#exit
Gateway#
%SYS-5-CONFIG_I: Configured from console by console
|
```

- **NOTE: You MUST take FULL SCREEN screenshots for each step(must show the taskbar and time stamp) of how you got your answers and submit the document as a PDF file. If you answer the question without providing the screenshots you WILL NOT be awarded any marks.**

TOTAL: 60mks

Task:

There's a memo that your company received indicating that someone might be trying to hack into it. the network. Your job is to put security measures in place to stop. unapproved entry into the network.

Scenario:

At **Acacia Pharmacy Corporation** you are employed as a network engineer. There are numerous devices on your company's network such as switches, routers and hosts. Six subnets are part of the network architecture.

HQ is connected to the internet via the **HQ ROUTER**.

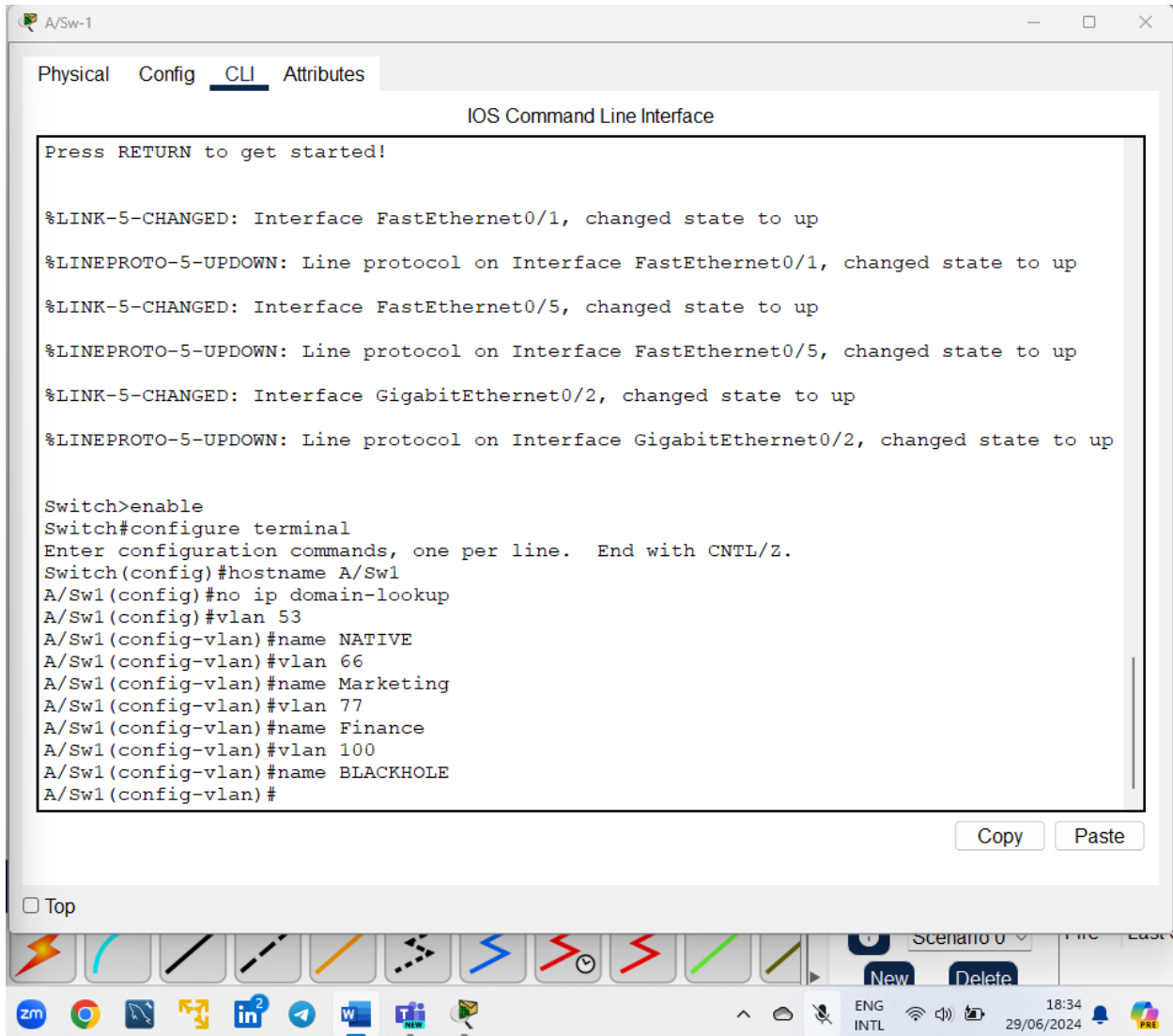
You must set up the region in a way that the connection is on a need basis as guided below.

NETWORK SETUP IN HQ

- You will configure the **distribution-layer switch** (D/Sw) with DHCP pools for the two subnets under it: **192.168.1.0 /28, 192.168.1.16 /28**. You will as well configure the Gig0/1 interface on the distribution switch to link with the Gig0/0/1 interface of the **HQ-ROUTER** using the IP address space **192.168.1.32 /30**.
- **NOTE:** Avoid typing in quotes (" ") wherever you see one. Instead, ONLY key in the word available within the quotes.

Task 1: Configure the Access Layer Switch (A/Sw1) within HQ. (15mks)

- a) Rename the hostname to "A/Sw1"
- b) Disable ip domain lookup
- c) Create the following vlans:
 - Vlan 53 and name it "NATIVE"
 - Vlan 66 and name it "Marketing"
 - Vlan 77 and name it "Finance"
 - Vlan 100 and name it "BLACKHOLE"



The screenshot shows a Cisco IOS Command Line Interface (CLI) window for a switch named 'A/Sw-1'. The window has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The CLI displays several status messages indicating that interfaces FastEthernet0/1, FastEthernet0/5, and GigabitEthernet0/2 have changed state to up. Below these messages, the user enters the command 'enable' to enter privileged EXEC mode, followed by 'configure terminal' to enter global configuration mode. The user then configures the switch hostname to 'A/Sw1', disables IP domain lookup, and creates four VLANs: VLAN 53 (named 'NATIVE'), VLAN 66 (named 'Marketing'), VLAN 77 (named 'Finance'), and VLAN 100 (named 'BLACKHOLE'). The CLI prompt returns to 'A/Sw1(config-vlan)#' after the last command.

```

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname A/Sw1
A/Sw1(config)#no ip domain-lookup
A/Sw1(config)#vlan 53
A/Sw1(config-vlan)#name NATIVE
A/Sw1(config-vlan)#vlan 66
A/Sw1(config-vlan)#name Marketing
A/Sw1(config-vlan)#vlan 77
A/Sw1(config-vlan)#name Finance
A/Sw1(config-vlan)#vlan 100
A/Sw1(config-vlan)#name BLACKHOLE
A/Sw1(config-vlan)#
  
```

d) Configure the following port interfaces accordingly:

- Fa0/1 to have access to vlan 66
- Enable bpdu guard on Fa0/1
- Fa0/5 to have access to vlan 77
- Enable bpdu guard on Fa0/1
- Gig0/2 should be a trunk port and strictly allow traffic from vlans 66, 77, and 53.
- While configuring Gig0/2 as trunk, designate vlan 53 as the native vlan.
- All unused ports to be assigned to vlan 100 and put in a shutdown state.

A/Sw-1

Physical Config CLI Attributes

IOS Command Line Interface

```
A/Sw1(config-vlan)#exit
A/Sw1(config)#interface Fa0/1
A/Sw1(config-if)#switchport mode access
^
% Invalid input detected at '^' marker.

A/Sw1(config-if)#switchport mode access
A/Sw1(config-if)#switchport access vlan 66
A/Sw1(config-if)#spanning-tree bpduguard enable
A/Sw1(config-if)#exit
A/Sw1(config)#interface Fa0/5
A/Sw1(config-if)#switchport mode access
A/Sw1(config-if)#switchport access vlan 77
A/Sw1(config-if)#spanning-tree bpduguard enable
A/Sw1(config-if)#exit
A/Sw1(config)#interface Gig0/2
A/Sw1(config-if)#switchport mode trunk

A/Sw1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

A/Sw1(config-if)#switchport trunk allowed vlan 53,66,77
A/Sw1(config-if)#switchport trunk native vlan 53
A/Sw1(config-if)%%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on GigabitEthernet0/2 VLAN53.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet0/2 on VLAN0053. Inconsistent local vlan.

exit
A/Sw1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (53), with Switch GigabitEthernet0/2 (1).

A/Sw1(config)#interface range Fa0/2-4, Fa0/6-24, Gig0/
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (53), with Switch GigabitEthernet0/2 (1).
1
A/Sw1(config-if-range)#switchport mode access
A/Sw1(config-if-range)#switchport access vlan 100
A/Sw1(config-if-range)#shutdown
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (53), with Switch GigabitEthernet0/2 (1).
n

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
```


A/Sw-1

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
A/Sw1(config-if-range)#exit
A/Sw1(config)#
```

21°C
Partly cloudy

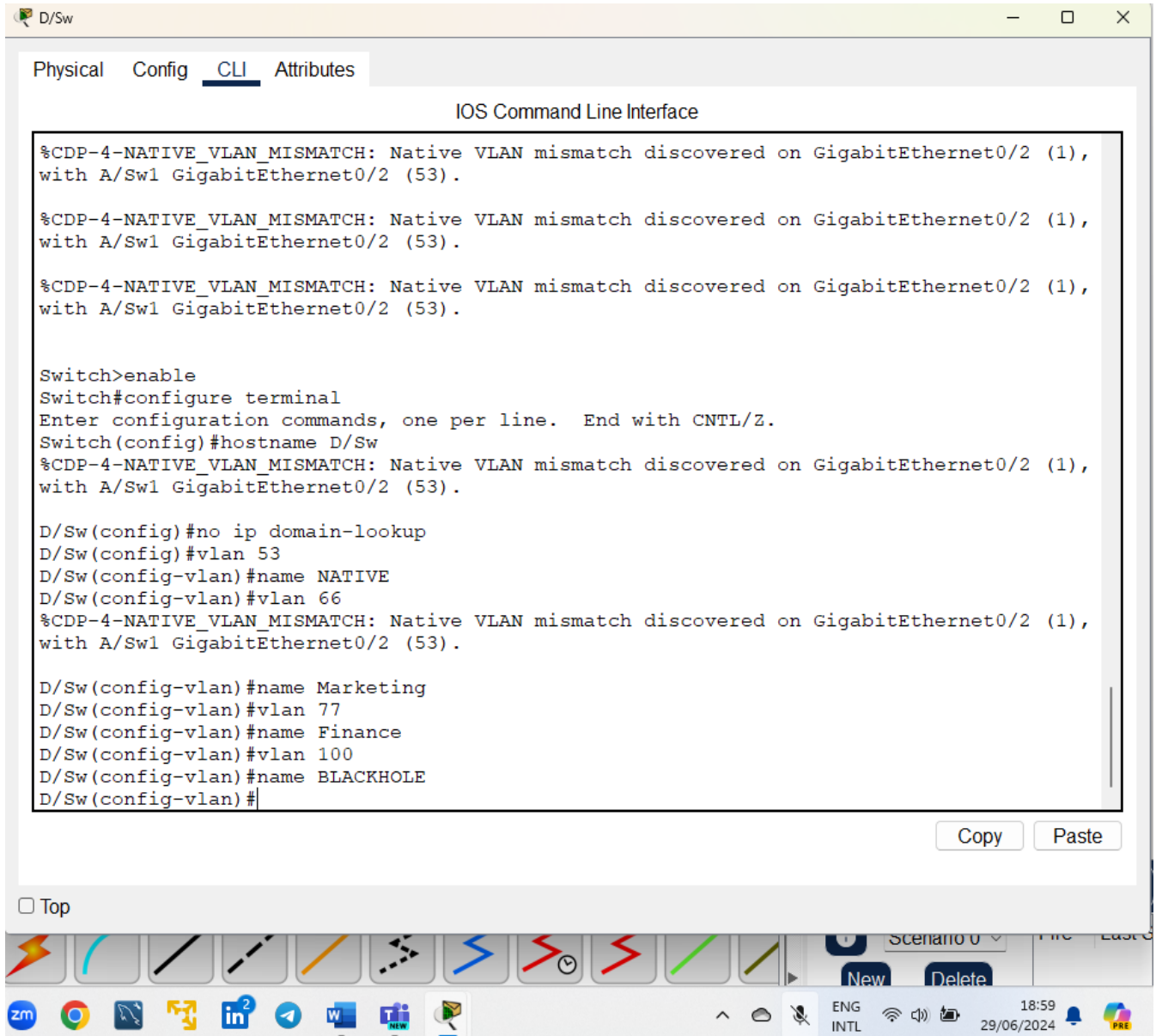


Task 2: Configure the Distribution Layer Switch (D/Sw) within HQ.(20mks)

- Rename the hostname to "D/Sw"
- Disable ip domain lookup

c) Create the following vlans:

- Vlan 53 and name it "NATIVE"
- Vlan 66 and name it "Marketing"
- Vlan 77 and name it "Finance"
- Vlan 100 and name it "BLACKHOLE"



```
D/Sw
Physical Config CLI Attributes
IOS Command Line Interface

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1),
with A/Sw1 GigabitEthernet0/2 (53).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1),
with A/Sw1 GigabitEthernet0/2 (53).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1),
with A/Sw1 GigabitEthernet0/2 (53).

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname D/Sw
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1),
with A/Sw1 GigabitEthernet0/2 (53).

D/Sw(config)#no ip domain-lookup
D/Sw(config)#vlan 53
D/Sw(config-vlan)#name NATIVE
D/Sw(config-vlan)#vlan 66
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (1),
with A/Sw1 GigabitEthernet0/2 (53).

D/Sw(config-vlan)#name Marketing
D/Sw(config-vlan)#vlan 77
D/Sw(config-vlan)#name Finance
D/Sw(config-vlan)#vlan 100
D/Sw(config-vlan)#name BLACKHOLE
D/Sw(config-vlan)#
```

Copy Paste

Top

Scenario 0

New Delete

ENG INTL

18:59 29/06/2024

interface Gig0/1

```
ip address 192.168.1.33 255.255.255.252
```

```
exit
```

```
interface Gig0/2
```

```
switchport mode trunk
```

```
switchport trunk allowed vlan 53,66,77
```

```
switchport trunk native vlan 53
```

```
exit
```

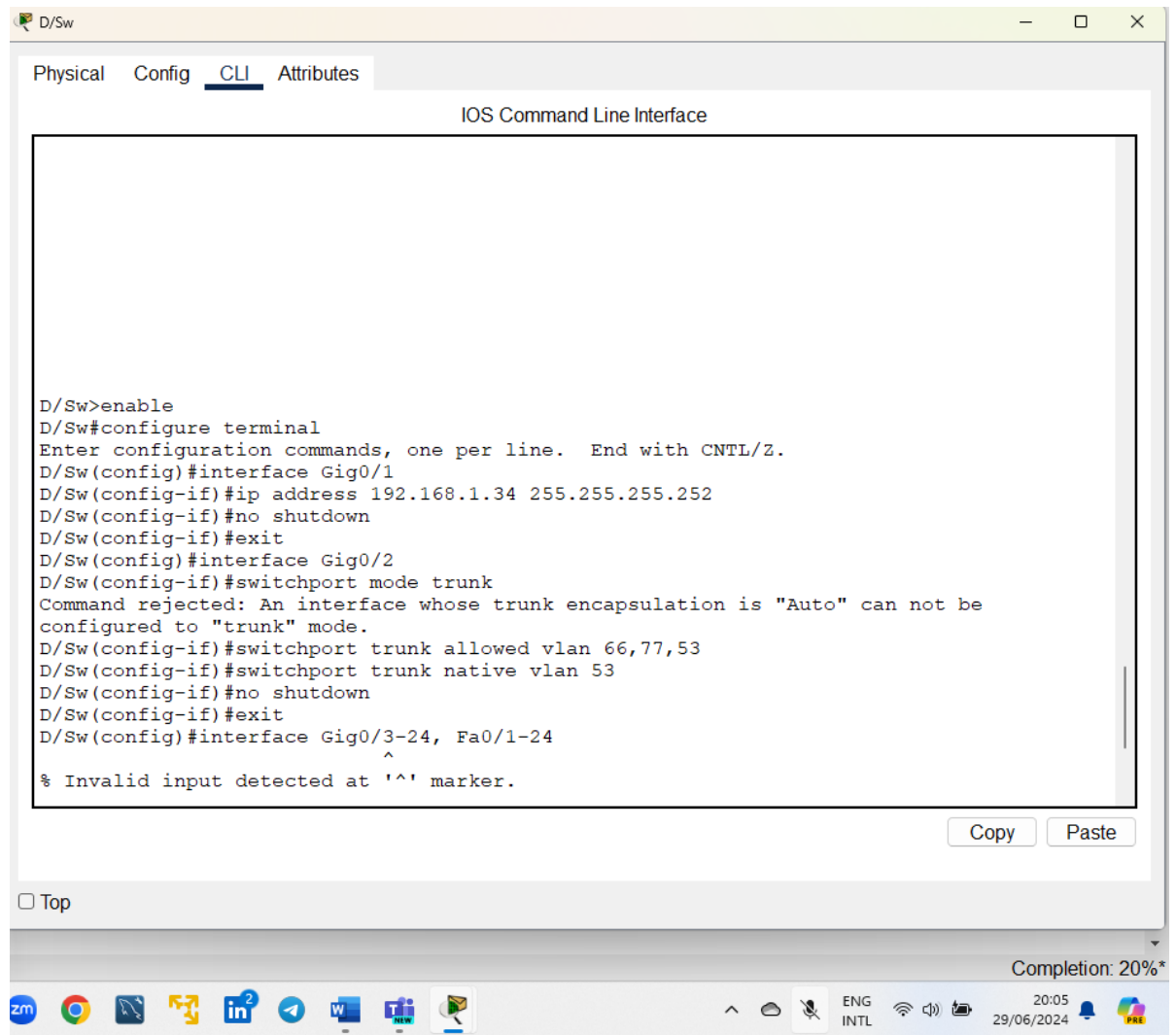
```
interface range Gig0/3-24, Fa0/1-24
```

```
switchport mode access
```

```
switchport access vlan 100
```

```
shutdown
```

```
exit
```

```
D/Sw>enable
D/Sw#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
D/Sw(config)#interface Gig0/1
D/Sw(config-if)#ip address 192.168.1.34 255.255.255.252
D/Sw(config-if)#no shutdown
D/Sw(config-if)#exit
D/Sw(config)#interface Gig0/2
D/Sw(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be
configured to "trunk" mode.
D/Sw(config-if)#switchport trunk allowed vlan 66,77,53
D/Sw(config-if)#switchport trunk native vlan 53
D/Sw(config-if)#no shutdown
D/Sw(config-if)#exit
D/Sw(config)#interface Gig0/3-24, Fa0/1-24
      ^
% Invalid input detected at '^' marker.
```

Completion: 20%*

h) Navigate to the desktop of both PC-1 and PC-2. Toggle the IP configuration mode from static to DHCP. Both PCs should now be automatically assigned with IP addresses.

PC-1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 169.254.42.46

Subnet Mask 255.255.0.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::207:ECFF:FE4C:2A2E

Default Gateway

DNS Server

802.1X


☐ Use 802.1X Security

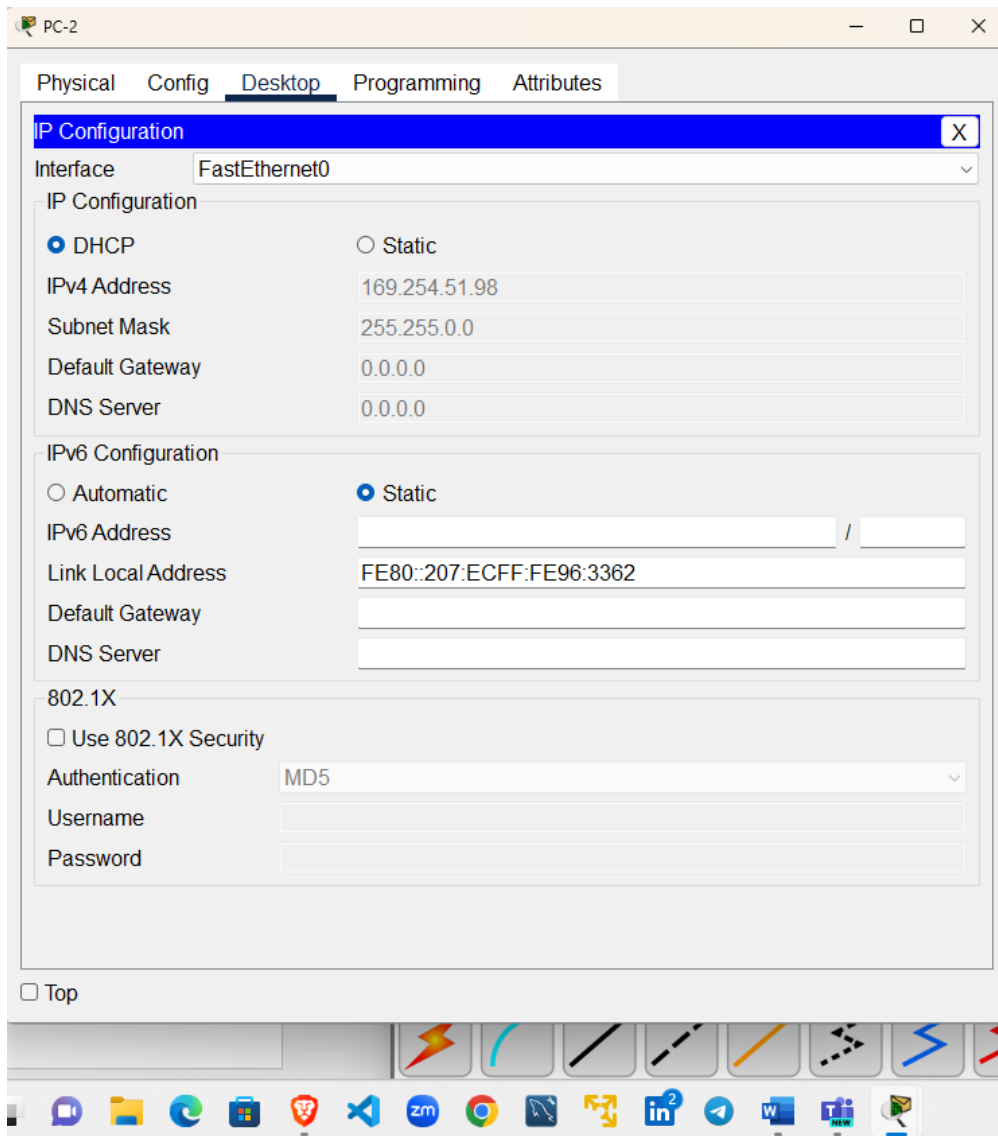
Authentication MD5

Username

Password

☐ Top



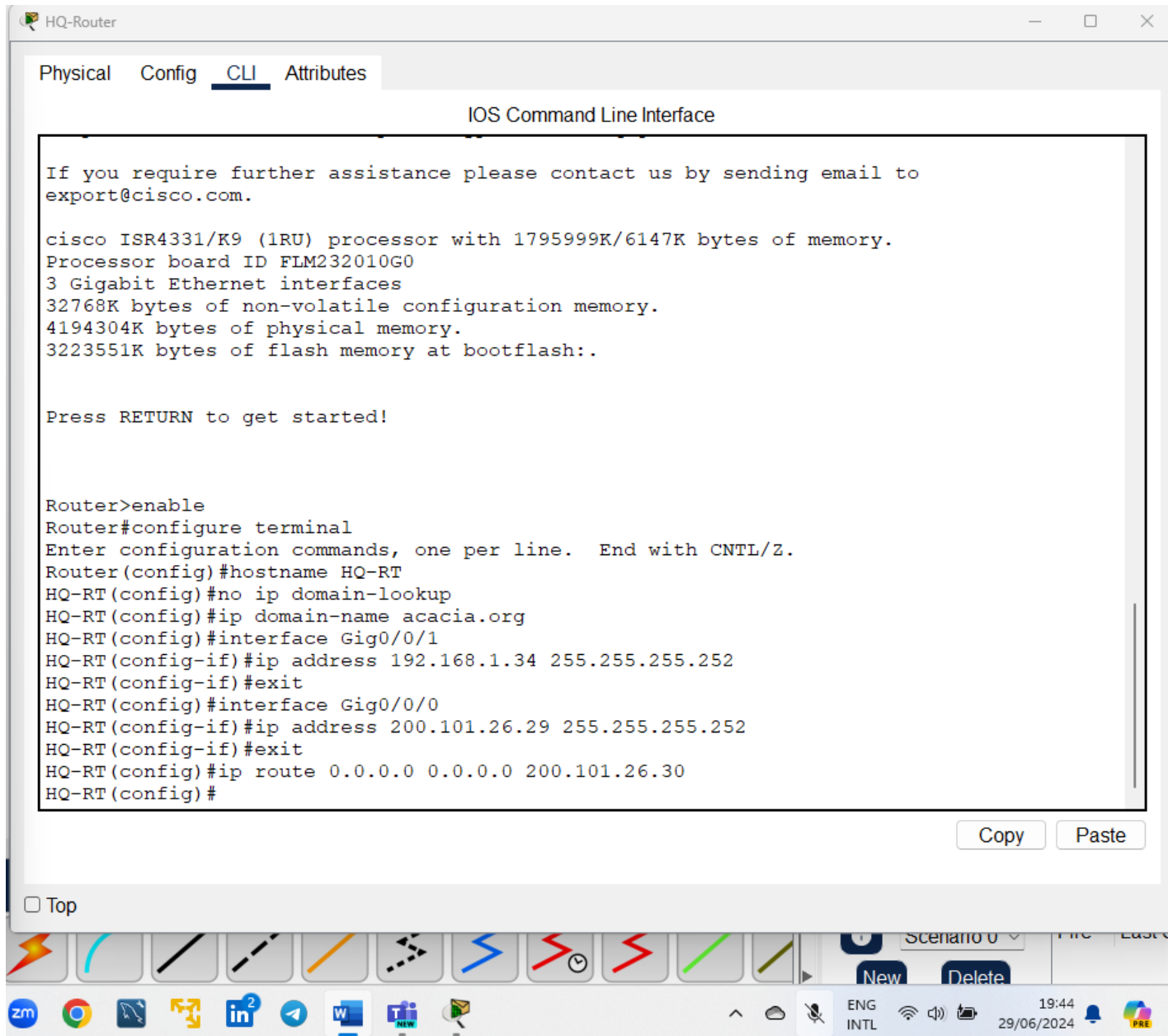


Task 3: Configure the HQ-ROUTER. (15mks)

- Rename the hostname to "HQ-RT"
- Disable ip domain lookup
- Set up the domain name "acacia.org" on the router.
- Configure the following port interfaces accordingly:

- Gig0/0/1 to be assigned the first usable IP address in the subnet 192.168.1.32 /30.
- Gig0/0/0 to be assigned the first usable IP address in the subnet 200.101.26.28 /30.

e) Set the default gateway on this router to be 200.101.26.30



The screenshot shows the HQ-Router configuration window with the CLI tab selected. The interface displays the following text:

```
If you require further assistance please contact us by sending email to
export@cisco.com.

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HQ-RT
HQ-RT(config)#no ip domain-lookup
HQ-RT(config)#ip domain-name acacia.org
HQ-RT(config)#interface Gig0/0/1
HQ-RT(config-if)#ip address 192.168.1.34 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#interface Gig0/0/0
HQ-RT(config-if)#ip address 200.101.26.29 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#ip route 0.0.0.0 0.0.0.0 200.101.26.30
HQ-RT(config)#
```

At the bottom of the window, there are buttons for "Copy" and "Paste". Below the configuration window, there is a "Top" button and a taskbar with various application icons. The system tray at the bottom right shows the date and time as 19:44 on 29/06/2024, along with network and system icons.

Task 4: Setup ABC-ROUTER device security. (10mks)

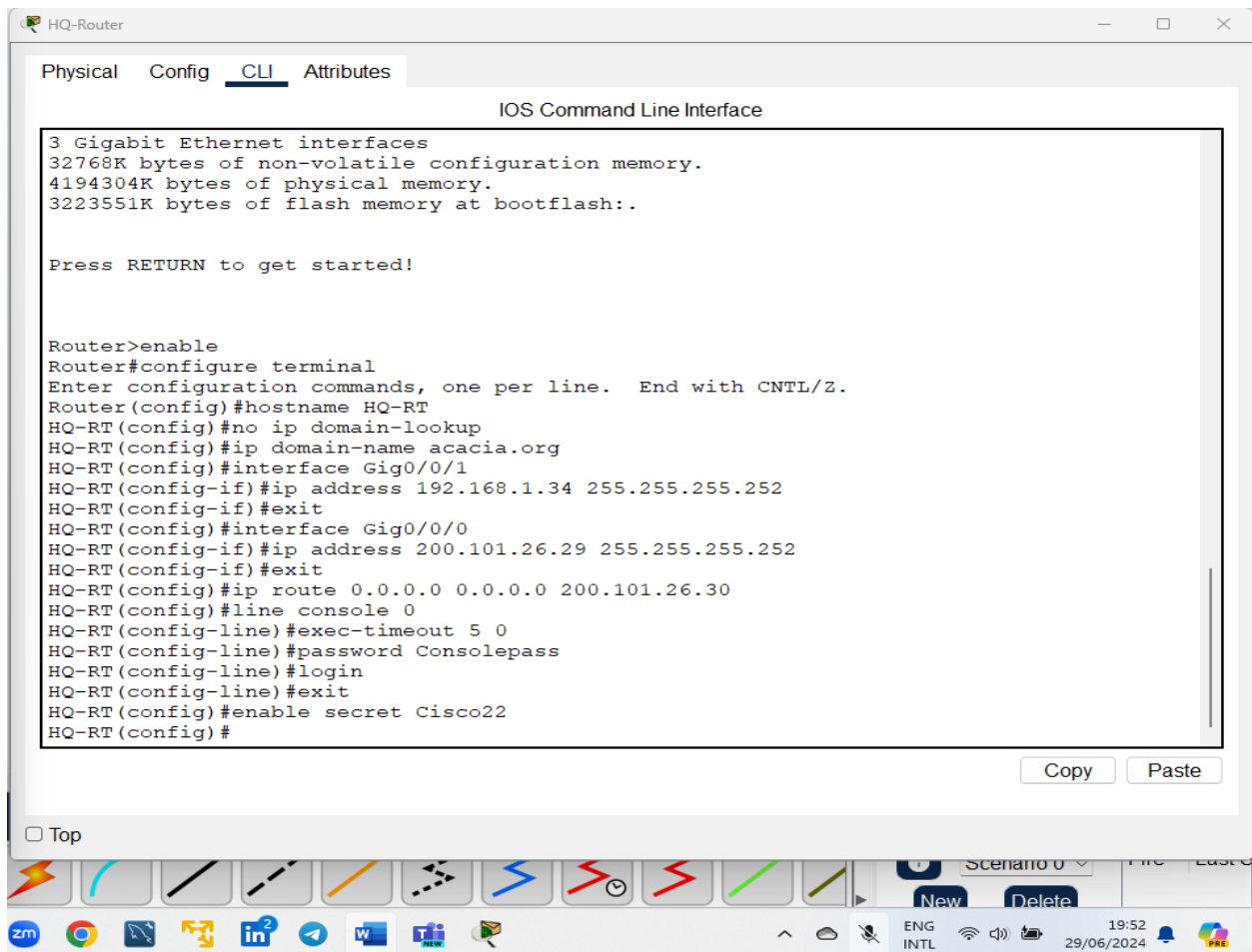
- In this task you will setup device security in the HQ-ROUTER such that a user will be authenticated when accessing the router's CLI.

a) To authenticate at the console level, configure the primary terminal line with the following

parameters:

- Exec-timeout = 5 minutes
- Password = "Consolepass"
- Require "login"

b) Assign the privileged level **secret** as "Cisco22" with the exec level as "15".



```

HQ-Router
Physical Config CLI Attributes
IOS Command Line Interface

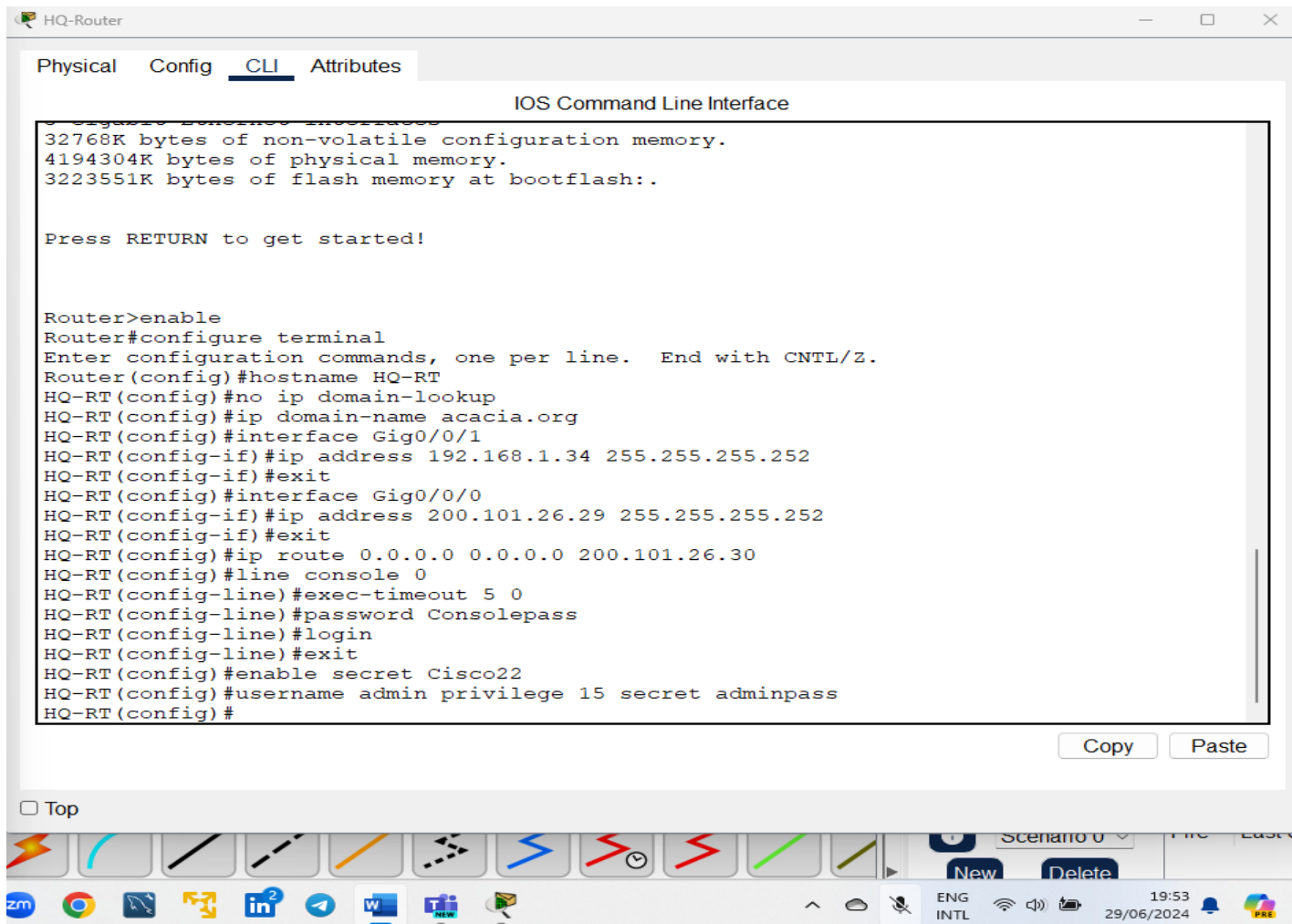
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname HQ-RT
HQ-RT(config)#no ip domain-lookup
HQ-RT(config)#ip domain-name acacia.org
HQ-RT(config)#interface Gig0/0/1
HQ-RT(config-if)#ip address 192.168.1.34 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#interface Gig0/0/0
HQ-RT(config-if)#ip address 200.101.26.29 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#ip route 0.0.0.0 0.0.0.0 200.101.26.30
HQ-RT(config)#line console 0
HQ-RT(config-line)#exec-timeout 5 0
HQ-RT(config-line)#password Consolepass
HQ-RT(config-line)#login
HQ-RT(config-line)#exit
HQ-RT(config)#enable secret Cisco22
HQ-RT(config)#
```

c) Establish User Name authentication with the following parameters:

- Username = "admin"
- Set user privilege level as "15"
- Specify the secret for the user as "adminpass"

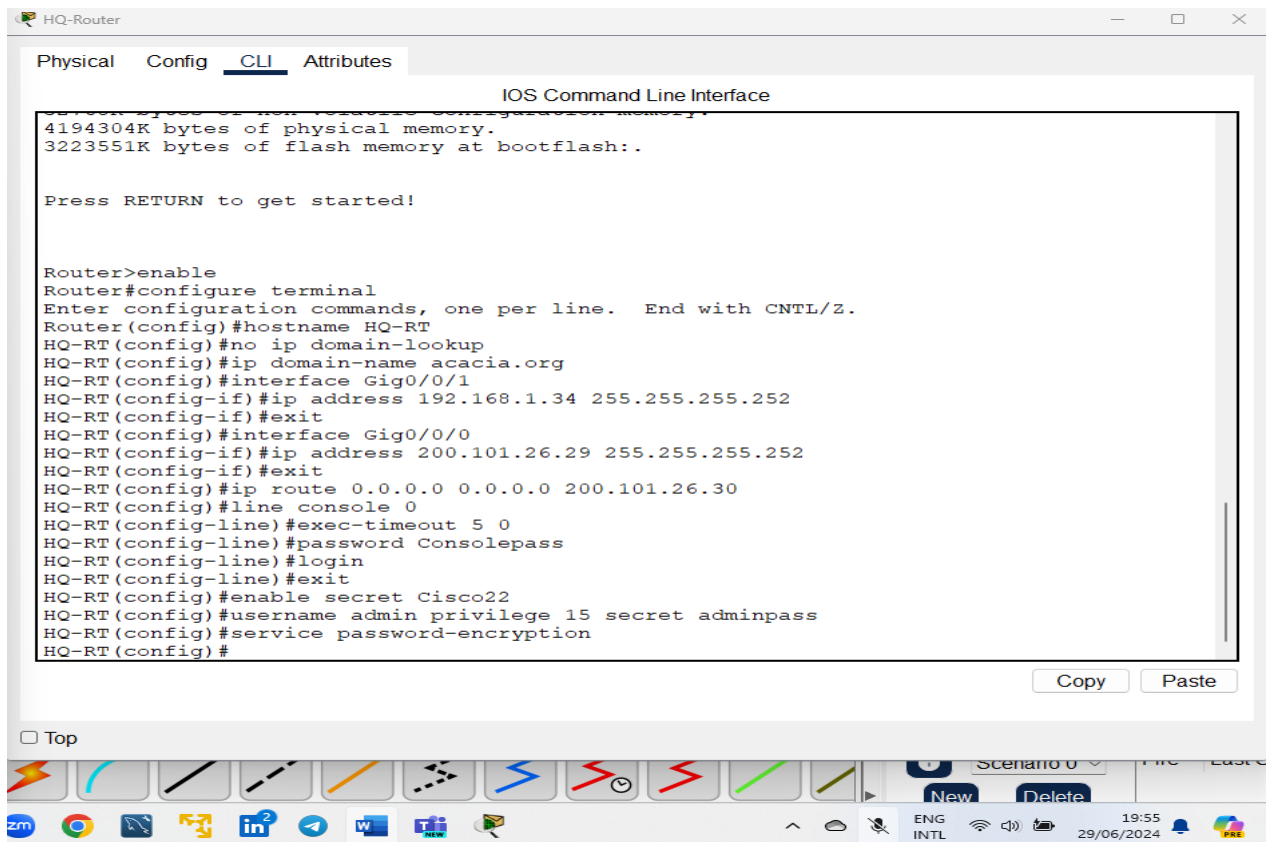


The screenshot shows the HQ-Router CLI interface with the following configuration commands entered:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname HQ-RT
HQ-RT(config)#no ip domain-lookup
HQ-RT(config)#ip domain-name acacia.org
HQ-RT(config)#interface Gig0/0/1
HQ-RT(config-if)#ip address 192.168.1.34 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#interface Gig0/0/0
HQ-RT(config-if)#ip address 200.101.26.29 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#ip route 0.0.0.0 0.0.0.0 200.101.26.30
HQ-RT(config)#line console 0
HQ-RT(config-line)#exec-timeout 5 0
HQ-RT(config-line)#password Consolepass
HQ-RT(config-line)#login
HQ-RT(config-line)#exit
HQ-RT(config)#enable secret Cisco22
HQ-RT(config)#username admin privilege 15 secret adminpass
HQ-RT(config)#
```

The interface also shows memory statistics at the top: 32768K bytes of non-volatile configuration memory, 4194304K bytes of physical memory, and 3223551K bytes of flash memory at bootflash:.

d) Encrypt all plain text system passwords (*hint* : service).



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname HQ-RT
HQ-RT(config)#no ip domain-lookup
HQ-RT(config)#ip domain-name acacia.org
HQ-RT(config)#interface Gig0/0/1
HQ-RT(config-if)#ip address 192.168.1.34 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#interface Gig0/0/0
HQ-RT(config-if)#ip address 200.101.26.29 255.255.255.252
HQ-RT(config-if)#exit
HQ-RT(config)#ip route 0.0.0.0 0.0.0.0 200.101.26.30
HQ-RT(config)#line console 0
HQ-RT(config-line)#exec-timeout 5 0
HQ-RT(config-line)#password Consolepass
HQ-RT(config-line)#login
HQ-RT(config-line)#exit
HQ-RT(config)#enable secret Cisco22
HQ-RT(config)#username admin privilege 15 secret adminpass
HQ-RT(config)#service password-encryption
HQ-RT(config)#
```

<<THE END>>