

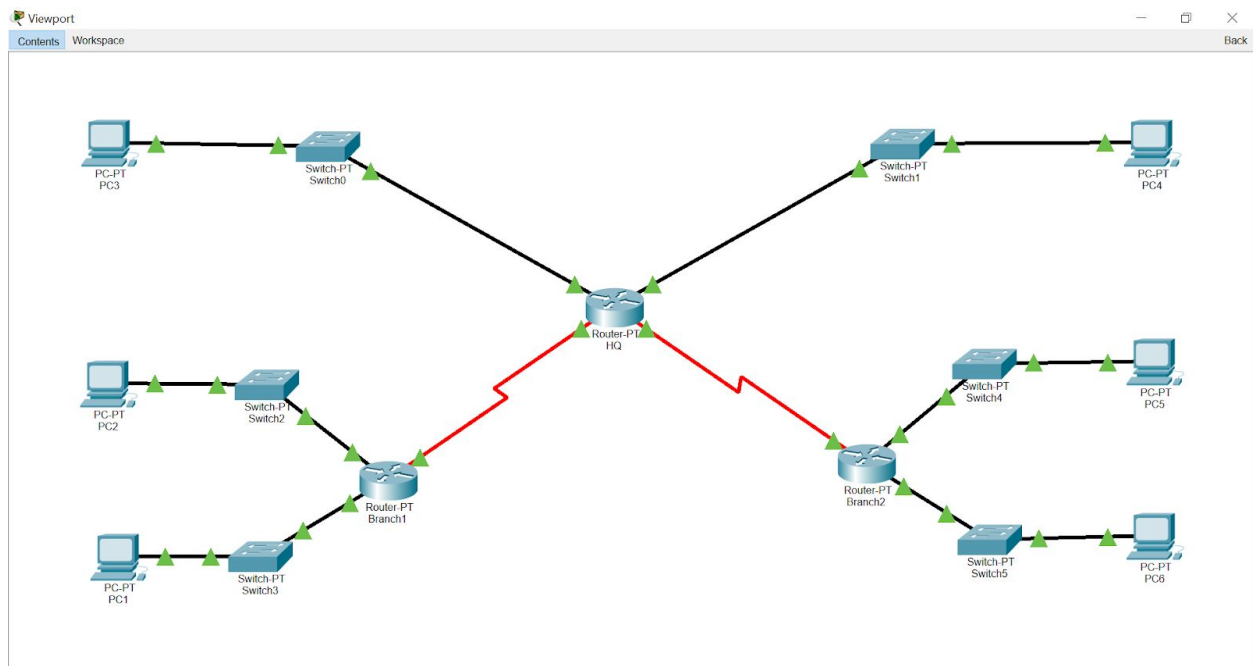
IT352: Information Assurance and Security

Lab Program 1

Name: Chinmayi C. Ramakrishna
Roll No.: 181IT113

Date of Submission: 27th Jan, 2021

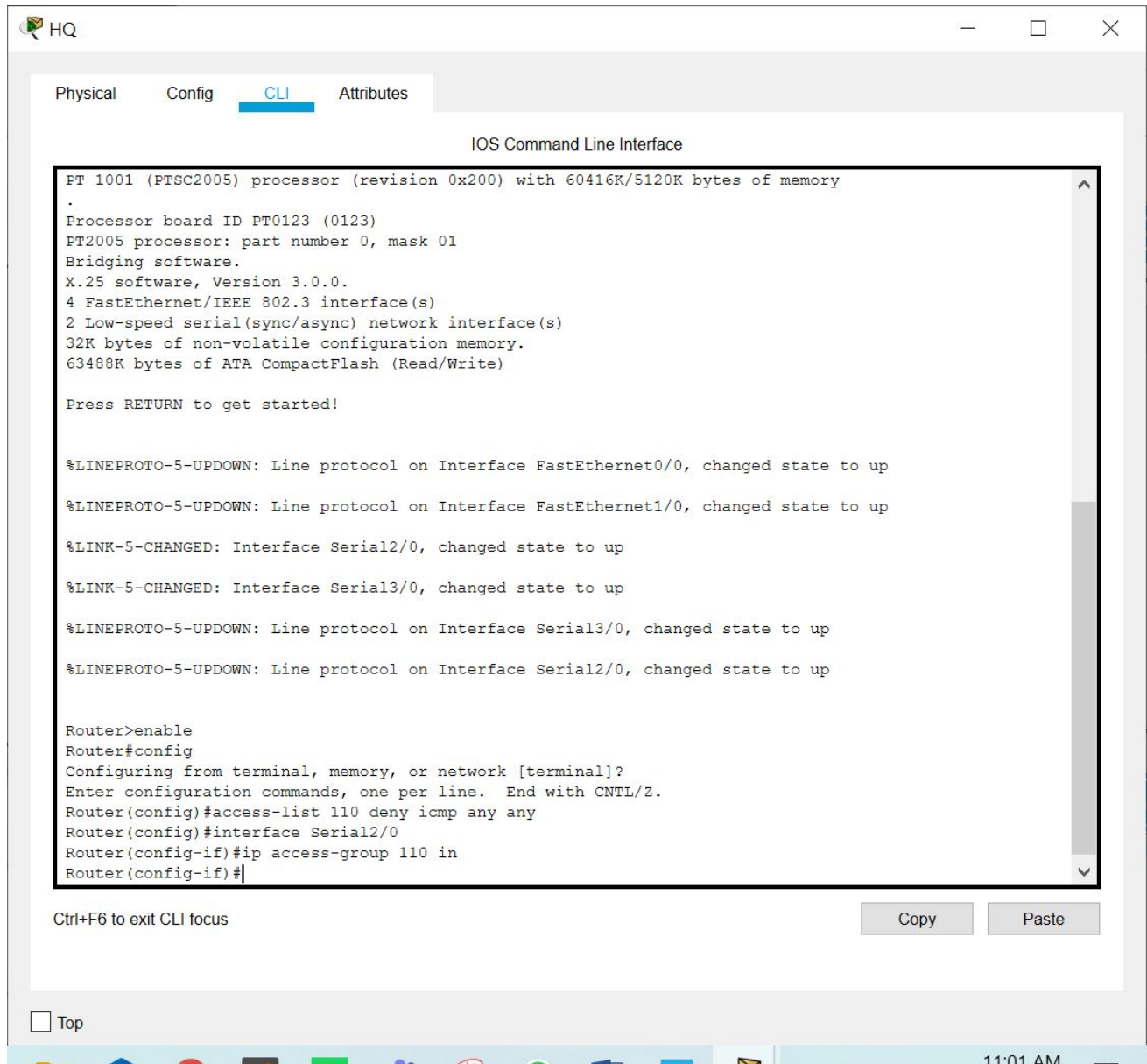
Topology



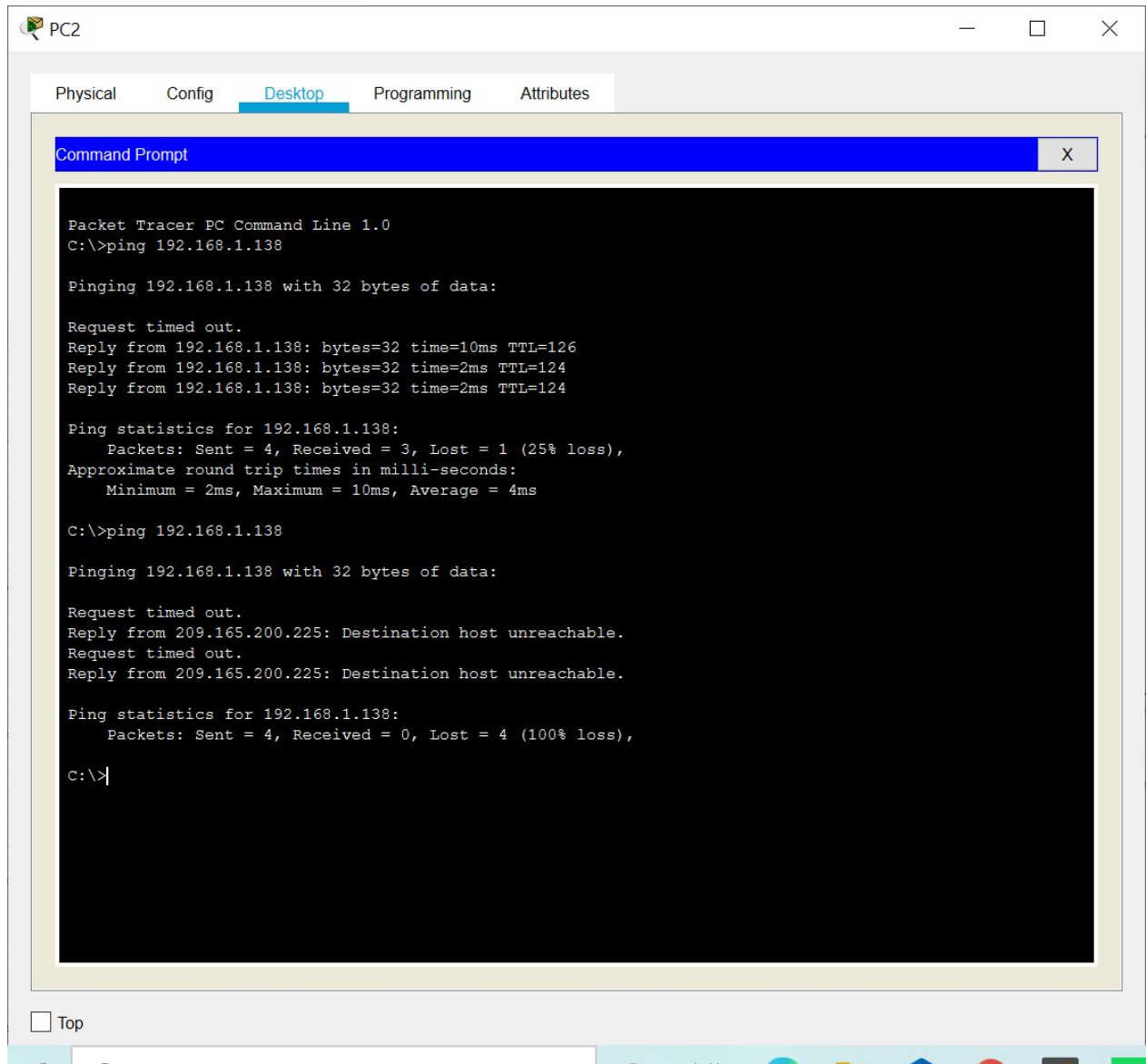
The topology consists of three routers separating traffic to 6 PCs. Firewall policies can be applied at each router to restrict traffic to each one of the network. Different firewall policies are independently applied at each router to understand how traffic is restricted in a network.

Test Case 1

HQ Router Firewall Policy: Blocks all incoming ICMP Echo requests.

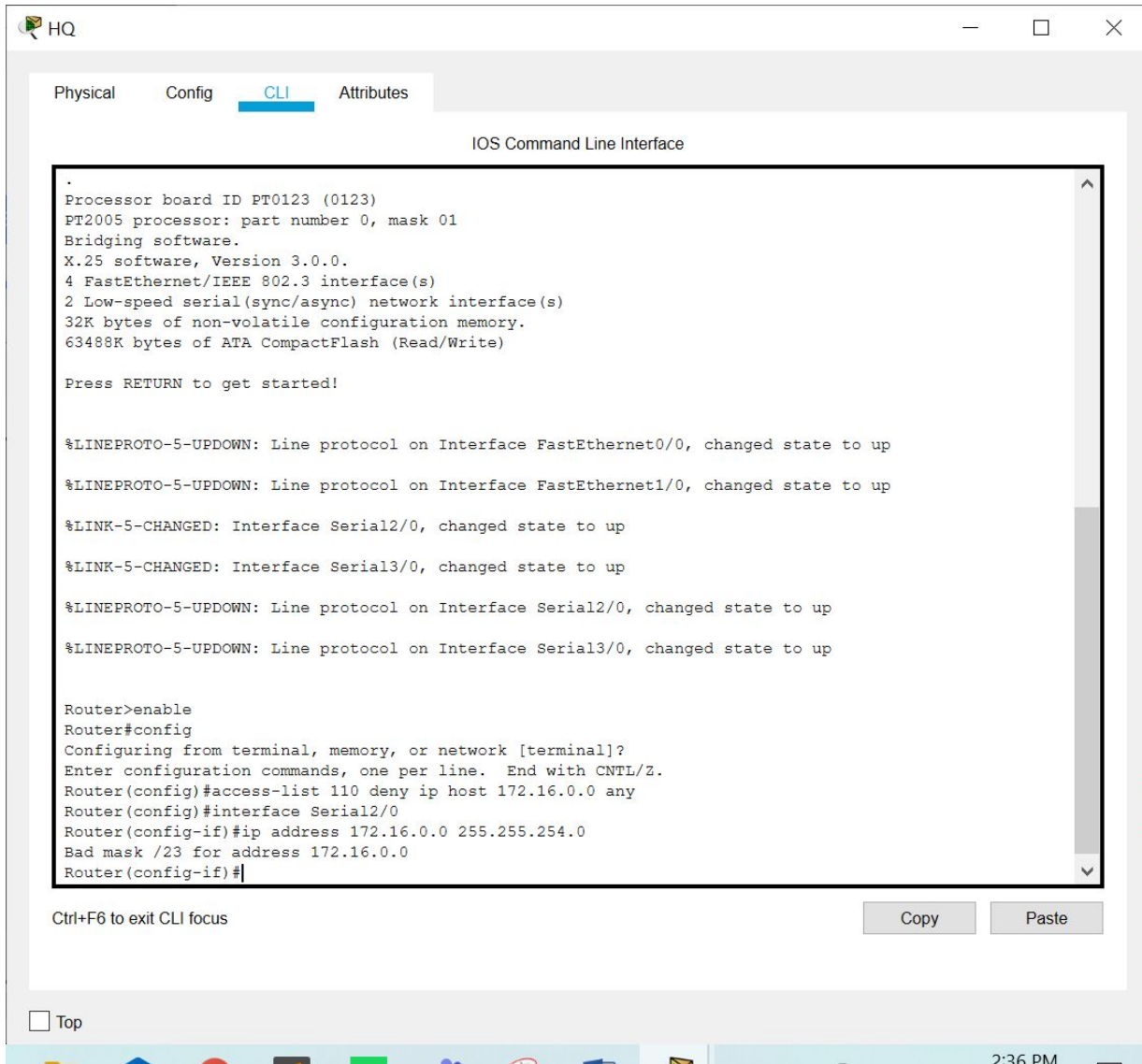


Before and after firewall policy: The traffic from PC2 is restricted by HQ Router.



Test Case 2

HQ Router Firewall Policy: Blocks any traffic incoming coming from 172.16.0.0/23 network.



The screenshot shows a web-based interface for a router named 'HQ'. The 'CLI' tab is selected, displaying the 'IOS Command Line Interface'. The interface shows the following text:

```
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

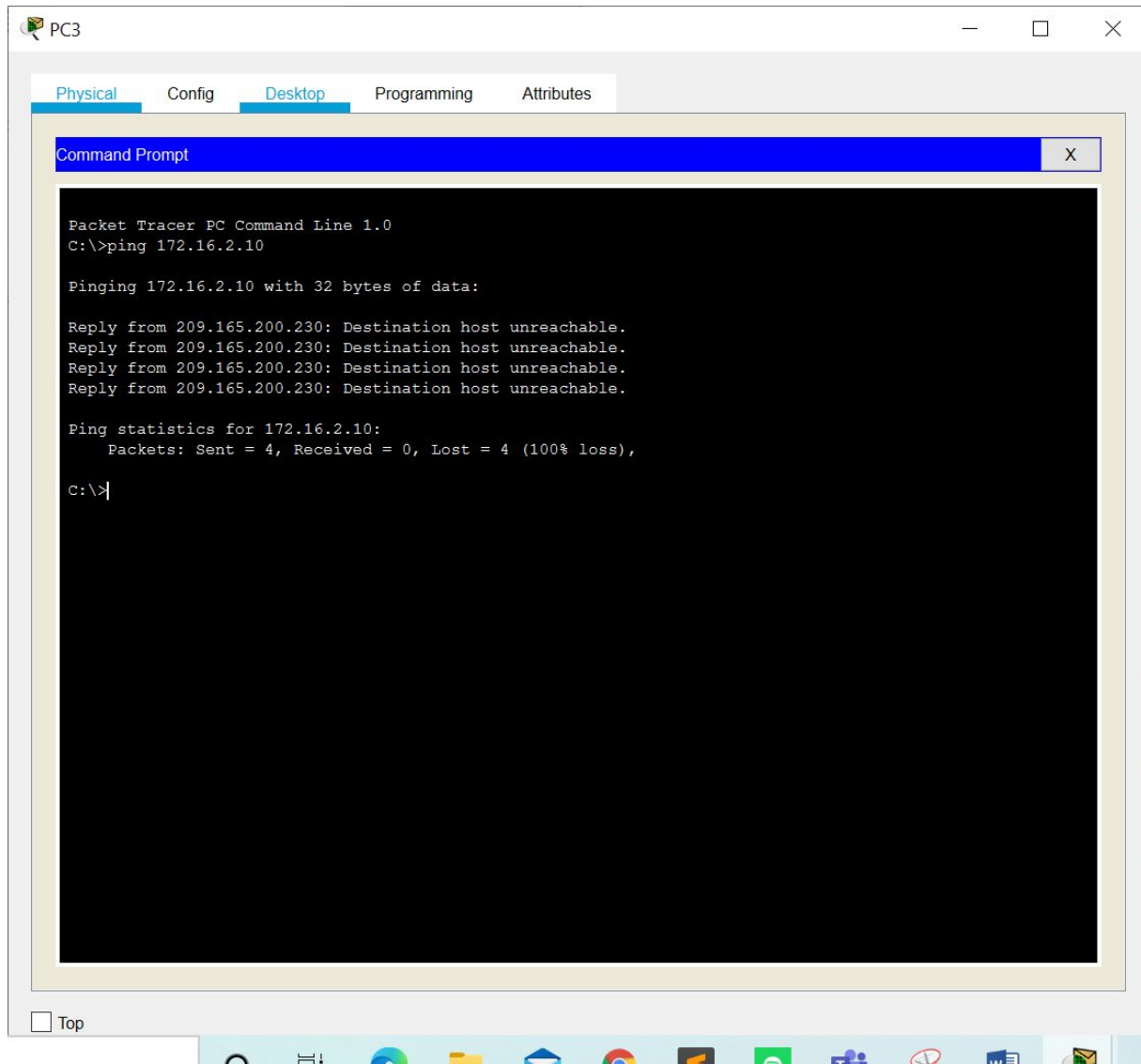
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINK-5-CHANGED: Interface Serial3/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

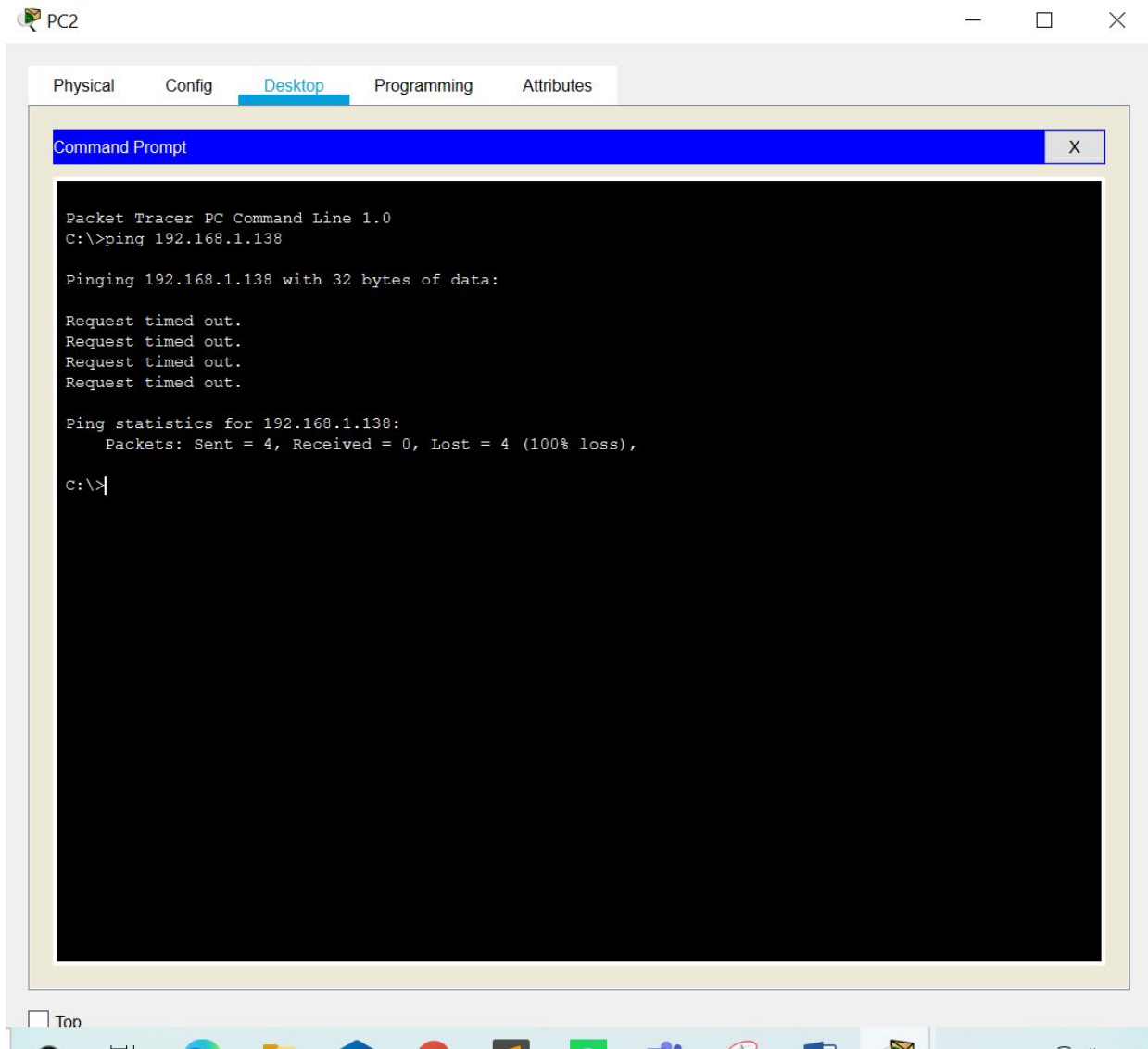
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 deny ip host 172.16.0.0 any
Router(config)#interface Serial2/0
Router(config-if)#ip address 172.16.0.0 255.255.254.0
Bad mask /23 for address 172.16.0.0
Router(config-if)#
```

Below the CLI window, there is a message 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'. At the bottom left, there is a 'Top' button. The bottom right corner of the window shows the time '2:36 PM'.

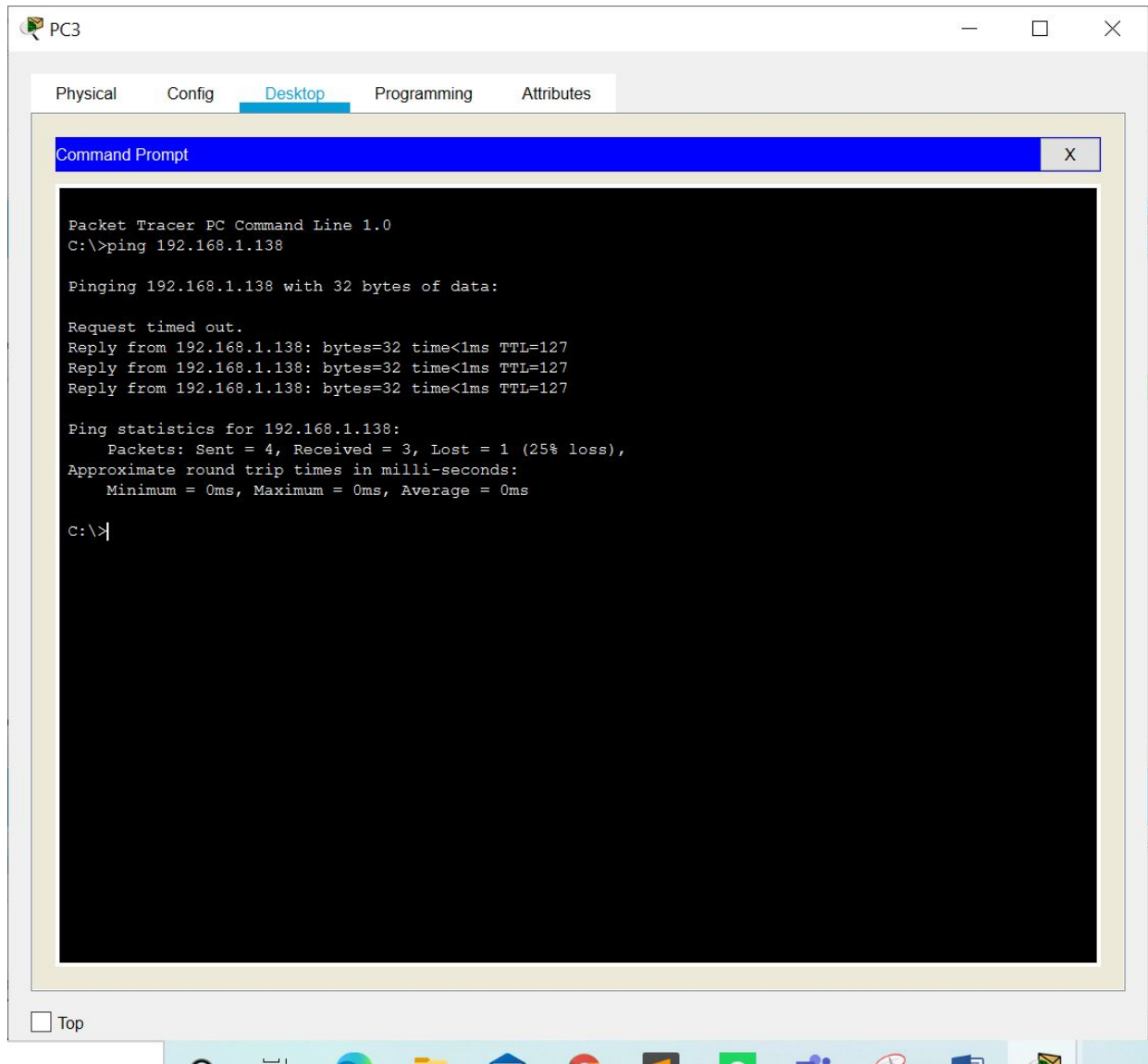
PC3 is unable to send the message to 172.16.0.0/23 network.



PC2 is unable to send message to an external network due to the restriction at HQ Router.



PC3 can send the message to the network 192.168.1.0/25. HQ Router has no firewall policy against network 192.168.1.0/25.



The screenshot shows a Packet Tracer interface for PC3. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 192.168.1.138. The output indicates that the ping was successful, with 3 out of 4 packets received and a 25% loss. The round trip times are all 0ms.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:

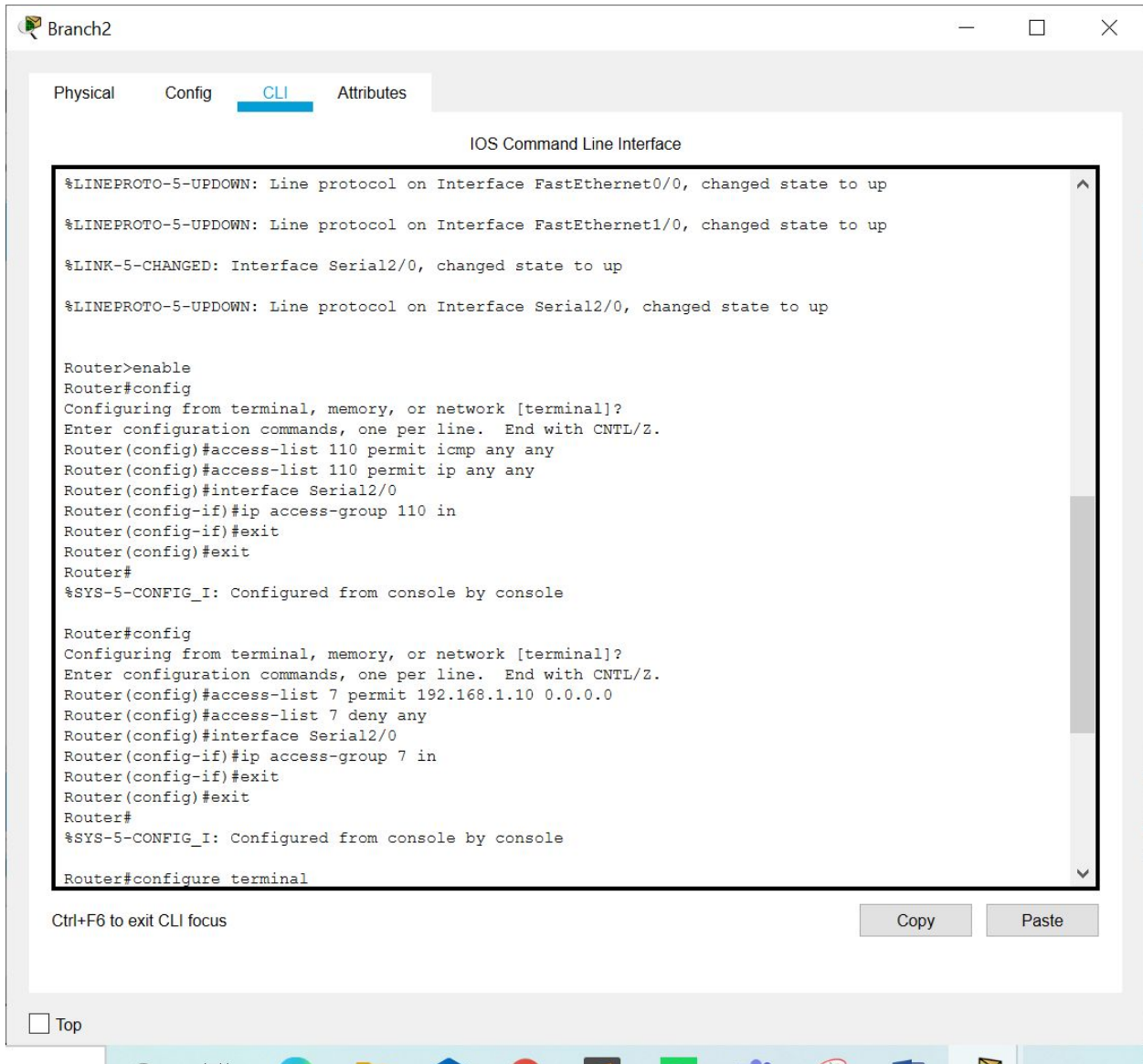
Request timed out.
Reply from 192.168.1.138: bytes=32 time<1ms TTL=127
Reply from 192.168.1.138: bytes=32 time<1ms TTL=127
Reply from 192.168.1.138: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.138:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Test Case 3:

Branch2 Router Firewall Policy: Allow any traffic incoming coming from PC3 and rest of the traffic is blocked.



The screenshot shows a web-based interface for a Branch2 router. The 'CLI' tab is selected, displaying the IOS Command Line Interface. The interface shows the following commands and output:

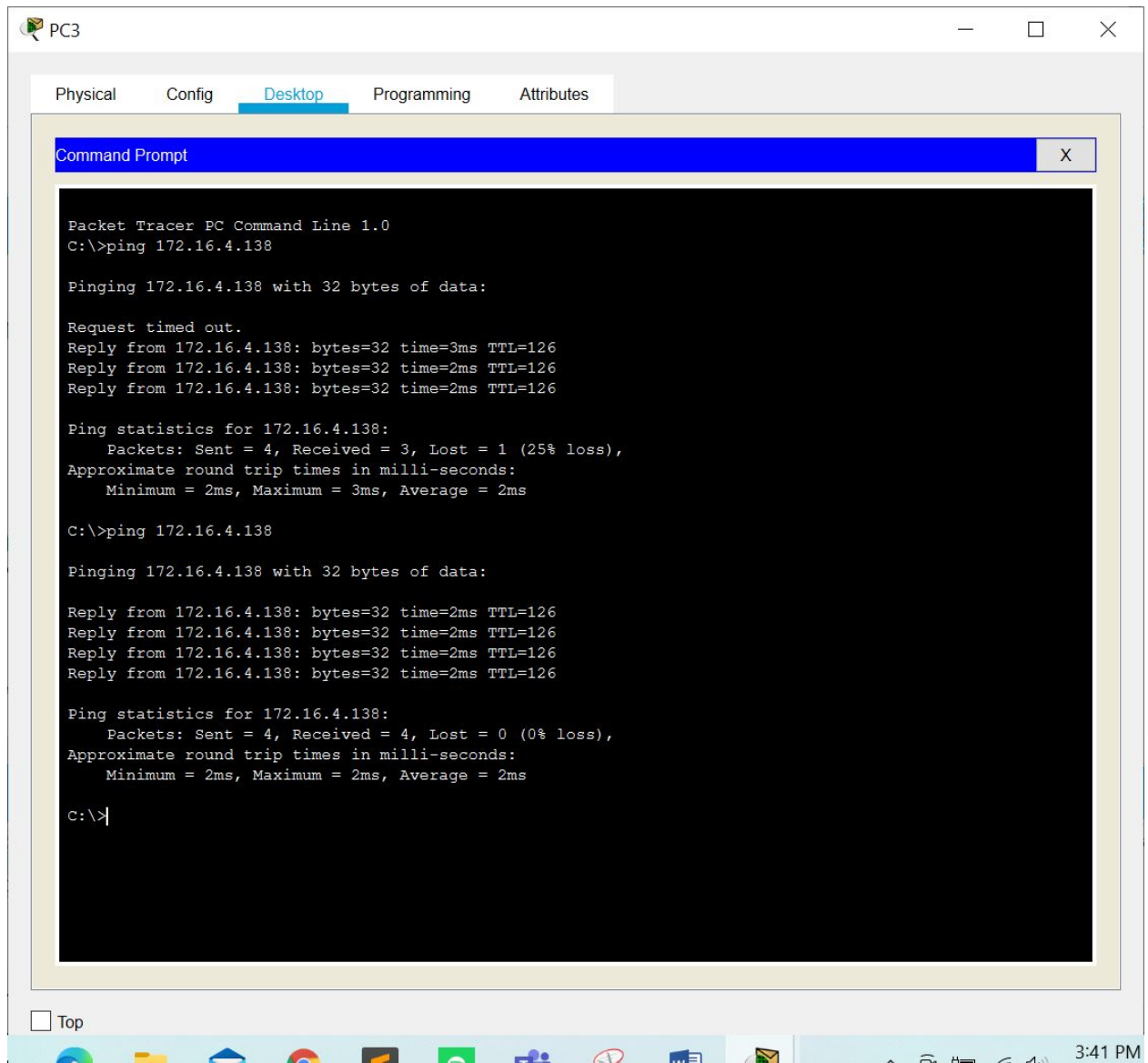
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 110 permit icmp any any
Router(config)#access-list 110 permit ip any any
Router(config)#interface Serial2/0
Router(config-if)#ip access-group 110 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 7 permit 192.168.1.10 0.0.0.0
Router(config)#access-list 7 deny any
Router(config)#interface Serial2/0
Router(config-if)#ip access-group 7 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

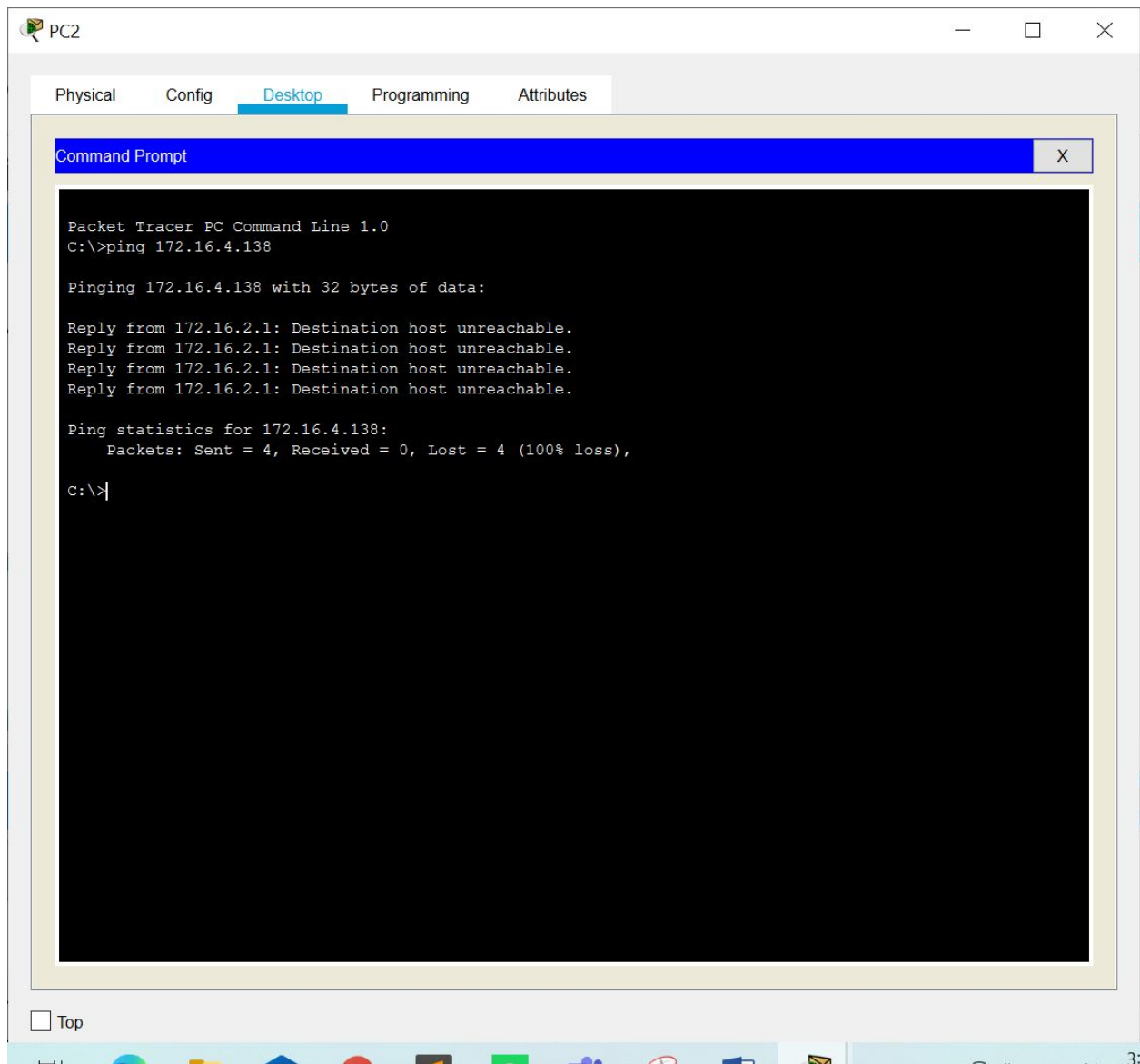
Router#configure terminal
```

At the bottom of the CLI window, there is a prompt 'Ctrl+F6 to exit CLI focus' and two buttons: 'Copy' and 'Paste'. A 'Top' button is located at the bottom left of the interface.

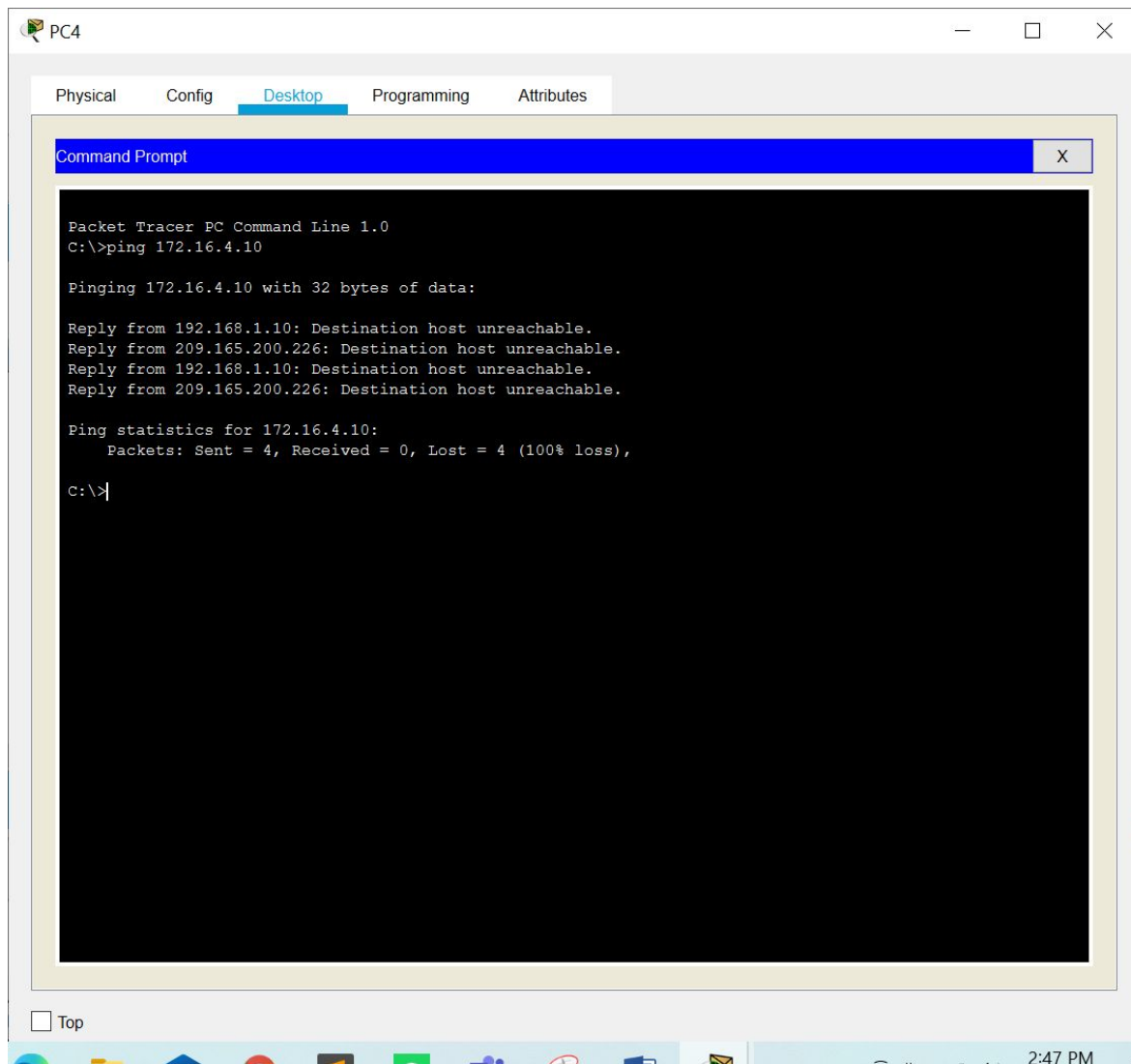
PC3 can send a message to the network at Branch1 Router.



PC2 cannot send any message to the network at the Branch1 Router due to firewall policy at the router.



PC4 cannot send any message to the network at the Branch1 Router due to firewall policy at the router.



The screenshot shows a Packet Tracer PC4 desktop environment. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The command prompt shows the execution of a ping command to 172.16.4.10, which fails with 100% loss. The taskbar at the bottom includes a 'Top' button and a system clock showing 2:47 PM.

```
PC4
Physical Config Desktop Programming Attributes
Command Prompt X
Packet Tracer PC Command Line 1.0
C:\>ping 172.16.4.10

Pinging 172.16.4.10 with 32 bytes of data:

Reply from 192.168.1.10: Destination host unreachable.
Reply from 209.165.200.226: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 209.165.200.226: Destination host unreachable.

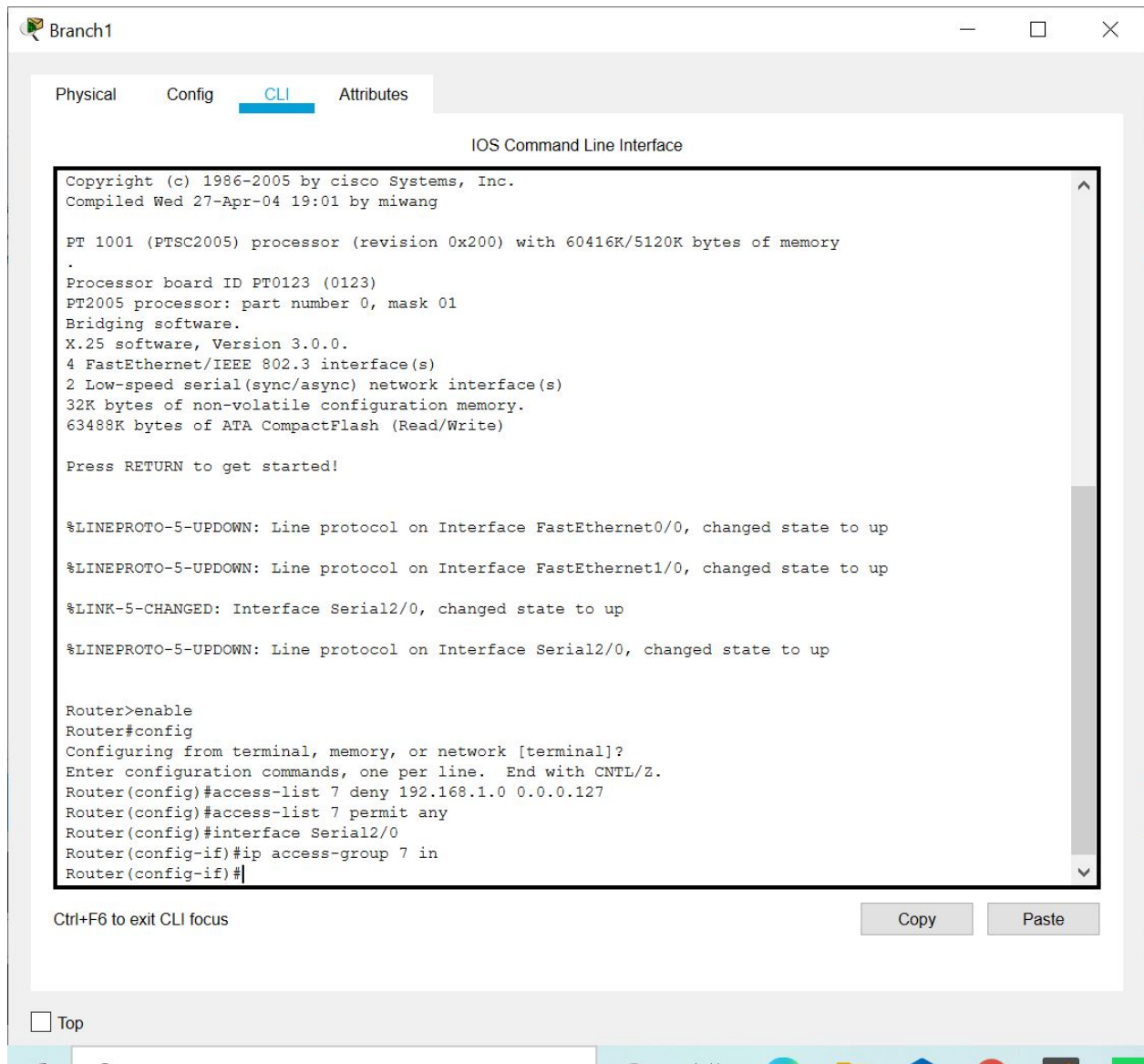
Ping statistics for 172.16.4.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

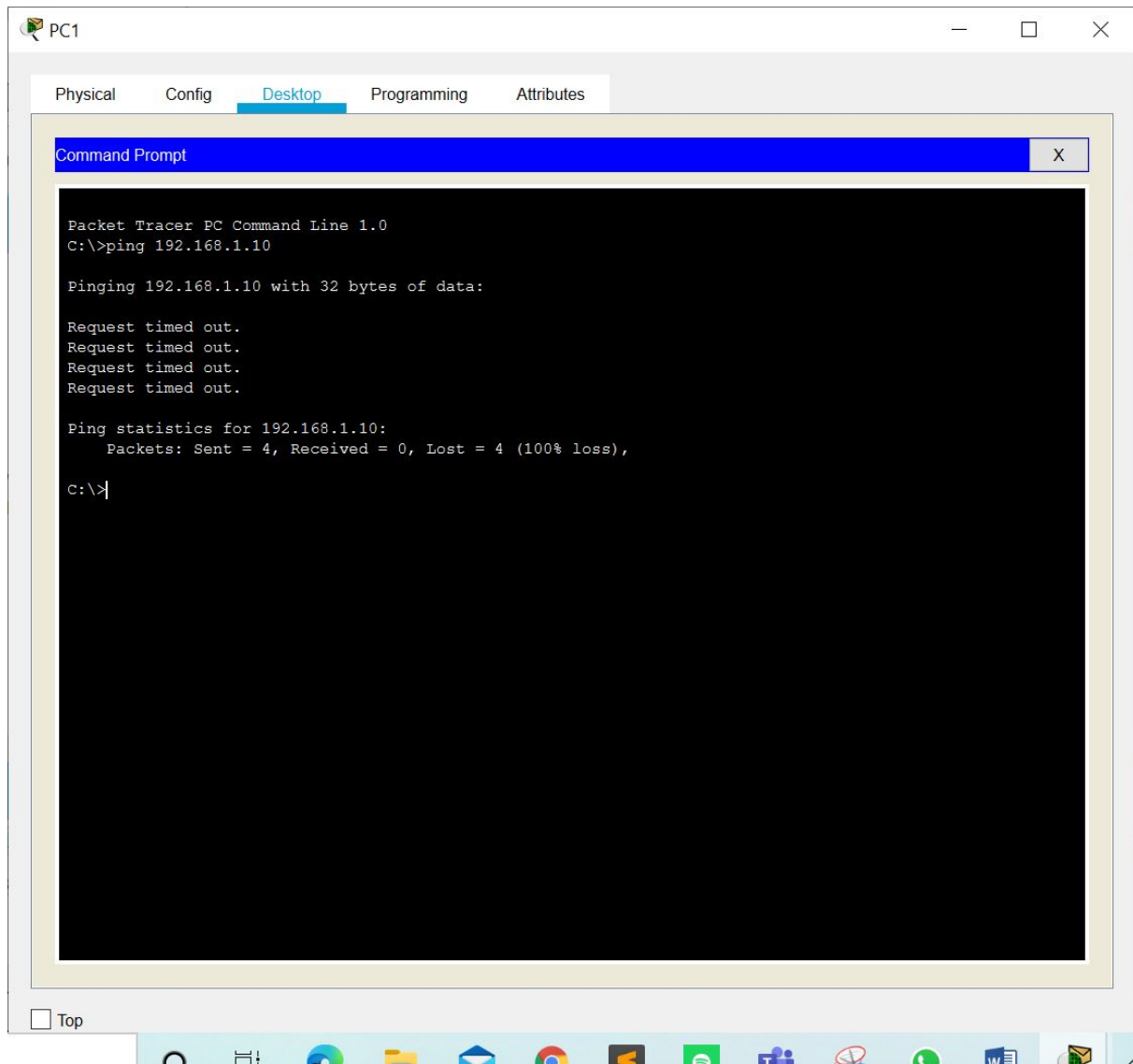
☐ Top 2:47 PM

Test Case 4

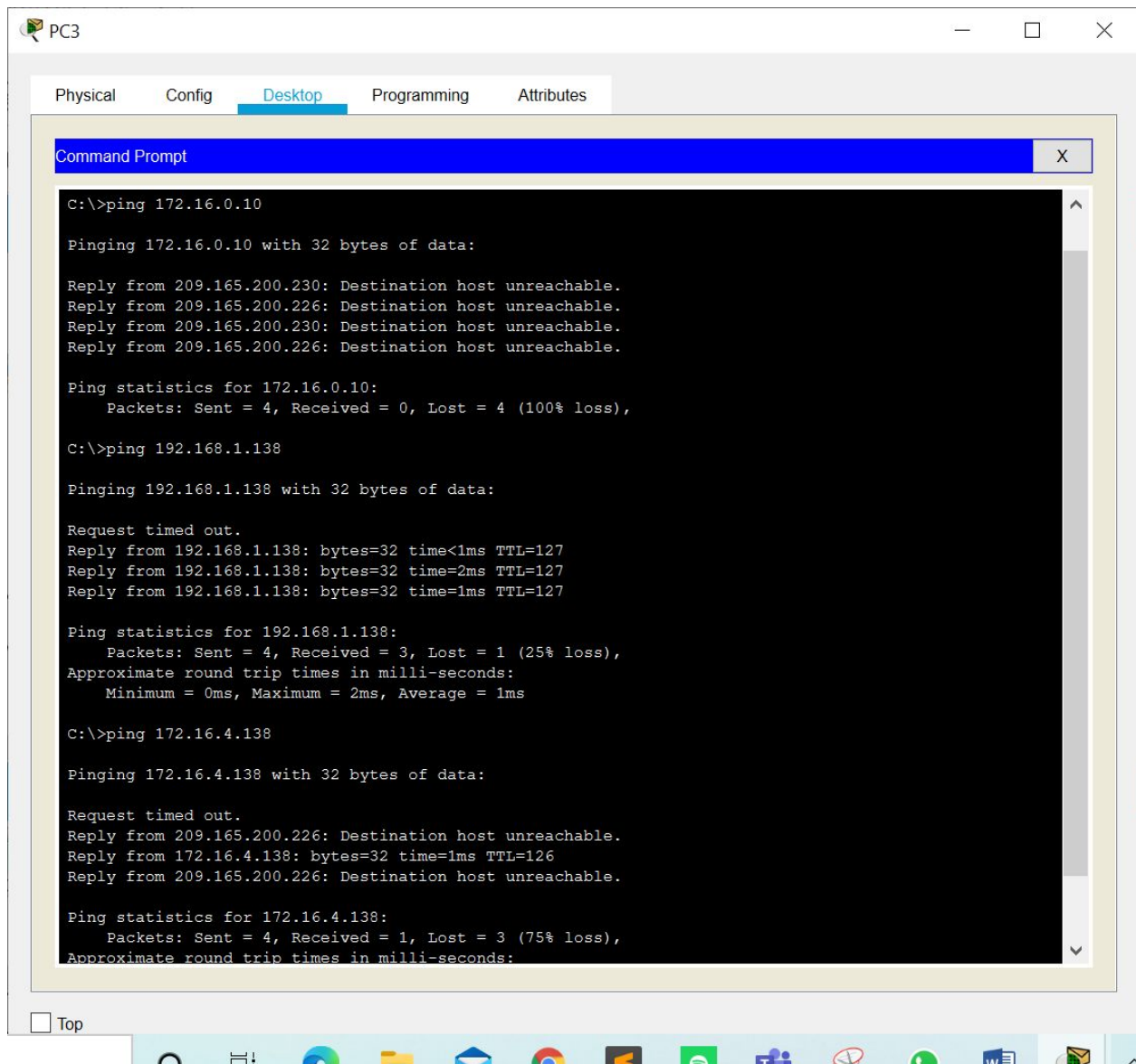
Branch1 Router Firewall Policy: Block any traffic incoming coming from any system belong to 192.168.1.0/25 network



PC1 -> PC3



PC3 -> PC1 and PC3 -> PC4



The screenshot shows a window titled "PC3" with tabs for "Physical", "Config", "Desktop" (selected), "Programming", and "Attributes". Inside the "Desktop" tab is a "Command Prompt" window. The Command Prompt displays the results of three ping commands executed from the C:\ directory.

```
C:\>ping 172.16.0.10

Pinging 172.16.0.10 with 32 bytes of data:

Reply from 209.165.200.230: Destination host unreachable.
Reply from 209.165.200.226: Destination host unreachable.
Reply from 209.165.200.230: Destination host unreachable.
Reply from 209.165.200.226: Destination host unreachable.

Ping statistics for 172.16.0.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.138

Pinging 192.168.1.138 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.138: bytes=32 time<1ms TTL=127
Reply from 192.168.1.138: bytes=32 time=2ms TTL=127
Reply from 192.168.1.138: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.1.138:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>ping 172.16.4.138

Pinging 172.16.4.138 with 32 bytes of data:

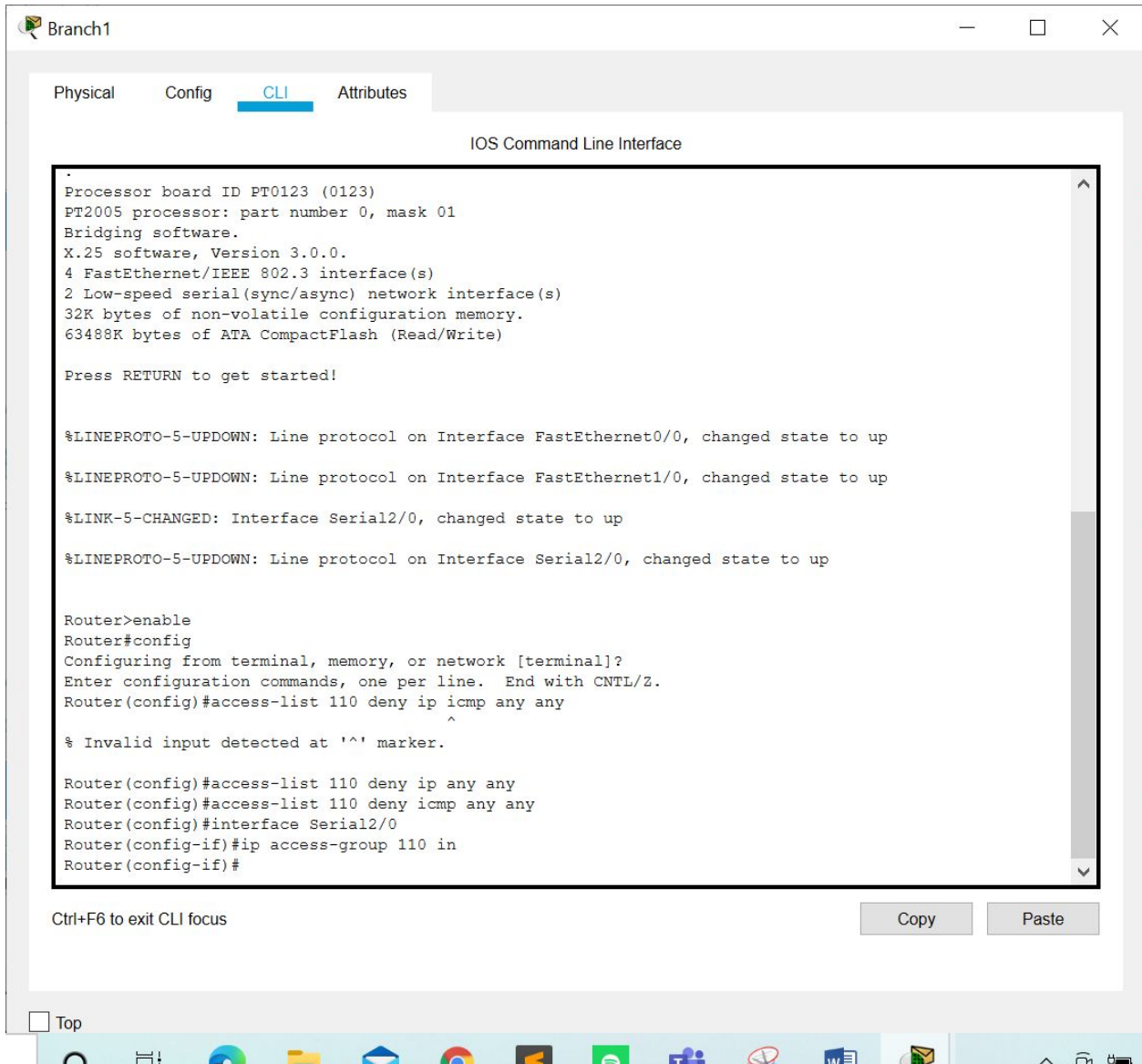
Request timed out.
Reply from 209.165.200.226: Destination host unreachable.
Reply from 172.16.4.138: bytes=32 time=1ms TTL=126
Reply from 209.165.200.226: Destination host unreachable.

Ping statistics for 172.16.4.138:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
```

At the bottom of the PC3 window, there is a "Top" button and a taskbar with various application icons.

Test Case 5:

Branch1 Router Firewall Policy: Block any traffic incoming coming from any network.



The screenshot shows a web-based interface for a Branch1 router. The 'CLI' tab is selected, displaying the IOS Command Line Interface. The interface shows system information, status messages, and the configuration of an access list to block incoming traffic.

```
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINK-5-CHANGED: Interface Serial2/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 110 deny ip icmp any any
^
% Invalid input detected at '^' marker.

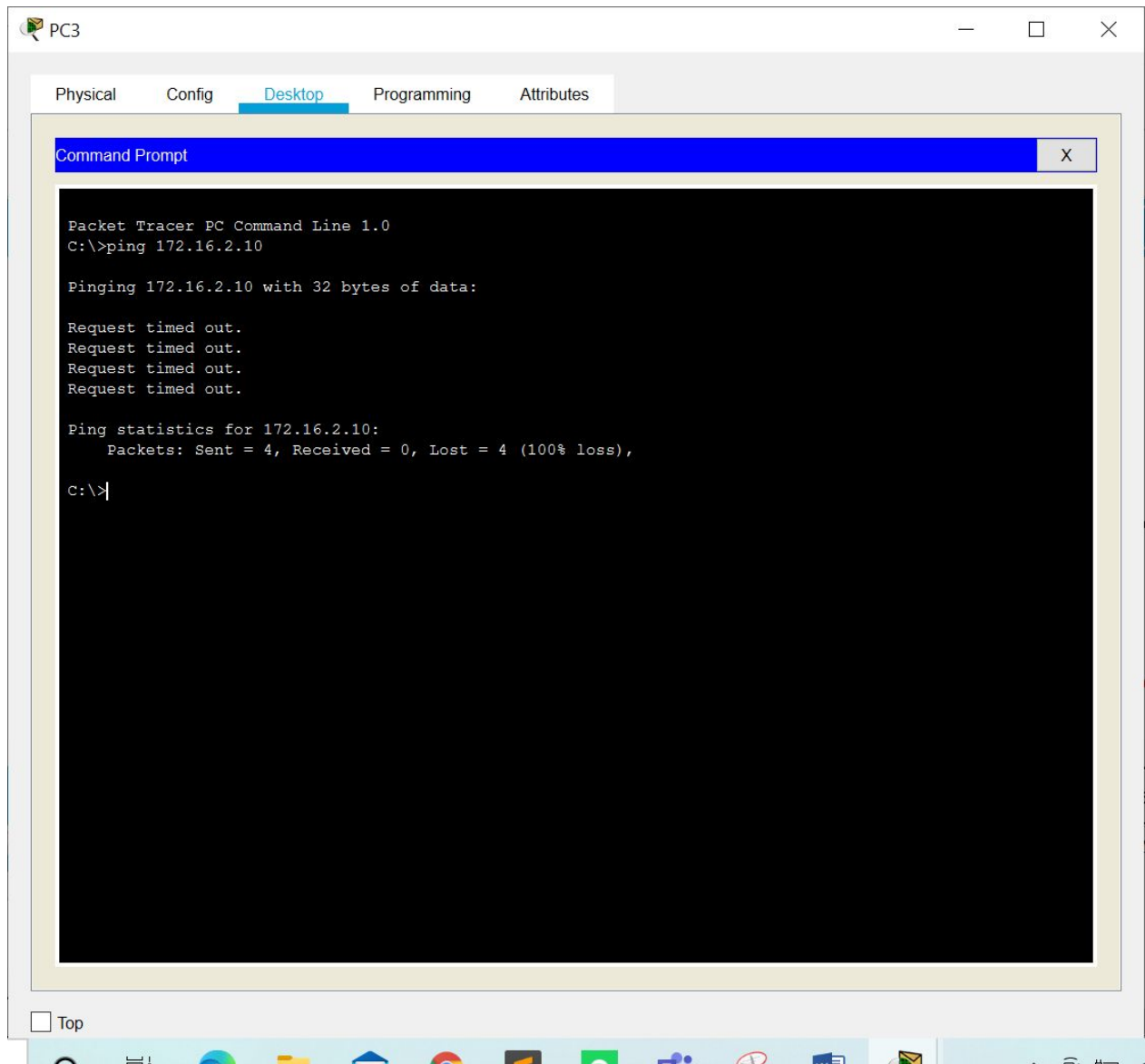
Router(config)#access-list 110 deny ip any any
Router(config)#access-list 110 deny icmp any any
Router(config)#interface Serial2/0
Router(config-if)#ip access-group 110 in
Router(config-if)#
```

Ctrl+F6 to exit CLI focus

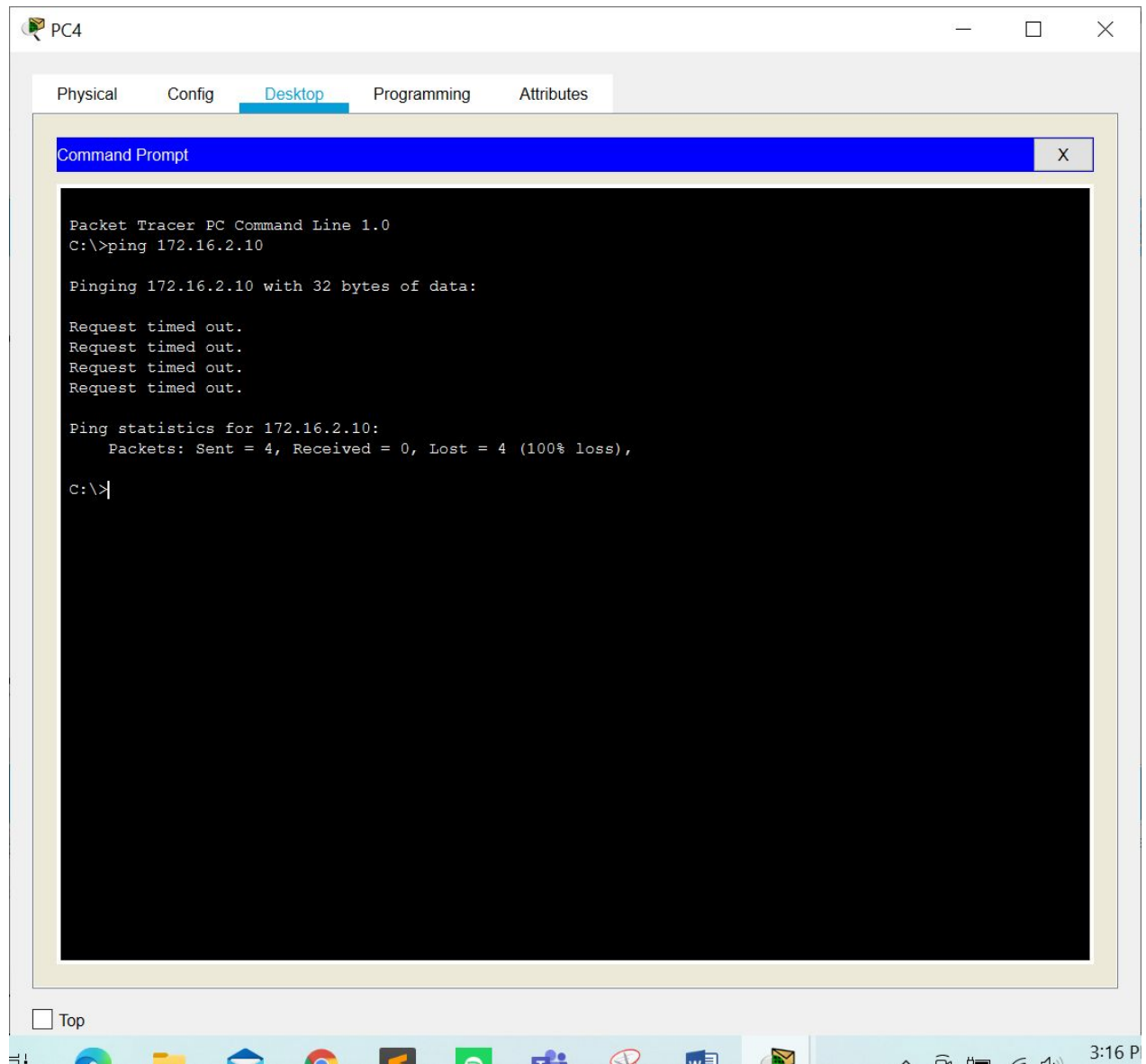
Copy Paste

Top

Branch1 Router blocks incoming traffic from PC3.



Branch1 Router blocks incoming traffic from PC4.



Branch1 Router blocks incoming traffic from PC5.

