

KEAMANAN SISTEM INFORMASI

Packet Tracer – Use Diagnostis Commands



Praktikan

[2141762149]

[ANISNA HILWA NADHIFAH]

[SISTEM INFORMASI BISNIS – 4C]



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

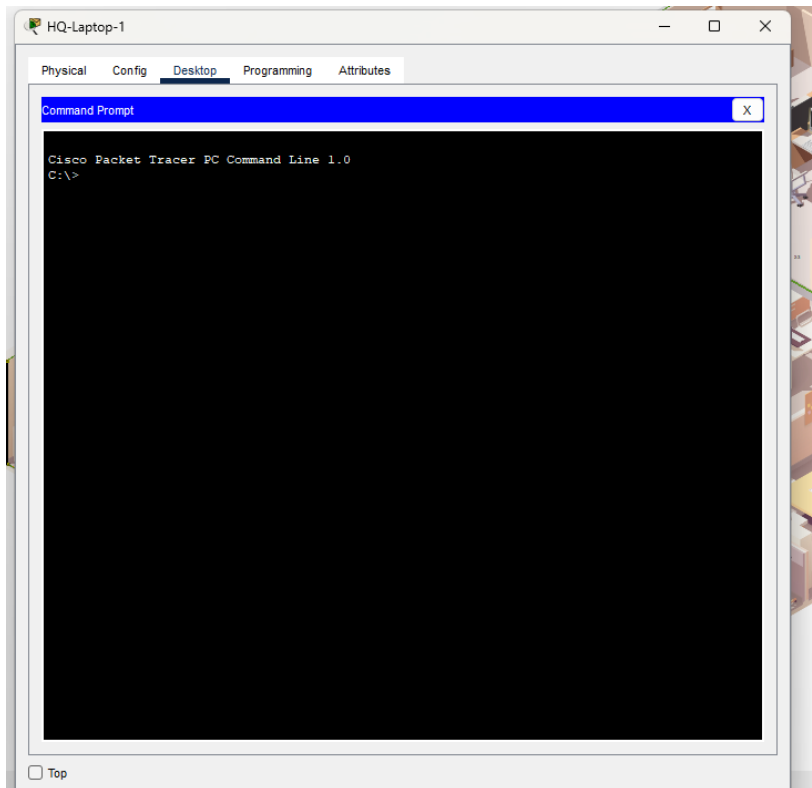
Part 1: Gather End User Device Settings

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.

```
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
```

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



IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 192.168.50.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.50.1

DNS Server: 10.2.0.125

169.256.0.0/16 address, because the wireless connection not may not be established.

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 192.168.50.4

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?

IPv4 addresses are the range 169.254.0.0/16, the method used to set these addresses is APIPA (Automatic Private IP Addressing). APIPA automatically assigns an IP address to a device when the device fails to obtain an IP address from a DHCP server.

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 c private IP addressing (APIPA).

Because the Laptop is unable to obtain IP Address from DHCP and instead using APIPA as a Fallback Mechanism If the IPv4 address is in the 169.254.0.0/16, wait a few seconds and repeat the ipconfig command.

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	192.168.50.1

DNS Servers	N/A
-------------	-----

Do you see a DNS server address? Explain.

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

- 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.....: 192.168.50.5
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                                192.168.50.1
    DHCP Servers.....: 192.168.50.1
    DHCPv6 IAID.....: 
    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:

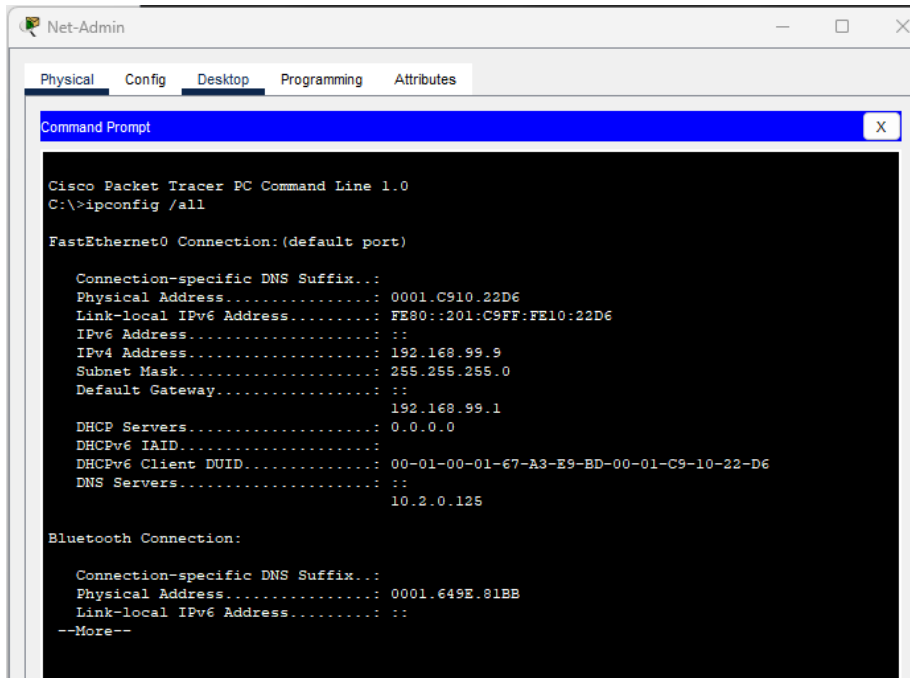
    Connection-specific DNS Suffix...: 
    Physical Address.....: 00E0.A3A2.D8AA
    Link-local IPv6 Address.....: ::
    IPv6 Address.....: ::
--More--
```

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

The DNS server address is 10.2.0.125

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

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

```

What is the IP addressing information displayed under the FastEthernet0 interface?

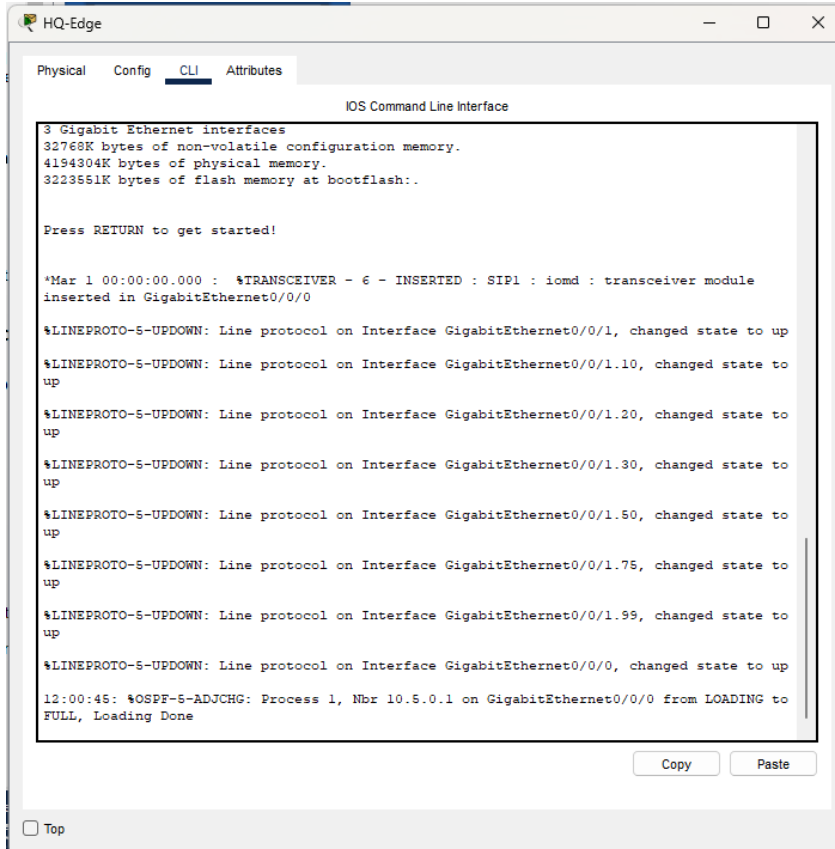
FastEthernet0	IP Addressing Information
Physical Address	0001.C910.22D6
Link-local IPv6 Address	FE80::201:C9FF:FE10:22D6
IPv6 Address	::
IPv4 Address	192.168.99.9
Subnet Mask	255.255.255.0
Default Gateway	192.168.99.1
DNS Servers	10.2.0.125

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	192.168.99.1
DNS Servers	0.0.0.0

Part 2: Gather Information about Network Devices

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

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





- 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, 00:17:41, GigabitEthernet0/0/0
O       10.0.0.32/29 [110/2] via 10.0.0.49, 00:17:41, 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, 00:17:41, GigabitEthernet0/0/0
O       10.2.0.0/16 [110/2] via 10.0.0.49, 00:17:41, 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--
```

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

The address for gateway is 0.0.0.0

Why is the next hop address not displayed?

Because there is still not explicitly configured

It is not explicitly configured.

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

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

```
HQ-Edge>
HQ-Edge>show running-config | begin ip route
```

The default route is configured with the outbound interface, not the next hop address.

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



- e. 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: 161

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?

The IPv4 is 10.0.0.49

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

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)

- f. 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 = 0/3/17 ms
```

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

```
HQ-Edge>show arp
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  10.0.0.49         36         0060.2FE1.903B  ARPA   GigabitEthernet0/0/0
Internet  10.0.0.50         -          0000.0C99.CB04  ARPA   GigabitEthernet0/0/0
HQ-Edge>
```

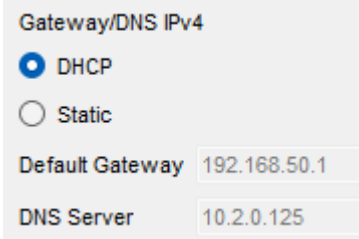
What is the MAC address of the interface on the ISP router that is connected to HQ-Edge?

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 and document their IPv4 addresses and Default Gateways.

Device	IPv4 Address	Default Gateway
1-1	<pre>FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::201:C7FF:FE54:EB5 IPv6 Address.: :: IPv4 Address.: 192.168.10.4 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.10.1</pre>	19.2.168.10.1
1-2	<pre>FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::202:4AFF:FE8A:D20E IPv6 Address.: :: IPv4 Address.: 192.168.10.5 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.10.1</pre>	19.2.168.10.1
1-3	<pre>FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::201:C9FF:FE9:887E IPv6 Address.: :: IPv4 Address.: 192.168.20.4 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.20.1</pre>	19.2.168.20.1
1-4	<pre>FastEthernet0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::201:97FF:FEBA:7BB0 IPv6 Address.: :: IPv4 Address.: 192.168.20.2 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.20.1</pre>	19.2.168.20.1
FL-1P		19.2.168.50.1
HQ-Laptop-1	<pre>Wireless0 Connection: (default port) Connection-specific DNS Suffix...: Link-local IPv6 Address: FE80::20A:F3FF:FE4:EEAA IPv6 Address.: :: IPv4 Address.: 192.168.50.4 Subnet Mask: 255.255.255.0 Default Gateway: :: 192.168.50.1</pre>	19.2.168.50.1



Device	IPv4 Address	Default Gateway
1-1	19.2.168.10.2	19.2.168.10.1
1-2	19.2.168.10.3	19.2.168.10.1
1-3	19.2.168.20.2	19.2.168.20.1
1-4	19.2.168.20.3	19.2.168.20.1
FL-1P	19.2.168.50.2	19.2.168.50.1
HQ-Laptop-1	19.2.168.50.3	19.2.168.50.1

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

c.

What information is displayed?

```
Cisco Packet Tracer PC Command Line 1.0
C:\>arp -a
No ARP Entries Found
C:\>
```

- 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=12ms 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 = 12ms, Average = 3ms
```

1-3

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time<1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=1ms TTL=128
Reply from 192.168.20.2: bytes=32 time=14ms TTL=128

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms
```



1-4

```
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Reply from 192.168.20.3: bytes=32 time=12ms TTL=128
Reply from 192.168.20.3: bytes=32 time<1ms TTL=128
Reply from 192.168.20.3: bytes=32 time<1ms TTL=128
Reply from 192.168.20.3: bytes=32 time=29ms TTL=128

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 29ms, Average = 10ms
```

HQ-Laptop-1

```
C:\>ping 192.168.50.3

Pinging 192.168.50.3 with 32 bytes of data:

Reply from 192.168.50.3: bytes=32 time=146ms TTL=128
Reply from 192.168.50.3: bytes=32 time=44ms TTL=128
Reply from 192.168.50.3: bytes=32 time=15ms TTL=128
Reply from 192.168.50.3: bytes=32 time=19ms TTL=128

Ping statistics for 192.168.50.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 146ms, Average = 56ms
```

- 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?

192.168.10.1	000a.41ea.6b47	dynamic
192.168.10.3	0002.4a8a.d20e	dynamic

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 192.168.10.0/24, 192.168.20.0/24, and 192.168.50.0/24 are on different VLANs.

- 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.

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

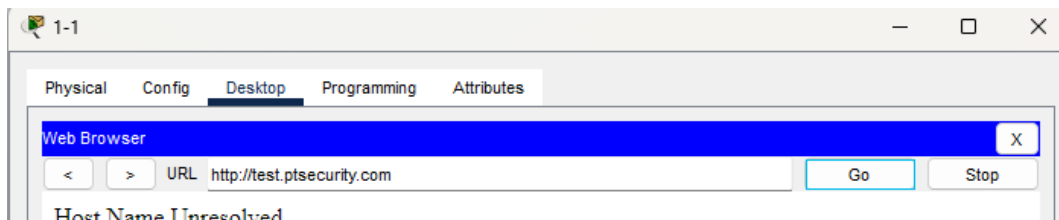
2 routers or hops.

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.

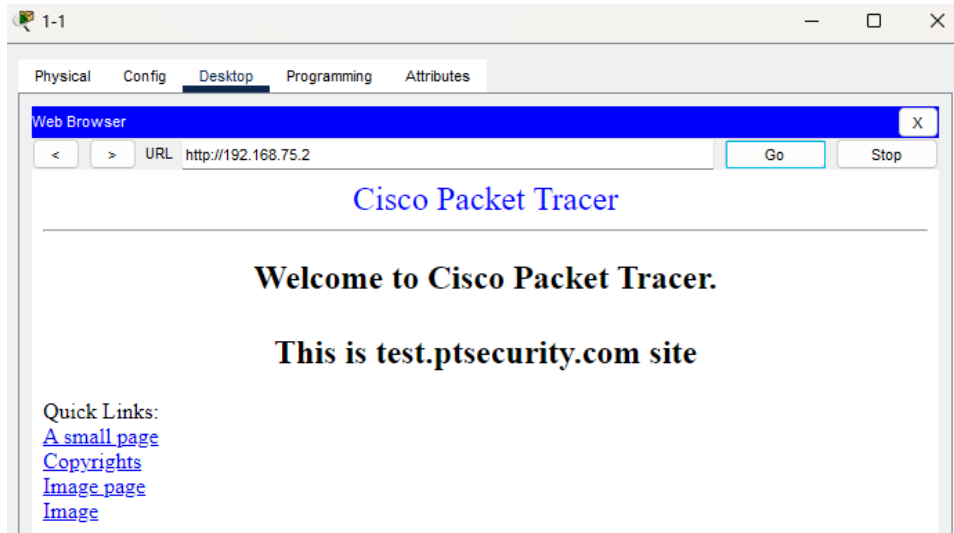
- On PC 1-1, close the **Command Prompt**, and then click **Web Browser**.
- Enter the URL **test.ptsecurity.com**



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

No, and the message is Host Name Unresolved

- Enter the IP address **192.168.75.2**.



Does the web page display?

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

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

- Close **Web Browser**, and then click **Command Prompt**.
- Enter the **ping test.ptsecurity.com** command.

```
C:\>arp -a
No ARP Entries Found
C:\>ping test.ptsecurity.com
Ping request could not find host test.ptsecurity.com. Please check the name and try again.
C:\>
```

What message is displayed?

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

What does the message indicate?

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

- 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.
C:\>
```



What message is displayed?

```
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

- 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'
C:\>
```

- 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 /?
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'
C:\>
```

What message is displayed?

```
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.

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),
```

What information is indicated by the message?

The DNS name resolution is successful, but the ping fail because either the host is disabled, or the reply from the host is disabled

- 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?

```
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 in the path that blocks the ping

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



Does the web page display?

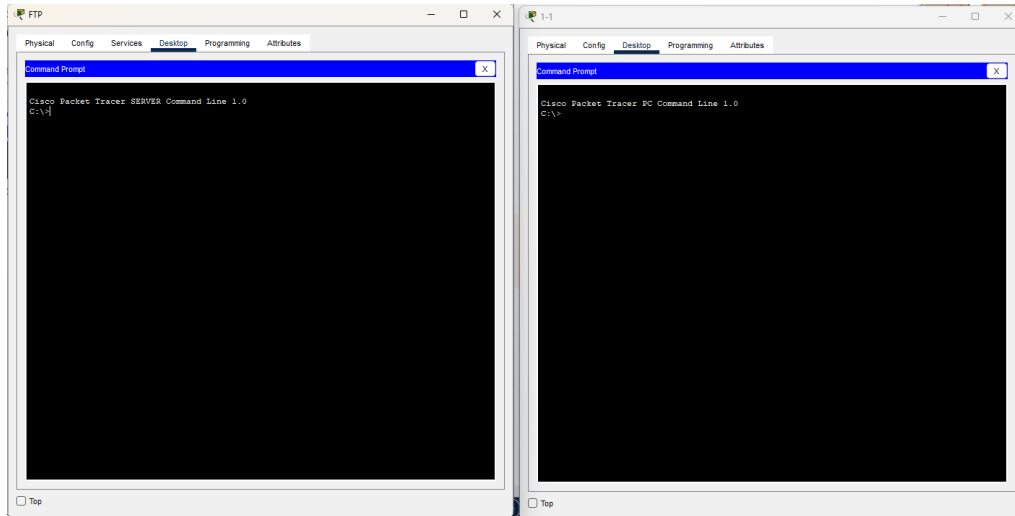
Yes

What conclusion can be drawn?

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

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

- Close **Web Browser**, and reopen **Command Prompt**.
- In **HQ**, click the **Wiring Closet**
- From the right rack, click the **FTP** server > **Desktop** tab > **Command Prompt**.
- 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 PC Command Line 1.0
C:\>netstat

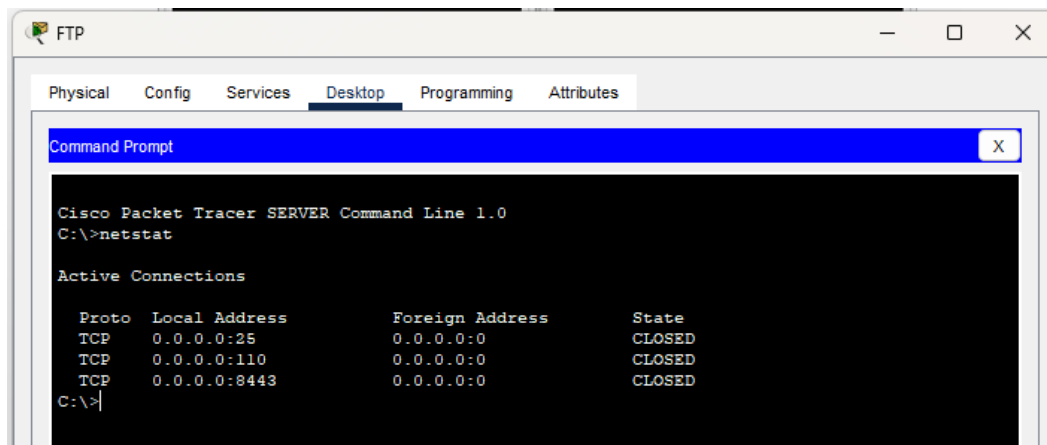
Active Connections

    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:\>
No data is shown
```

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



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:\>

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.

```
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.

```
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:
```

- i. 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         192.168.10.2:1025       ESTABLISHED
C:\>
```

What message is displayed? Is there any new information?

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



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

```
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:|
```

- k. 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         192.168.10.2:1029       ESTABLISHED
    TCP    192.168.75.2:1032       192.168.10.2:1030       CLOSED
C:\>|
```

Does the displayed information change?

Yes, with a entry shows TCP 192.168.75.2:1032 192.168.10.2:1030 CLOSED

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

```
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>
```

- m. 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         192.168.10.2:1026       ESTABLISHED
    TCP    192.168.75.2:1032       192.168.10.2:1030       CLOSED
C:\>
```

Does the displayed information change?

No, with a entry shows of TCP 192.168.75.2:21 192.168.10.2:1026 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 operation is complete

- 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 0.101 secs (425 bytes/sec)
ftp>
```

- p. 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         192.168.10.2:1029      ESTABLISHED
    TCP    192.168.75.2:1036       192.168.10.2:1032      CLOSING
```

Does the displayed information change?

Yes, with a entry shows of TCP 192.168.75.2:1036 192.168.10.2:1032 CLOSING

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

```
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      CLOSED
```

Does the displayed information change?

Yes, with a entry shows of TCP 192.168.75.2:21 192.168.10.2:1029 CLOSED

- 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

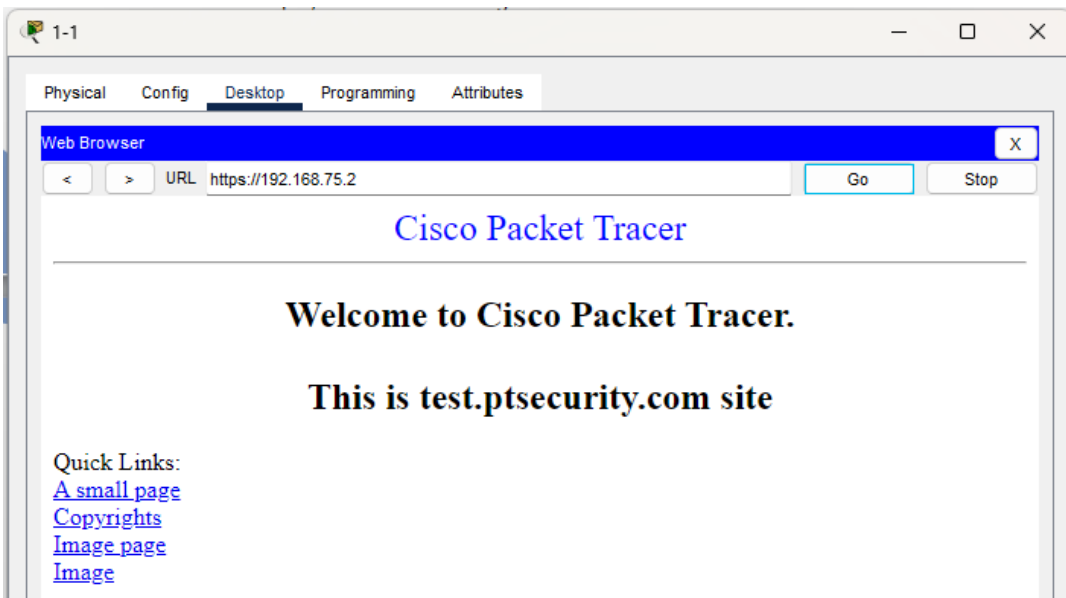
Active Connections

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          192.168.10.2:1029       CLOSED
```

Does the displayed information change?

Yes, with a entry shows of TCP 192.168.75.2:21 192.168.10.2:1029 CLOSED

- t. From **PC 1-1**, close **Command Prompt**, and then open **Web Browser**.
 u. Navigate to **192.168.75.2**.



- 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?

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.

What does this new entry indicate?

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 web browser, after which the TCP connection is closed.