ABC LIMITED NETWORK DESIGN

Max Krause

MAX K NETWORKING 3 Cherrywood Cres

Table of Contents

Design the addresses for all internal subnets. Configure the IP address for all devices in the given topology according to the requirement and verify. (10 marks) 2

OSPF-enabled routers must recognize each other on the network before they can share information. DR and BDR routers are then elected to reduce the number of adjacencies and flooding of LSAs. In the local district part, assign the following router IDs: 4

BH-1 provides a connection to ISP. 11

NAT provides the translation of private addresses to public addresses. Please configure static and dynamic NAT for all traffic entering and exiting the company network. (3 marks) Then use the simulation results to elaborate the actions that are involved when an internal host (e.g. Host B6) attempts to send a packet to the external ISP server. (2 marks) 12

Static NAT: 13

Dynamic NAT: 16

Scenario: 17

Once you have obtained a successful end-to-end connection, for improving the network security, please consider applying ACL to secure the network traffic. Create an ACL, only the Service PC is allowed to remote access to LD-1 and BH-1 router. Please verify and explain how ACL processes packets. (5 marks) 18

Create an extended ACL that will deny HTTP traffic from devices in LAN 3, 4, 5, and 6 to the Web Server in LAN1 but allow other traffic to go through. HTTP uses TCP on port 80. Please verify and explain how ACL processes packets. (5 marks) 21

IPsec Report 22

Design the addresses for all internal subnets. Configure the IP address for all devices in the given topology according to the requirement and verify. (10 marks)

Student ID: 11745025

2nd & 3rd Octet -> (50.25)

LAN1 10.50.25.0/29 – IP Range .1 -.6

LAN2 10.50.25.8/29 – IP Range .9 -.14

LAN3 10.50.25.16/29 – IP Range .17 -.22

LAN4 10.50.25.24/29 – IP Range .25 -.30

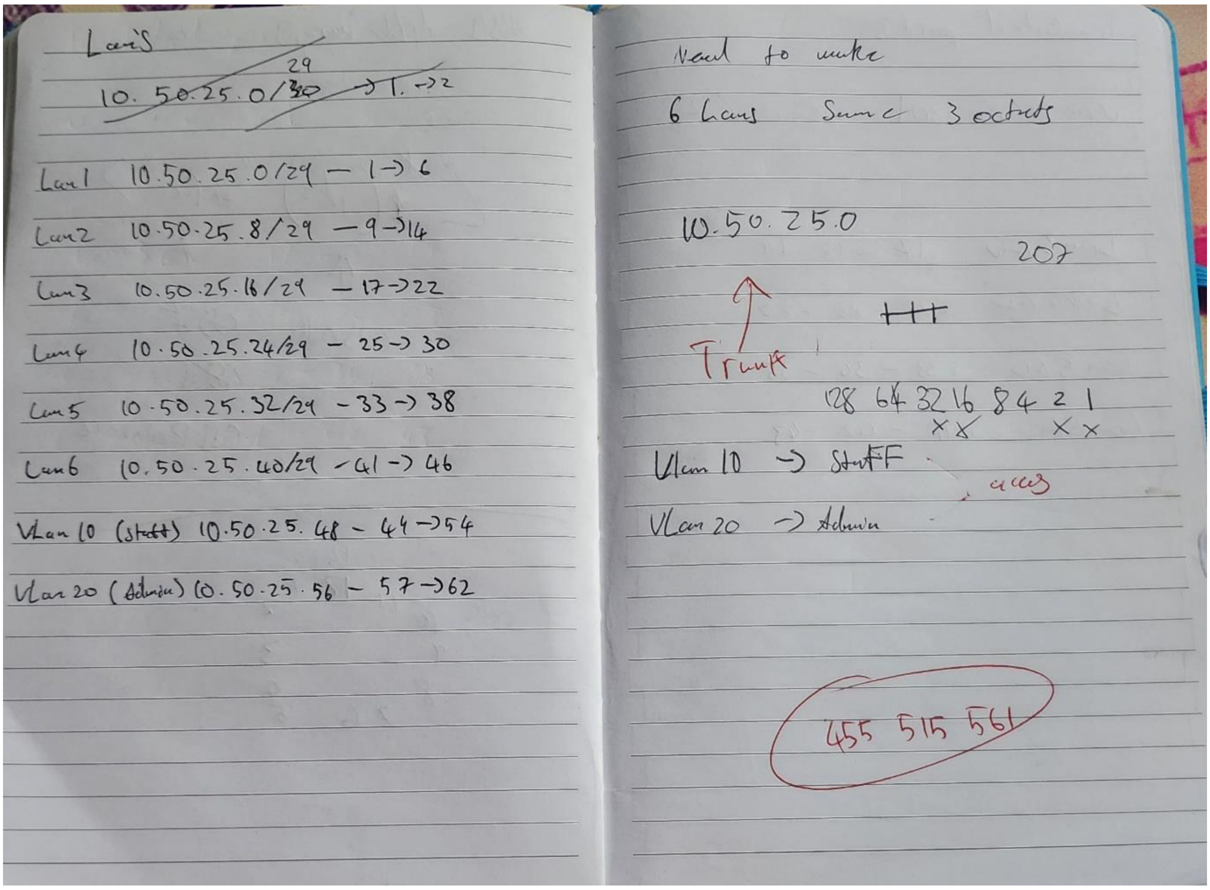
LAN5 10.50.25.32/29 – IP Range .33 -.38

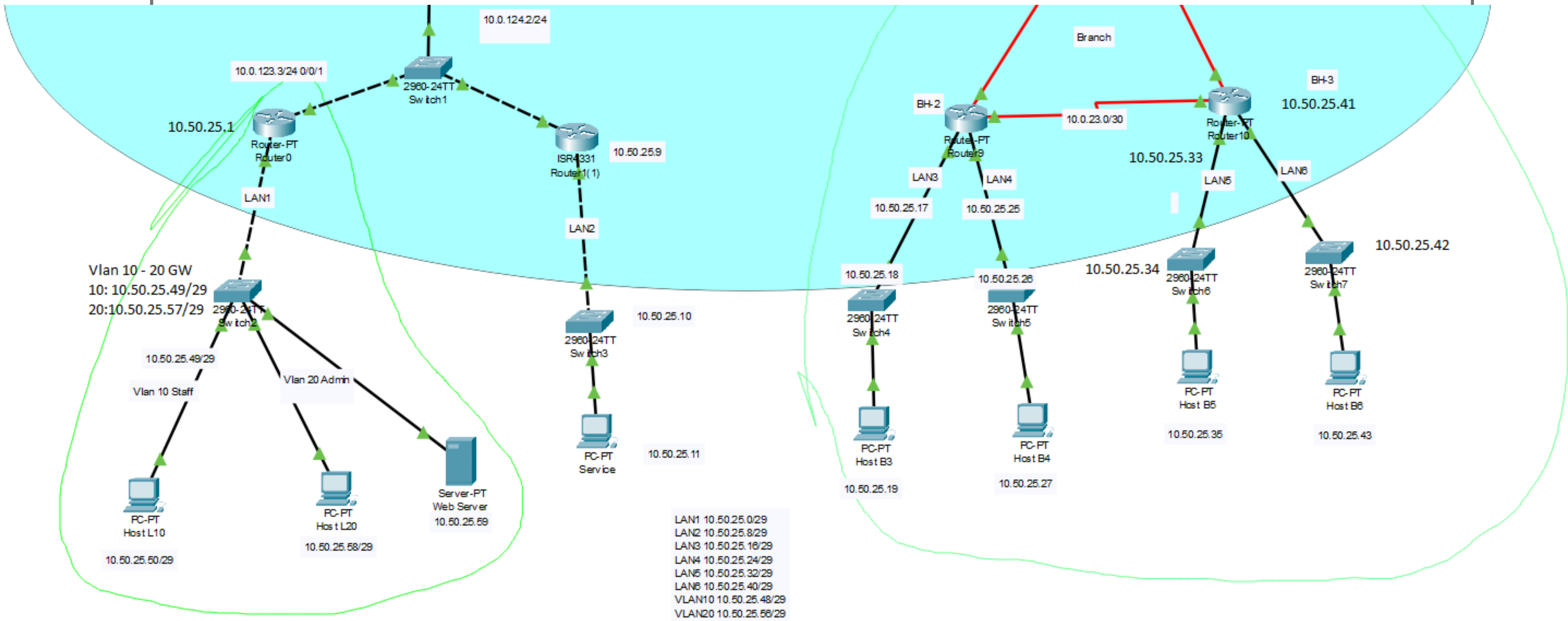
LAN6 10.50.25.40/29 – IP Range .41 -.46

VLAN10 10.50.25.48/29 – IP Range .49 -.54

VLAN20 10.50.25.56/29 – IP Range .57 -.62

Below is me trying to figure out the IP ranges back at the beginning of assesment:

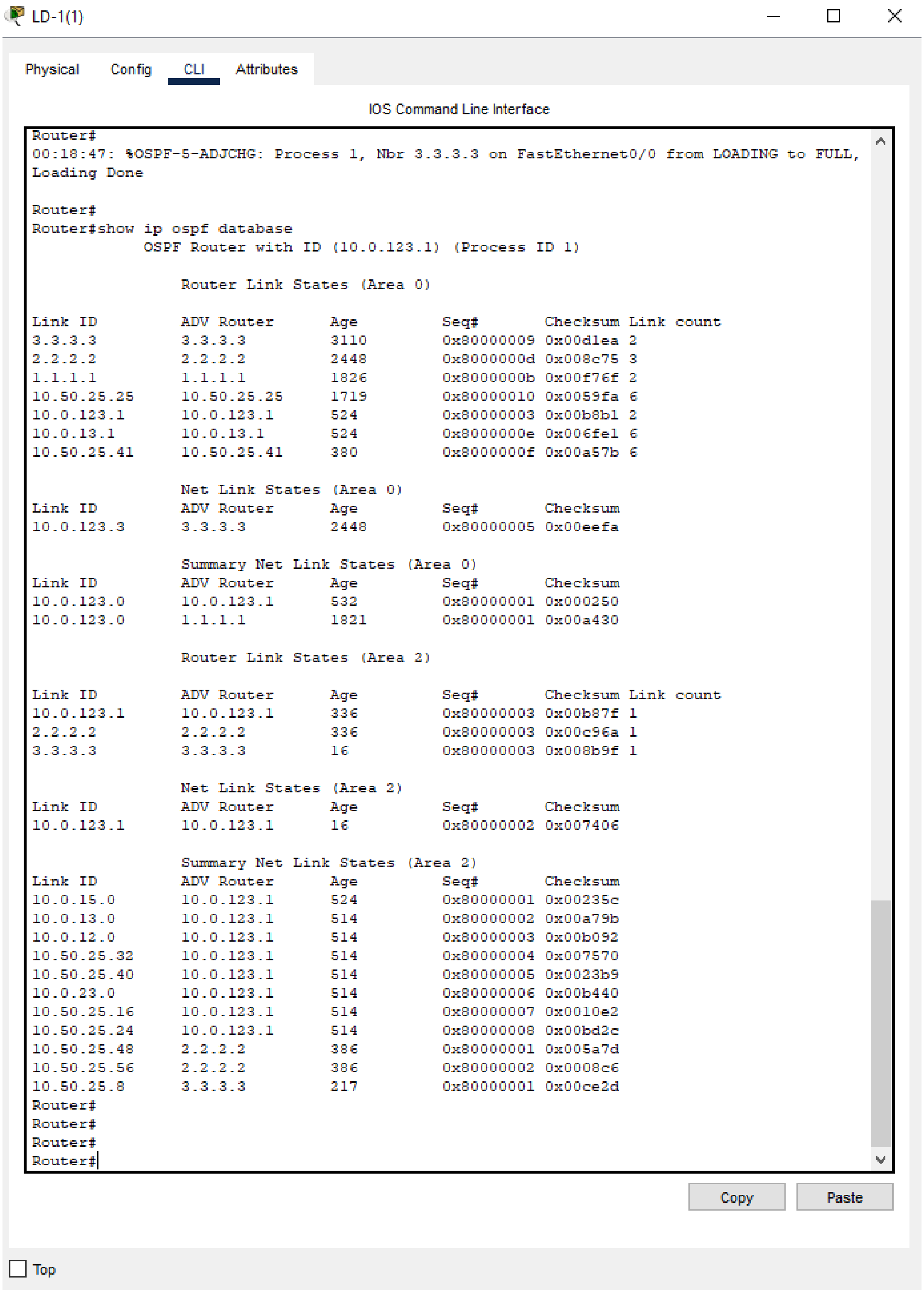




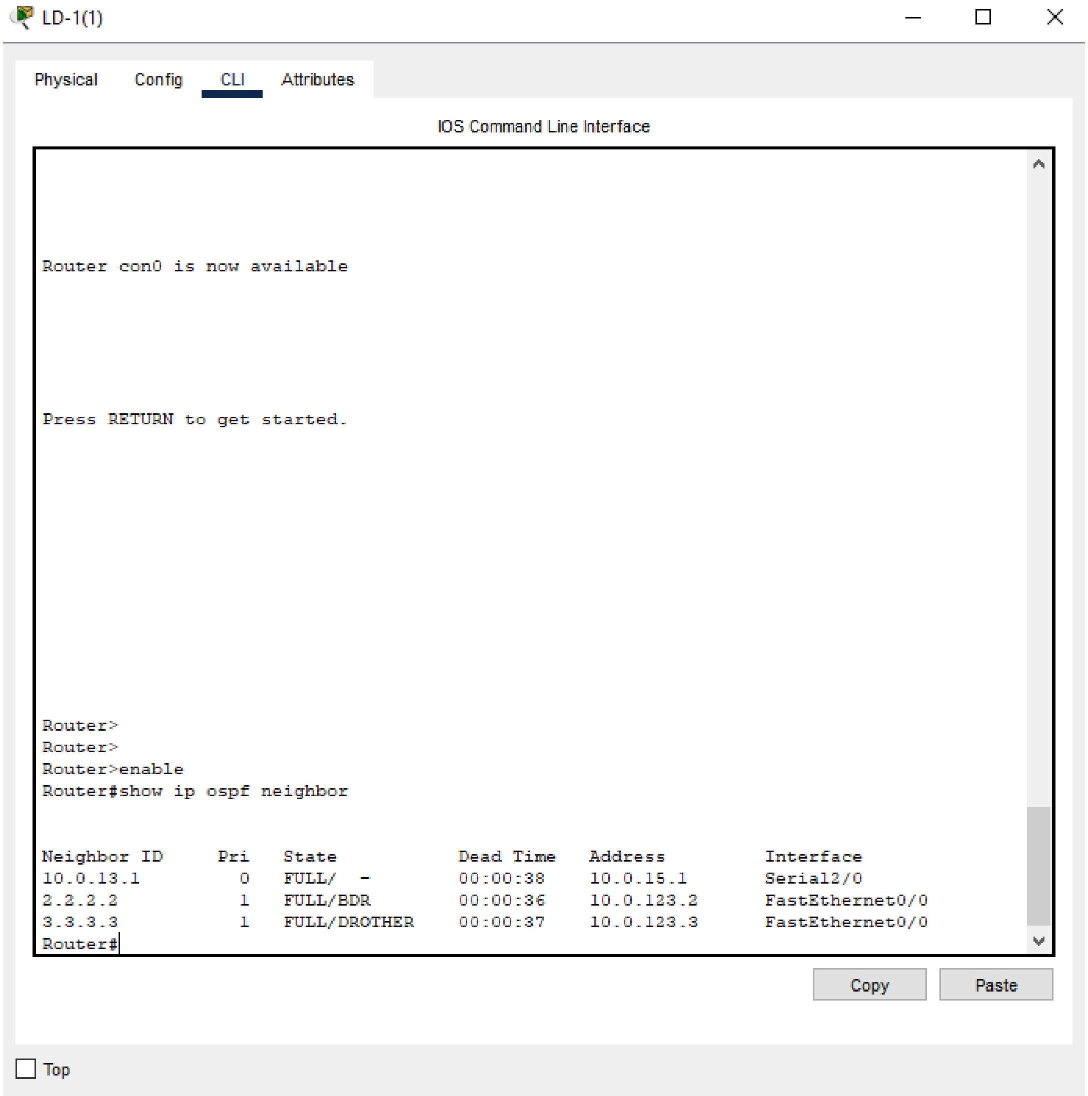
All Internal networks have operating subnets as per the screen capture above

OSPF-enabled routers must recognize each other on the network before they can share information. DR and BDR routers are then elected to reduce the number of adjacencies and flooding of LSAs. In the local district part, assign the following router IDs:

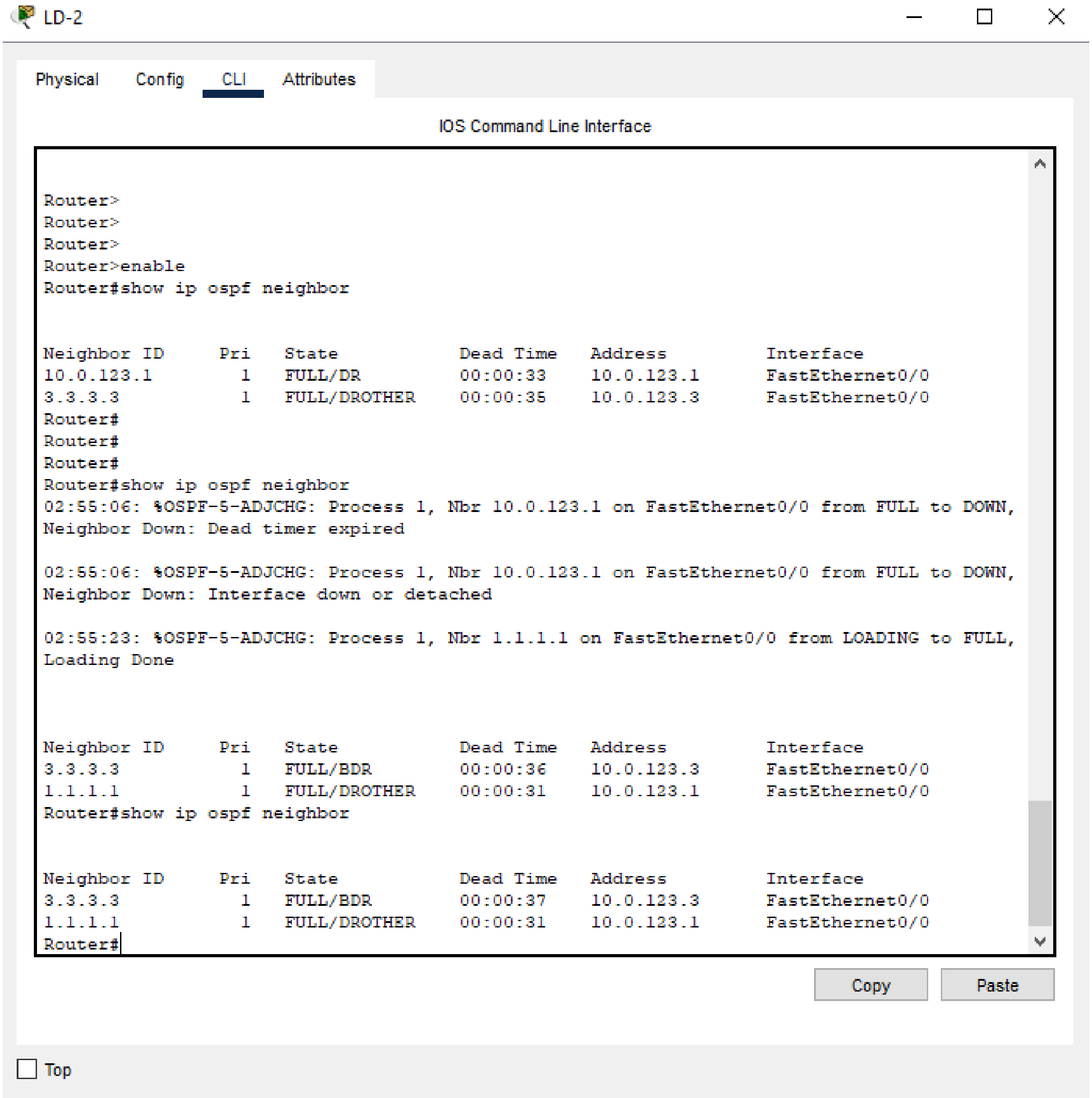
LD-1: 1.1.1.1




```
Router#
00:18:47: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on FastEthernet0/0 from LOADING to FULL,
Loading Done

Router#
Router#show ip ospf database
            OSPF Router with ID (10.0.123.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
3.3.3.3         3.3.3.3         3110        0x80000009 0x00d1ea 2
2.2.2.2         2.2.2.2         2448        0x8000000d 0x008c75 3
1.1.1.1         1.1.1.1         1826        0x8000000b 0x00f76f 2
10.50.25.25     10.50.25.25     1719        0x80000010 0x0059fa 6
10.0.123.1      10.0.123.1      524         0x80000003 0x00b8b1 2
10.0.13.1       10.0.13.1       524         0x8000000e 0x006fe1 6
10.50.25.41     10.50.25.41     380         0x8000000f 0x00a57b 6

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.3      3.3.3.3         2448        0x80000005 0x00eefa

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.0      10.0.123.1      532         0x80000001 0x000250
10.0.123.0      1.1.1.1         1821        0x80000001 0x00a430

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.123.1      10.0.123.1      336         0x80000003 0x00b87f 1
2.2.2.2         2.2.2.2         336         0x80000003 0x00c96a 1
3.3.3.3         3.3.3.3         16          0x80000003 0x008b9f 1

                Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.1      10.0.123.1      16          0x80000002 0x007406

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.15.0       10.0.123.1      524         0x80000001 0x00235c
10.0.13.0       10.0.123.1      514         0x80000002 0x00a79b
10.0.12.0       10.0.123.1      514         0x80000003 0x00b092
10.50.25.32     10.0.123.1      514         0x80000004 0x007570
10.50.25.40     10.0.123.1      514         0x80000005 0x0023b9
10.0.23.0       10.0.123.1      514         0x80000006 0x00b440
10.50.25.16     10.0.123.1      514         0x80000007 0x0010e2
10.50.25.24     10.0.123.1      514         0x80000008 0x00bd2c
10.50.25.48     2.2.2.2         386         0x80000001 0x005a7d
10.50.25.56     2.2.2.2         386         0x80000002 0x0008c6
10.50.25.8      3.3.3.3         217         0x80000001 0x00ce2d
Router#
Router#
Router#
Router#
```


LD-1(1)
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router con0 is now available
Press RETURN to get started.
Router>
Router>
Router>enable
Router#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.0.13.1 0 FULL/ - 00:00:38 10.0.15.1 Serial2/0
2.2.2.2 1 FULL/BDR 00:00:36 10.0.123.2 FastEthernet0/0
3.3.3.3 1 FULL/DROTHER 00:00:37 10.0.123.3 FastEthernet0/0
Router#
Copy
Paste
Top

LD-2: 2.2.2.2




```
Router>
Router>
Router>
Router>enable
Router#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.123.1        1   FULL/DR         00:00:33    10.0.123.1      FastEthernet0/0
3.3.3.3           1   FULL/DROTHER    00:00:35    10.0.123.3      FastEthernet0/0
Router#
Router#
Router#
Router#show ip ospf neighbor
02:55:06: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.123.1 on FastEthernet0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired

02:55:06: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.123.1 on FastEthernet0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

02:55:23: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on FastEthernet0/0 from LOADING to FULL,
Loading Done



Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:36    10.0.123.3      FastEthernet0/0
1.1.1.1           1   FULL/DROTHER    00:00:31    10.0.123.1      FastEthernet0/0
Router#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           1   FULL/BDR        00:00:37    10.0.123.3      FastEthernet0/0
1.1.1.1           1   FULL/DROTHER    00:00:31    10.0.123.1      FastEthernet0/0
Router#
```

LD-2

Physical Config CLI Attributes

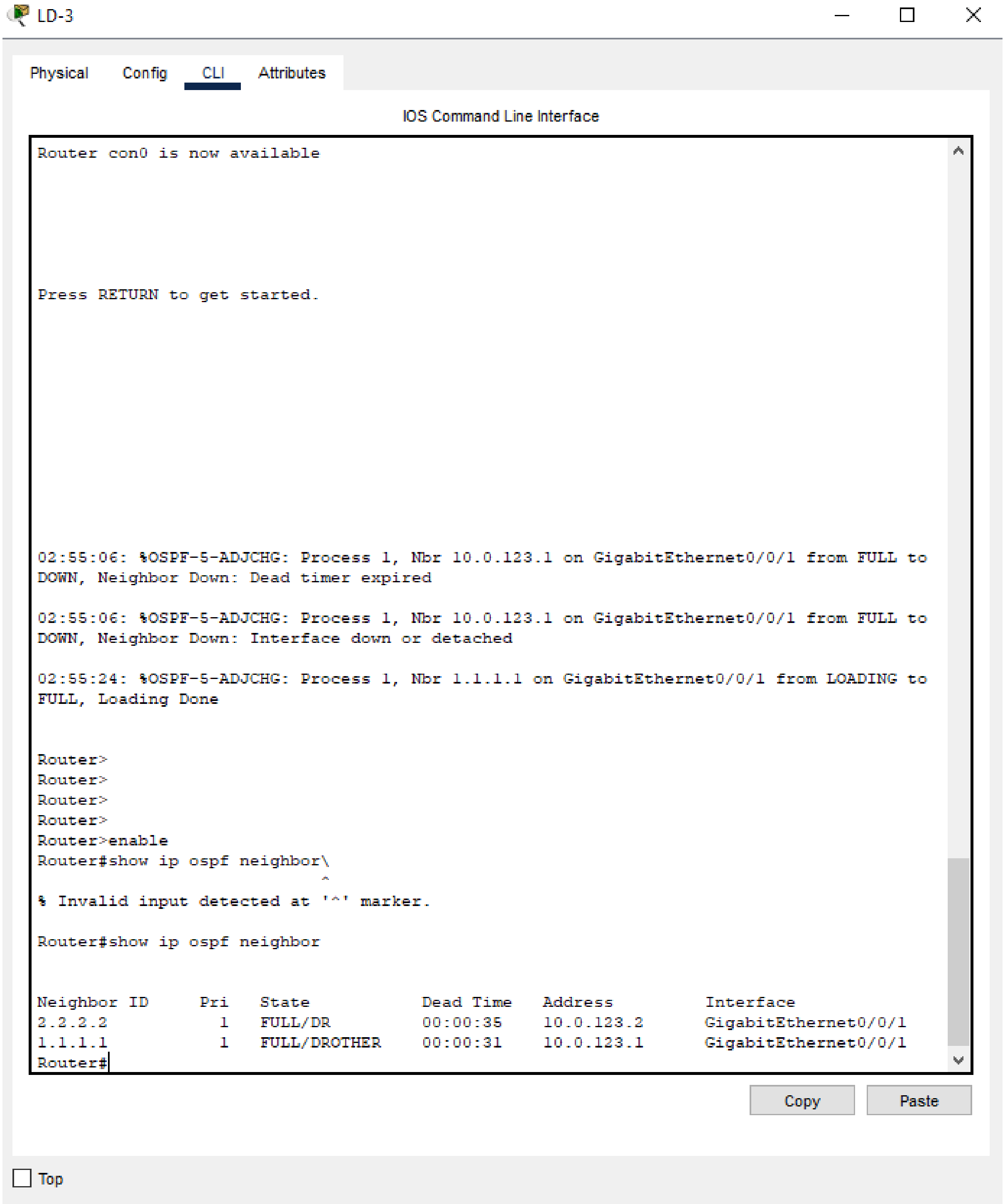
IOS Command Line Interface

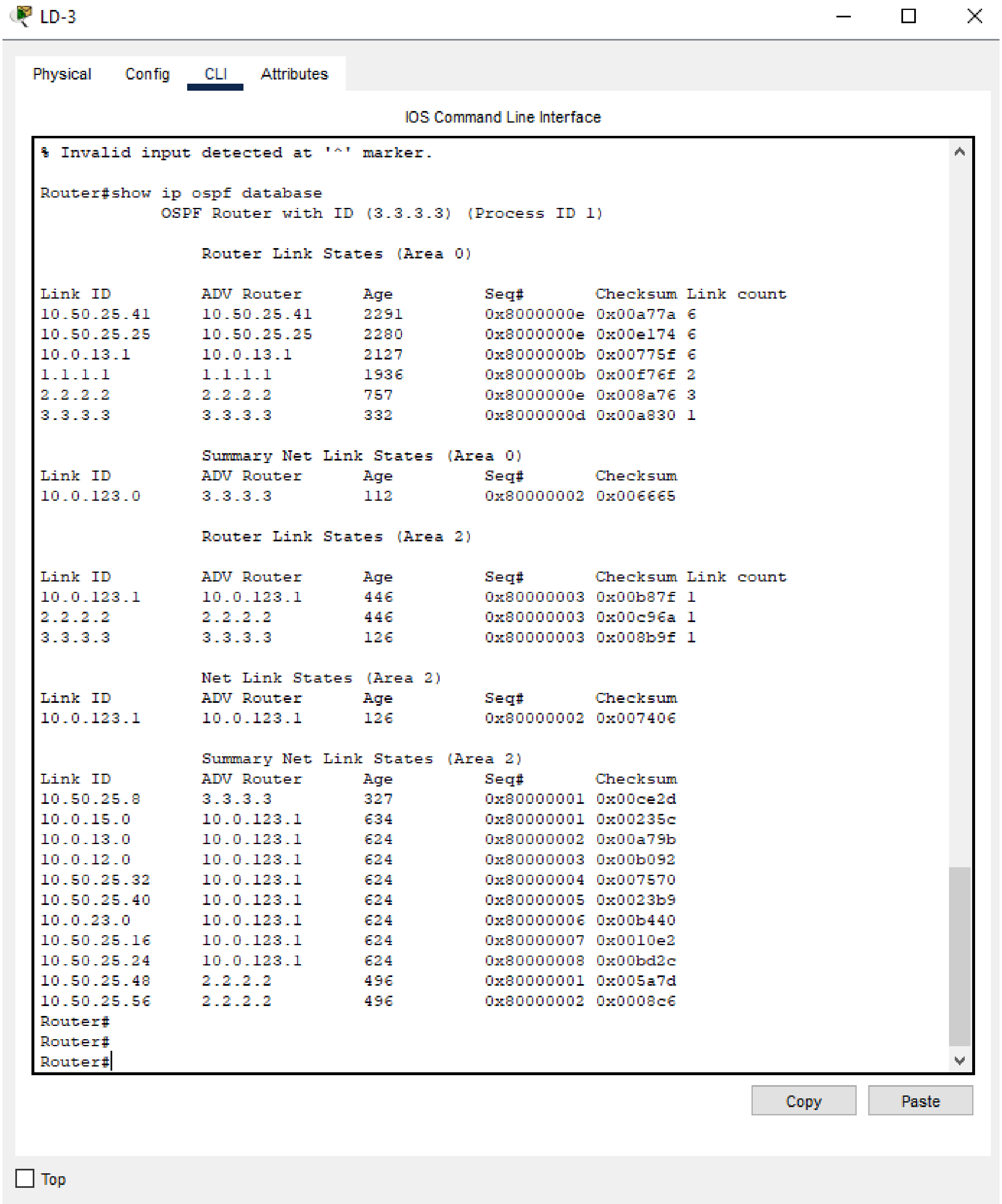
```
Loading Done

Router#
Router#
Router#
Router#
Router#show ip ospf database
            OSPF Router with ID (2.2.2.2) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.50.25.41     10.50.25.41     2248        0x8000000e 0x00a77a 6
10.50.25.25     10.50.25.25     2237        0x8000000e 0x00e174 6
10.0.13.1       10.0.13.1       2084        0x8000000b 0x00775f 6
1.1.1.1         1.1.1.1         1893        0x8000000b 0x00f76f 2
3.3.3.3         3.3.3.3         1376        0x8000000a 0x00cfeb 2
2.2.2.2         2.2.2.2         458         0x80000012 0x00e13a 2

                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.3      3.3.3.3         568         0x8000000a 0x00e6c1

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.0      2.2.2.2         438         0x80000001 0x00864a

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
2.2.2.2         2.2.2.2         403         0x80000003 0x00c96a 1
10.0.123.1      10.0.123.1      403         0x80000003 0x00b87f 1
3.3.3.3         3.3.3.3         83          0x80000003 0x008b9f 1

                Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.1      10.0.123.1      83          0x80000002 0x007406

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.50.25.48     2.2.2.2         453         0x80000001 0x005a7d
10.50.25.56     2.2.2.2         453         0x80000002 0x0008c6
10.0.15.0       10.0.123.1      591         0x80000001 0x00235c
10.0.13.0       10.0.123.1      581         0x80000002 0x00a79b
10.0.12.0       10.0.123.1      581         0x80000003 0x00b092
10.50.25.32     10.0.123.1      581         0x80000004 0x007570
10.50.25.40     10.0.123.1      581         0x80000005 0x0023b9
10.0.23.0       10.0.123.1      581         0x80000006 0x00b440
10.50.25.16     10.0.123.1      581         0x80000007 0x0010e2
10.50.25.24     10.0.123.1      581         0x80000008 0x00bd2c
10.50.25.8      3.3.3.3         284         0x80000001 0x00ce2d
Router#
Router#
Router#
```

Copy Paste

Top

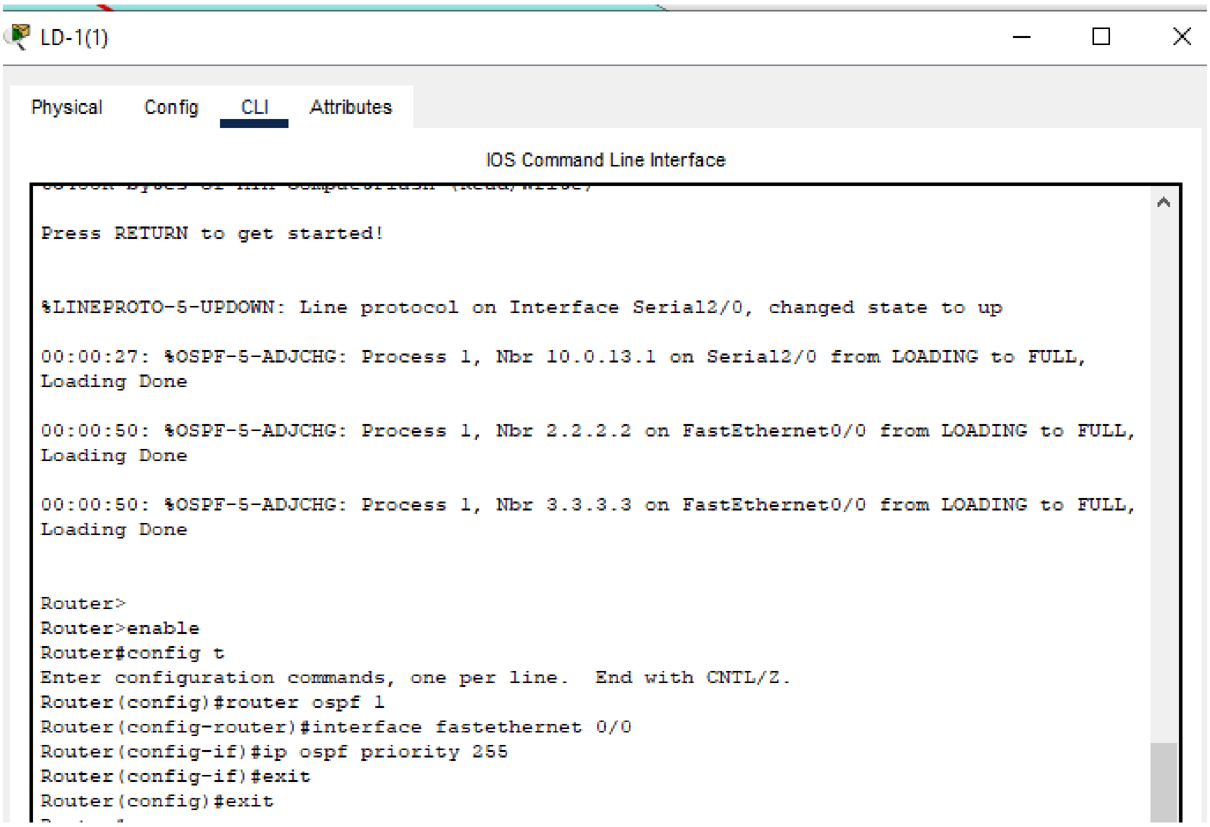
LD-3: 3.3.3.3


LD-3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router con0 is now available
Press RETURN to get started.
02:55:06: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.123.1 on GigabitEthernet0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
02:55:06: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.123.1 on GigabitEthernet0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
02:55:24: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet0/0/1 from LOADING to FULL, Loading Done
Router>
Router>
Router>
Router>
Router>enable
Router#show ip ospf neighbor\
^
% Invalid input detected at '^' marker.
Router#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1 FULL/DR 00:00:35 10.0.123.2 GigabitEthernet0/0/1
1.1.1.1 1 FULL/DROTHER 00:00:31 10.0.123.1 GigabitEthernet0/0/1
Router#
Copy
Paste
Top




```
% Invalid input detected at '^' marker.

Router#show ip ospf database
            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.50.25.41     10.50.25.41     2291        0x8000000e 0x00a77a 6
10.50.25.25     10.50.25.25     2280        0x8000000e 0x00e174 6
10.0.13.1       10.0.13.1       2127        0x8000000b 0x00775f 6
1.1.1.1         1.1.1.1         1936        0x8000000b 0x00f76f 2
2.2.2.2         2.2.2.2         757         0x8000000e 0x008a76 3
3.3.3.3         3.3.3.3         332         0x8000000d 0x00a830 1

                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.0      3.3.3.3         112         0x80000002 0x006665

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.123.1      10.0.123.1      446         0x80000003 0x00b87f 1
2.2.2.2         2.2.2.2         446         0x80000003 0x00c96a 1
3.3.3.3         3.3.3.3         126         0x80000003 0x008b9f 1

                Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.0.123.1      10.0.123.1      126         0x80000002 0x007406

                Summary Net Link States (Area 2)
Link ID         ADV Router      Age         Seq#       Checksum
10.50.25.8      3.3.3.3         327         0x80000001 0x00ce2d
10.0.15.0       10.0.123.1      634         0x80000001 0x00235c
10.0.13.0       10.0.123.1      624         0x80000002 0x00a79b
10.0.12.0       10.0.123.1      624         0x80000003 0x00b092
10.50.25.32     10.0.123.1      624         0x80000004 0x007570
10.50.25.40     10.0.123.1      624         0x80000005 0x0023b9
10.0.23.0       10.0.123.1      624         0x80000006 0x00b440
10.50.25.16     10.0.123.1      624         0x80000007 0x0010e2
10.50.25.24     10.0.123.1      624         0x80000008 0x00bd2c
10.50.25.48     2.2.2.2         496         0x80000001 0x005a7d
10.50.25.56     2.2.2.2         496         0x80000002 0x0008c6
Router#
Router#
Router#
```

Active OSPF on all routers. Please gather appropriate OSPF messages (e.g. OSPF database and OSPF neighbors) to elaborate on the DR and BDR election. (5 marks)

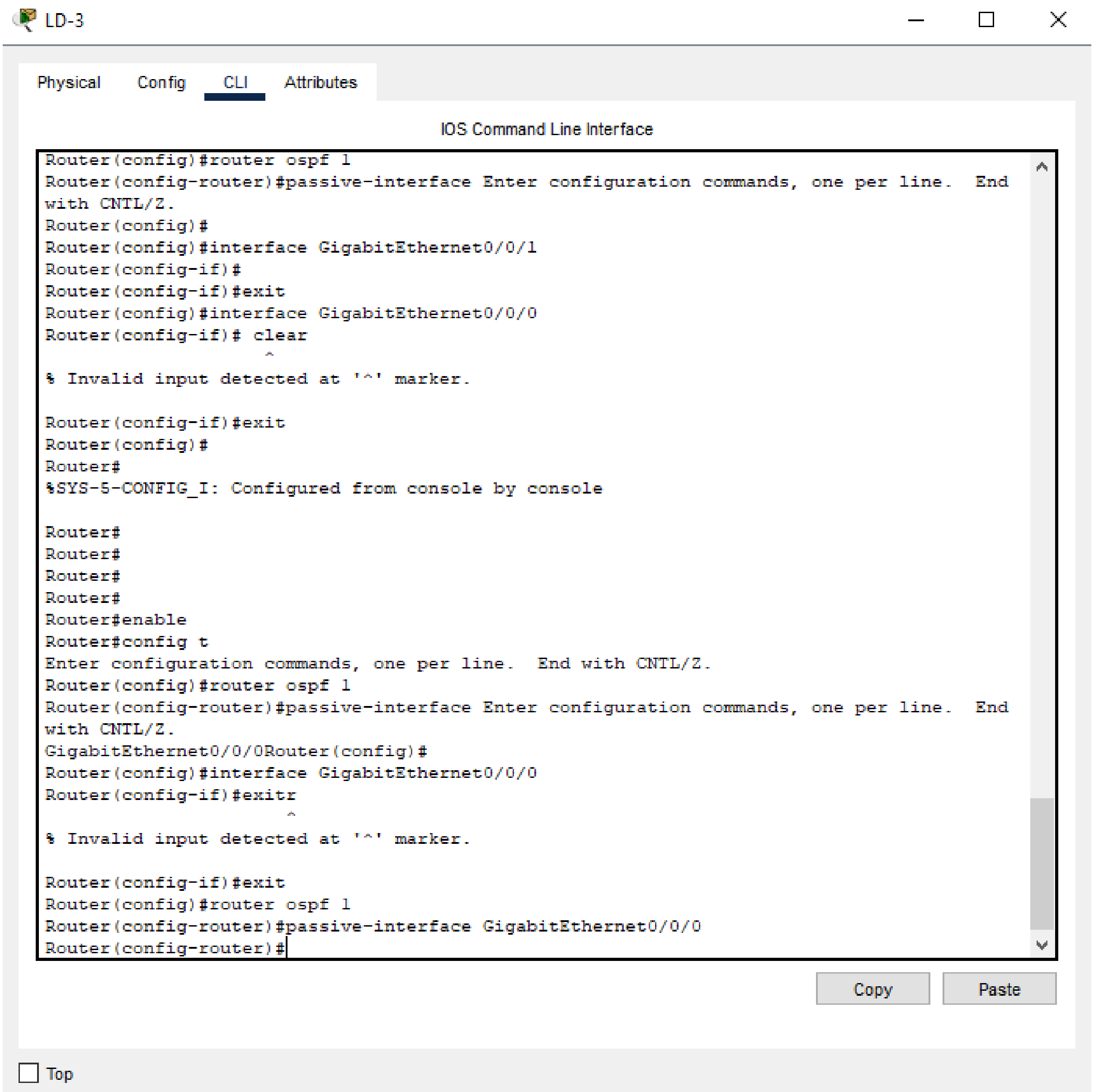


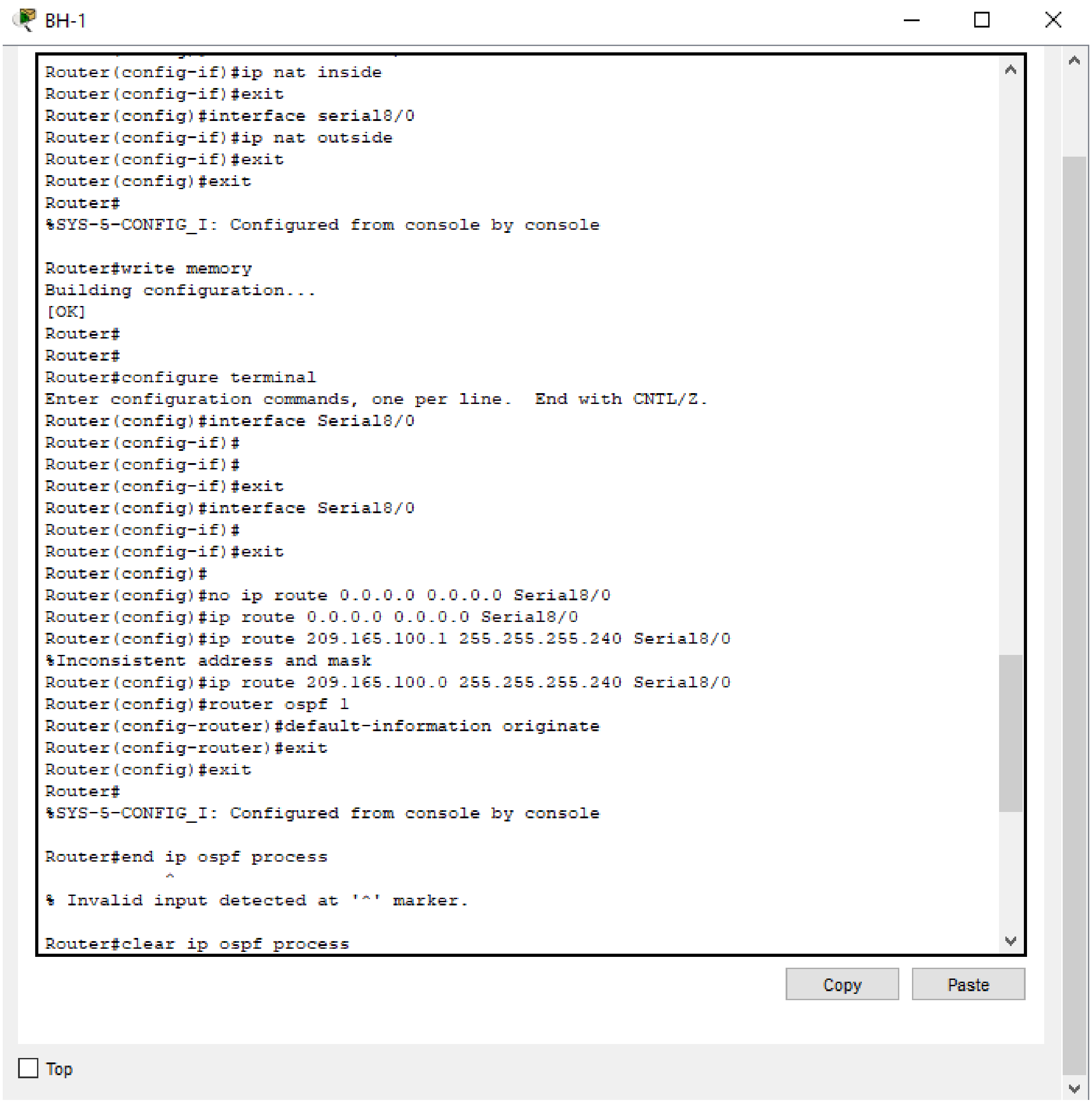
LD-1 was selected as the DR router because it connects the local district back to area 0 and to the external ISP connection. To gather appropriate OSPF messages to elaborate on the DR and BDR election, we would look at OSPF Hello packets exchanged between routers on the network segment where LD-1 is located. These packets would contain information about OSPF priorities and router IDs, which are crucial for the election process.

3. **BH-1 provides a connection to ISP.** The best practice is to have a default route to the ISP and automatically distribute the default route to all routers in the network for network management. Please propose the simplest and best way to make BH-1 is the DR router. Configure the OSPF so that routing updates are not sent into networks where OSPF updates are not required. (5 marks)

Setting BH-1 as the DR router for area 0 is best achieved by setting its local ports with OSPF neighbors to 255 priority, as for distribution the default route to other router this is best achieved via the (default-information originate) command as it configures OSPF to advertise the default route as I have made it present in the routing table.

To configure OSPF so that updates are not sent to non-OSPF routers the (passive-interface “INT ID”) command should be run for each non-OSPF adjacency on each OSPF enabled router. See example LD-3 below.



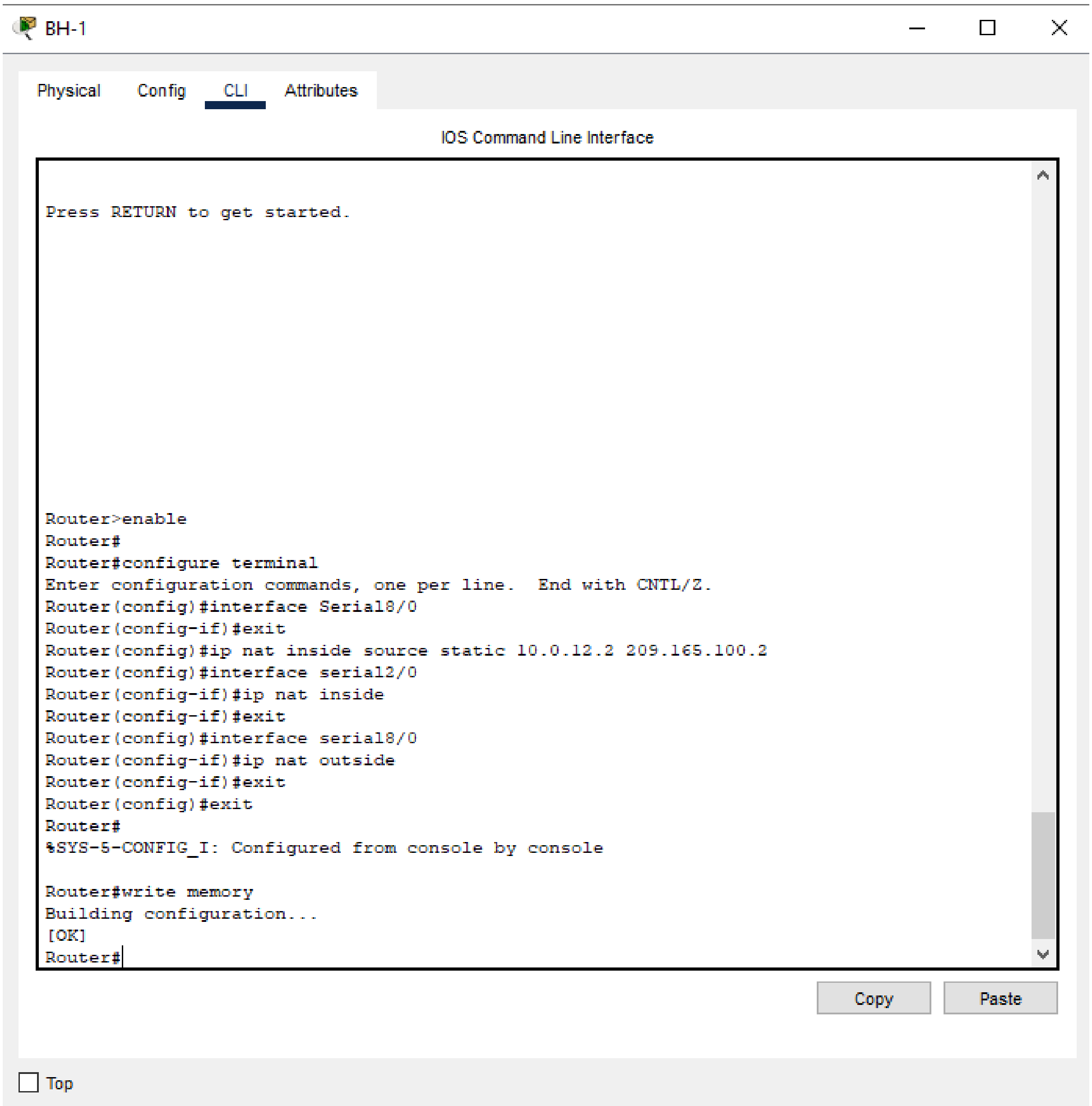


```
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial8/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write memory
Building configuration...
[OK]
Router#
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial8/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial8/0
Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#no ip route 0.0.0.0 0.0.0.0 Serial8/0
Router(config)#ip route 0.0.0.0 0.0.0.0 Serial8/0
Router(config)#ip route 209.165.100.1 255.255.255.240 Serial8/0
%Inconsistent address and mask
Router(config)#ip route 209.165.100.0 255.255.255.240 Serial8/0
Router(config)#router ospf 1
Router(config-router)#default-information originate
Router(config-router)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#end ip ospf process
            ^
% Invalid input detected at '^' marker.

Router#clear ip ospf process
```

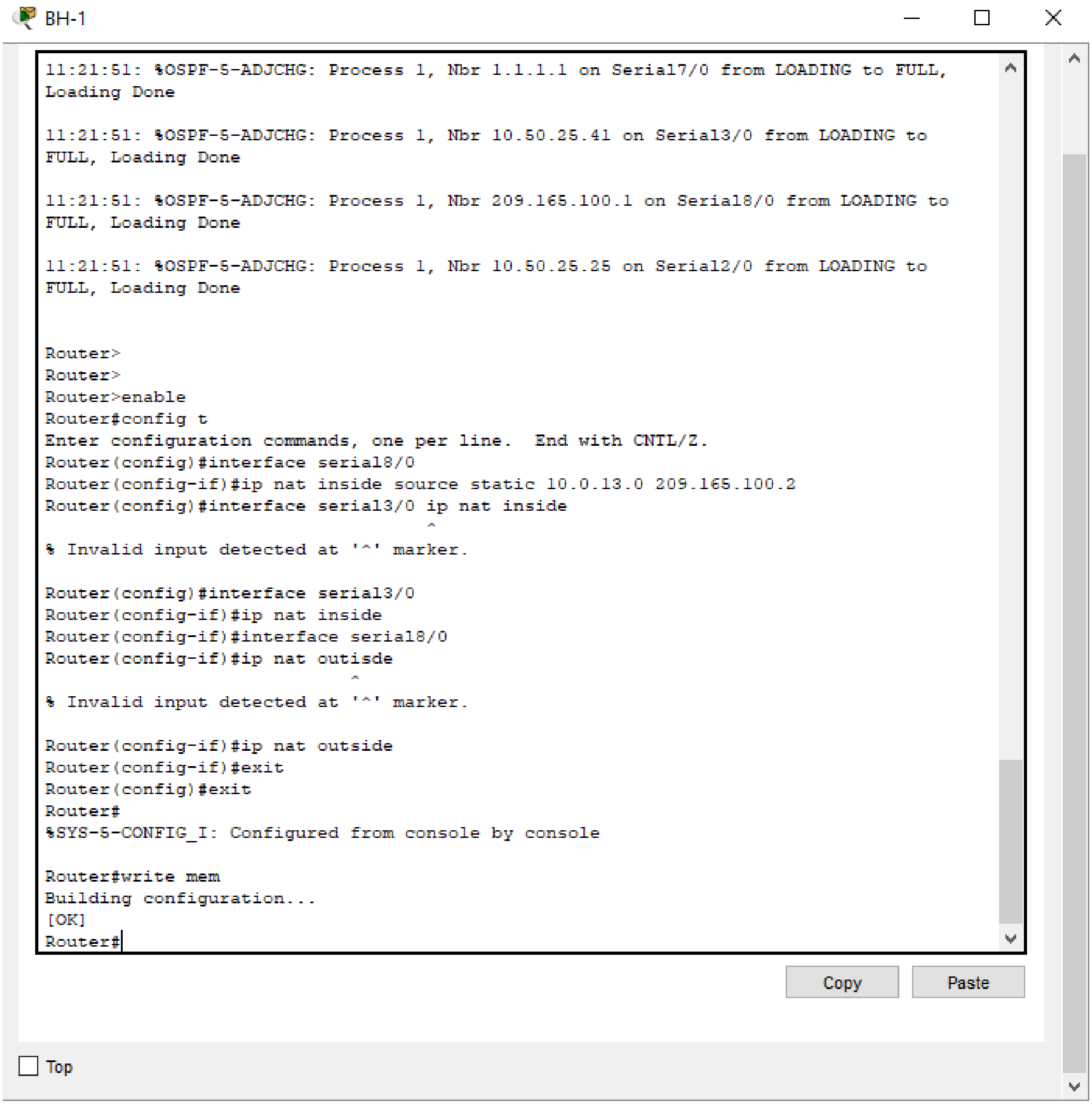
NAT provides the translation of private addresses to public addresses. Please configure static and dynamic NAT for all traffic entering and exiting the company network. (3 marks) Then use the simulation results to elaborate the actions that are involved when an internal host (e.g. Host B6) attempts to send a packet to the external ISP server. (2 marks)

Static NAT:

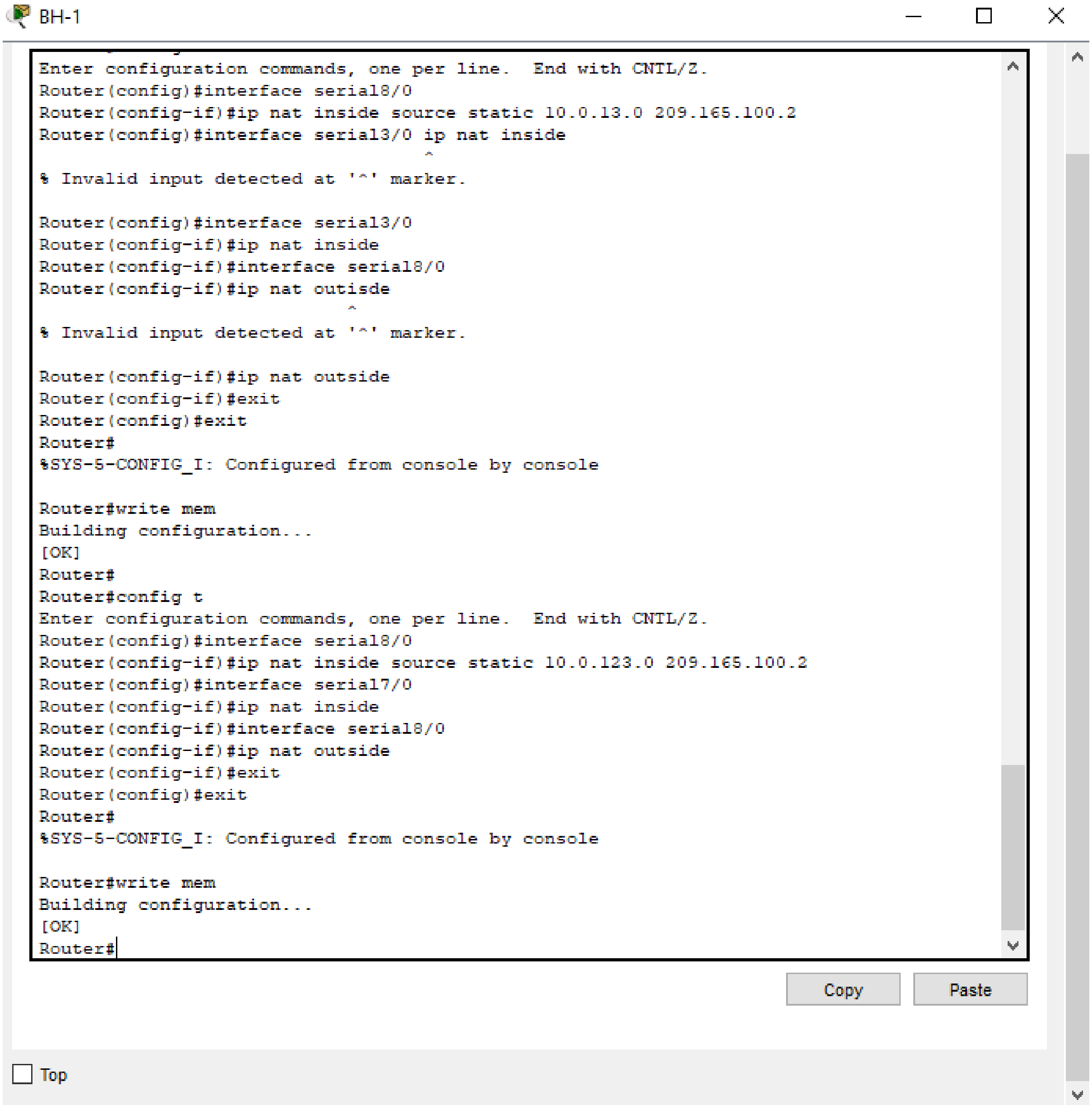
Below is the configuration for a static NAT for network 10.0.12.0/24.



Below is the configuration for a static NAT for network 10.0.13.0/24



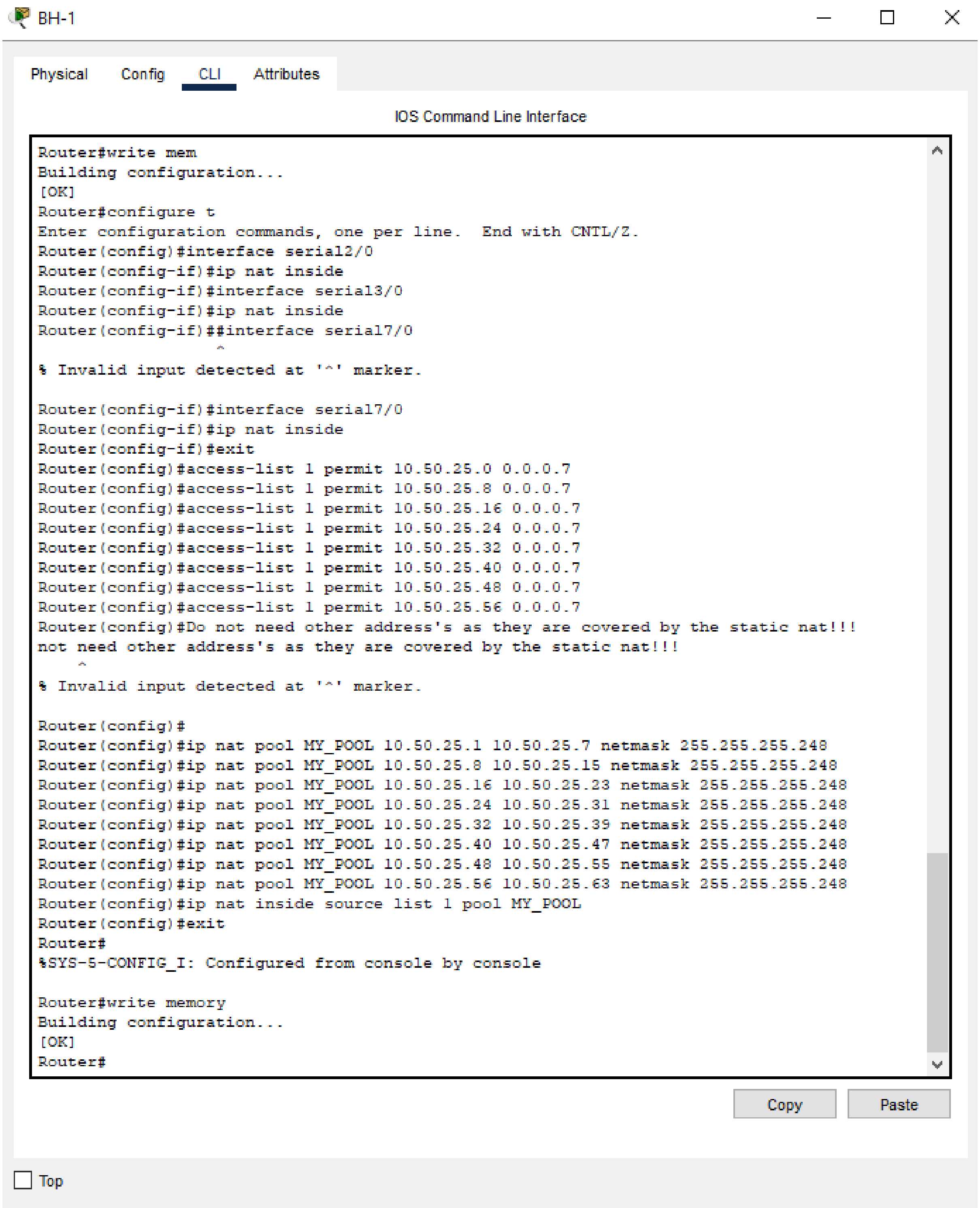
Below is the configuration for a static NAT for network 10.0.123.0/24




```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial8/0
Router(config-if)#ip nat inside source static 10.0.13.0 209.165.100.2
Router(config)#interface serial3/0 ip nat inside
                                    ^
% Invalid input detected at '^' marker.

Router(config)#interface serial3/0
Router(config-if)#ip nat inside
Router(config-if)#interface serial8/0
Router(config-if)#ip nat outisde
                             ^
% Invalid input detected at '^' marker.

Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write mem
Building configuration...
[OK]
Router#
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface serial8/0
Router(config-if)#ip nat inside source static 10.0.123.0 209.165.100.2
Router(config)#interface serial7/0
Router(config-if)#ip nat inside
Router(config-if)#interface serial8/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#write mem
Building configuration...
[OK]
Router#
```

Dynamic NAT:

Below is the configuration of a dynamic NAT for BH-1:



Scenario:

Host B6 (10.50.25.43/29) Sends a Packet:

Host B6 sends a packet to the destination ISP server.

The packet's source IP address is 10.50.25.43 (private IP) and the destination IP address is the ISP server's public IP(200.100.100.1).

Packet Reaches Router BH-1:

Router BH-1 receives the packet from Host B6.

The router checks its NAT configuration.

It finds that there is a NAT translation rule for outgoing traffic.

The router translates the source IP address of the packet from 10.50.25.43/29 (private IP) to a public IP address from the NAT pool (dynamically assigned in this case).

The router updates the packet's source IP address and forwards it towards the destination ISP server.

Packet Reaches ISP Network:

ISP servers receive the packet with the translated public IP address as the source.

Response Packet from ISP Server:

The ISP server sends a response packet to the translated public IP address.

This packet arrives at the router BH-1.

Router BH-1 Translates Destination Address:

Router BH-1 checks its NAT table to find the translation entry for the destination IP address.

If the router has stateful NAT configured, it remembers the original translation and translates the destination IP back to the private IP address of Host B6.

The router updates the destination IP address of the packet and forwards it to Host B6.

Host B6 Receives Response:

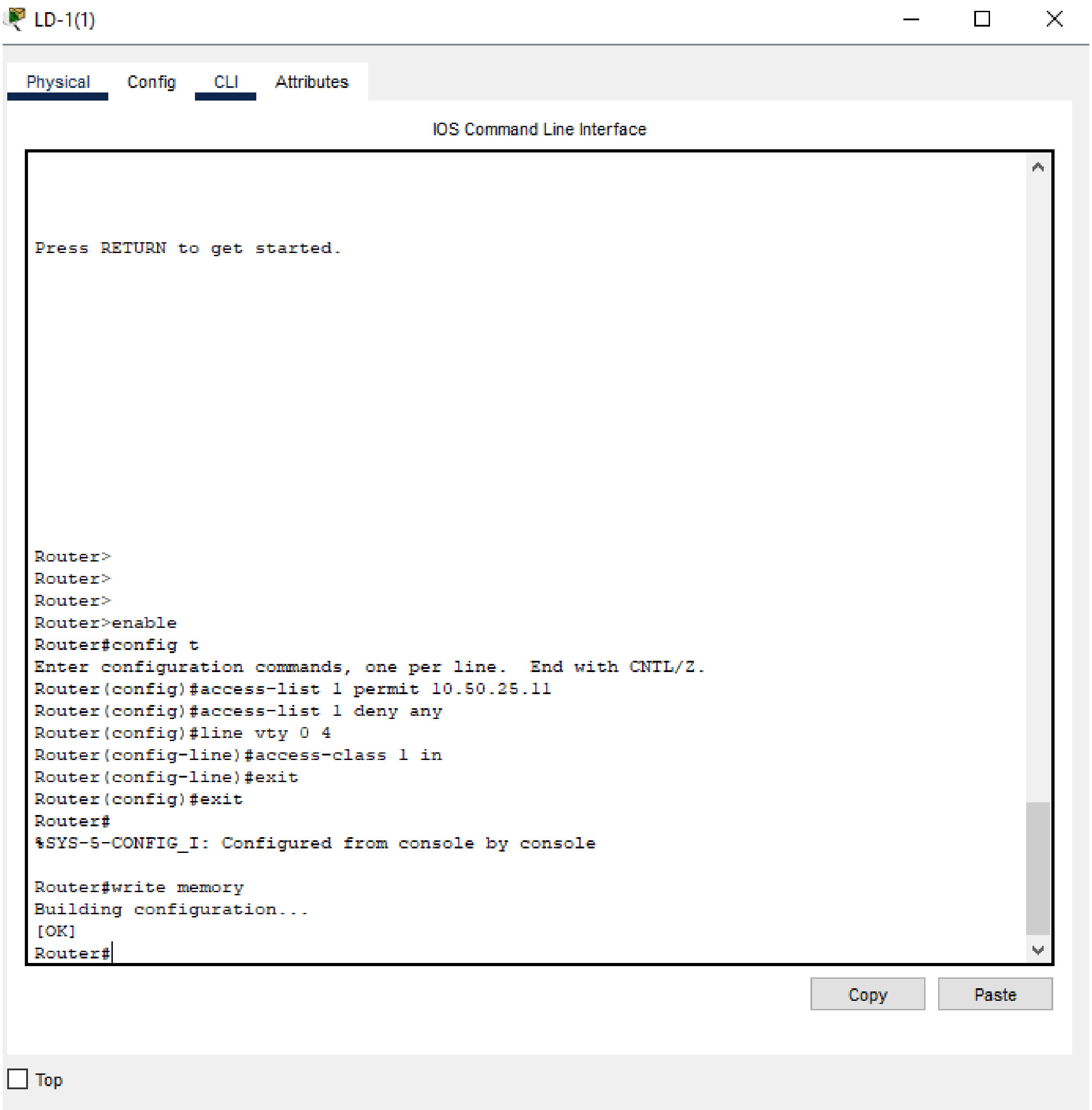
Host B6 receives the response packet from the ISP server.

Since the destination IP address is its own private IP address, Host B6 processes the packet.

This process allows Host B6 to communicate with the external ISP server through Router BH-1 while NAT translates the private IP addresses to public ones for external communication.

Once you have obtained a successful end-to-end connection, for improving the network security, please consider applying ACL to secure the network traffic. Create an ACL, only the Service PC is allowed to remote access to LD-1 and BH-1 router. Please verify and explain how ACL processes packets. (5 marks)

Below is the configuration for LD-1 ACL to prevent remote access to it and BH-1 from all except service PC (10.50.25.11)



Access List Creation:

Access Control Lists are used to control traffic entering or leaving an interface based on the criteria defined within the control list.

In this case, I created an ACL numbered 1 using the access-list command. The permit statement allows traffic the Service PC's IP address while the deny any statement denies all other traffic.

Application to Interface:

Once the ACL is defined, it needs to be applied to the appropriate interface using the access-class command.

In this example, it's applied to the Virtual Terminal lines (line vty 0 4), which control remote access to the router.

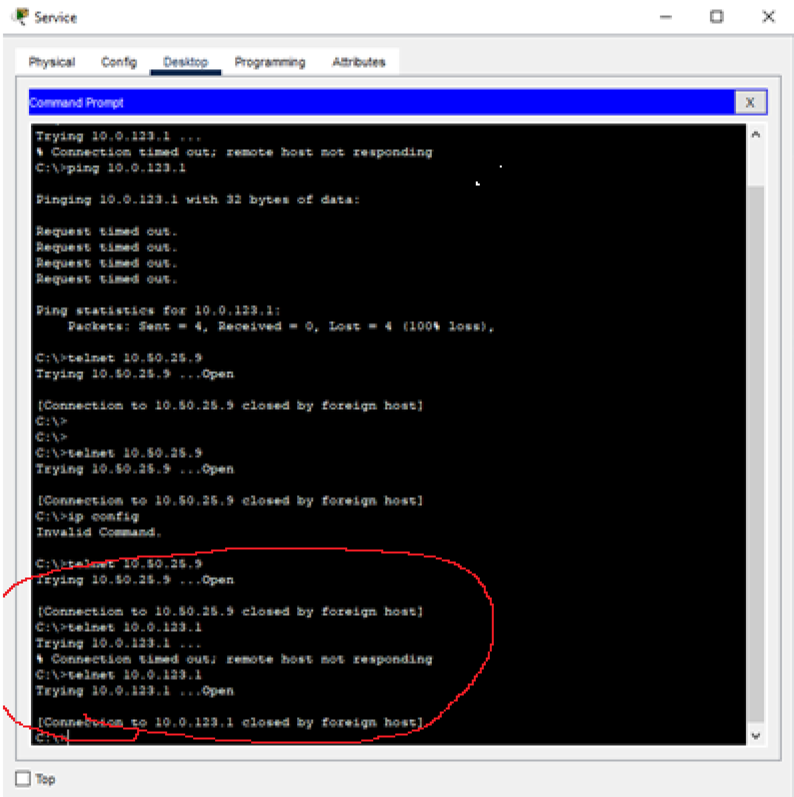
Processing Packets:

When a packet arrives at the router's interface, the router checks the ACL applied to that interface.

If the ACL allows the packet (i.e., the packet matches a permit statement), the router forwards it according to its routing table.

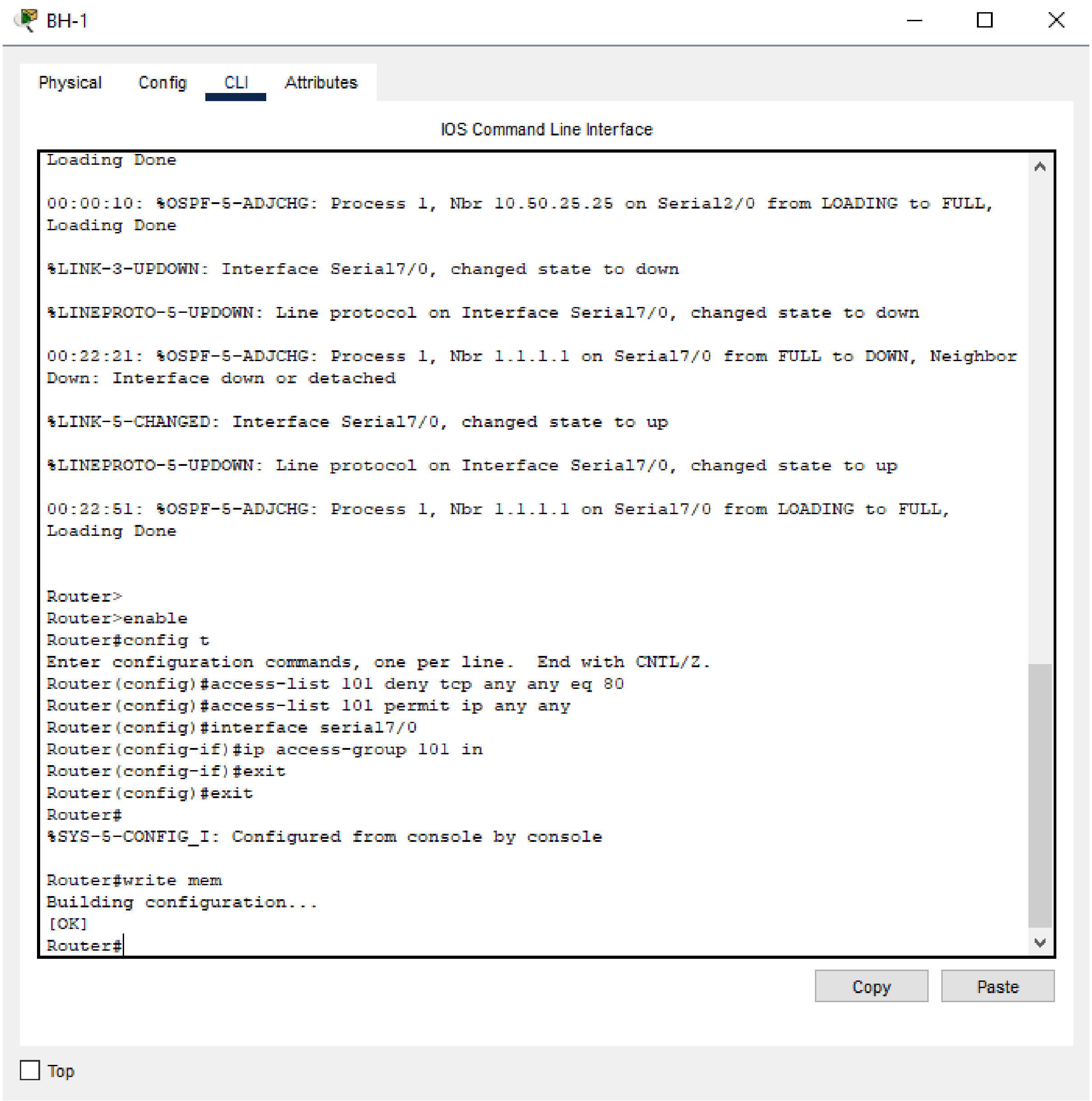
If the ACL denies the packet (i.e., the packet matches a deny statement), the router drops the packet and doesn't process it further.

Below is a capture of a telnet to LD-1 after changing the Ip to be outside the ACL and then back to the ACL specified address.


Service
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Trying 10.0.123.1 ...
% Connection timed out; remote host not responding
C:\>ping 10.0.123.1
Pinging 10.0.123.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.123.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>telnet 10.50.25.9
Trying 10.50.25.9 ...Open
[Connection to 10.50.25.9 closed by foreign host]
C:\>
C:\>
C:\>telnet 10.50.25.9
Trying 10.50.25.9 ...Open
[Connection to 10.50.25.9 closed by foreign host]
C:\>ip config
Invalid Command.
C:\>telnet 10.50.25.9
Trying 10.50.25.9 ...Open
[Connection to 10.50.25.9 closed by foreign host]
C:\>telnet 10.0.123.1
Trying 10.0.123.1 ...
% Connection timed out; remote host not responding
C:\>telnet 10.0.123.1
Trying 10.0.123.1 ...Open
[Connection to 10.0.123.1 closed by foreign host]
C:\>
Top

Create an extended ACL that will deny HTTP traffic from devices in LAN 3, 4, 5, and 6 to the Web Server in LAN1 but allow other traffic to go through. HTTP uses TCP on port 80. Please verify and explain how ACL processes packets. (5 marks)

Below is the ACL configuration for BH-1 that blocks http traffic from LAN's 3,4,5 &6 from accessing the LAN1 web server.



I decided the easiest way to process all LANs getting HTTP traffic blocked was to run an implicit deny on TCP traffic on port 80 (HTTP). This means all TCP packets are denied by default. Following this, the easiest way to let the rest through the ACL was with match conditions. Essentially, the ACL checks the packet to see if it meets the conditions of NOT TCP port 80. If this check comes true, the packet is forwarded. You also need to specify the interface the ACL is applied on – I chose Serial 7 as it connects to the rest of the network, with LAN 1 situated there.

IPsec Report

Introduction

In today's society, network technologies play a crucial and pivotal role in enabling seamless communication and data exchange across various platforms and devices. Among the many of network technologies, my Favorite one and the one I have had most experience with at work is the one I will be studying today: IPsec VPN's, this technology offers unique solutions to address different networking challenges, ranging from securing communication channels to ensuring encrypted transmission. In this report, we delve into the top three most cited research articles related to IPsec technologies in the IEEE Xplore database, aiming to analyse their contributions, implications, and future directions.

Summary of Papers:

"Hardware Architecture of NIST Lightweight Cryptography Applied in IPSec for High-Throughput Low-Latency IoT Networks"

Authors: Zhang, Q., Wang, L., Li, Z.

Publication Year: 2019

This paper delves into the application of IPsec tunnels being implemented into IoT networks with a feasible speed capacity, this research study presents a hardware architecture intended for implementing a more lightweight encryption methodology within IPSec. The authors suggest new and more effective ways of implementing solutions to a common problem of using too much processing power in order to have secure transmission within IoT devices with limited resources. They indicated how well this worked to improve the applicable security of IoT networks while minimising the potential latency and resource overhead that is normally required traditionally. This work establishes the foundation for more feasible IPSec implementations in IoT environments and advances the field of IoT security as a wehole.

"P4sec: Automated Deployment of 802.1X, IPsec, and MACsec Network Protection in P4-Based SDN"

Authors: Li, H., Zhang, Y., Wang, G., Chen, W.

Publication Year: 2022

In this study, SDN's are introduced to P4sec, this is described within the articel as an automated deployment that enables complete network protection, it includes integration to including 802.1X and IPsec. The authors use P4's programmability to automate the deployment of various security mechanisms this was stated to be a direct response of the modern networking world as the requirement to integrate new versatile solutions becomes ever present. They prove the viability and efficiency of P4sec in improving a network security while maintaining a plausible level of performance in SDN environments through comprehensive testing and assesment. This work further pushes the field of network security and offers useful insights into securing SDN infrastructures with programmable and easier to deploy network tools.

"IPsec Cryptographic Algorithm Invocation Considering Performance and Security for SDN Southbound Interface Communication"

Authors: Wang, H., Liu, C., Zhang, S.

Publication Year: 2023

This study looks to improve the implementation of IPsec in SDN environments, this study examines this by comparing the security and performance consequences of applying ipsec encryption to interface communication. According to pre-determined network conditions and security requirements, the writers of the articel suggests an intelligent algorithm selection that dynamically modifies encryption algorithms based upon the systems needs and use case this in turns means prioritising speed in high network usage times and then security when off peak. They show the feasibility of their process in maximising the trade-off between security and performance in SDN communications with a series of comprehensive simulations and experiments.

Conclusion:

The research articles discussed contribute to advancing our understanding of IPsec technologies when applied in modern networking environments with performance and security constraints in mind. They highlight the importance of ensuring network security whilst maximising the performance of our networks in both speed and efficiency.

The studies hihglight the importance of striking a balance between security requirements and performance considerations in network deployments within both corporate applications and IoT environments too.

They provide valuable insights into the challenges and opportunities associated with integrating traditional encryption networking protocols with emerging technologies like SDN and cloud computing emphasising the need for continuous innovation and optimization to meet the evolving demands of modern networking environments.

Using exploration and optimisation techniques to mitigate performance overhead in IPsec VPN and SDN's whilst considering real-world deployment scenarios and dynamic network conditions that will allow for greater networking capacity and efficiency in the future meaning a greater more interconnected society all done more securely and more effectively.

References:

Zhang, Q., Wang, L., & Li, Z. (2019). Hardware architecture of NIST lightweight cryptography applied in IPSec for high-throughput low-latency IoT networks. IEEE Transactions on Network and Service Management. URL: https://ieeexplore.ieee.org/document/10224261

Li, H., Zhang, Y., Wang, G., & Chen, W. (2022). P4sec: Automated deployment of 802.1X, IPsec, and MACsec network protection in P4-based SDN. IEEE Transactions on Network and Service Management. URL: https://ieeexplore.ieee.org/document/10144756

Wang, H., Liu, C., & Zhang, S. (2023). IPsec cryptographic algorithm invocation considering performance and security for SDN southbound interface communication. IEEE Transactions on Network and Service Management. URL: https://ieeexplore.ieee.org/document/9212388