Nama : Yusufa Haidar

Kelas : SIB-3C

Absen : 21

Packet Tracer - Use Diagnostic Commands

Objectives

Part 1: Gather End User Device Settings

Part 2: Gather Information about Network Devices

Part 3: Diagnose Connectivity Issues

Background / Scenario

In this Packet Tracer (PT) activity, you will use various commands to gather device information and troubleshoot device configuration and connectivity issues. Device information includes IP address, default gateway, and DNS server settings. These settings are critical to enable a device to communicate on networks and connect to the internet.

Instructions

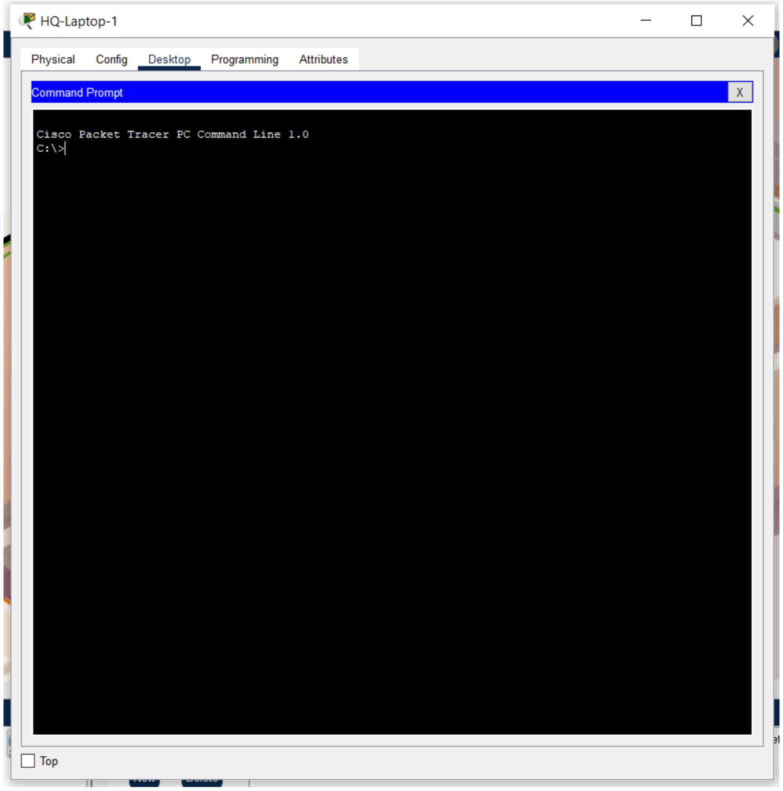
Part 1: Gather End User Device Settings

In this part, you will document the IP address settings for end devices.

Step 1: Document the IP address settings for HQ-Laptop-1.

a. The activity opens in the **HQ** cluster. The **Wiring Closet** is the tall, black chassis in the bottom left corner of the first floor. Locate all the devices on the first floor: PCs **1-1**, **1-2**, **1-3**, and **1-4**; printer **FL-1P**; and **HQ-Laptop-1**.

b. Click **HQ-Laptop-1** > **Desktop** tab > **Command Prompt**.



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

c. Enter the **ipconfig** command.

Which IPv4 address is displayed for the **Wireless0 Connection**?

169.254.238.170

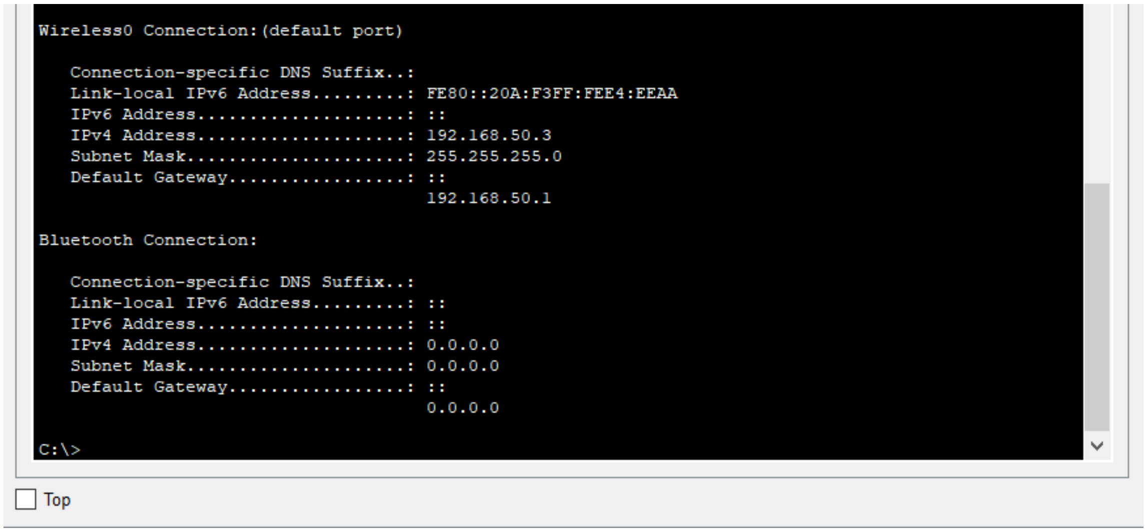
It may show as 169.254.0.0/16 address because the wireless connection may not be established yet. The address will be within the 192.168.50.0/24 network.

If the IPv4 address is in the 169.254.0.0/16 range, what method is being used to assign IPv4 addresses? Why is the laptop assigned an IPv4 address in the 169.254.0.0/16 range?

Because the Laptop is unable to obtain IP Address from DHCP and instead using APIPA as a Fallback Mechanism

It indicates that the device was unable to obtain addressing from a DHCP server. Therefore, the device assigned itself an address 169.254.0.0/16 pool used for automatic private IP addressing (APIPA).

If the IPv4 address is in the 169.254.0.0/16, wait a few seconds and repeat the **ipconfig** command.



```
Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.50.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.50.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>
```

When the IPv4 address is no longer from 169.254.0.0/16 range, what is the IP addressing information displayed? Record your answers in the table below.

Wireless0	IP Addressing Information
Link-local IPv6 Address	FE80::20A:F3FF:FEE4:EEAA
IPv6 Address	::
IPv4 Address	192.168.50.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
DNS Servers	Empty

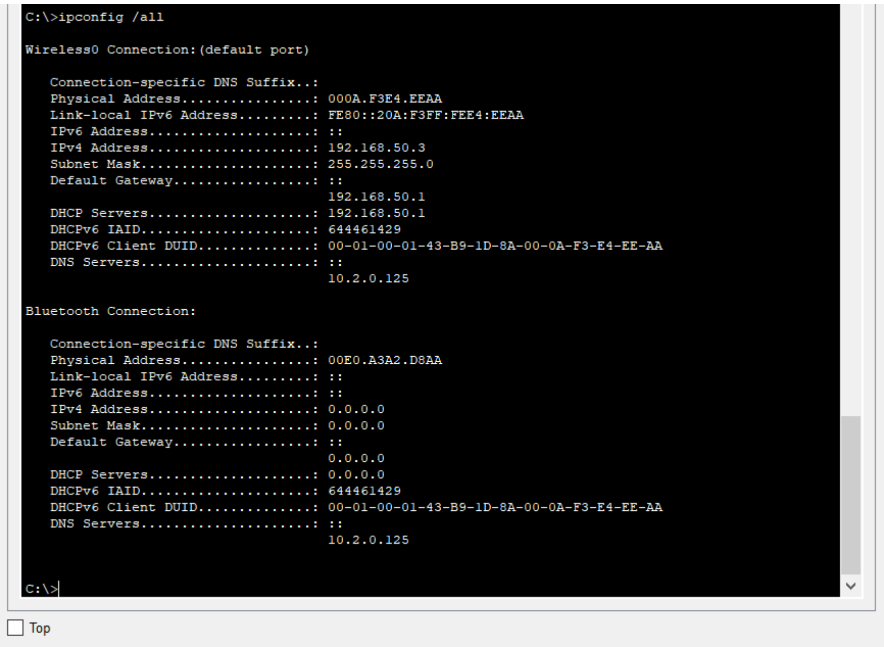
Wireless0	IP Addressing Information
Link-local IPv6 Address	FE80::20A:F3FF:FEE4:EEAA
IPv6 Address	::
IPv4 Address	192.168.50.4 (it may vary, but will be within the 192.168.50.0/24 range)
Subnet Mask	255.255.255.0
Default Gateway	192168.50.1
DNS Servers	N/A

Do you see a DNS server address? Explain.

No, because ipconfig doesn’t show any of the DNS Server Address

The ipconfig command does not report the DNS server address.

d. Enter the **ipconfig /all** command.



```
C:\>ipconfig /all

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 000A.F3E4.EEAA
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.50.3
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.50.1
   DHCP Servers....................: 192.168.50.1
   DHCPv6 IAID.....................: 644461429
   DHCPv6 Client DUID..............: 00-01-00-01-43-B9-1D-8A-00-0A-F3-E4-EE-AA
   DNS Servers.....................: ::
                                     10.2.0.125

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.A3A2.D8AA
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 644461429
   DHCPv6 Client DUID..............: 00-01-00-01-43-B9-1D-8A-00-0A-F3-E4-EE-AA
   DNS Servers.....................: ::
                                     10.2.0.125


C:\>
```

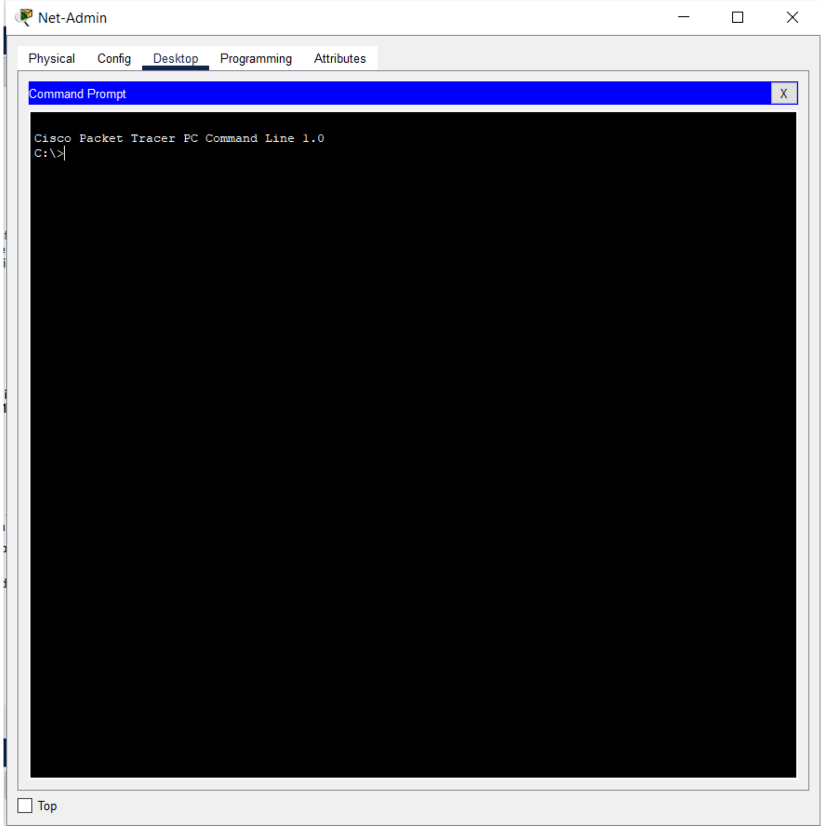
Do you see the DNS server address? What is it?

10.2.0.125

10.2.0.125

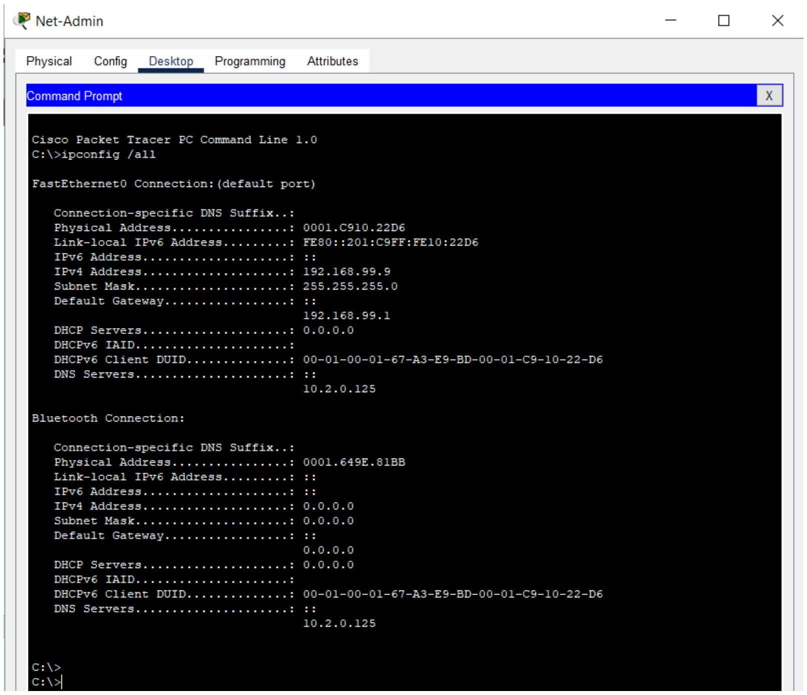
Step 2: Document the IP address settings for Net-Admin.

a. Click **Wiring Closet** > **Net-Admin** > **Desktop** tab > **Command Prompt**.



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

b. Enter the **ipconfig /all** command.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C910.22D6
   Link-local IPv6 Address.........: FE80::201:C9FF:FE10:22D6
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.99.9
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.99.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-67-A3-E9-BD-00-01-C9-10-22-D6
   DNS Servers.....................: ::
                                     10.2.0.125

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.649E.81BB
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-67-A3-E9-BD-00-01-C9-10-22-D6
   DNS Servers.....................: ::
                                     10.2.0.125


C:\>
C:\>
```

What is the IP addressing information displayed under the FastEthernet0 interface? Record your answers in the table below.

FastEthernet0	IP Addressing Information
Physical Address	001.C910.22D6
Link-local IPv6 Address	FE80::201:C9FF:FE10:22D6
IPv6 Address	::
IPv4 Address	192.168.99.9
Subnet Mask	255.255.255.0
Default Gateway	192.168.99.1
DNS Servers	10.2.0.125

FastEthernet0	IP Addressing Information
Physical Address	0001.C910.22D6 (it may vary)
Link-local IPv6 Address	FE80::201:C9FF:FE10:22D6
IPv6 Address	::
IPv4 Address	192.168.99.9
Subnet Mask	255.255.255.0
Default Gateway	192168.99.1
DNS Servers	0.0.0.0

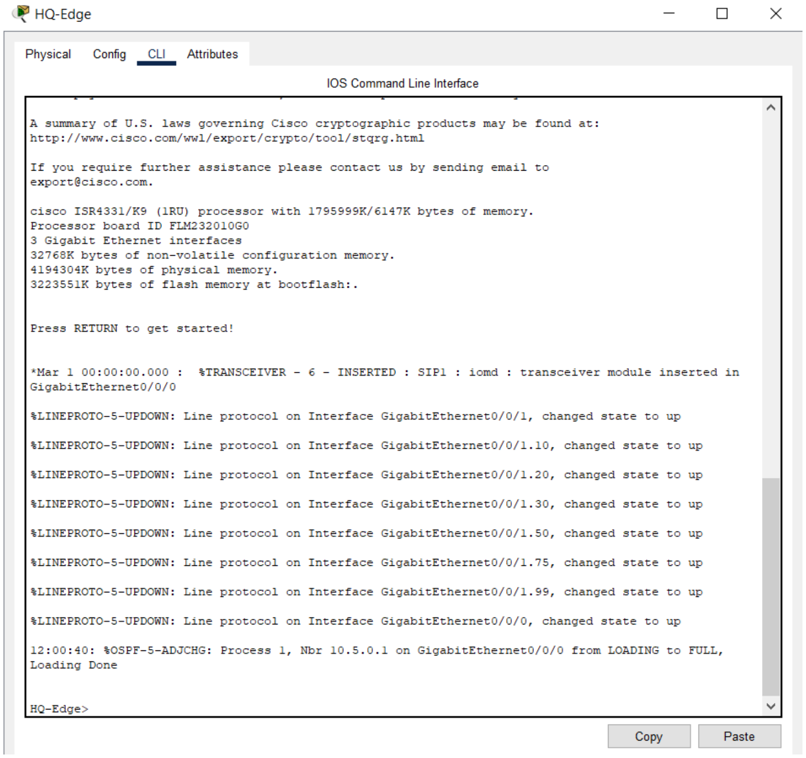
Part 2: Gather Information about Network Devices

In this part, you will document information about the link to ISP. You will then document the IP addressing information for all the end devices in HQ and discover that devices belong to different virtual local area networks (VLANs).

Step 1: Gather network connection information about the link between HQ and ISP.

The **HQ-Edge** router is the router between the HQ network and the ISP. We need to identify the upstream device information located in the ISP.

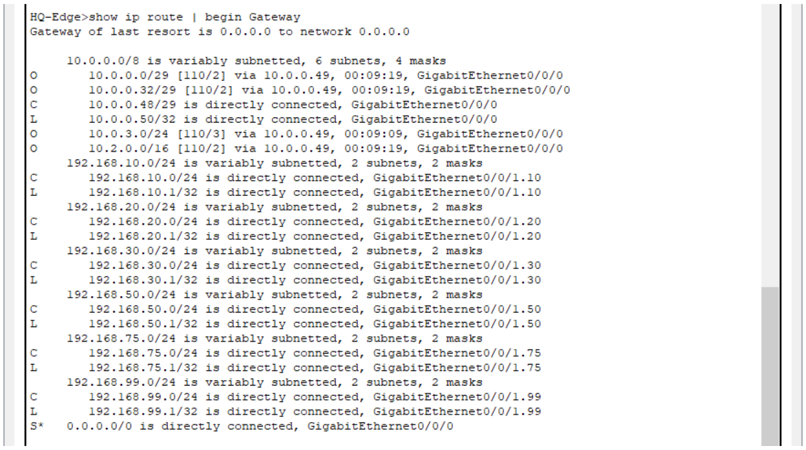
a. In the **Wiring Closet** left rack, click **HQ-Edge** > **CLI** tab.



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

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!


*Mar 1 00:00:00.000 :  %TRANSCEIVER - 6 - INSERTED : SIP1 : iomd : transceiver module inserted in
GigabitEthernet0/0/0

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.75, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

12:00:40: %OSPF-5-ADJCHG: Process 1, Nbr 10.5.0.1 on GigabitEthernet0/0/0 from LOADING to FULL,
Loading Done


HQ-Edge>
```

b. Press **Enter** to get the **HQ-Edge>** prompt, and then enter the **enable** command.

c. Enter the **show ip route | begin Gateway** command.



```
HQ-Edge>show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 4 masks
O       10.0.0.0/29 [110/2] via 10.0.0.49, 00:09:19, GigabitEthernet0/0/0
O       10.0.0.32/29 [110/2] via 10.0.0.49, 00:09:19, GigabitEthernet0/0/0
C       10.0.0.48/29 is directly connected, GigabitEthernet0/0/0
L       10.0.0.50/32 is directly connected, GigabitEthernet0/0/0
O       10.0.3.0/24 [110/3] via 10.0.0.49, 00:09:09, GigabitEthernet0/0/0
O       10.2.0.0/16 [110/2] via 10.0.0.49, 00:09:19, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/1.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/1.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0/1.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0/1.20
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0/1.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0/1.30
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, GigabitEthernet0/0/1.50
L       192.168.50.1/32 is directly connected, GigabitEthernet0/0/1.50
     192.168.75.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.75.0/24 is directly connected, GigabitEthernet0/0/1.75
L       192.168.75.1/32 is directly connected, GigabitEthernet0/0/1.75
     192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.99.0/24 is directly connected, GigabitEthernet0/0/1.99
L       192.168.99.1/32 is directly connected, GigabitEthernet0/0/1.99
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/0/0
```

What is the address for the gateway of last resort (or default gateway)?

0.0.0.0

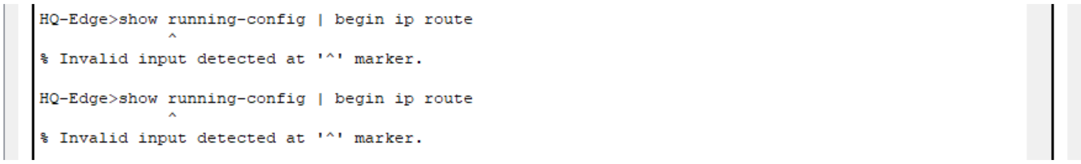
0.0.0.0

Why is the next hop address not displayed?

Because there is still no configuration

It is not explicitly configured.

c. Enter the **show running-config | begin ip route** command.



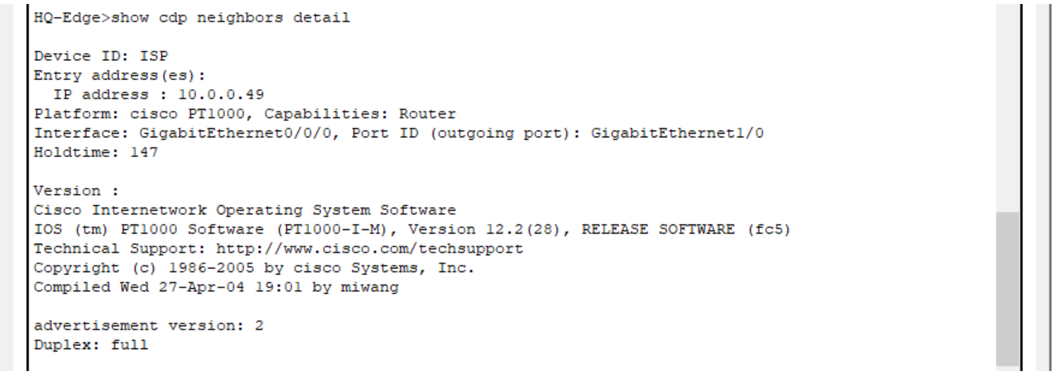
```
HQ-Edge>show running-config | begin ip route
             ^
% Invalid input detected at '^' marker.

HQ-Edge>show running-config | begin ip route
             ^
% Invalid input detected at '^' marker.
```

How is the default route configured? Does it use the next hop address?

(Terjadi invalid input, sedangkan untuk command sudah saya copy paste dari instruksi)

It is configured with the exit interface instead of next hop address.

d. Enter the **show cdp neighbors detail** command.



```
HQ-Edge>show cdp neighbors detail

Device ID: ISP
Entry address(es):
  IP address : 10.0.0.49
Platform: cisco PT1000, Capabilities: Router
Interface: GigabitEthernet0/0/0, Port ID (outgoing port): GigabitEthernet1/0
Holdtime: 147

Version :
Cisco Internetwork Operating System Software
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
```

What is the IPv4 address of the next hop (ISP) address?

10.0.0.49

10.0.0.49

Which port on the ISP router is connected to **HQ-Edge**?

GigabitEthernet 1/0

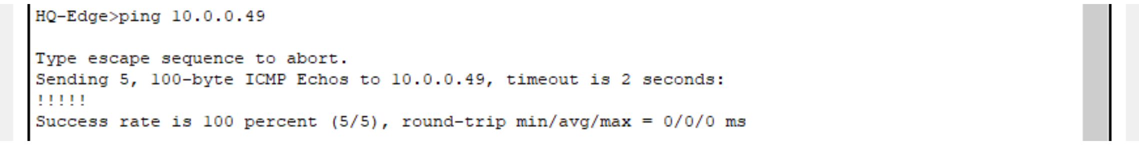
GigabitEthernet 1/0

What IOS version is used on the ISP router?

IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

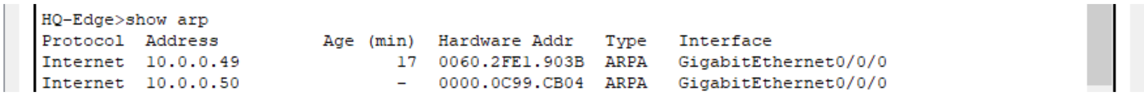
IOS (tm) PT1000 Software (PT1000-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

e. Enter the **ping 10.0.0.49** command.



```
HQ-Edge>ping 10.0.0.49

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.49, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

f. Enter the **show arp** command.



```
HQ-Edge>show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.49               17  0060.2FE1.903B  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.50                -  0000.0C99.CB04  ARPA   GigabitEthernet0/0/0
```

What is the MAC address of the interface on the **ISP** router that is connected to **HQ-Edge**?

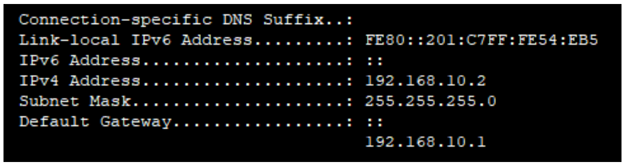
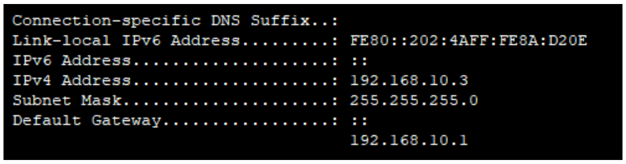
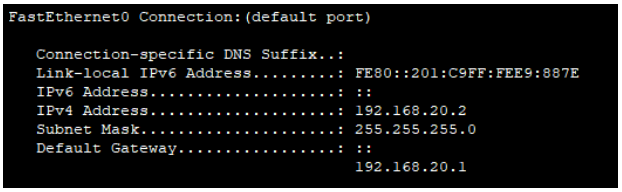
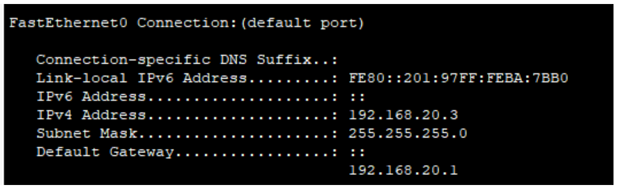
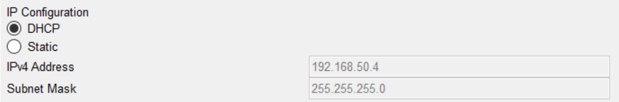
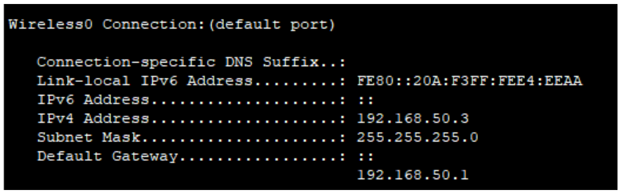
0060.2FE1.903B

0060.2FE1.903B

h. Close **HQ-Edge** and exit the **Wiring Closet**.

Step 2: Gather network connection information about the devices in HQ.

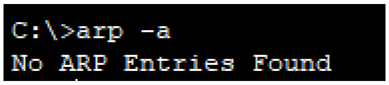
a. From **1-1**, **1-2**, **1-3**, **1-4**, **FL-1P**, and **HQ-Laptop-1**, use the **ipconfig** command to find their IPv4 addresses and Default Gateways.

Device	IPv4 Address	Default Gateway
1-1	 Connection-specific DNS Suffix..: Link-local IPv6 Address.........: FE80::201:C7FF:FE54:EB5 IPv6 Address....................: :: IPv4 Address....................: 192.168.10.2 Subnet Mask.....................: 255.255.255.0 Default Gateway.................: :: 192.168.10.1	192.168.10.1
1-2	 Connection-specific DNS Suffix..: Link-local IPv6 Address.........: FE80::202:4AFF:FE8A:D20E IPv6 Address....................: :: IPv4 Address....................: 192.168.10.3 Subnet Mask.....................: 255.255.255.0 Default Gateway.................: :: 192.168.10.1	192.168.10.1
1-3	 FastEthernet0 Connection:(default port) Connection-specific DNS Suffix..: Link-local IPv6 Address.........: FE80::201:C9FF:FEE9:887E IPv6 Address....................: :: IPv4 Address....................: 192.168.20.2 Subnet Mask.....................: 255.255.255.0 Default Gateway.................: :: 192.168.20.1	192.168.20.1
1-4	 FastEthernet0 Connection:(default port) Connection-specific DNS Suffix..: Link-local IPv6 Address.........: FE80::201:97FF:FEBA:7BB0 IPv6 Address....................: :: IPv4 Address....................: 192.168.20.3 Subnet Mask.....................: 255.255.255.0 Default Gateway.................: :: 192.168.20.1	192.168.20.1
FL-1P	 IP Configuration ● DHCP ○ Static IPv4 Address 192.168.50.4 Subnet Mask 255.255.255.0	192.168.50.1
HQ-Laptop-1	 Wireless0 Connection:(default port) Connection-specific DNS Suffix..: Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA IPv6 Address....................: :: IPv4 Address....................: 192.168.50.3 Subnet Mask.....................: 255.255.255.0 Default Gateway.................: :: 192.168.50.1	192.168.50.1

Device	IPv4 Address	Default Gateway
1-1	192.168.10.2	192.168.10.1
1-2	192.168.10.3	192.168.10.1

Device	IPv4 Address	Default Gateway
1-3	192.168.20.2	192.168.20.1
1-4	192.168.20.3	192.168.20.1
FL-1P	192.168.50.2	192.168.50.1
HQ-Laptop-1	192.168.50.3	192.168.50.1

b. From PC **1-1**, open **Command Prompt**, and then enter the **arp -a** command.



```
C:\>arp -a
No ARP Entries Found
```

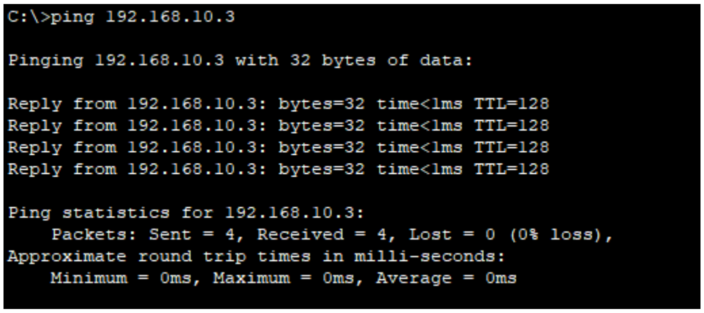
What information is displayed?

No ARP Entries Found

No ARP Entries Found.

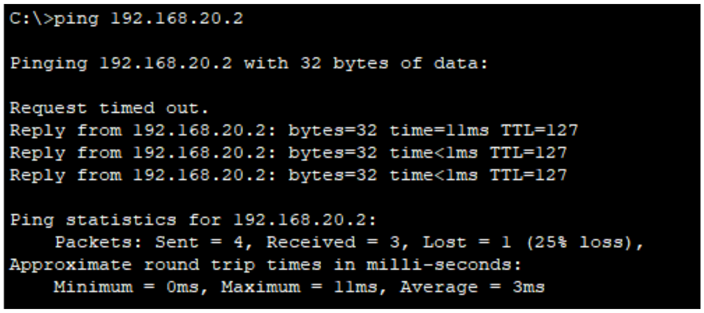
c. Use the **ping** command to ping **1-2**, **1-3**, **1-4**, **FL-1P**, and **HQ-Laptop-1**.

1-2



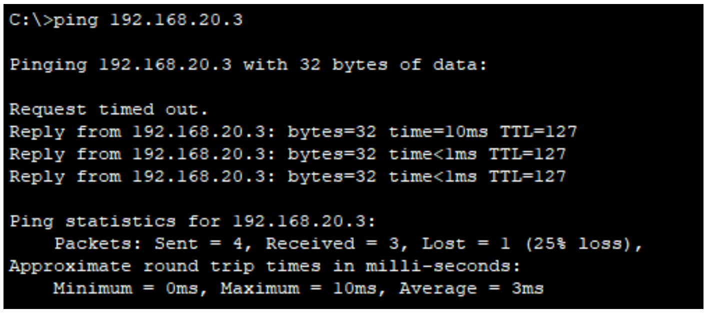
```
C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1-3



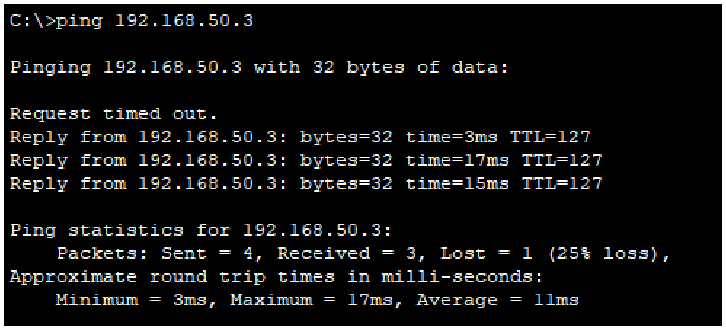
```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=11ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127
Reply from 192.168.20.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

1-4



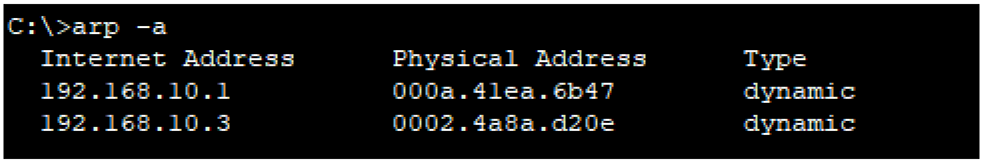
```
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=10ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127
Reply from 192.168.20.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

HQ-Laptop-1



```
C:\>ping 192.168.50.3

Pinging 192.168.50.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.50.3: bytes=32 time=3ms TTL=127
Reply from 192.168.50.3: bytes=32 time=17ms TTL=127
Reply from 192.168.50.3: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 17ms, Average = 11ms
```

d. Enter the **arp -a** command.



```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.10.1          000a.41ea.6b47        dynamic
  192.168.10.3          0002.4a8a.d20e        dynamic
```

What information is displayed?

Internet Address	Physical Address	Type
192.168.10.1	000a.41ea.6b47	dynamic
192.168.10.3	0002.4a8a.d20e	dynamic

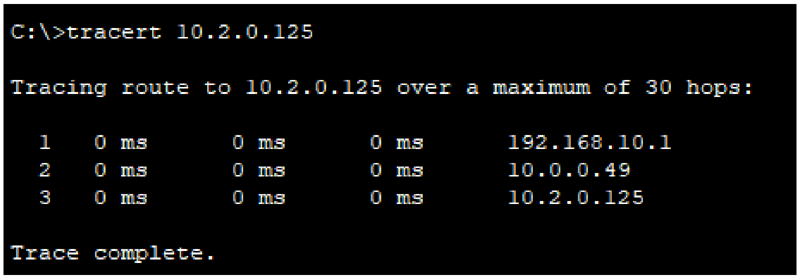
```
  Internet Address      Physical Address      Type
  192.168.10.1          000a.41ea.6b47        dynamic
  192.168.10.3          0002.4a8a.d20e        dynamic
ARP provides a table that maps known MAC addresses to their associated IP
addresses.
```

Why do the entries in the ARP table not contain information about devices in the 192.168.20.0 and 192.168.50.0 networks while the ping is successful?

Because the ARP only contain entries of a device that is on the same local Subnet.

192.168.10.0/24, 192.168.20.0/24, and 192.168.50.0/24 are on different VLANs. Ping from 192.168.10.0 network to other VLAN networks would need to go through the default gateway first. Therefore, the ARP table only contains the information about devices within the same network or the same VLAN.

e. To find the route a packet takes to reach the DNS server, enter the tracert 10.2.0.125 command.



```
C:\>tracert 10.2.0.125

Tracing route to 10.2.0.125 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.10.1
  2   0 ms      0 ms      0 ms      10.0.0.49
  3   0 ms      0 ms      0 ms      10.2.0.125

Trace complete.
```

What information is displayed?

```
Tracing route to 10.2.0.125 over a maximum of 30 hops:


 1   0 ms      0 ms      0 ms      192.168.10.1
 2   0 ms      0 ms      0 ms      10.0.0.49
 3   0 ms      0 ms      0 ms      10.2.0.125


Trace complete.
```

```
Tracing route to 10.2.0.125 over a maximum of 30 hops:

  1    0 ms       2 ms       0 ms       192.168.10.1
  2    12 ms      0 ms       0 ms       10.0.0.49
  3    1 ms       0 ms       0 ms       10.2.0.125
```

How many routers, or hops, are between PC 1-1 and the DNS server?

Only 2

2

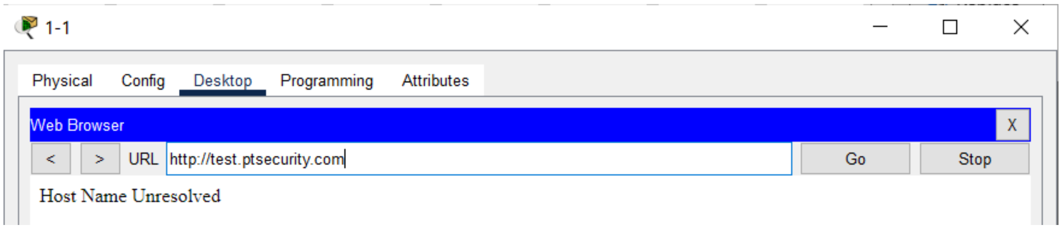
Part 3: Diagnose Connectivity Issues

In this part, you will use a variety of diagnostic commands and techniques. You will use the **nslookup** command to query a DNS server and troubleshoot a DNS database. You will then diagnose why a ping fails but web access is successful. Finally, you will use the **netstat** command to discover which ports are listening on the target device.

Step 1: Test a URL to investigate a connectivity issue.

a. On PC **1-1**, close the **Command Prompt**, and then click **Web Browser.**

b. Enter the URL **test.ptsecurity.com**.



http://test.ptsecurity.com

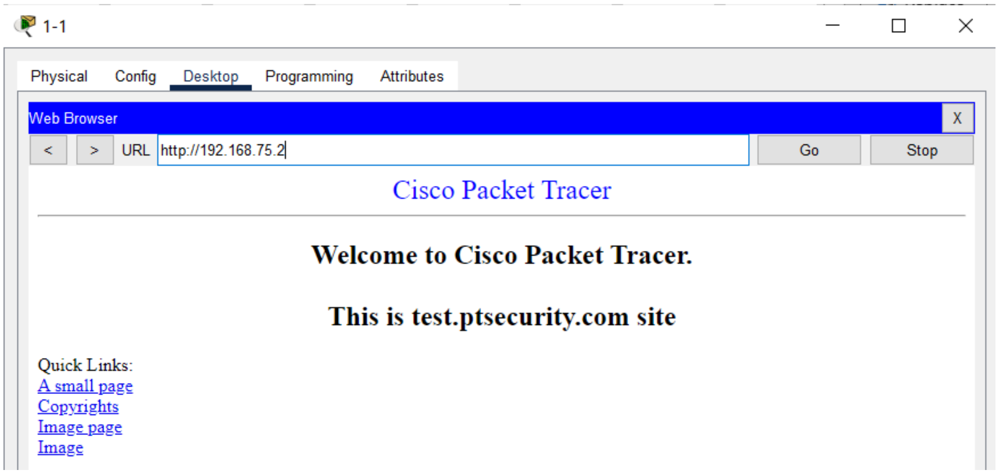
Host Name Unresolved

Does the web page display? If not, what is the message?

No, and the message is Host Name Unresolved

No, it does not. The message is â€œHost Name Unresolvedâ€• .

b. Enter the IP address **192.168.75.2**.



http://192.168.75.2

Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

This is test.ptsecurity.com site

Quick Links:
A small page
Copyrights
Image page
Image

Does the web page display?

Yes

Yes

Why does the web page display by using the IP address but not the domain name?

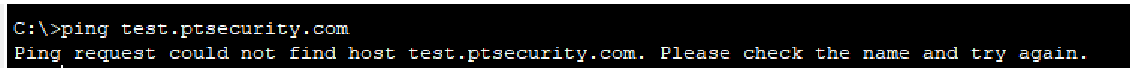
Because the PC can’t resolve the domain name

The PC cannot resolve the domain name to the IP address.

Step 2: Use the nslookup command to verify DNS service.

a. Close **Web Browser**, and then click **Command Prompt**.

b. Enter the **ping test.ptsecurity.com** command.



```
C:\>ping test.ptsecurity.com
Ping request could not find host test.ptsecurity.com. Please check the name and try again.
```

What message is displayed?

Ping request could not find host test.ptsecurity.com. Please check the name and try again.

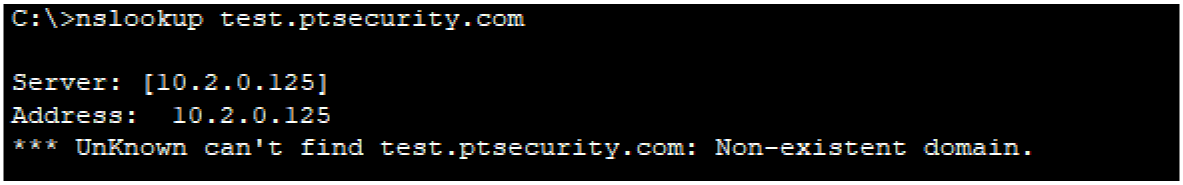
Ping request could not find host test.ptsecurity.com. Please check the name and try again.

What does the message indicate?

The DNS / Domain is not in the DNS Server

The DNS entry is not in the database of the DNS server.

c. Enter the **nslookup test.ptsecurity.com** command.



```
C:\>nslookup test.ptsecurity.com

Server: [10.2.0.125]
Address:  10.2.0.125
*** UnKnown can't find test.ptsecurity.com: Non-existent domain.
```

What message is displayed?

Server: [10.2.0.125]

Address: 10.2.0.125

*** UnKnown can't find test.ptsecurity.com: Non-existent domain.

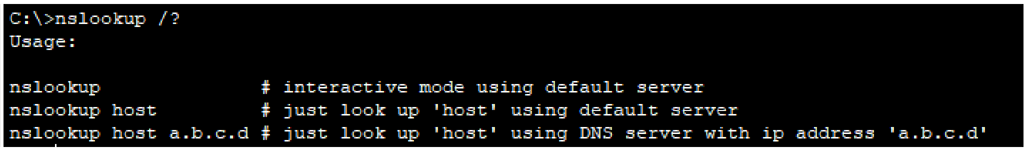
```
Server: [10.2.0.125]
Address:  10.2.0.125
*** UnKnown can't find test.ptsecurity.com: Non-existent domain.
```

Which server is the default DNS server?

10.2.0.125

10.2.0.125

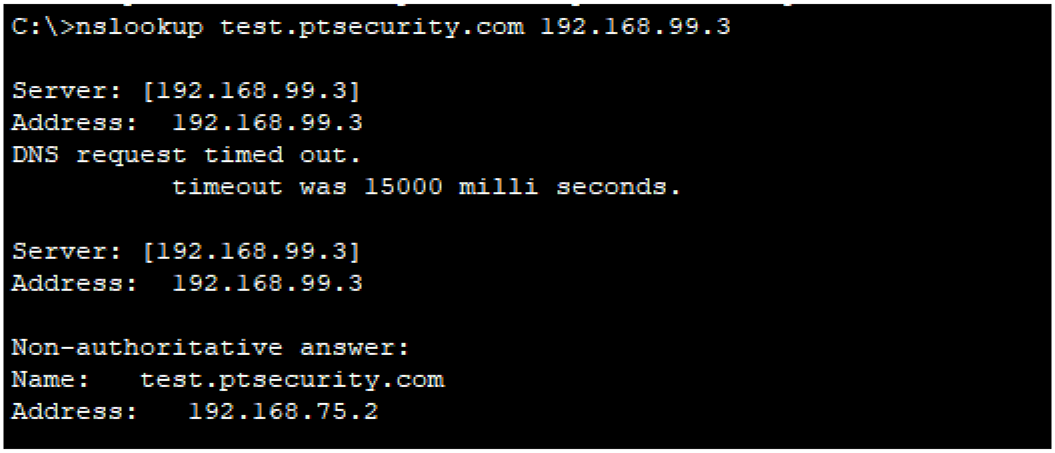
d. The **nslookup** command supports the use of alternate DNS server. Enter the **nslookup /?** command to learn options available for the command.



```
C:\>nslookup /?
Usage:

nslookup              # interactive mode using default server
nslookup host         # just look up 'host' using default server
nslookup host a.b.c.d # just look up 'host' using DNS server with ip address 'a.b.c.d'
```

e. Enter the **nslookup test.ptsecurity.com 192.168.99.3** command and press **Enter**.

Note: Packet Tracer may take several seconds to converge.



```
C:\>nslookup test.ptsecurity.com 192.168.99.3

Server: [192.168.99.3]
Address:  192.168.99.3
DNS request timed out.
          timeout was 15000 milli seconds.

Server: [192.168.99.3]
Address:  192.168.99.3

Non-authoritative answer:
Name:   test.ptsecurity.com
Address:   192.168.75.2
```

What message is displayed?

C:\>nslookup test.ptsecurity.com 192.168.99.3

Server: [192.168.99.3]

Address: 192.168.99.3

DNS request timed out.

timeout was 15000 milli seconds.

Server: [192.168.99.3]

Address: 192.168.99.3

Non-authoritative answer:

Name: test.ptsecurity.com

Address: 192.168.75.2

```
C:\> nslookup test.ptsecurity.com 192.168.99.3
Server: [192.168.99.3]
Address:  192.168.99.3

Non-authoritative answer:
Name:    test.ptsecurity.com
Address:   192.168.75.2
```

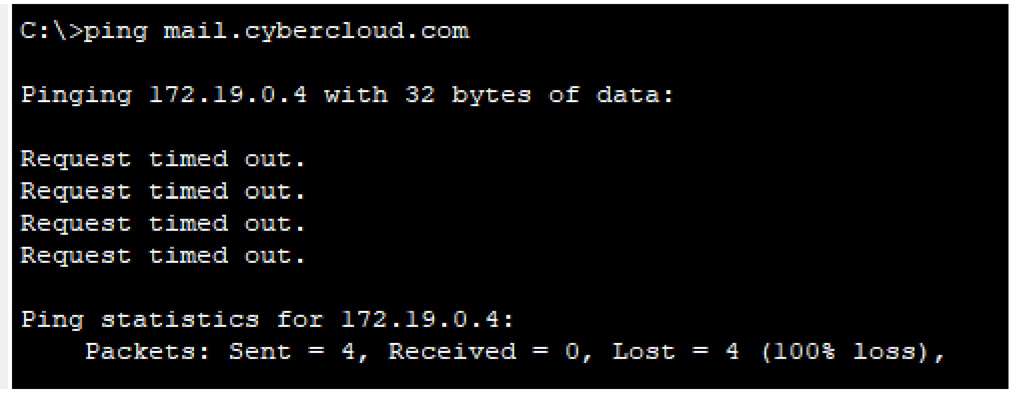
In Step 2c, why is the domain name unable to be resolved?

Because when the domain name is entered the PC cannot resolve through the DNS Server, this because the DNS doesn’t contain any information about the domain.

When a domain name is entered in the URL box, the PC is trying to resolve it through the default DNS server. In this case, the default DNS server does not contain the information in its database.

Step 3: Use output from the ping command to diagnose connectivity issues.

a. Enter the **ping mail.cybercloud.com** command.



```
C:\>ping mail.cybercloud.com

Pinging 172.19.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

What message is displayed?

C:\>ping mail.cybercloud.com

Pinging 172.19.0.4 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 172.19.0.4:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

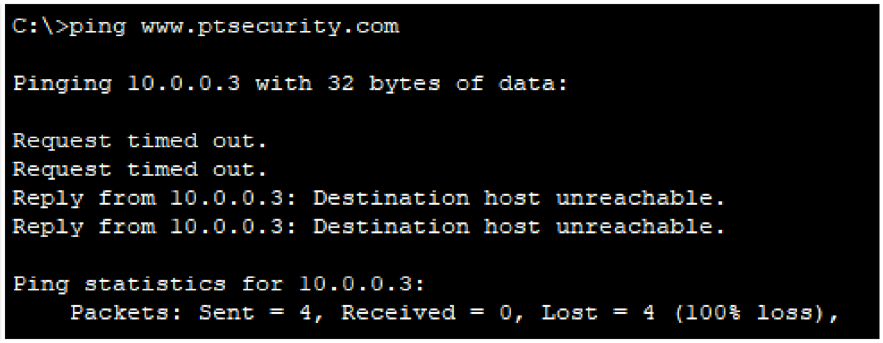
```
C:\> ping mail.cybercloud.com
Pinging 172.19.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.0.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

What information is indicated by the message?

The DNS is founded, but the ping fail because either the host is disabled, or the reply from the host is disabled

The DNS name resolution is successful. However, the ping failed. Possible reasons are that the host is inactive or the ICMP echo/echo-reply is disabled on the host.

b. Enter the **ping www.ptsecurity.com** command.



```
C:\>ping www.ptsecurity.com

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

What message is displayed?

C:\>ping www.ptsecurity.com

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.

Request timed out.

Reply from 10.0.0.3: Destination host unreachable.

Reply from 10.0.0.3: Destination host unreachable.

Ping statistics for 10.0.0.3:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

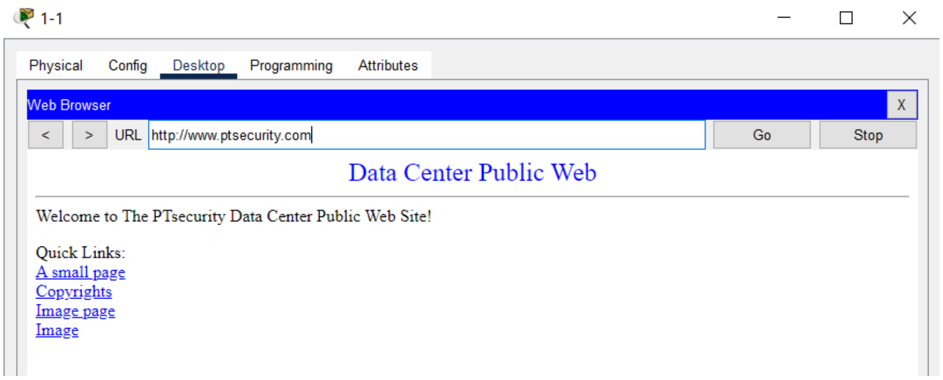
```
Pinging 10.0.0.3 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.

Ping statistics for 10.0.0.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

What information is indicated by the message?

The firewall is blocking the ping

There is a firewall in the path that blocks the ping to the destination.

c. Close the **Command Prompt**, open **Web Browser**, and then navigate to **www.ptsecurity.com**.



http://www.ptsecurity.com

Data Center Public Web

Welcome to The PTsecurity Data Center Public Web Site!

Quick Links:
A small page
Copyrights
Image page
Image

Does the web page display?

Yes

Yes

What conclusion can be drawn?

The host is already running, even though the ping is blocked

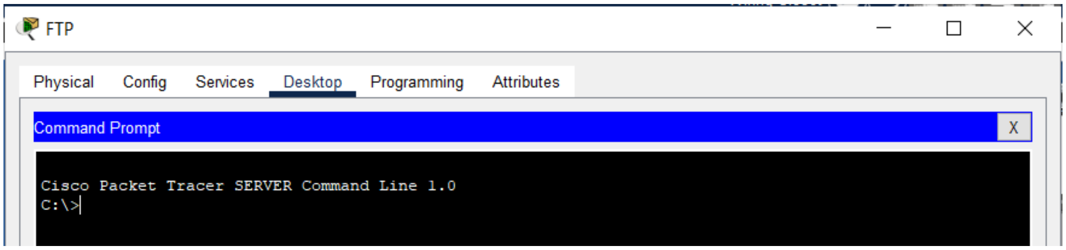
The web host is running; however, the ping to the web server is blocked.

Step 4: Use the netstat command to find active and listening ports.

a. Close **Web Browser**, and reopen **Command Prompt**.

b. In **HQ**, click the **Wiring Closet**

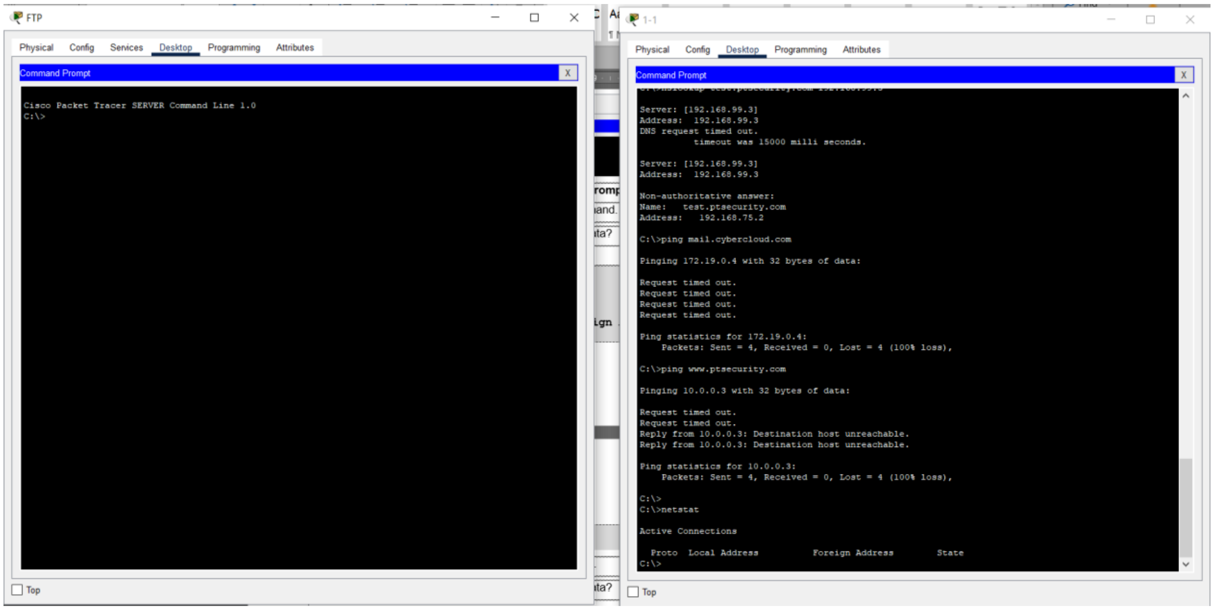
c. From the right rack, click the **FTP** server > **Desktop** tab > **Command Prompt**.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>
```

d. Arrange the PC **1-1** and FTP server **Command Prompt** windows side by side.

e. From the PC **1-1** window, enter the **netstat** command.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>
```

```
Server: [192.168.99.3]
Address:  192.168.99.3
DNS request timed out.
          timeout was 15000 milli seconds.

Server: [192.168.99.3]
Address:  192.168.99.3

Non-authoritative answer:
Name:   test.ptsecurity.com
Address:   192.168.75.2

C:\>ping mail.cybercloud.com

Pinging 172.19.0.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.19.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping www.ptsecurity.com

Pinging 10.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 10.0.0.3: Destination host unreachable.
Reply from 10.0.0.3: Destination host unreachable.

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
C:\>
```

What message is displayed? Does it show any data?

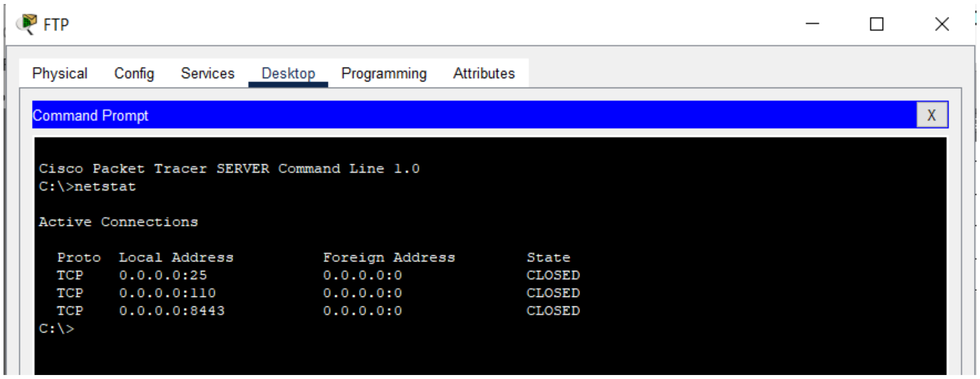
C:\>netstat

Active Connections

Proto Local Address   Foreign Address   State

```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
C:\>

No data is shown.
```

e. From the **FTP** server, enter the **netstat** command.



```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
C:\>
```

What message is displayed? Does it show any data?

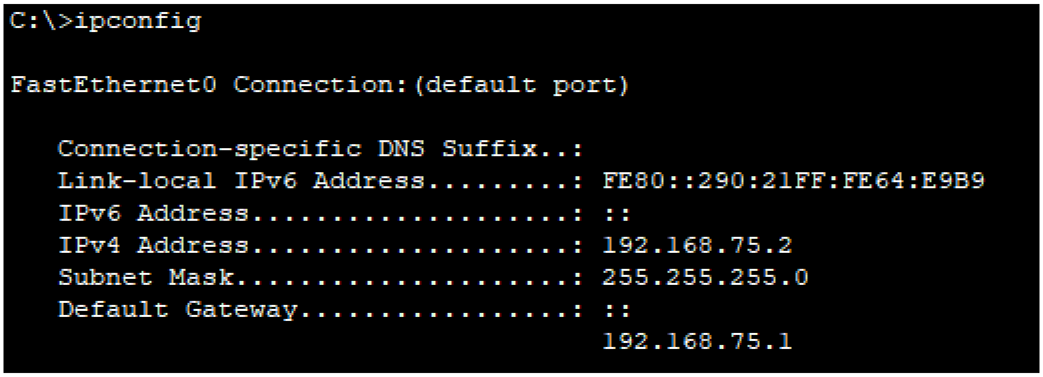
C:\>netstat

Active Connections

```
 Proto  Local Address        Foreign Address       State
 TCP    0.0.0.0:25           0.0.0.0:0             CLOSED
 TCP    0.0.0.0:110          0.0.0.0:0             CLOSED
     TCP    0.0.0.0:8443         0.0.0.0:0             CLOSED
```

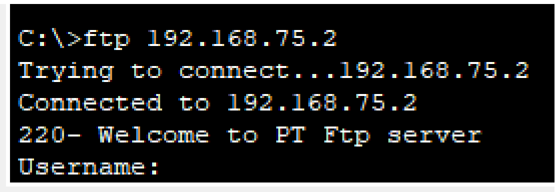
```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address            State
  TCP    0.0.0.0:25              0.0.0.0:0                CLOSED
  TCP    0.0.0.0:110             0.0.0.0:0                CLOSED
  TCP    0.0.0.0:8443            0.0.0.0:0                CLOSED
C:\>

It shows no active connection to other devices and no listening ports.
```

f. On **FTP** server, enter the **ipconfig** command to determine its IP address.



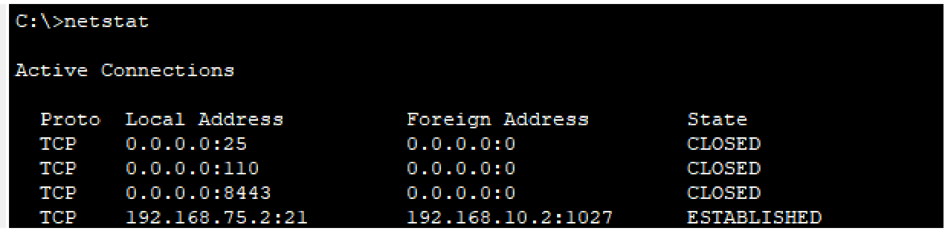
```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::290:21FF:FE64:E9B9
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.75.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.75.1
```

g. From **PC 1-1**, start an FTP session with the FTP server.



```
C:\>ftp 192.168.75.2
Trying to connect...192.168.75.2
Connected to 192.168.75.2
220- Welcome to PT Ftp server
Username:
```

h. On the **FTP** server, enter the **netstat** command.



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1027      ESTABLISHED
```

What message is displayed? Is there any new information?

Yes, there is another entry of TCP 192.168.75.2:21 192.168.10.2:1027 ESTABLISHED

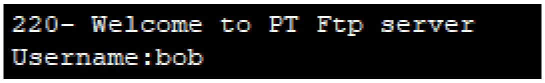
Yes, a new entry shows TCP 192.168.75.2:21 192.168.10.3:1025 ESTABLISHED.

Which port is the listening port and what is the status of the connection?

The port is 21, and the connection is already ESTABLISHED

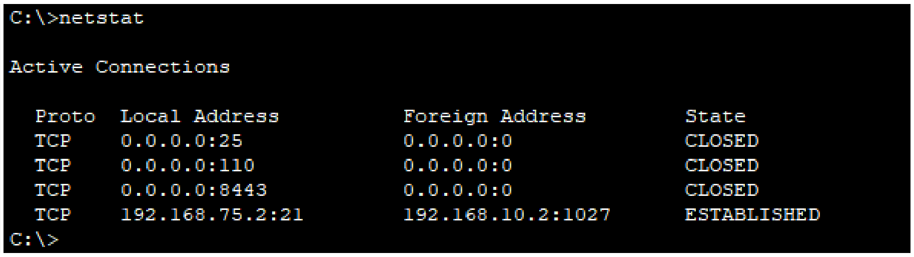
The listening port is TCP 21 and the TCP connection is established.

i. From PC **1-1**, enter **bob** as the username.



```
220- Welcome to PT Ftp server
Username:bob
```

j. From the **FTP** server, enter the **netstat** command.



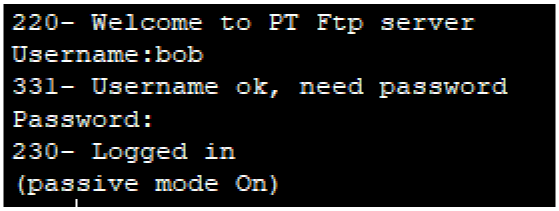
```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1027      ESTABLISHED
C:\>
```

Does the displayed information change?

Yes

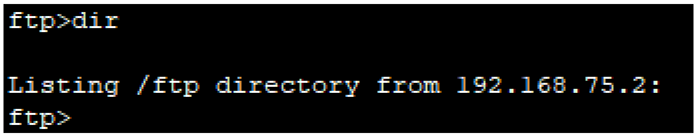
No.

k. From **PC 1-1**, enter **cisco123** as the password.



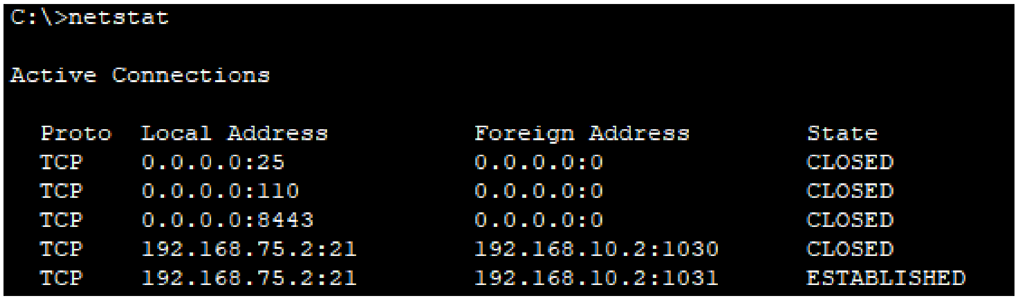
```
220- Welcome to PT Ftp server
Username:bob
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

l. From **PC 1-1**, enter the **dir** command.



```
ftp>dir

Listing /ftp directory from 192.168.75.2:
ftp>
```

n. From the **FTP** server, enter the **netstat** command.



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1030      CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1031      ESTABLISHED
```

Does the displayed information change?

Yes, with the information of TCP 192.168.75.2:21 192.168.10.2:1030 CLOSED

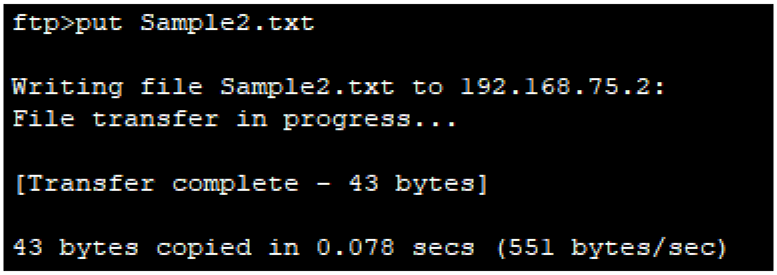
Yes. A new entry shows TCP 192.168.75.2:1028 192.168.10.3:1028 CLOSED.

What is indicated by this new entry?

New TCP Connection is opened to transfer file in the FTP directory and the connection is closed when the process is complete

A new TCP connection is opened to transfer the file names in the FTP directory and the connection is closed after the operation completes.

o. From **PC 1-1**, enter the **put Sample2.txt** command and press **Enter**. This will upload the Sample2.txt file to the **FTP** server.



```
ftp>put Sample2.txt

Writing file Sample2.txt to 192.168.75.2:
File transfer in progress...

[Transfer complete - 43 bytes]

43 bytes copied in 0.078 secs (551 bytes/sec)
```

p. From the **FTP** server, enter the **netstat** command.

Does the displayed information change?

No, because the process is too fast, so there is no new entry

Yes. A new entry shows:
TCP 192.168.75.2:1030 192.168.10.3:1029 CLOSING.

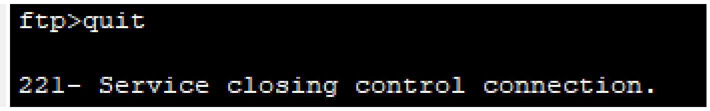
q. Wait for a few seconds and then enter the **netstat** command again.

Does the displayed information change?

Because the process is too fast then the entry that is supposed to be in there is already gone

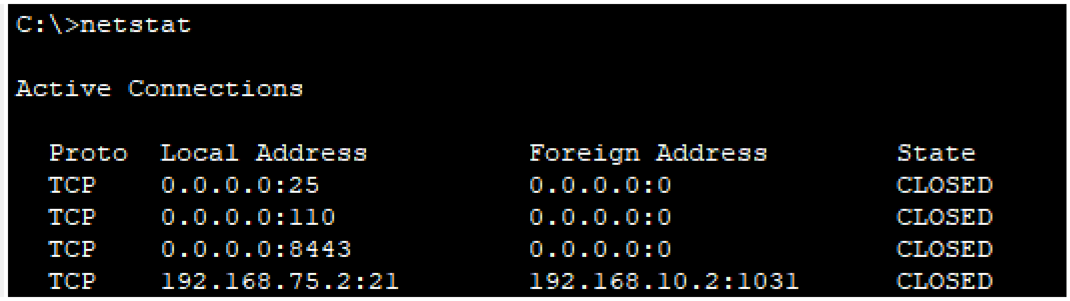
Yes. The â€œCLOSINGâ€• line is gone.

r. From **PC 1-1**, enter the **quit** command.



```
ftp>quit

221- Service closing control connection.
```

s. From the **FTP** server, enter the **netstat** command.



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
  TCP    192.168.75.2:21        192.168.10.2:1031      CLOSED
```

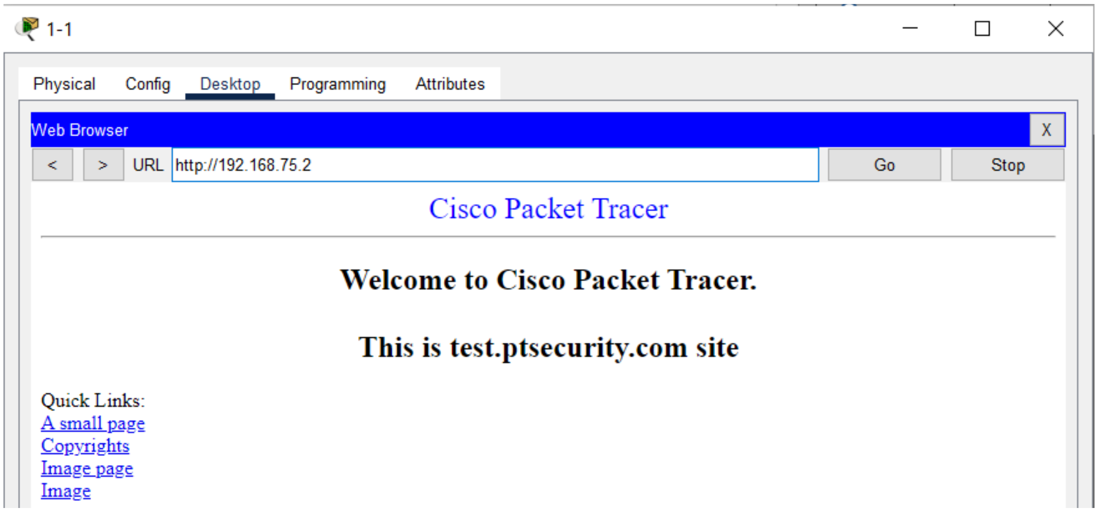
Does the displayed information change?

Yes, now the connection of TCP 192.168.75.2:21 192.168.10.2:1031 is already CLOSED

Yes. Now the TCP connection between 192.168.75.2:21 and 192.168.10.2:1027 is CLOSED.

t. From **PC 1-1**, close **Command Prompt**, and then open **Web Browser**.

u. Navigate to **192.168.75.2**.



http://192.168.75.2

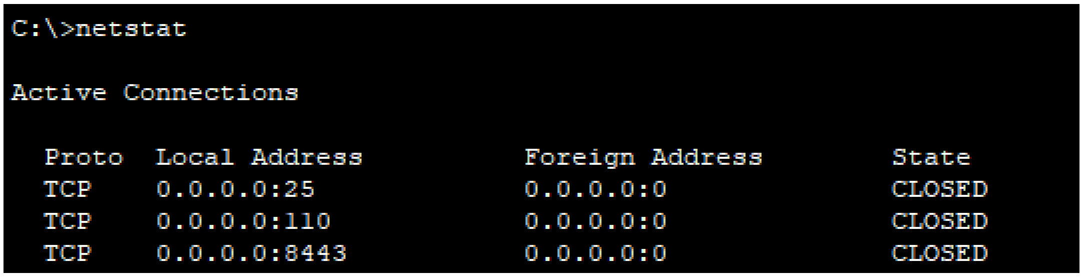
Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

This is test.ptsecurity.com site

Quick Links:
A small page
Copyrights
Image page
Image

v. From the **FTP** server, enter the **netstat** command.



```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              CLOSED
  TCP    0.0.0.0:110            0.0.0.0:0              CLOSED
  TCP    0.0.0.0:8443           0.0.0.0:0              CLOSED
```

Does the displayed information change?

I think it supposed to change, but again the process happen too fast.

Yes. A new entry shows TCP 192.168.75.2:80 192.168.10.2:1030 CLOSED.

What does this new entry indicate?

Since the entry is not happening on my end, I will use the Cisco clue as my reference.

The new entry indicate that the 192.168.10.2 is requesting to open a web page. And the TCP Connection is closed

A web page request is made by the host 192.168.10.2. The web page is transmitted (displayed on the web browser of PC 1-1) and the TCP connection is closed.