

Date: 15/01/2024

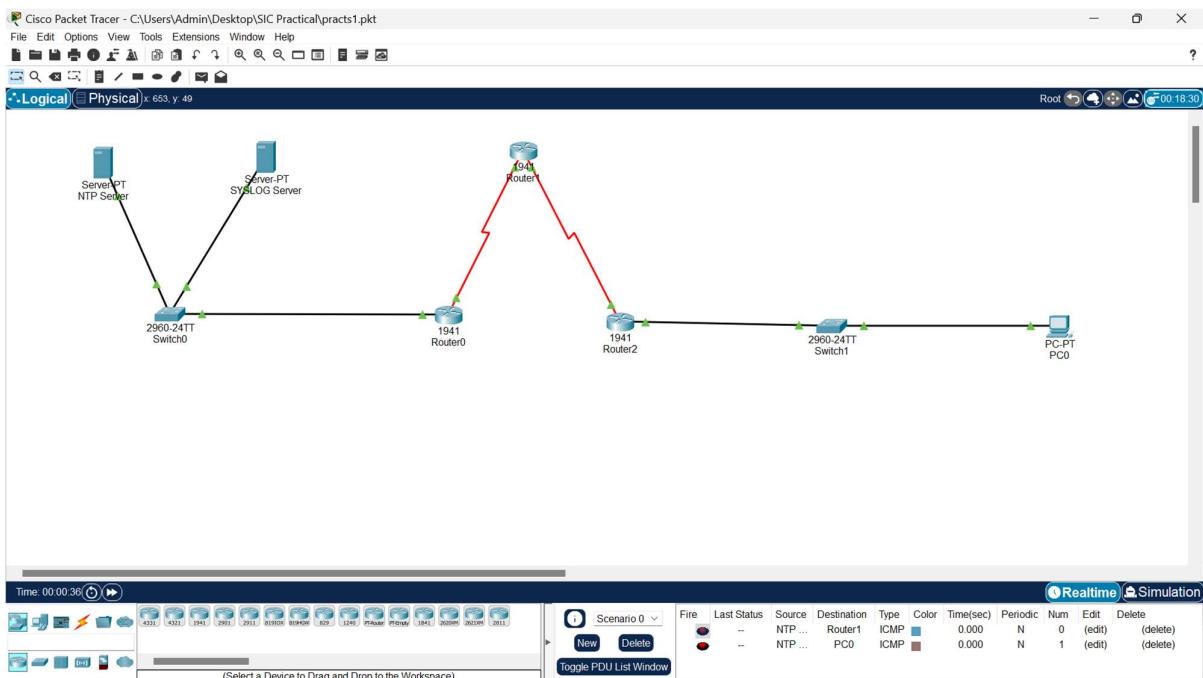
Security in Computing

Practical 1:

➤ Aim: Configure Routers

- a. OSPF MD5 authentication
- b. NTP
- c. to log messages to the SYSLOG server
- d. to support SSH connections.

➤ Topology Diagram

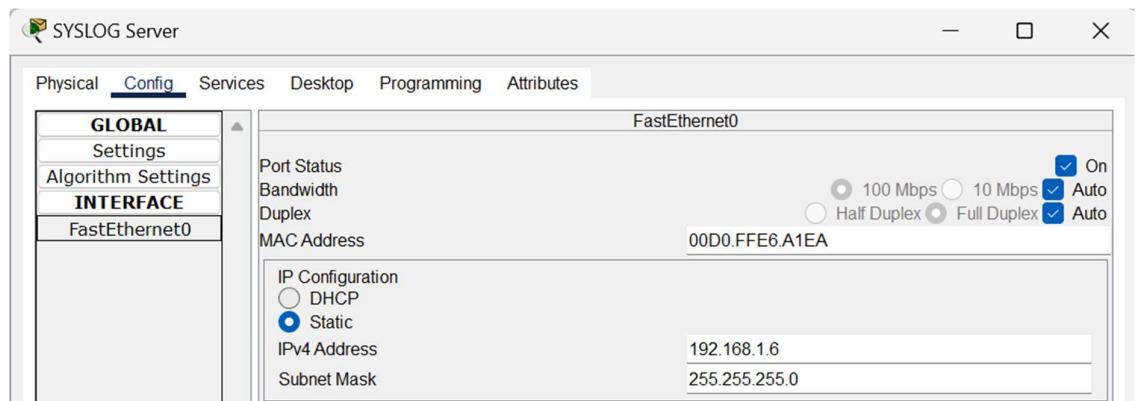


➤ Assigning IP Addresses

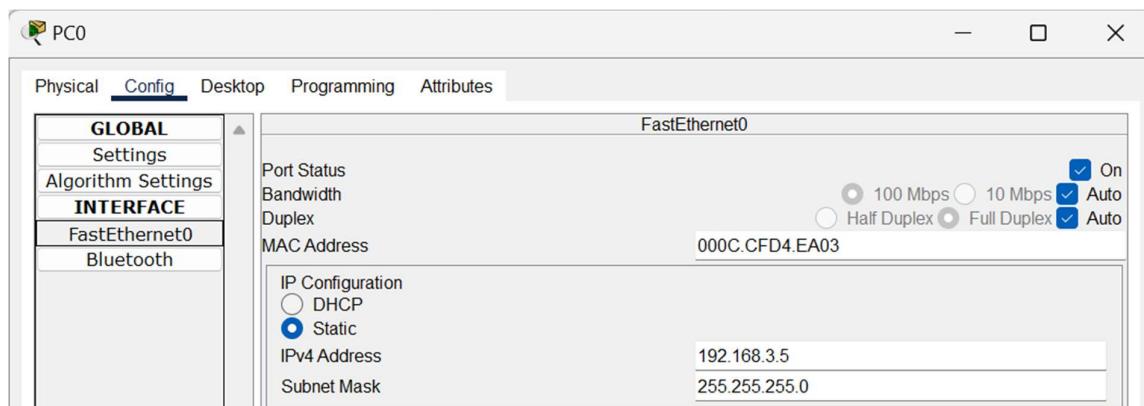
1. NTP Server



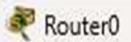
2. SYSLOG Server



3. PC-0



4. Router 0



Router0

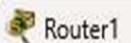
Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R0
R0(config)#interface GigabitEthernet0/0
R0(config-if)#ip address 192.168.1.1 255.255.255.0
R0(config-if)#no shut
R0(config-if)#interface Serial0/0/0
R0(config-if)#ip address 10.1.1.1 255.255.255.252
R0(config-if)#no shut
R0(config-if)#^Z
R0#
%SYS-5-CONFIG_I: Configured from console by console

R0#exit
```

5. Router 1



Router1

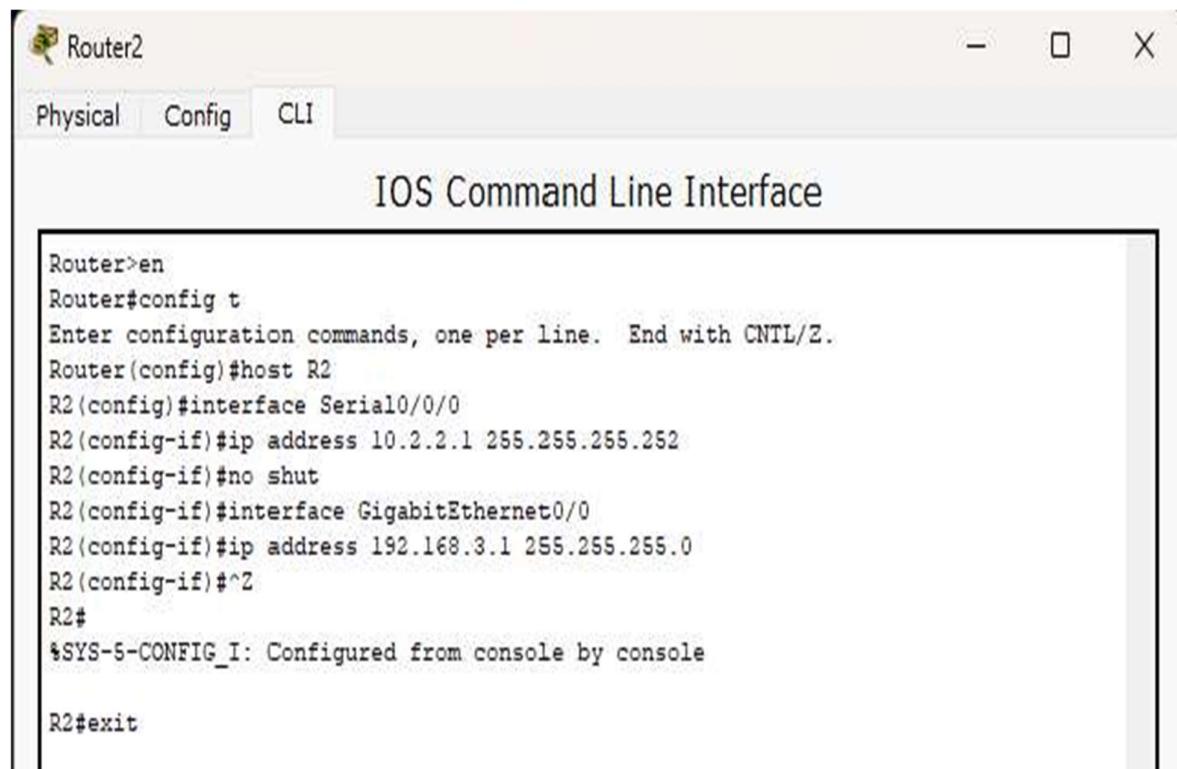
Physical Config CLI

IOS Command Line Interface

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R1
R1(config)#interface Serial0/0/0
R1(config-if)#ip address 10.1.1.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#interface Serial0/0/1
R1(config-if)#ip address 10.2.2.2 255.255.255.252
R1(config-if)#no shut
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

6. Router 2



The image shows a software application window titled "Router2". The window has three tabs at the top: "Physical", "Config", and "CLI". The "CLI" tab is selected and active. Below the tabs, the title "IOS Command Line Interface" is displayed. The main area of the window contains the following IOS configuration command output:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host R2
R2(config)#interface Serial0/0/0
R2(config-if)#ip address 10.2.2.1 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface GigabitEthernet0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#+Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

➤ Displaying IP Address Details of Routers

1. Router 0

```
R0>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0    192.168.1.1    YES manual up           up
GigabitEthernet0/1    unassigned     YES unset   administratively down down
Serial0/0/0          10.1.1.1      YES manual up           up
Serial0/0/1          unassigned     YES unset   administratively down down
Vlan1                unassigned     YES unset   administratively down down
--
```

2. Router 1

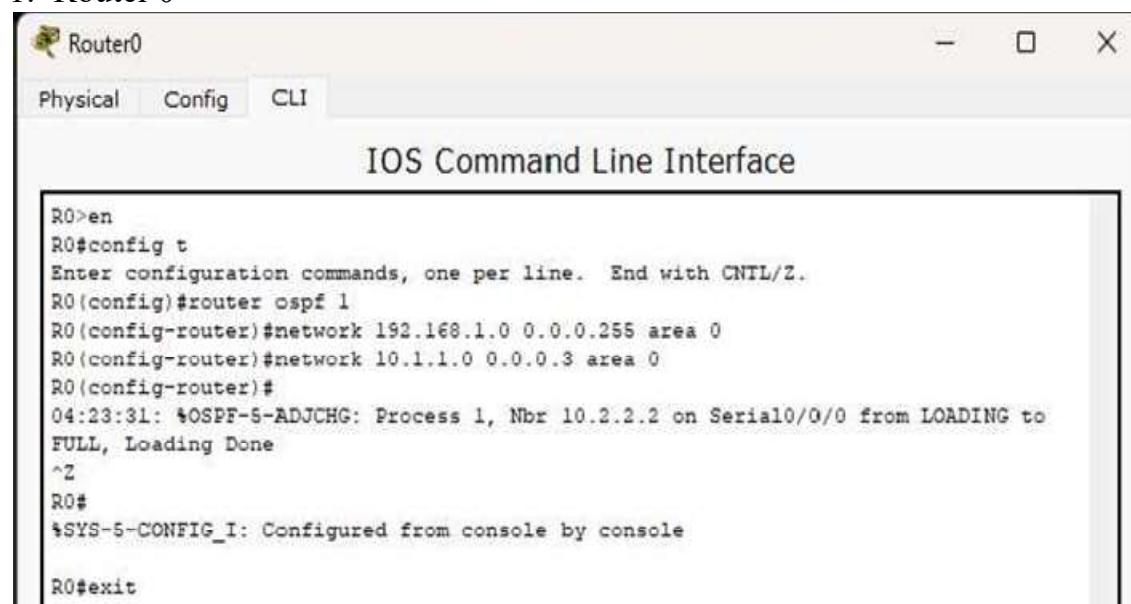
```
R1>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  unassigned      YES unset  administratively down down
GigabitEthernet0/1  unassigned      YES unset  administratively down down
Serial0/0/0         10.1.1.2       YES manual up           up
Serial0/0/1         10.2.2.2       YES manual up           up
Vlan1              unassigned      YES unset  administratively down down
```

3. Router 2

```
R2>show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.3.1    YES manual up           up
GigabitEthernet0/1  unassigned      YES unset  administratively down down
Serial0/0/0         10.2.2.1       YES manual up           up
Serial0/0/1         unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
```

➤ Configure OSPF on routes

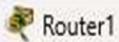
1. Router 0



The screenshot shows a Cisco IOS Command Line Interface window titled "Router0". The window has tabs for "Physical", "Config", and "CLI", with "CLI" currently selected. The main area displays the configuration commands for Router 0:

```
Router0#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router0(config)#router ospf 1
Router0(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router0(config-router)#network 10.1.1.0 0.0.0.3 area 0
Router0(config-router)#
04:23:31: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from LOADING to
FULL, Loading Done
^Z
Router0#
%SYS-5-CONFIG_I: Configured from console by console
Router0#exit
```

2. Router 1



Router1 - □ X

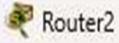
Physical Config CLI

IOS Command Line Interface

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#network 10.2.2.0 0.0.0.3 area 0
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

3. Router 2



Router2 - □ X

Physical Config CLI

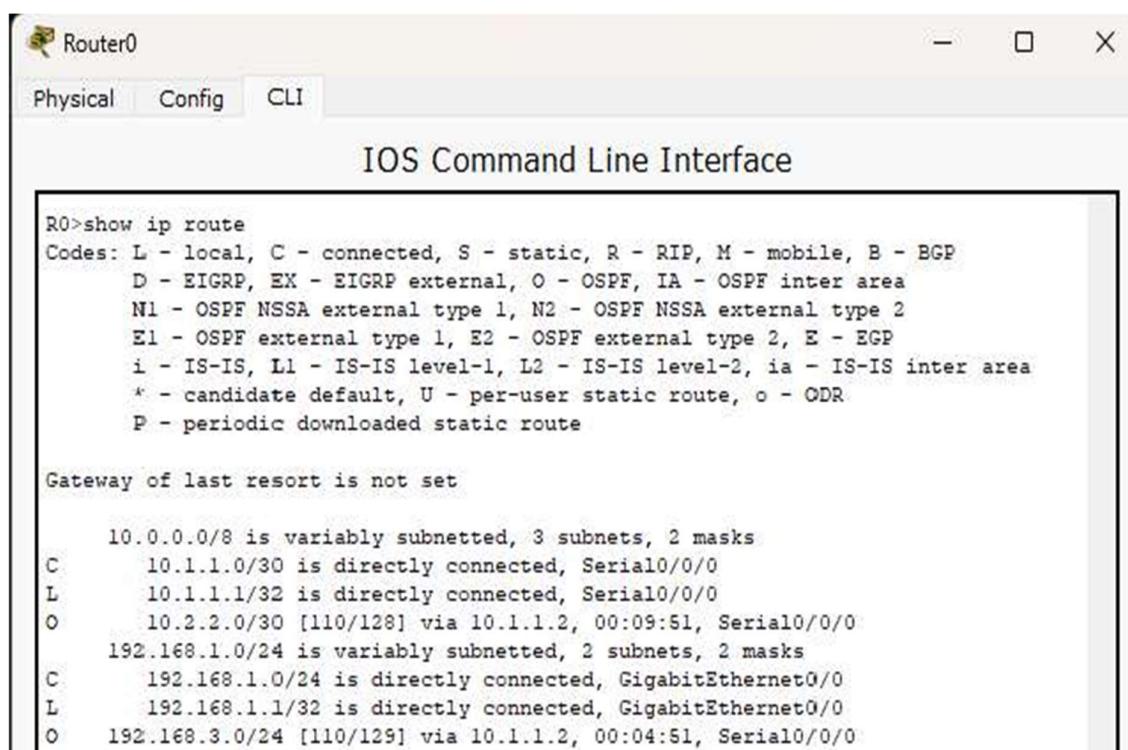
IOS Command Line Interface

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#network 192.168.3.0 0.0.0.255 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#exit
```

➤ **Displaying routing table of routers**

1. Router 0



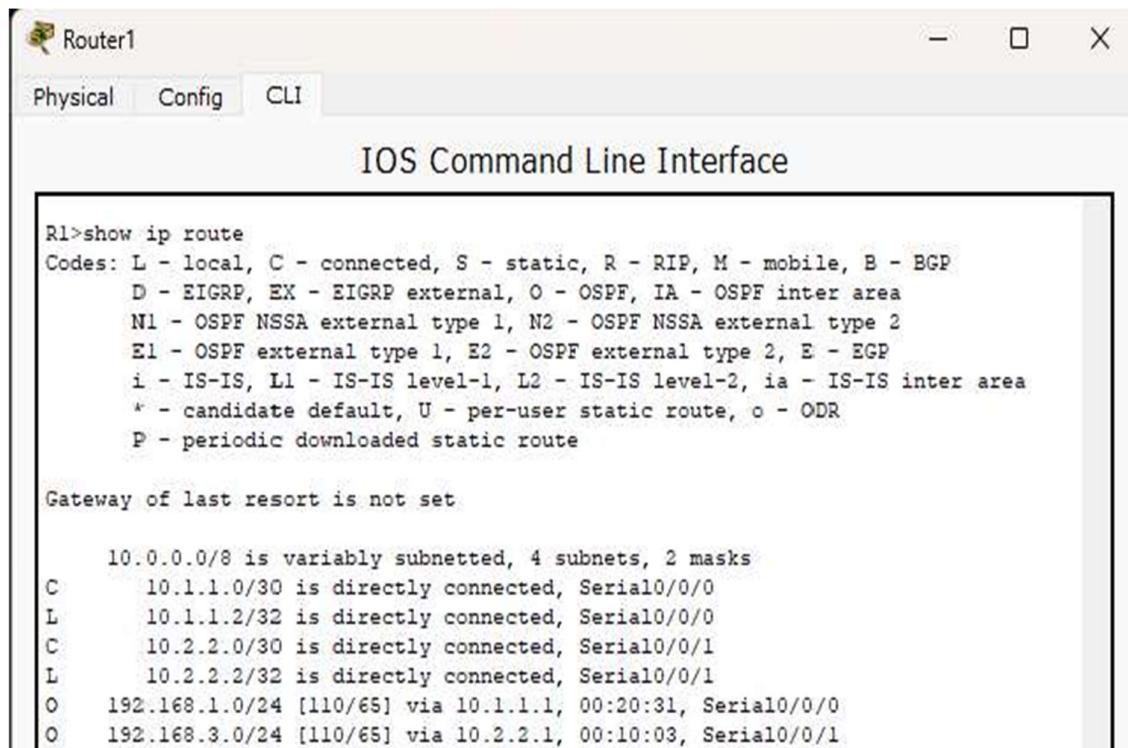
The screenshot shows a window titled "Router0" with three tabs: "Physical", "Config", and "CLI". The "CLI" tab is selected and displays the output of the "show ip route" command. The output includes route codes and descriptions for various network routes.

```
R0>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, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
O        10.2.2.0/30 [110/128] via 10.1.1.2, 00:09:51, Serial0/0/0
          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
O        192.168.3.0/24 [110/129] via 10.1.1.2, 00:04:51, Serial0/0/0
```

2. Router 1



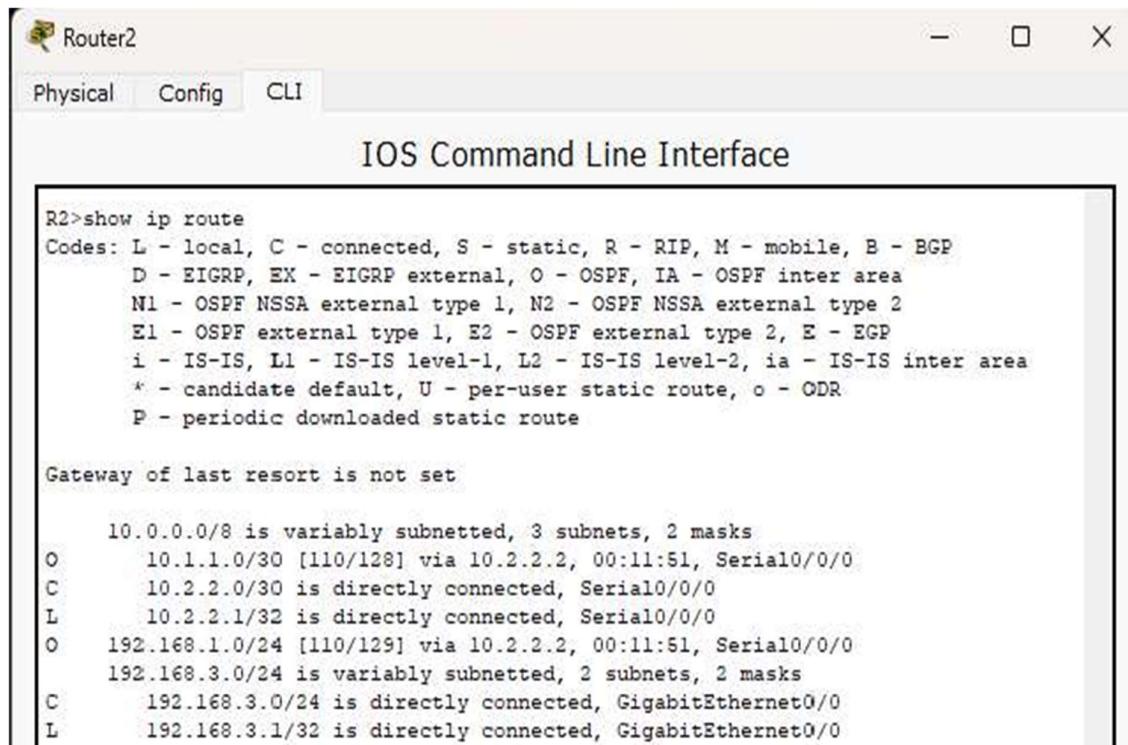
The screenshot shows a window titled "Router1" with three tabs: "Physical", "Config", and "CLI". The "CLI" tab is selected and displays the output of the "show ip route" command. The output includes route codes and descriptions for various network routes.

```
R1>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, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
O        192.168.1.0/24 [110/65] via 10.1.1.1, 00:20:31, Serial0/0/0
O        192.168.3.0/24 [110/65] via 10.2.2.1, 00:10:03, Serial0/0/1
```

3. Router 2



The image shows a software application window titled "Router2". At the top, there are three tabs: "Physical", "Config", and "CLI". The "CLI" tab is selected, and the main area displays the output of the "show ip route" command. The output includes route codes, gateway information, and a list of routes with their details.

```
R2>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, 3 subnets, 2 masks
O        10.1.1.0/30 [110/128] via 10.2.2.2, 00:11:51, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/0
L        10.2.2.1/32 is directly connected, Serial0/0/0
O        192.168.1.0/24 [110/129] via 10.2.2.2, 00:11:51, Serial0/0/0
          192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, GigabitEthernet0/0
L        192.168.3.1/32 is directly connected, GigabitEthernet0/0
```

A. OSPF MD5 authentication

➤ Configure OSPF MD5 authentication on Routers

1. Router 0

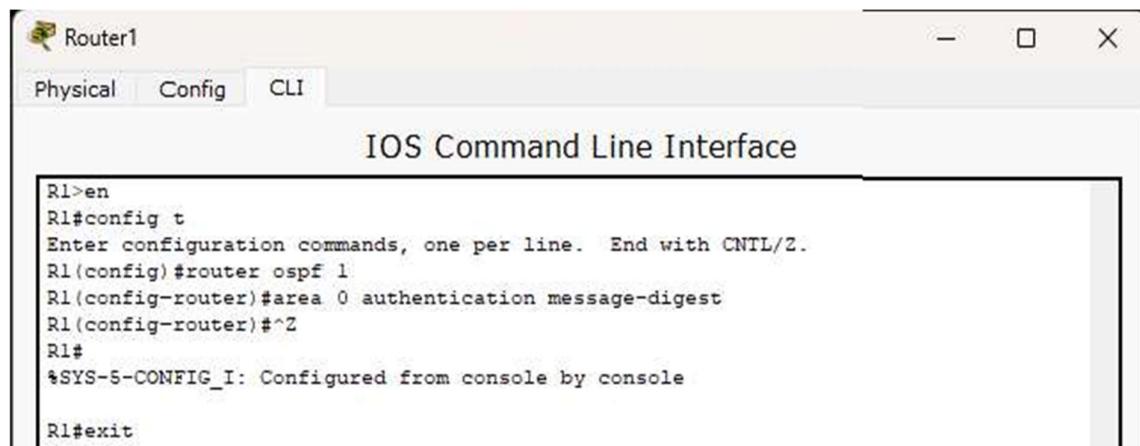


The image shows a computer window titled "Router0" with a tab bar at the top labeled "Physical", "Config", and "CLI". The "CLI" tab is active. Below the tab bar is the title "IOS Command Line Interface". The main area contains the following command-line session:

```
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#router ospf 1
R0(config-router)#area 0 authentication message-digest
R0(config-router)#+Z
R0#
%SYS-5-CONFIG_I: Configured from console by console

R0#exit
```

2. Router 1

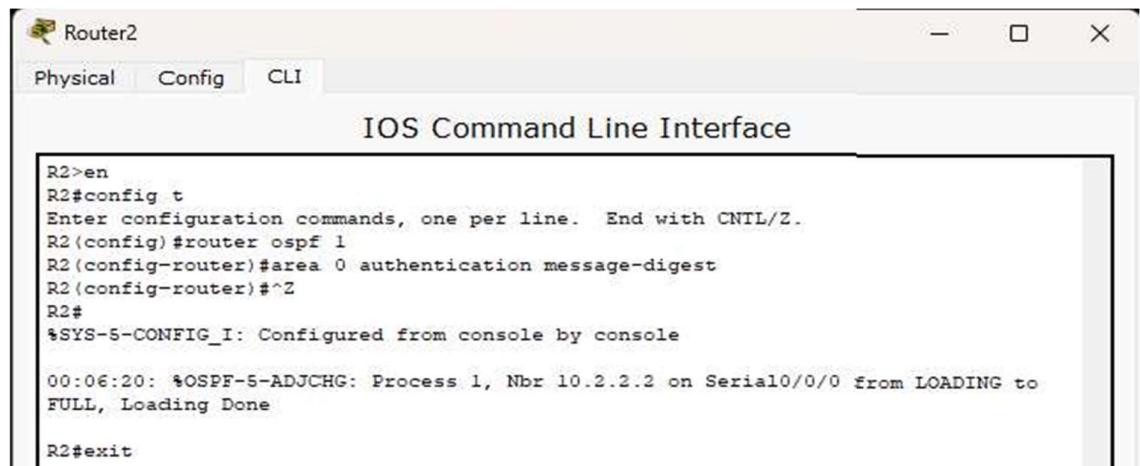


The image shows a computer window titled "Router1" with a tab bar at the top labeled "Physical", "Config", and "CLI". The "CLI" tab is active. Below the tab bar is the title "IOS Command Line Interface". The main area contains the following command-line session:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#area 0 authentication message-digest
R1(config-router)#+Z
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#exit
```

3. Router 2



The image shows a computer window titled "Router2" with a tab bar at the top labeled "Physical", "Config", and "CLI". The "CLI" tab is active. Below the tab bar is the title "IOS Command Line Interface". The main area contains the following command-line session:

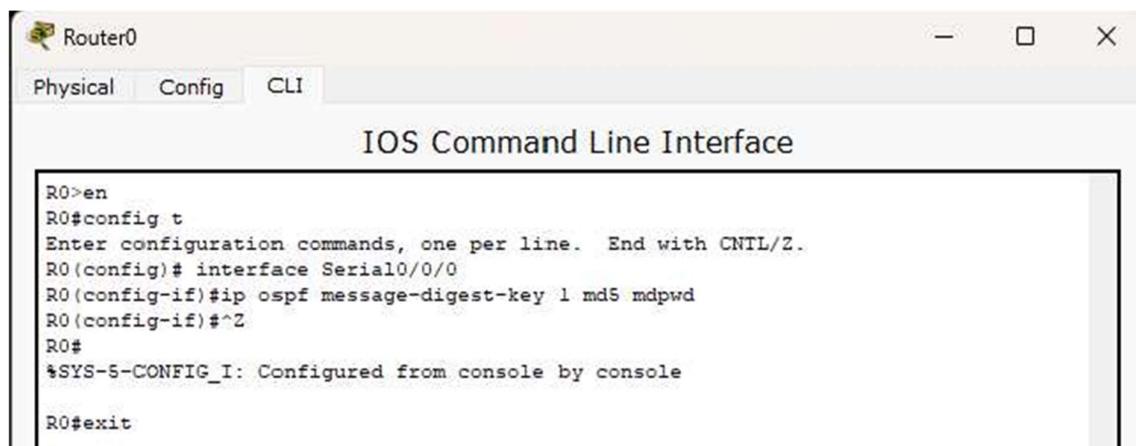
```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#area 0 authentication message-digest
R2(config-router)#+Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

00:06:20: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from LOADING to
FULL, Loading Done

R2#exit
```

➤ Configure the MD5 key for all the routers

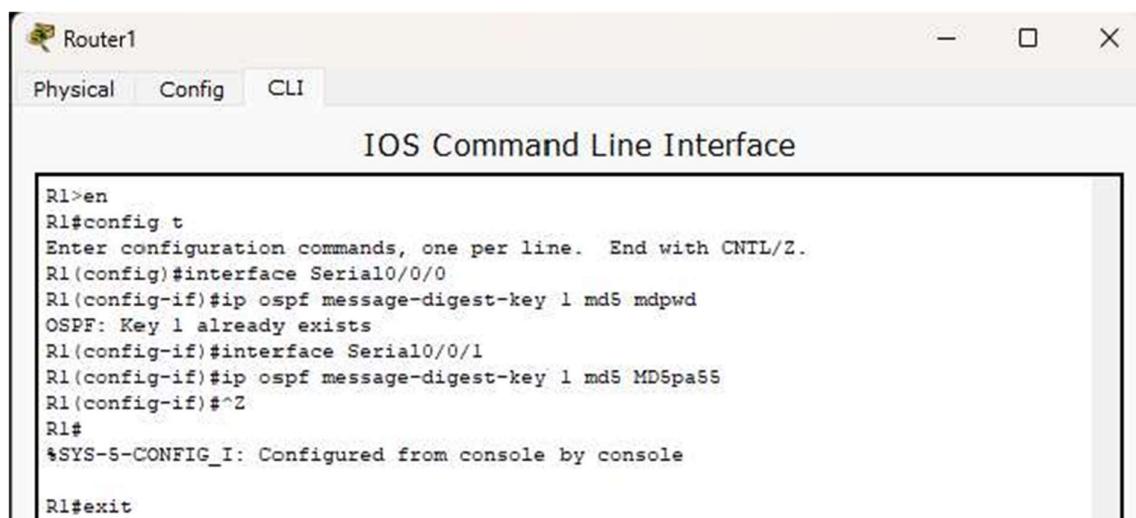
1. Router 0



The window title is "Router0". The tab bar shows "Physical", "Config" (which is selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)# interface Serial0/0/0
R0(config-if)#ip ospf message-digest-key 1 md5 mdpwd
R0(config-if)#^Z
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#exit
```

2. Router 1



The window title is "Router1". The tab bar shows "Physical", "Config" (selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Serial0/0/0
R1(config-if)#ip ospf message-digest-key 1 md5 mdpwd
OSPF: Key 1 already exists
R1(config-if)#interface Serial0/0/1
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R1(config-if)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

3. Router 2

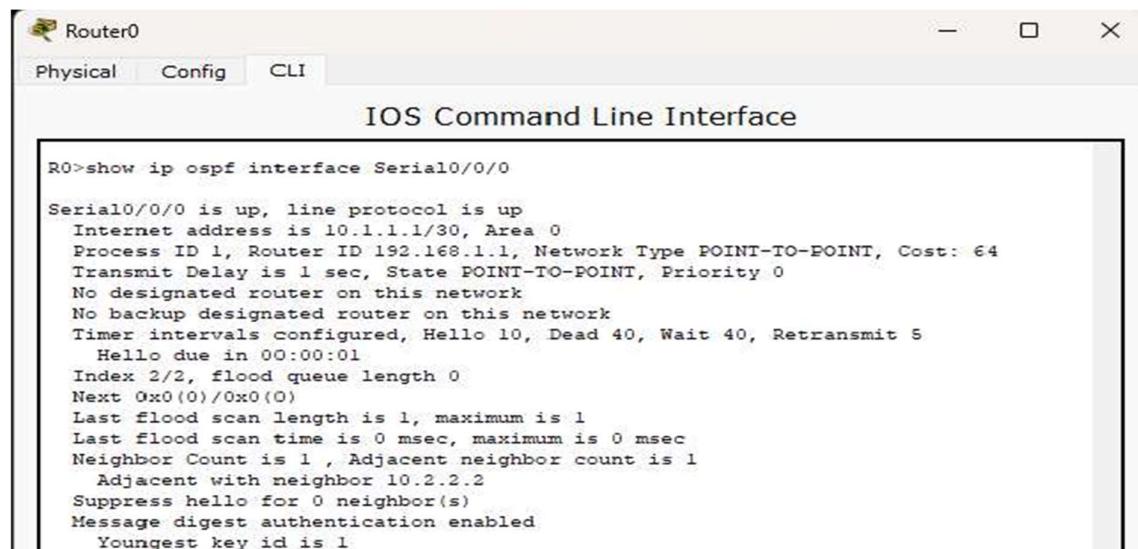


The window title is "Router2". The tab bar shows "Physical", "Config" (selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R2>en
R2# config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Serial0/0/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ **Displaying OSPF details of all the routers**

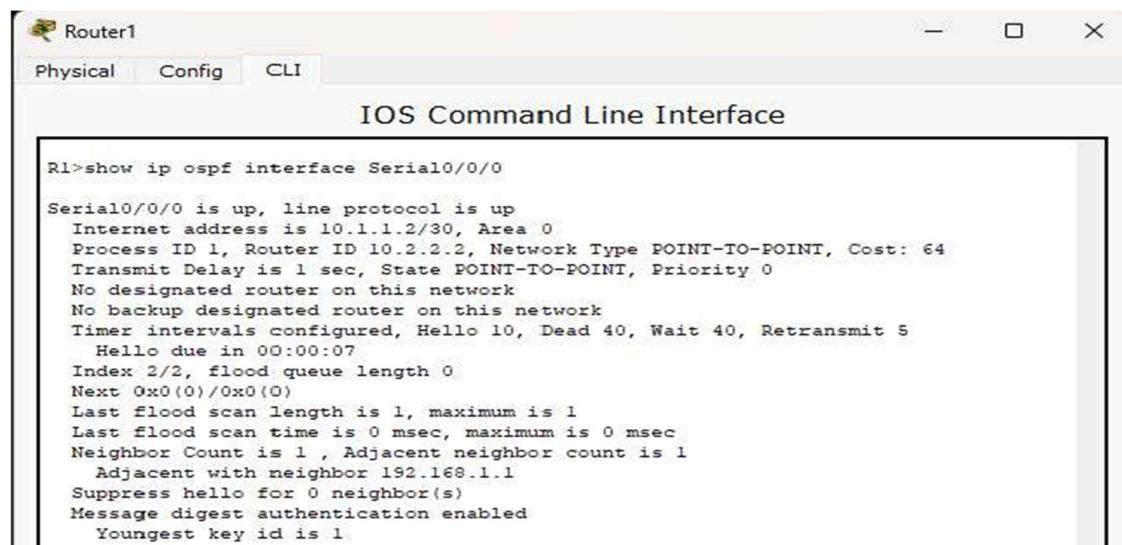
1. Router 0



The screenshot shows a software interface titled "Router0" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is selected, displaying the output of the command "R0>show ip ospf interface Serial0/0/0". The output provides detailed information about the OSPF interface, including its state, IP address, process ID, and neighbor count.

```
R0>show ip ospf interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30, Area 0
  Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next Ox0(0)/Ox0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

2. Router 1



The screenshot shows a software interface titled "Router1" with tabs for "Physical", "Config", and "CLI". The "CLI" tab is selected, displaying the output of the command "R1>show ip ospf interface Serial0/0/0". The output is identical to Router 0, showing the configuration and state of the OSPF interface on Serial0/0/0.

```
R1>show ip ospf interface Serial0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 2/2, flood queue length 0
  Next Ox0(0)/Ox0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Router1

Physical Config CLI

IOS Command Line Interface

```
R1>show ip ospf interface Serial0/0/1

Serial0/0/1 is up, line protocol is up
  Internet address is 10.2.2.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.3.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

3. Router 2

Router2

Physical Config CLI

IOS Command Line Interface

```
R2>show ip ospf interface Serial0/0/0

Serial0/0/0 is up, line protocol is up
  Internet address is 10.2.2.1/30, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

B. NTP

➤ Check Clock Time in the routers

1. Router 0

```
R0>show clock  
*0:49:14.954 UTC Mon Mar 1 1993  
R0>
```

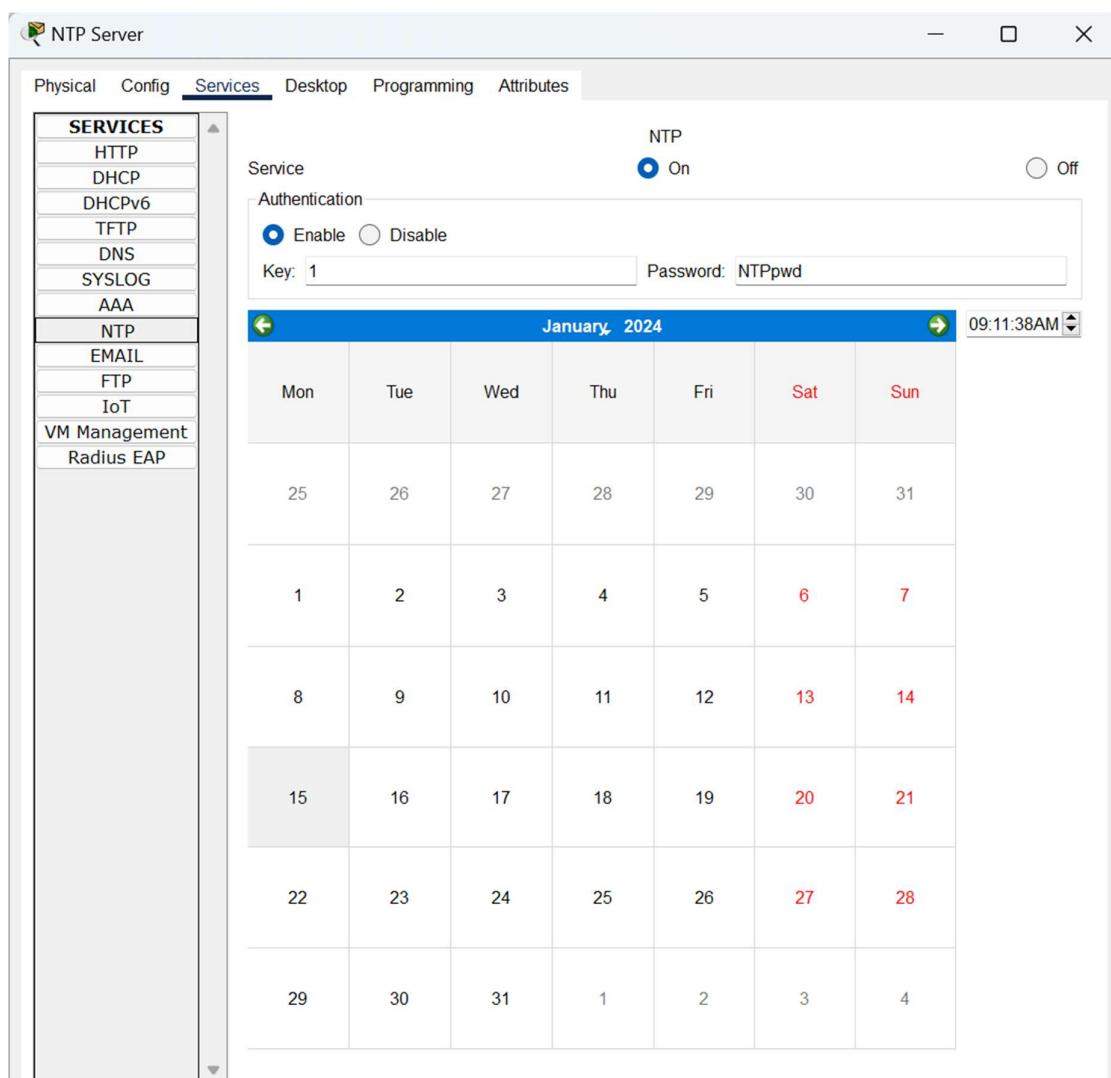
2. Router 1

```
R1>show clock  
*0:51:40.343 UTC Mon Mar 1 1993  
R1>
```

3. Router 2

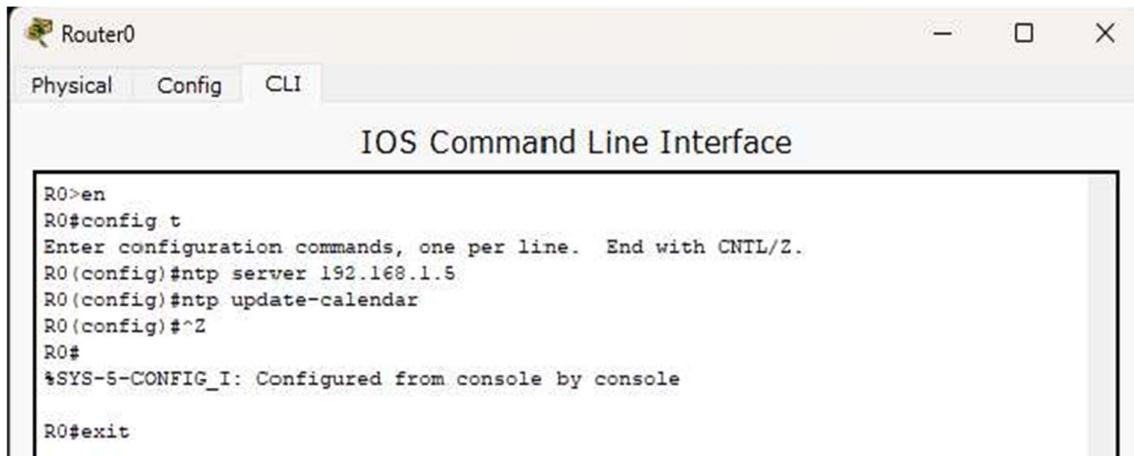
```
R2>show clock  
*0:53:5.140 UTC Mon Mar 1 1993  
R2>
```

➤ Configure NTP Server



➤ Configure NTP Client

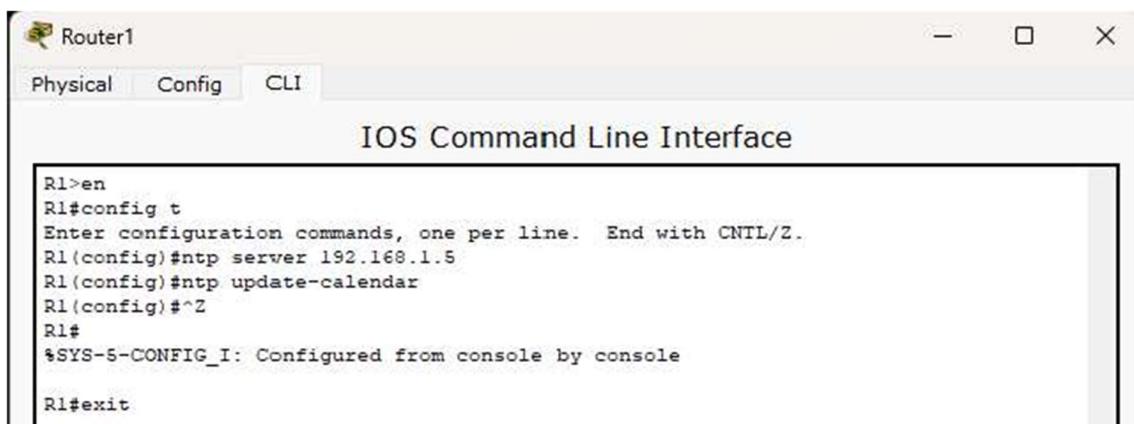
1. Router 0



The window title is "Router0". The tab bar shows "Physical", "Config" (which is selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R0>en
R0#config t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#ntp server 192.168.1.5
R0(config)#ntp update-calendar
R0(config)#^Z
R0#
%SYS-5-CONFIG_I: Configured from console by console
R0#exit
```

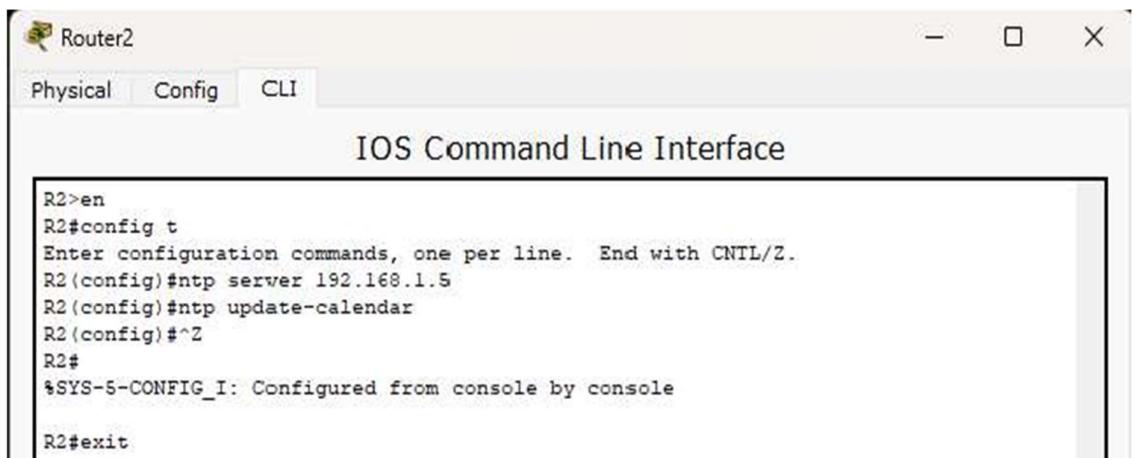
2. Router 1



The window title is "Router1". The tab bar shows "Physical", "Config" (selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#ntp update-calendar
R1(config)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#exit
```

3. Router 2



The window title is "Router2". The tab bar shows "Physical", "Config" (selected), and "CLI". The main area is titled "IOS Command Line Interface". The command history is as follows:

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#ntp update-calendar
R2(config)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ **Configure NTP authentication and to timestamp log messages on the routers**

1. Router 0

```
R0>show clock  
9:14:41.811 UTC Mon Jan 15 2024  
R0>en  
R0#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R0(config)#ntp authenticate  
R0(config)#ntp trusted-key 1  
R0(config)#ntp authentication-key 1 md5 NTPpwd  
R0(config)#service timestamps log datetime msec  
R0(config)#+Z  
R0#  
*Jan 15, 09:21:16.2121: %SYS-5-CONFIG_I: Configured from console by console
```

2. Router 1

```
R1>en  
R1#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#ntp authenticate  
R1(config)#ntp trusted-key 1  
R1(config)#ntp authentication-key 1 md5 NTPpwd  
R1(config)#service timestamps log datetime msec  
R1(config)#+Z  
R1#  
*Jan 15, 09:23:58.2323: %SYS-5-CONFIG_I: Configured from console by console
```

3. Router 2

```
R2>en  
R2#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#ntp authenticate  
R2(config)#ntp trusted-key 1  
R2(config)#ntp authentication-key 1 md5 NTPpwd  
R2(config)#service timestamps log datetime msec  
R2(config)#+Z  
R2#  
*Jan 15, 09:25:55.2525: %SYS-5-CONFIG_I: Configured from console by console
```

➤ **Check updated UTC Clock Time in the routers**

1. Router 0

```
R0>show clock  
9:14:41.811 UTC Mon Jan 15 2024  
R0>
```

2. Router 1

```
R1>show clock  
9:16:20.807 UTC Mon Jan 15 2024  
R1>
```

3. Router 2

```
R2>show clock  
9:17:35.379 UTC Mon Jan 15 2024  
R2>
```

C. SYSLOG

➤ **Configure Routers to Log Messages to the SYSLOG Server**

1. Router 0

```
R0>en  
R0#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R0(config)#logging host 192.168.1.6  
R0(config)#^Z  
R0#  
*Jan 15, 09:29:38.2929: %SYS-5-CONFIG_I: Configured from console by console
```

2. Router 1

```
R1>en  
R1#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#logging host 192.168.1.6  
R1(config)#^Z  
R1#  
*Jan 15, 09:30:45.3030: %SYS-5-CONFIG_I: Configured from console by console
```

3. Router 2

```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#logging host 192.168.1.6
R2(config)#+^Z
R2#
*Jan 15, 09:32:06.3232: %SYS-5-CONFIG_I: Configured from console by console
```

➤ Verify logging configuration on Routers

1. Router 0

```
Router0
Physical Config CLI

R0#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 20 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
                  filtering disabled
Buffer logging: disabled, xml disabled,
                  filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 20 message lines logged
              Logging to 192.168.1.6 (udp port 514, audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

2. Router 1



```
R1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
    0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

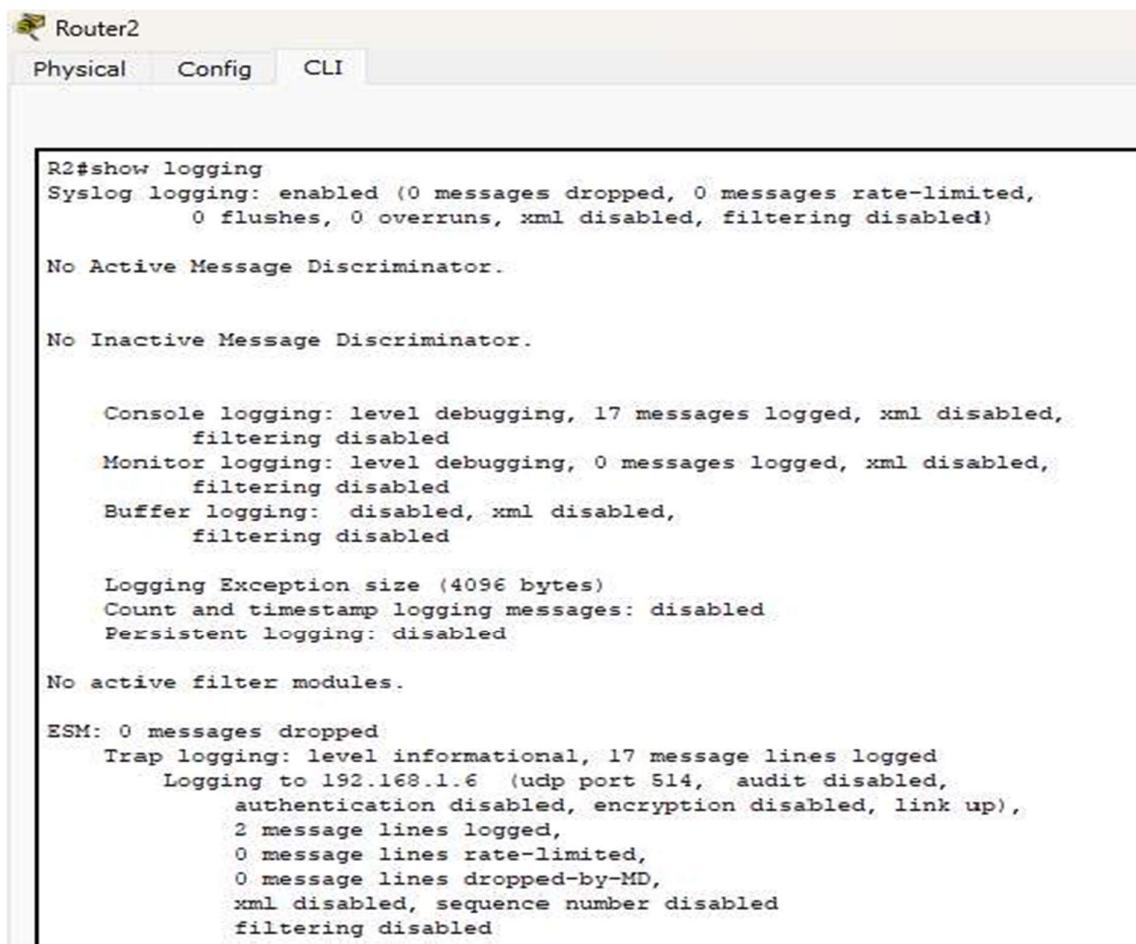
Console logging: level debugging, 30 messages logged, xml disabled,
    filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
    filtering disabled
Buffer logging: disabled, xml disabled,
    filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 30 message lines logged
    Logging to 192.168.1.6 (udp port 514, audit disabled,
        authentication disabled, encryption disabled, link up),
    2 message lines logged,
    0 message lines rate-limited,
    0 message lines dropped-by-MD,
    xml disabled, sequence number disabled
    filtering disabled
...
...
```

3. Router 2



```
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

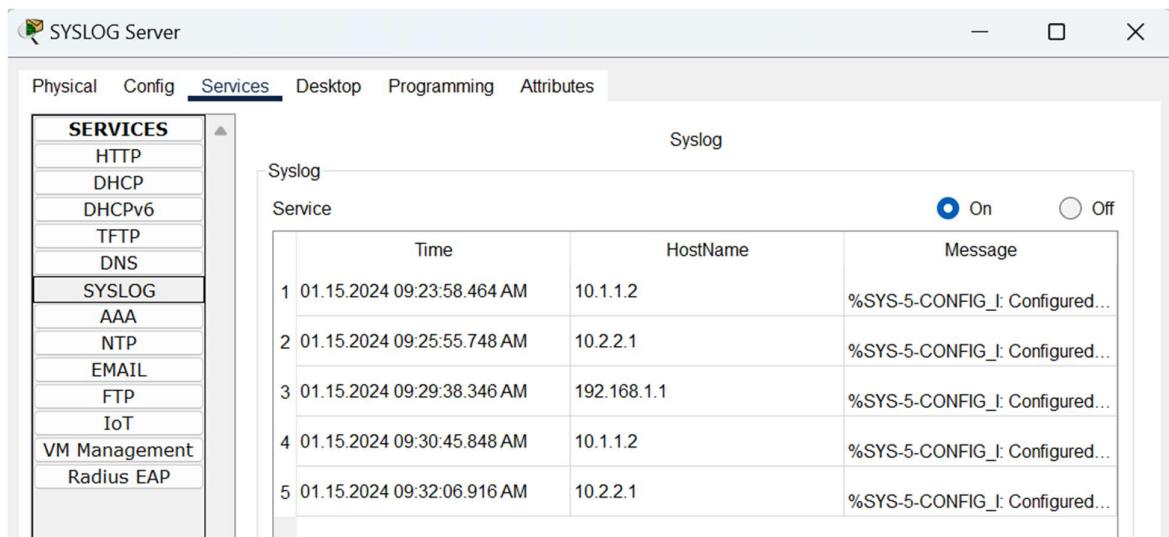
Console logging: level debugging, 17 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
                  filtering disabled
Buffer logging: disabled, xml disabled,
                  filtering disabled

Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.

ESM: 0 messages dropped
Trap logging: level informational, 17 message lines logged
              Logging to 192.168.1.6 (udp port 514, audit disabled,
              authentication disabled, encryption disabled, link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
```

➤ Examine logs of the SYSLOG Server



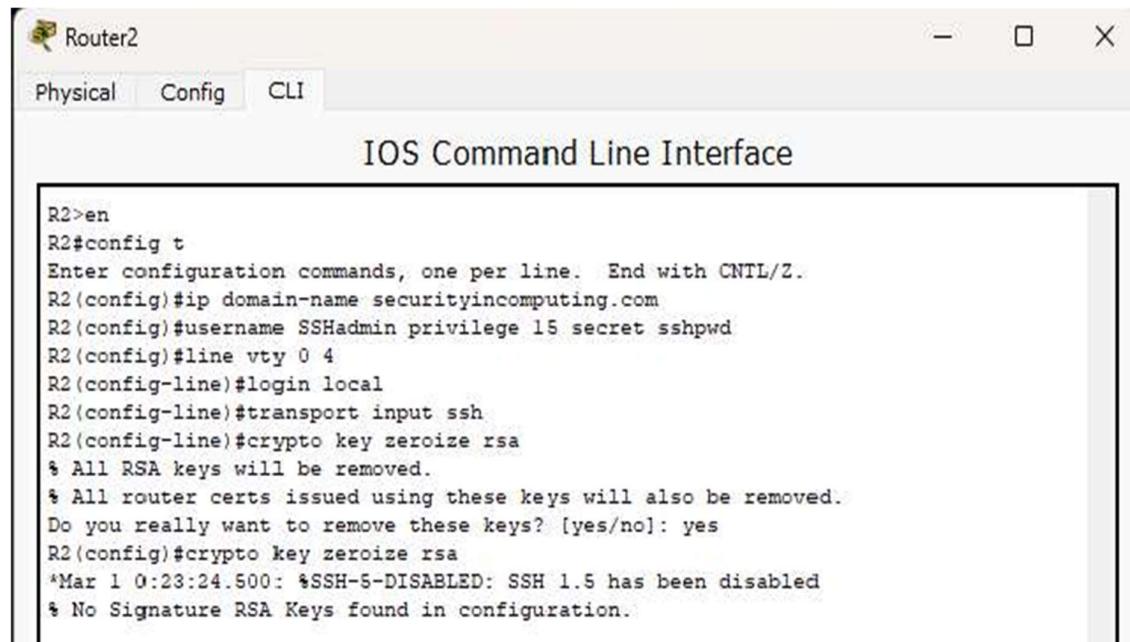
The screenshot shows the 'SYSLOG Server' application window. The 'Services' tab is selected in the navigation bar. On the left, a sidebar lists various services: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG (which is currently selected), AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main pane displays a table titled 'Syslog' under the 'Service' section. The table has columns for Time, HostName, and Message. There are five log entries listed:

Time	HostName	Message
1 01.15.2024 09:23:58.464 AM	10.1.1.2	%SYS-5-CONFIG_I: Configured...
2 01.15.2024 09:25:55.748 AM	10.2.2.1	%SYS-5-CONFIG_I: Configured...
3 01.15.2024 09:29:38.346 AM	192.168.1.1	%SYS-5-CONFIG_I: Configured...
4 01.15.2024 09:30:45.848 AM	10.1.1.2	%SYS-5-CONFIG_I: Configured...
5 01.15.2024 09:32:06.916 AM	10.2.2.1	%SYS-5-CONFIG_I: Configured...

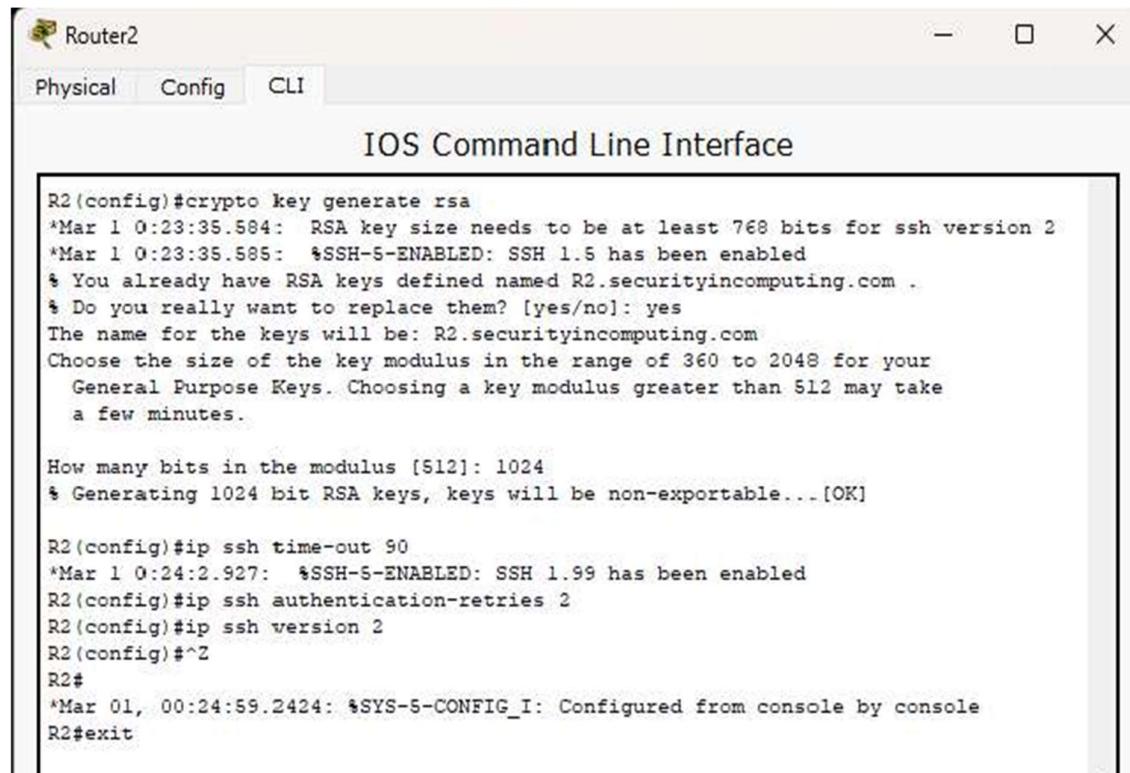
D. SSH

➤ Configure SSH on R2

Router 2



```
R2>en
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip domain-name securityincomputing.com
R2(config)#username SSHadmin privilege 15 secret sshpwd
R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
R2(config)#crypto key zeroize rsa
*Mar 1 0:23:24.500: %SSH-5-DISABLED: SSH 1.5 has been disabled
% No Signature RSA Keys found in configuration.
```



```
R2(config)#crypto key generate rsa
*Mar 1 0:23:35.584: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:23:35.585: %SSH-5-ENABLED: SSH 1.5 has been enabled
% You already have RSA keys defined named R2.securityincomputing.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R2.securityincomputing.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]

R2(config)#ip ssh time-out 90
*Mar 1 0:24:2.927: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config)#ip ssh authentication-retries 2
R2(config)#ip ssh version 2
R2(config)#^Z
R2#
*Mar 01, 00:24:59.2424: %SYS-5-CONFIG_I: Configured from console by console
R2#exit
```

➤ Connect to R2 using telnet and SSH on PC

```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.3.1
Trying 192.168.3.1 ...Open
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHAdmin 192.168.3.1
Password:
R2#
```

➤ Checking Connections by passing packets:

