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.

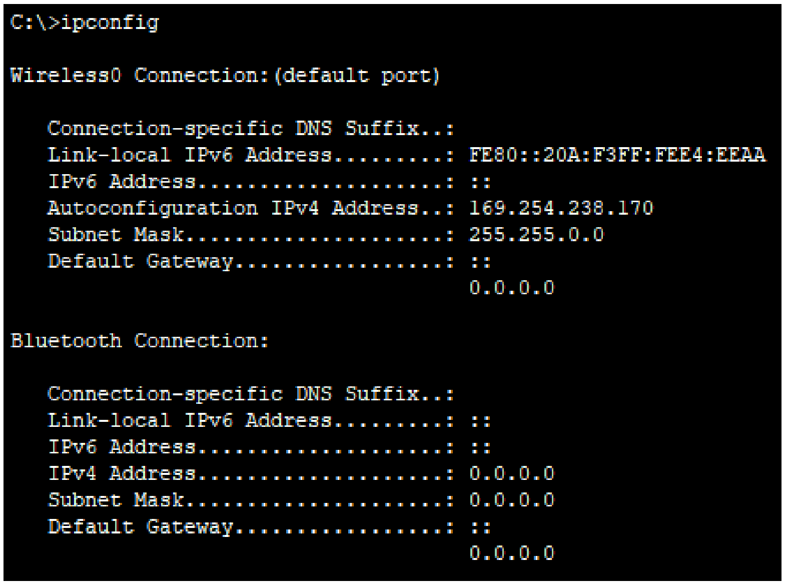
Step 1: Document the IP address settings for HQ-Laptop-1.

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**.

c. Enter the **ipconfig** command.

Which IPv4 address is displayed for the **Wireless0 Connection**? [Answer] 169.254.238.170



```
C:\>ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   Autoconfiguration IPv4 Address..: 169.254.238.170
   Subnet Mask.....................: 255.255.0.0
   Default Gateway.................: ::
                                     0.0.0.0

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
```

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.

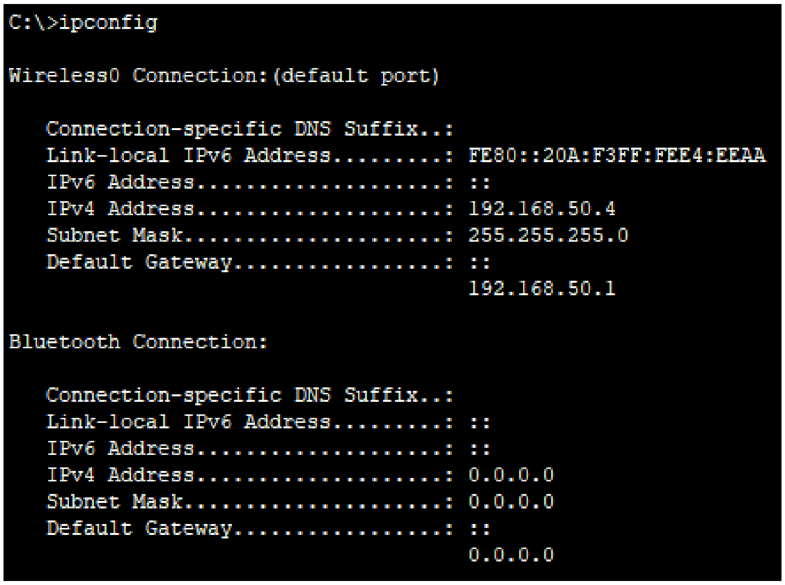
If the IPv4 address is in the 169.254.0.0/16 range, what method is being used to assign IPv4 addresses? Why is the laptop assigned an IPv4 address in the 169.254.0.0/16 range?

[Answer]

The device is using Automatic Private IP Addressing (APIPA). This happens when the laptop is unable to obtain an IP address from a DHCP server. When the DHCP server is unreachable, the device assigns itself an IP address from the 169.254.0.0/16 range to allow limited local communication on the network.

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.



```
C:\>ipconfig

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::20A:F3FF:FEE4:EEAA
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.50.4
   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
```

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.

[Answer]

Wireless0	IP Addressing Information
Link-local IPv6 Address	FE80::20A:F3FF:FEE4
IPv6 Address	::
IPv4 Address	192.168.50.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
DNS Servers	Not shown in the output

Do you see a DNS server address? Explain.

[Answer]

No, the ipconfig command does not report the DNS server address by default. To see the DNS server address, you would need to run the command ipconfig /all. This provides more detailed information, including DNS server addresses, MAC addresses, and other configuration details that are not shown in the basic ipconfig output.

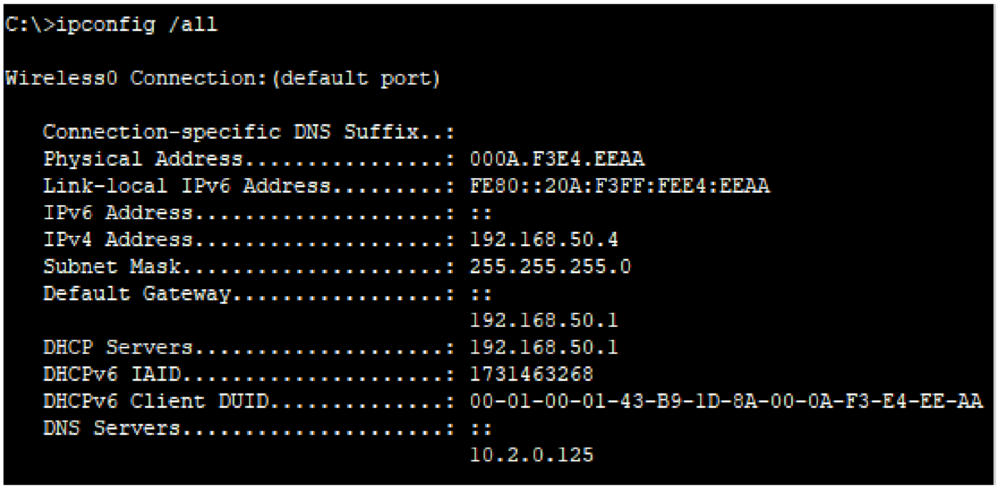
The ipconfig command does not report the DNS server address.

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

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

[Answer]

Yes, after running the ipconfig /all command, the DNS server address is displayed. The DNS server address is **10.2.0.125**.



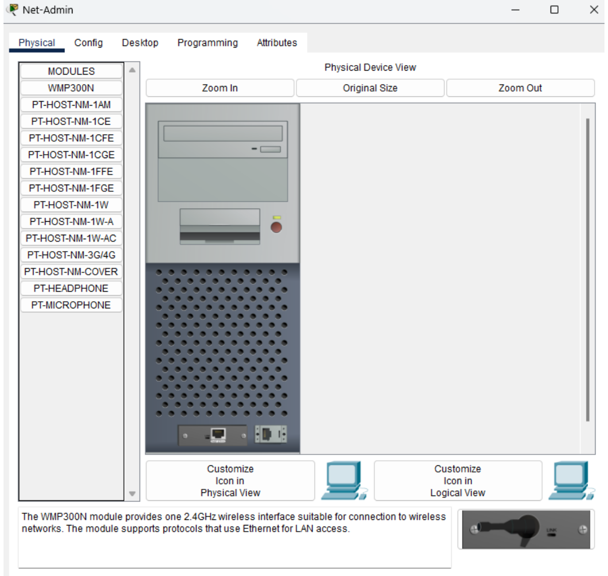
```
C:\>ipconfig /all

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....................: 192.168.50.4
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.50.1
   DHCP Servers....................: 192.168.50.1
   DHCPv6 IAID.....................: 1731463268
   DHCPv6 Client DUID..............: 00-01-00-01-43-B9-1D-8A-00-0A-F3-E4-EE-AA
   DNS Servers.....................: ::
                                     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**.

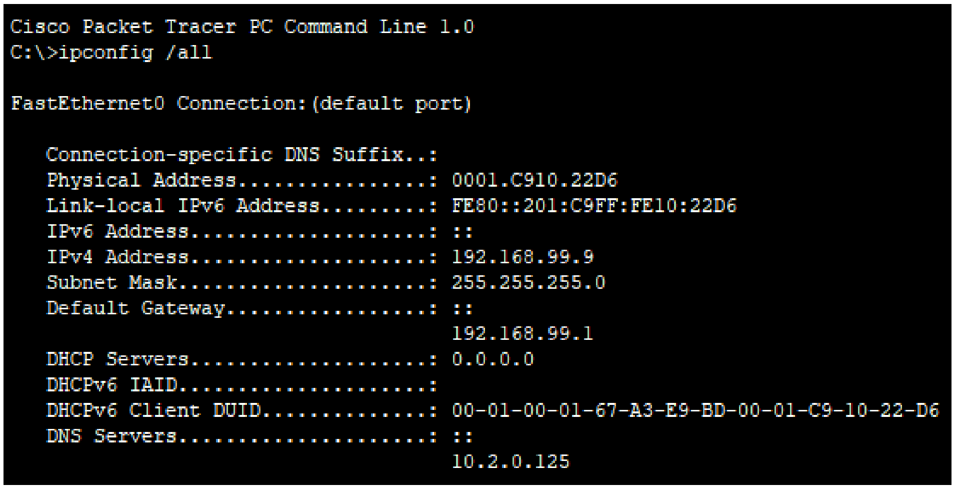
[Answer]



The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

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

[Answer]



```
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
```

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

[Answer]

FastEthernet0	IP Addressing Information
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	::
DNS Servers	192.168.99.1

Part 2: Gather Information about Network Devices

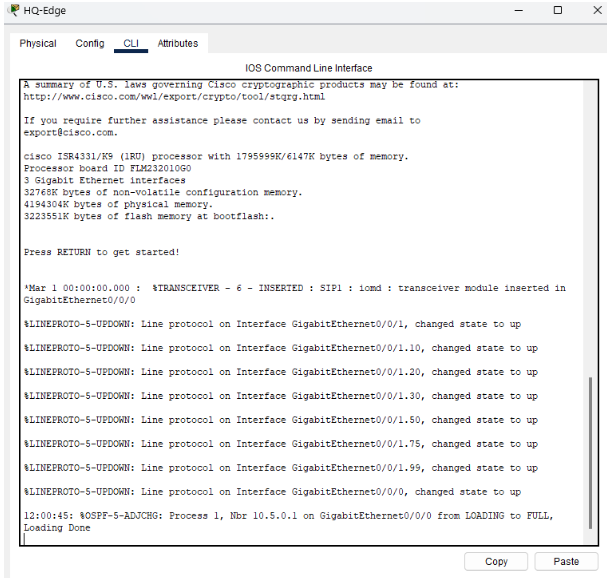
In this part, you will document information about the link to ISP. You will then document the IP addressing information for all the end devices in HQ and discover that devices belong to different virtual local area networks (VLANs).

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.

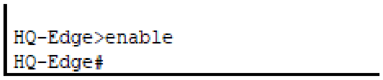
[Answer]



```
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

12:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 10.5.0.1 on GigabitEthernet0/0/0 from LOADING to FULL,
Loading Done
```

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

[Answer]

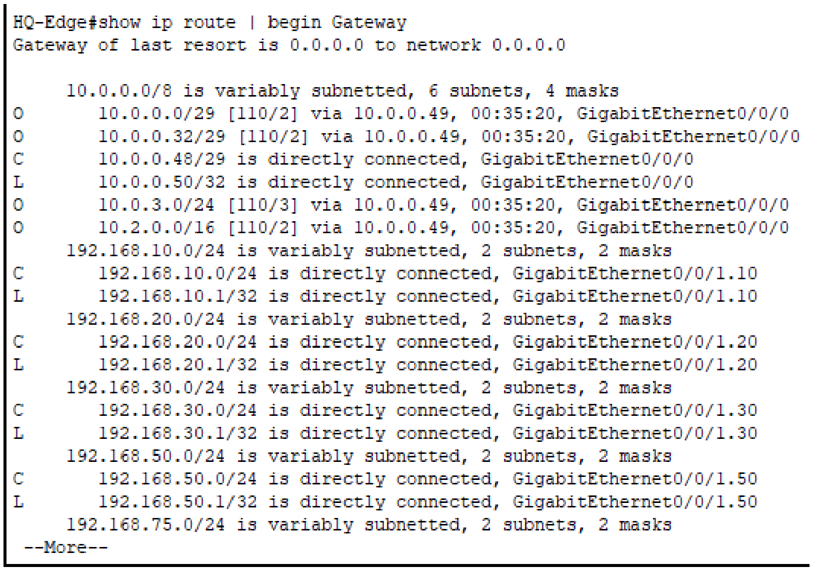


```
HQ-Edge>enable
HQ-Edge#
```

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

What is the address for the gateway of last resort (or default gateway)? [Answer] 0.0.0.0

This address indicates that any traffic that does not have a specific route in the routing table will be forwarded to the next hop associated with this gateway.



```
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, 00:35:20, GigabitEthernet0/0/0
O       10.0.0.32/29 [110/2] via 10.0.0.49, 00:35:20, 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, 00:35:20, GigabitEthernet0/0/0
O       10.2.0.0/16 [110/2] via 10.0.0.49, 00:35:20, 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
 --More--
```

0.0.0.0

Why is the next hop address not displayed?

[Answer]

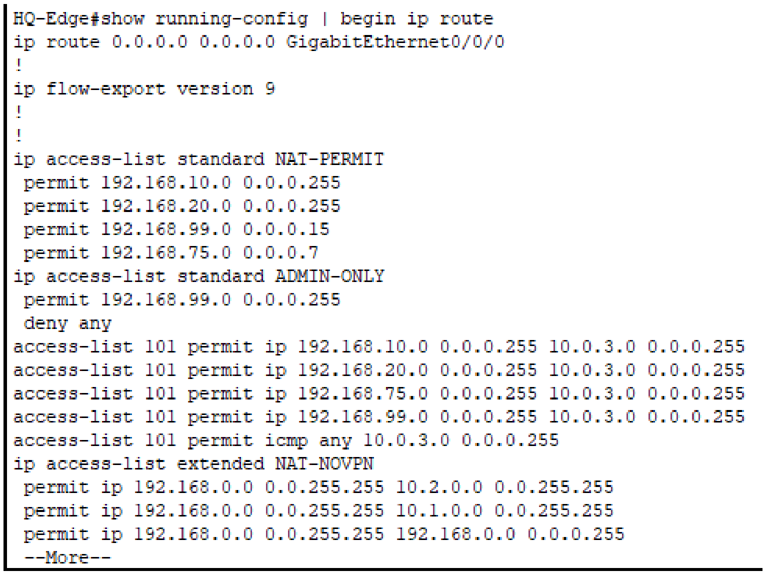
The next hop address may not be displayed if:

- The router is using a directly connected link to the ISP. In this case, the routing table shows the exit interface (e.g., a serial or Ethernet interface) instead of a next hop IP address.
- Alternatively, if the ISP network is configured to use a default route with the exit interface, the next hop IP address might not be necessary as the router already knows where to forward the traffic through the directly connected interface.

It is not explicitly configured.

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

[Answer]



```
HQ-Edge#show running-config | begin ip route
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
!
ip flow-export version 9
!
!
ip access-list standard NAT-PERMIT
 permit 192.168.10.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.99.0 0.0.0.15
 permit 192.168.75.0 0.0.0.7
ip access-list standard ADMIN-ONLY
 permit 192.168.99.0 0.0.0.255
 deny any
access-list 101 permit ip 192.168.10.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.20.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.75.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit ip 192.168.99.0 0.0.0.255 10.0.3.0 0.0.0.255
access-list 101 permit icmp any 10.0.3.0 0.0.0.255
ip access-list extended NAT-NOVPN
 permit ip 192.168.0.0 0.0.255.255 10.2.0.0 0.0.255.255
 permit ip 192.168.0.0 0.0.255.255 10.1.0.0 0.0.255.255
 permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.0.255
 --More--
```

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

- Configuration:
  - The default route is configured as ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0.
  - This means that any traffic destined for an IP address not found in the routing table is forwarded out of the interface GigabitEthernet0/0/0.
- Next Hop Address:

  The default route does not use a specific next hop IP address. Instead, it specifies an exit interface (GigabitEthernet0/0/0). This indicates that the router will forward all unknown destinations to the specified interface, and the next hop address is resolved through this interface directly.

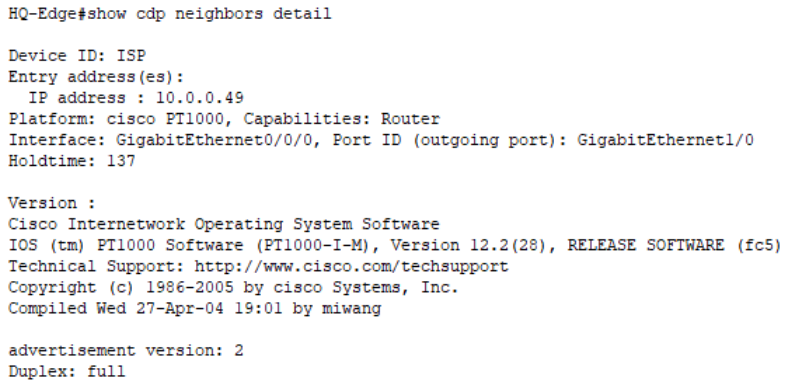
It is configured with the exit interface instead of next hop address.

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

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

[Answer]

The IPv4 address of the next hop (ISP) is **10.0.0.49**.



```
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: 137

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
```

10.0.0.49

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

[Answer]

The port on the ISP router connected to HQ-Edge is **GigabitEthernet1/0**.

GigabitEthernet 1/0

What IOS version is used on the ISP router?

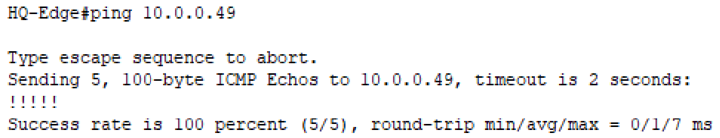
[Answer]

The IOS version used on the ISP router is **12.2(28)**.

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

f. Enter the **ping 10.0.0.49** command.

[Answer]

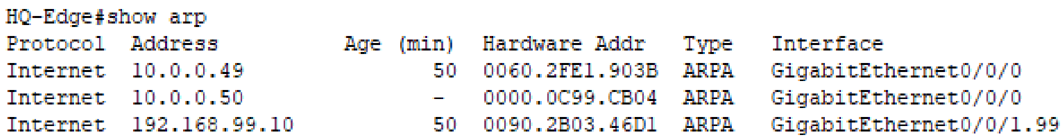


```
HQ-Edge#ping 10.0.0.49

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 = 0/1/7 ms
```

g. Enter the **show arp** command.

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

[Answer]



```
HQ-Edge#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.49               50  0060.2FE1.903B  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.50                -  0000.0C99.CB04  ARPA   GigabitEthernet0/0/0
Internet  192.168.99.10           50  0090.2B03.46D1  ARPA   GigabitEthernet0/0/1.99
```

The MAC address of the interface on the ISP router connected to HQ-Edge is **0060.2FE1.903B**. This address corresponds to the IP address **10.0.0.49**.

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.

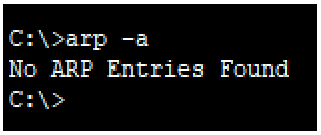
Device	IPv4 Address	Default Gateway
1-1	192.168.10.2	192.168.10.1
1-2	192.168.10.3	192.168.10.1
1-3	192.168.20.3	192.168.20.1
1-4	192.168.20.2	192.168.20.1
FL-1P	192.168.50.2	192.168.50.1
HQ-Laptop-1	192.168.50.4	192.168.50.1

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

What information is displayed?

[Answer]

No ARP Entries Found if the ARP table is empty or if the devices have not yet communicated.



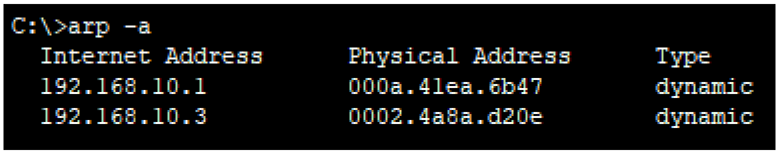
```
C:\>arp -a
No ARP Entries Found
C:\>
```

No ARP Entries Found.

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

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

What information is displayed? [Answer]



```
C:\>arp -a
  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?

[Answer]

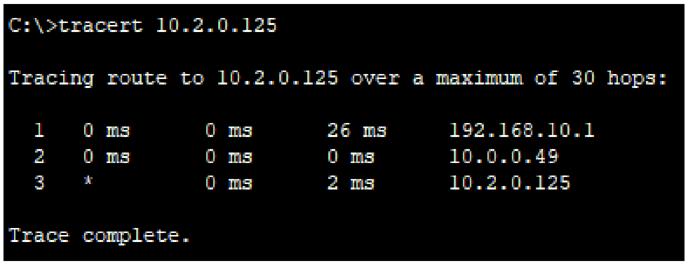
When dealing with VLANs, each VLAN is essentially its own subnet. To communicate between VLANs, packets need to be routed through a device that can handle inter-VLAN routing, typically a router or a Layer 3 switch.

- ARP Table: Displays MAC addresses of devices within the same VLAN because ARP is used to map IP addresses to MAC addresses only for devices directly reachable within the same subnet.
- Default Gateway: The default gateway or router interfaces handle traffic between different VLANs. When you ping a device on a different VLAN, the packet first goes to the default gateway, which then routes it to the appropriate VLAN.

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.

What information is displayed? [Answer]



```
C:\>tracert 10.2.0.125

Tracing route to 10.2.0.125 over a maximum of 30 hops:

  1    0 ms     0 ms    26 ms    192.168.10.1
  2    0 ms     0 ms     0 ms    10.0.0.49
  3    *        0 ms     2 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?

[Answer]

Based on the tracert command output earlier, there are two routers or hops between PC 1-1 and the DNS server (10.2.0.125). Here's the breakdown:

- Hop 1: The first router is 192.168.10.1, which is the default gateway for the 192.168.10.0/24 network.
- Hop 2: The second router is 10.0.0.49, which likely handles routing between VLANs or subnets.

The destination IP 10.2.0.125 is reached in the third hop.

2

Part 3: Diagnose Connectivity Issues

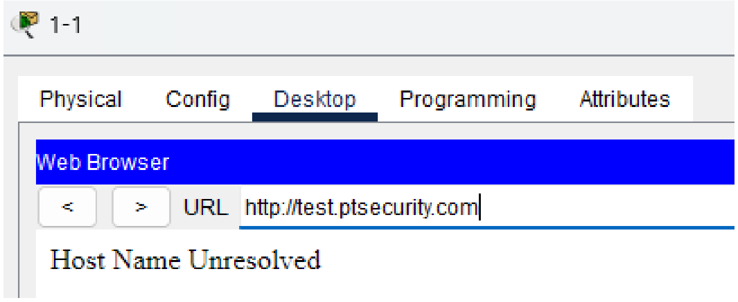
In this part, you will use a variety of diagnostic commands and techniques. You will use the **nslookup** command to query a DNS server and troubleshoot a DNS database. You will then diagnose why a ping fails but web access is successful. Finally, you will use the **netstat** command to discover which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

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



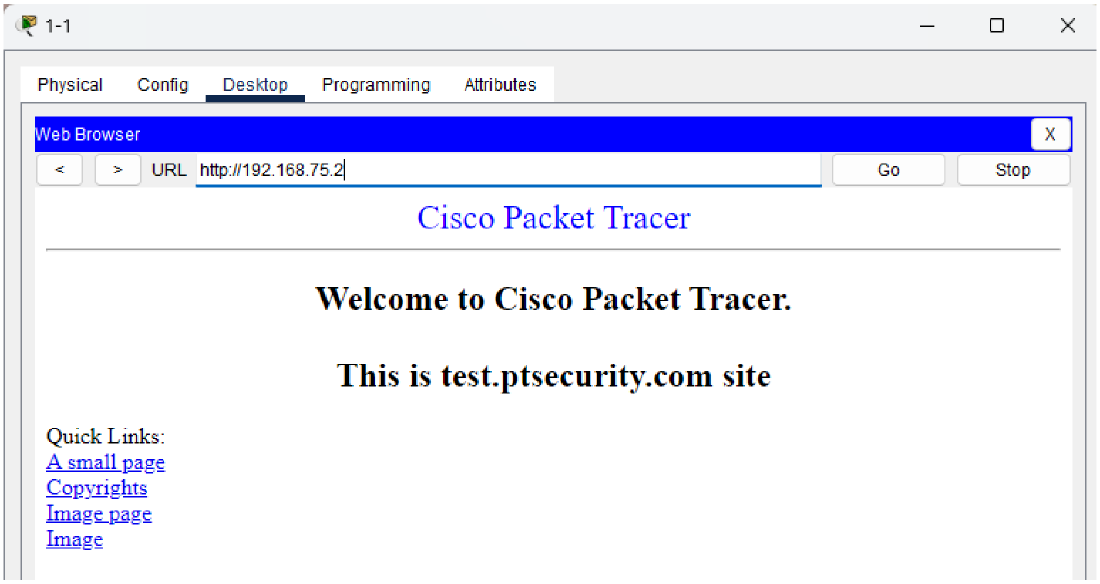
http://test.ptsecurity.com

Host Name Unresolved

No, it does not. The message is “Host Name Unresolved”.

c. Enter the IP address **192.168.75.2**.

Does the web page display? [Answer]



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

Yes

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

[Answer]

The web page displays when using the IP address because the PC can directly reach the server at that IP address. This bypasses the need for DNS resolution, as the address is directly used to access the web server.

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

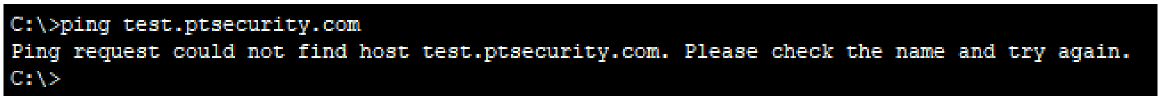
Step 2: Use the nslookup command to verify DNS service.

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

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

What message is displayed?

[Answer]



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

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

What does the message indicate?

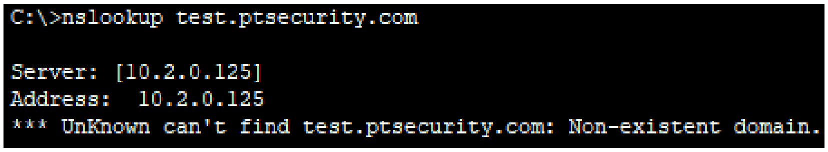
[Answer]

DNS entry is not in the database of the DNS server, it means that the DNS server does not have a record for the domain name `test.ptsecurity.com`

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

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

What message is displayed? [Answer]



```
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.
```

```
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? [Answer] 10.2.0.125

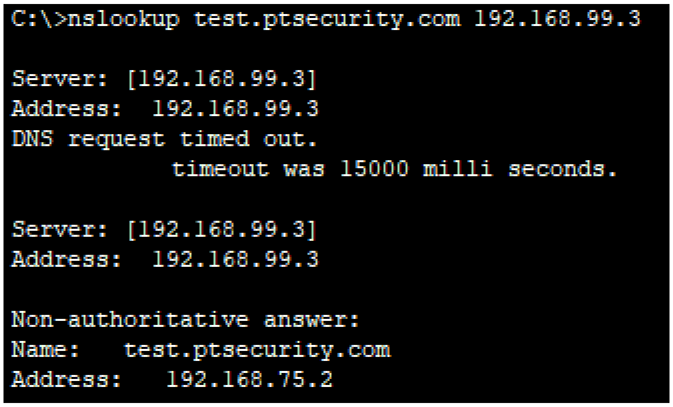
10.2.0.125

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

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

Note: Packet Tracer may take several seconds to converge.

What message is displayed? [Answer]



```
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?

[Answer]

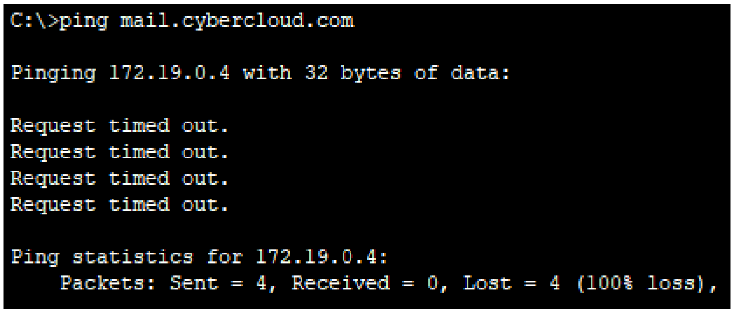
When a domain name is entered into the URL bar, the PC attempts to resolve it using the default DNS server. In this instance, the default DNS server lacks the necessary information in its database.

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.

What message is displayed? [Answer]



```
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?

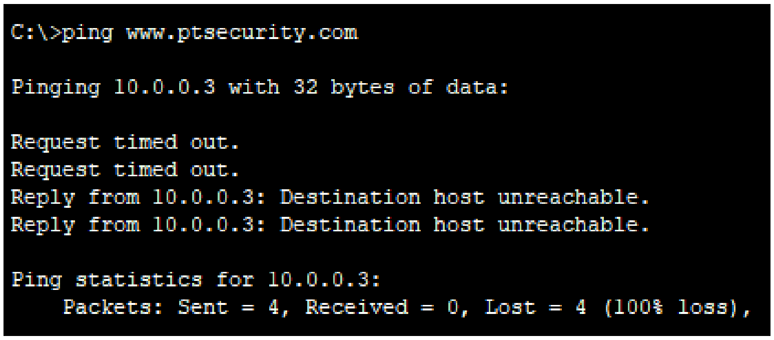
[Answer]

The DNS name resolution is successful, but the ping fails. This could be because the host is inactive or the ICMP echo/echo-reply feature is disabled on the host.

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.

What message is displayed? [Answer]



```
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?

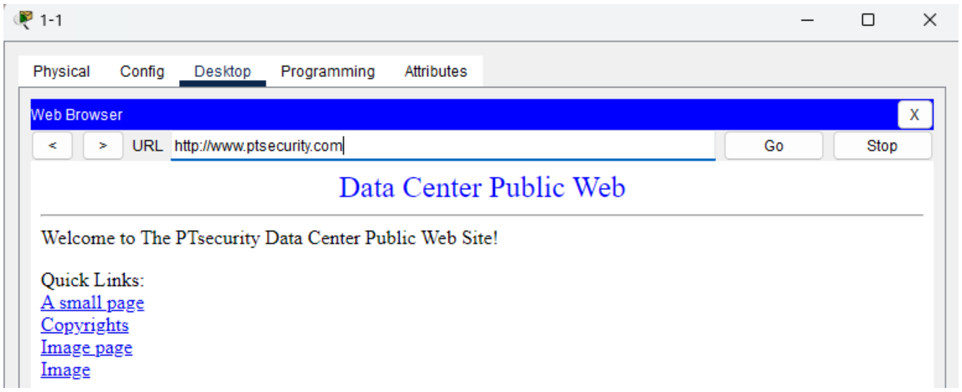
[Answer]

A firewall along the path might be blocking the ping to the destination.

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**.

Does the web page display? [Answer]



Data Center Public Web

Welcome to The PTsecurity Data Center Public Web Site!

Quick Links:
A small page
Copyrights
Image page
Image

Yes

What conclusion can be drawn?

[Answer]

The web host is operational, but the ping requests to the web server are being blocked. This could be due to a firewall or security settings that prevent ICMP echo requests from reaching the server or receiving replies. The server might be configured to ignore or block ICMP packets while still allowing other types of traffic, such as HTTP or HTTPS, to pass through.

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.

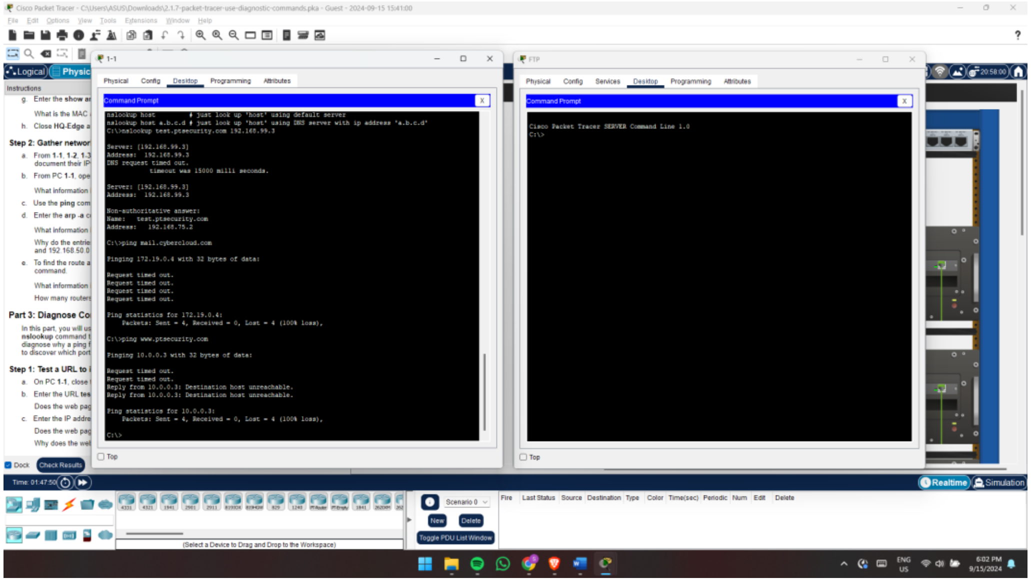
a. Close **Web Browser**, and reopen **Command Prompt**.

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

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

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

[Answer]



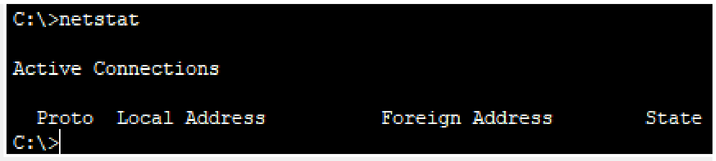
```
nslookup host         # just look up 'host' using default server
nslookup host a.b.c.d # just look up 'host' using DNS server with ip address 'a.b.c.d'
C:\>nslookup test.ptsecurity.com 192.168.99.3

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:\>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:\>
```

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

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

What message is displayed? Does it show any data?

[Answer]



```
C:\>netstat

Active Connections

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

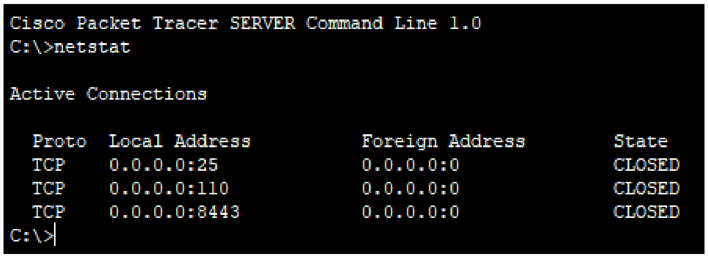
```
C:\>netstat

Active Connections

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

No data is shown.

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

What message is displayed? Does it show any data?

[Answer]



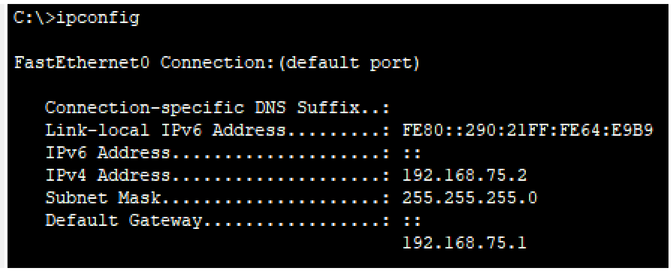
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>netstat

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:\>
```

```
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.

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

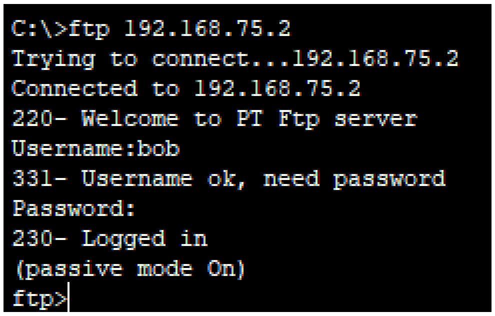
[Answer]



```
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
```

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

[Answer]

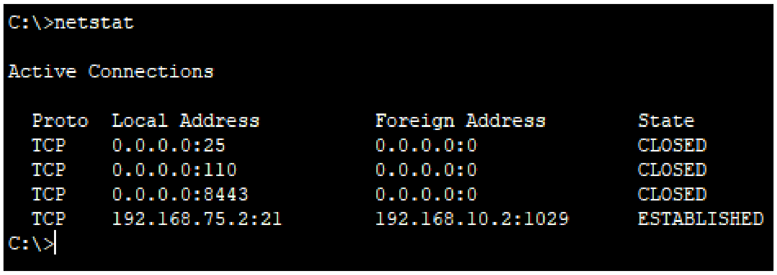


```
C:\>ftp 192.168.75.2
Trying to connect...192.168.75.2
Connected to 192.168.75.2
220- Welcome to PT Ftp server
Username:bob
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

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

What message is displayed? Is there any new information?

[Answer]



```
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        192.168.10.2:1029      ESTABLISHED
C:\>
```

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?

[Answer]

In the output provided:

- The listening port is 21, which is the standard FTP port. The local address (192.168.75.2:21) represents the FTP server, and it is actively listening for FTP connections.
- The status of the connection between the FTP server (192.168.75.2:21) and the client (192.168.10.2:1029, which is likely PC 1-1) is ESTABLISHED, meaning that the FTP session is active and data can be transferred between the two devices.

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

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

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

Does the displayed information change?

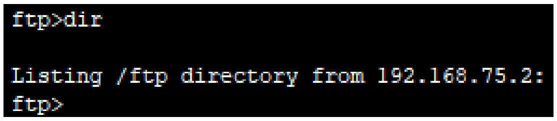
[Answer] No

No.

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

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

[Answer]



```
ftp>dir

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

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

Does the displayed information change?

[Answer]

This new entry indicates that a TCP connection was successfully established between the FTP server (192.168.75.2) and the client (192.168.10.3) to complete an operation, such as file transfer or directory listing. After the task was finished, the connection was 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?

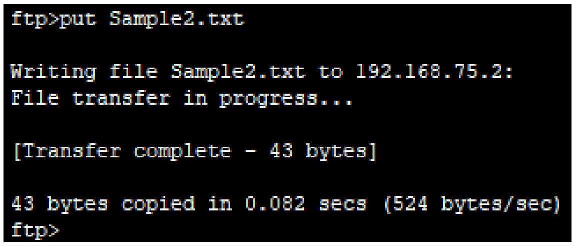
[Answer]

The new entry TCP 192.168.75.2:1028 192.168.10.3:1028 CLOSED indicates that a new TCP connection was established to transfer file names from the FTP directory. Once the file transfer operation was completed, the connection was closed. This shows the successful execution of the FTP session.

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.

[Answer]



```
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 0.082 secs (524 bytes/sec)
ftp>
```

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

Does the displayed information change?

[Answer]

Yes, the displayed information changes. A new entry appears, showing:

TCP 192.168.75.2:1030 192.168.10.3:1029 CLOSING, indicating that a TCP connection between the FTP server (192.168.75.2) and another device (192.168.10.3) is in the process of closing.

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.

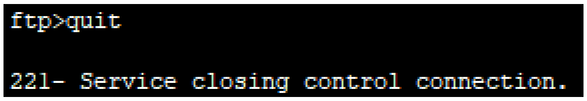
Does the displayed information change?

[Answer]

Yes, after waiting a few seconds and entering the netstat command again, the information has changed. The "CLOSING" line is now gone, indicating that the TCP connection has fully closed.

Yes. The “CLOSING” 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.

Does the displayed information change?

[Answer]

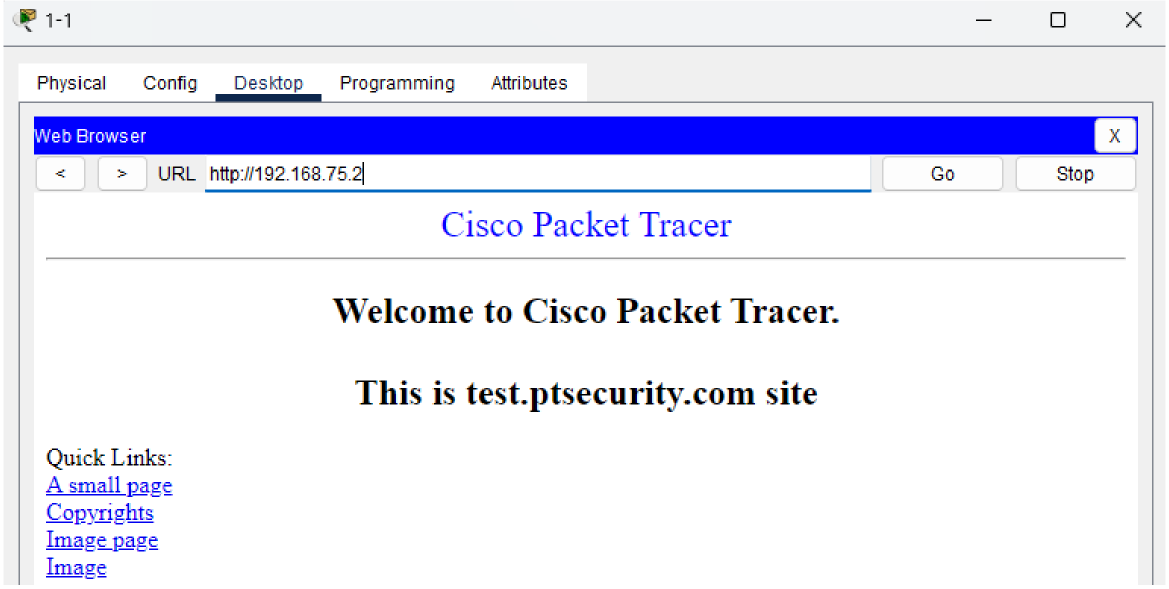
Yes, the TCP connection between 192.168.75.2 on port 21 (FTP server) and 192.168.10.2 on port 1027 (the client) is now closed, indicating that the FTP session has ended and the connection was terminated successfully.

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**.

[Answer]



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.

Does the displayed information change?

[Answer]

Yes, a new entry appears indicating that the TCP connection between 192.168.75.2 on port 80 (the web server) and 192.168.10.2 on port 1030 (the requesting host) is now closed. This shows that the web page request was completed and the connection was terminated.

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

What does this new entry indicate?

[Answer]

The host at 192.168.10.2 makes a request for a web page. The page is successfully delivered and displayed on PC 1-1's web browser, after which the TCP connection is terminated.

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.