Nama : Mochammad Aldo Rizky

NIM : 2141762002

Kelas : SIB 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.

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

The IPv4 address displayed for Wireless0 Connection may be in the range 169.254.0.0/16 because the laptop has not obtained an address from DHCP, and this is an automatic IP address (APIPA).

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?

The method used to assign IPv4 addresses is Automatic Private IP Addressing (APIPA). Laptops are assigned IPv4 addresses in the range 169.254.0.0/16 because they cannot obtain addresses from a DHCP server. APIPA allows devices to continue communicating within the local network even without DHCP.

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.

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
IPv6 Address	::
IPv4 Address	192.168.50.4 (may vary, but will be in the range 192.168.50.0/24)
Subnet Mask	255.255.255.0
Default Gateway	192.168.50.1
DNS Servers	N/A

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.

The regular ipconfig command does not report the DNS server addresses in this case.

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?

Yes, the DNS server address displayed is 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**.

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

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

FastEthernet0	IP Addressing Information
Physical Address	0001.C910.22D6 (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	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.

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

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

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

The default gateway is 0.0.0.0, which indicates that all traffic that does not have a specific route will be sent to the network connected through the GigabitEthernet0/0/0 interface.

0.0.0.0

Why is the next hop address not displayed?

The next hop address is not shown because the default route (0.0.0.0/0) is a direct route to the network interface, which is GigabitEthernet0/0/0. In this case, the device is directly connected to the ISP or another device that does not require an additional hop through another router. Thus, there is no next hop other than the interface itself.

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?

The default route is configured using the outgoing interface GigabitEthernet0/0/0, and does not use a next hop address. This means that traffic that does not have a more specific route will be sent directly out through this interface without needing to specify a next hop IP address.

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?

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

10.0.0.49

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

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

GigabitEthernet 1/0

What IOS version is used on the ISP router?

The IOS version used on the ISP router is Cisco Internetwork Operating System Software IOS (tm) PT1000 Software, Version 12.2(28), RELEASE SOFTWARE (fc5).

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

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

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

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

The MAC address of the interface on the ISP router connected to the HQ-Edge is 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	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	192.168.50.3	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
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.

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**.

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

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

ARP provides a table that maps known MAC addresses to their associated IP addresses.

```
  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?

The networks 192.168.10.0/24, 192.168.20.0/24, and 192.168.50.0/24 are on different VLANs. When pinging from the 192.168.10.0 network to another network on a different VLAN, the traffic must first go through the default gateway. Since ARP only records MAC addresses for devices on the same network (in the same VLAN), the ARP table only contains information about devices on the local 192.168.10.0/24 network, and not from other VLANs.

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?

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 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?

There are 2 hops between PC 1-1 and the DNS server.

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?

No, the web page is not displayed. The message is "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?

Yes, the web page is displayed.

Yes

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

Web pages are displayed using IP addresses because the PC cannot resolve domain names to IP addresses. This indicates a problem with DNS resolution, where the request to translate a domain name to an IP address fails, but when the IP address is entered directly, a connection can be established without the need for DNS.

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?

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 message indicates that the DNS entry for test.ptsecurity.com does not exist in the DNS server database or that the PC cannot contact the DNS server to resolve the domain name to an IP address.

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

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

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?

The default DNS server is 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?

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?

When a domain name is entered in the URL box, the PC tries to resolve it through the default DNS server. In this case, the default DNS server (10.2. 0.125) does not have an entry for that domain name in its database, so it cannot resolve the domain name test.ptsecurity.com.

However, when using the alternative DNS server (192.168. 99.3), the domain information is successfully found and parsed.

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?

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?

DNS name resolution is successful, as mail.cybercloud.com is successfully resolved to 172.19.0.4. However, ping fails. Possible causes are that host 172.19.0.4 is down or ICMP echo request/reply (ping) 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?

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 message indicates that there is a firewall or other device in the path that is blocking the ping to the destination. Although the server 10.0.0.3 is reachable, the destination host is not reachable via ICMP.

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?

Yes, the web page is displayed.

Yes

What conclusion can be drawn?

The web host www.ptsecurity.com is running and accessible via HTTP/HTTPS, but pings to the web server are blocked, likely by a firewall or security settings that disable ICMP.

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.

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

What message is displayed? Does it show any data?

Active Connections

Proto Local Address Foreign Address State

```
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?

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.
```

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

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

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

What message is displayed? Is there any new information?

TCP 192.168.75.2:21 192.168.10.3:1025 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 listening port is TCP 21, which is the standard port for FTP. The connection status is ESTABLISHED, indicating that a TCP connection has been established between PC 1-1 and the FTP server.

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?

NO, the information displayed does not change after entering the username.

No.

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

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

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

Does the displayed information change?

Yes, TCP 192.168.75.2:1028 192.168.10.3:1028 TERTUTUP

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

What is indicated by this new entry?

This new entry indicates that a temporary TCP connection was opened to transfer data (file names in the FTP directory) from the FTP server to PC 1-1. Once the operation is complete, the connection is immediately closed.

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.

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

Does the displayed information change?

Yes, TCP 192.168.75.2:1030 192.168.10.3:1029 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?

Yes. The line with the status "CLOSING" is no longer there, indicating that the temporary connection has been closed.

Yes. The “CLOSING” line is gone.

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

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

Does the displayed information change?

Yes. The TCP connection between 192.168.75.2:21 (the FTP server port) and 192.168.10.2:1027 (PC 1-1 port) was closed, indicating that the FTP session has ended.

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**.

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

Does the displayed information change?

Yes. New entries show: TCP 192.168.75.2:80 192.168.10.2:1030 CLOSED.

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

What does this new entry indicate?

This entry indicates that a web page request was made by host 192.168.10.2 (PC 1-1) over port 80 (HTTP). After the web page was transmitted to PC 1-1 and displayed in the browser, the TCP connection was 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.