Networking Academy

NAME: BEATRICE ANN DAVID A23CS0055

LAB 1:
10.3.5: Packet Tracer - Troubleshoot Default Gateway Issues

Addressing Table (UPDATED)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.2	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.11.2	255.255.255.0	192.168.11.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.10.11	255.255.255.0	192.168.10.1
PC3	NIC	192.168.11.10	255.255.255.0	192.168.11.1
PC4	NIC	192.168.11.11	255.255.255.0	192.168.11.1

Objectives

Part 1: Verify Network Documentation and Isolate Problems Part

2: Implement, Verify, and Document Solutions

Background

For a device to communicate across multiple networks, it must be configured with an IP address, subnet mask, and a default gateway. The default gateway is used when the host wants to send a packet to a device on another network. The default gateway address is generally the address of the router interface which is attached to the local network that the host is connected to. In this activity, you will finish documenting the network. You will then verify the network documentation by testing end-to-end connectivity and troubleshooting issues. The troubleshooting method you will use consists of the following steps:

a. Verify the network documentation and use tests to isolate problems.

b. Determine an appropriate solution for a given problem.

c. Implement the solution.

d. Test to verify the problem is resolved.

e. Document the solution.

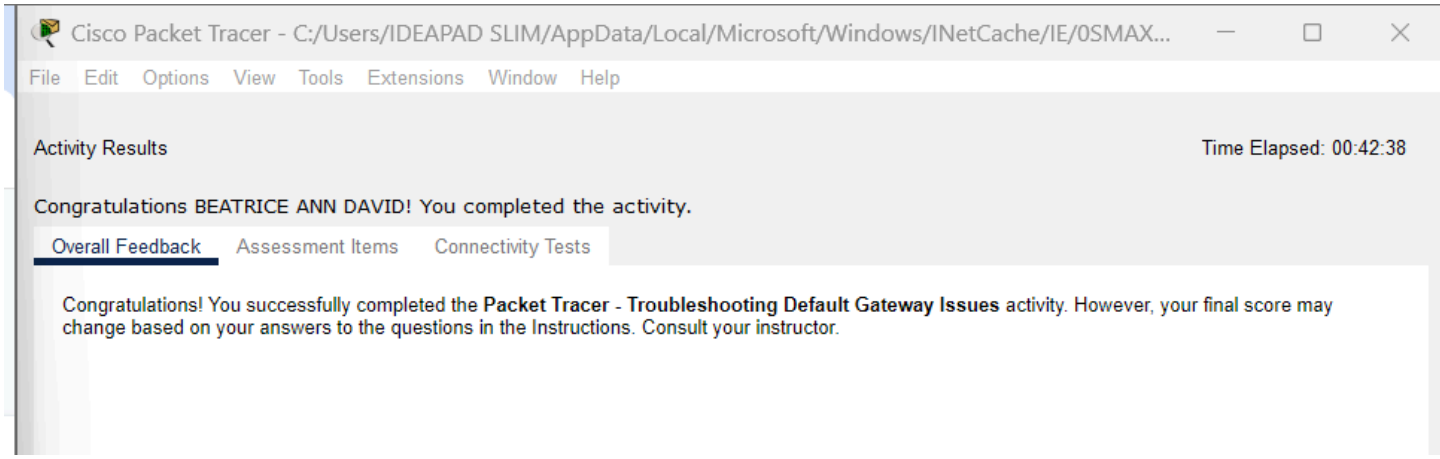
Throughout your CCNA studies, you will encounter different descriptions of the troubleshooting method, as well as different ways to test and document issues and solutions. This is intentional. There is no set standard or template for troubleshooting. Each organization develops unique processes and documentation standards (even if that process is “we don’t have one”). However, all effective troubleshooting methodologies generally include the steps above.

Note: If you are proficient with default gateway configurations, this activity might seem more involved than it should be. You can, most likely, quickly discover and solve all the connectivity issues faster than following these

procedures. However, as you proceed in your studies, the networks and problems you encounter will become increasingly more complex. In such situations, the only effective way to isolate and solve issues is to use a methodical approach such as the one used in this activity.

Screenshots:

A. Result:



B. Working:

Part 1: Verify Network Documentation and Isolate Problems

In Part 1 of this activity, complete the documentation and perform connectivity tests to discover issues. In addition, you will determine an appropriate solution for implementation in Part 2.

Step 1: Verify the network documentation and isolate any problems.

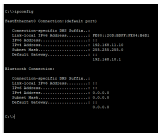
a. Before you can effectively test a network, you must have complete documentation. Notice in the **Addressing Table** that some information is missing. Complete the **Addressing Table** by filling in the missing default gateway information for the switches and the PCs.

DONE. It's on Page 1.

b. Test connectivity to devices on the same network. By isolating and correcting any local access issues, you can better test remote connectivity with the confidence that local connectivity is operational.

A verification plan can be as simple as a list of connectivity tests. Use the following tests to verify local connectivity and isolate any access issues. The first issue is already documented, but you must implement and verify the solution during Part 2.

Testing and Verification Documentation

Test	Successful?	Issues	Solution	Verified
PC1 to PC2	**No**	**IP address on PC1** 	**Change PC1 IP address**	**Verify**
PC1 to S1	**NO**	**Default Gateway on S1**	**Configure Default Gateway**	**Verify**

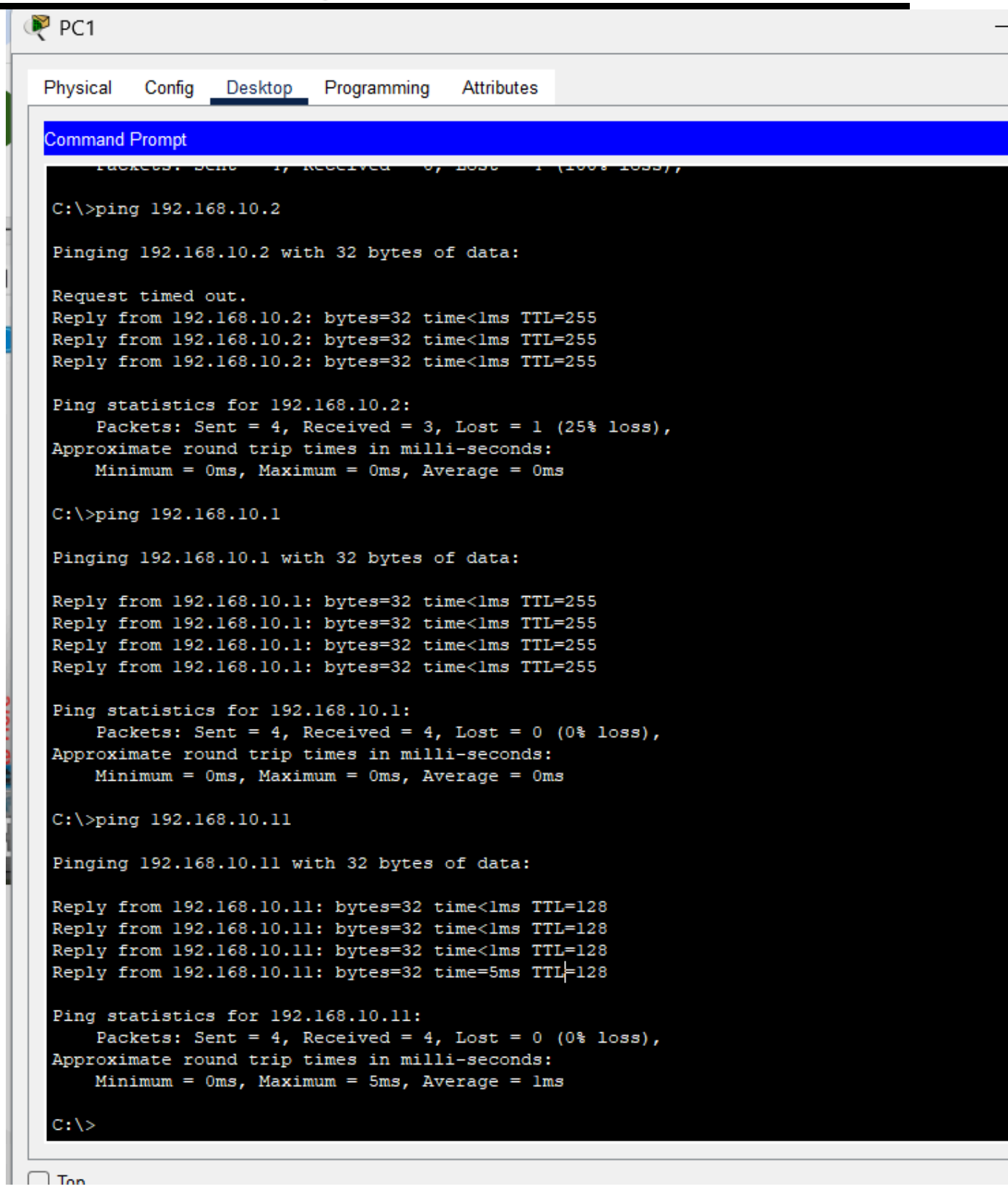
		S1>enable S1#show running-config Building configuration... Current configuration : 1096 bytes ! version 15.0 no service timestamps log datetime msec no service timestamps debug datetime msec no service password-encryption ! hostname S1 ! ! ! ! ! ! spanning-tree mode pvst spanning-tree extend system-id ! interface FastEthernet0/1 ! interface FastEthernet0/2 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 ! interface FastEthernet0/8 !		
PC1 to R1	**NO**	**IP address on PC1** ! ! ! interface GigabitEthernet0/0 ip address 192.168.10.1 255.255.255.0 duplex auto speed auto ! interface GigabitEthernet0/1 ip address 192.168.11.1 255.255.255.0 duplex auto speed auto ! interface Vlan1 no ip address shutdown ! ip classless ! ip flow-export version 9 ! ! ! !	**Change PC1 address**	**Verify**
PC2 to S1	**Yes**	C:\>ping 192.168.10.2 Pinging 192.168.10.2 with 32 bytes of data: Request timed out. Reply from 192.168.10.2: bytes=32 time<1ms TTL=255 Reply from 192.168.10.2: bytes=32 time<1ms TTL=255 Reply from 192.168.10.2: bytes=32 time<1ms TTL=255 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>	-	Verify
PC2 to R1	**Yes**	C:\>ping 192.168.10.1 Pinging 192.168.10.1 with 32 bytes of data: Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Reply from 192.168.10.1: bytes=32 time<1ms TTL=255 Ping statistics for 192.168.10.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>	-	**Verify**
PC3 to PC4	**Yes**	C:\>ping 192.168.11.11 Pinging 192.168.11.11 with 32 bytes of data: Reply from 192.168.11.11: bytes=32 time<1ms TTL=128 Reply from 192.168.11.11: bytes=32 time<1ms TTL=128 Reply from 192.168.11.11: bytes=32 time<1ms TTL=128 Reply from 192.168.11.11: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.11.11: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\>	-	**Verify**
PC3 to S2	**No**	**Wrong IP address used to ping** C:\>ping 192.168.11.2 Pinging 192.168.11.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.11.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\>	**Use the interface g0/0 ip address**	**Verify**
PC4 to PC3	**Yes**	C:\>ping 192.168.11.10 Pinging 192.168.11.10 with 32 bytes of data: Reply from 192.168.11.10: bytes=32 time=5ms TTL=128 Reply from 192.168.11.10: bytes=32 time<1ms TTL=128 Reply from 192.168.11.10: bytes=32 time<1ms TTL=128 Reply from 192.168.11.10: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.11.10: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 5ms, Average = 1ms C:\>	-	**Verify**
PC4 to S2	**No**	C:\>ping 192.168.11.2 Pinging 192.168.11.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.11.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), **Wrong IP address used to ping**	**Use the gateway ip address**	**Verify**

Note: The table is an example; you must create your own document. You can use paper and pencil to draw a table, or you can use a text editor or spreadsheet. Consult your instructor if you need further guidance.

c. Test connectivity to remote devices (such as from PC1 to PC4) and document any problems. This is frequently referred to as *end-to-end connectivity*. This means that all devices in a network have the full connectivity allowed by the network policy.

Note: Remote connectivity testing may not be possible yet, because you must first resolve local connectivity issues. After you have solved those issues, return to this step and test connectivity between networks.

Packet Tracer - Troubleshoot Default Gateway Issues



PC3

```
C:\>ping 192.168.11.2

Pinging 192.168.11.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.11.2: bytes=32 time<1ms TTL=255
Reply from 192.168.11.2: bytes=32 time<1ms TTL=255
Reply from 192.168.11.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.11.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 2: Determine an appropriate solution for the problem.

a. Using your knowledge of the way networks operate and your device configuration skills, search for the cause of the problem. For example, S1 is not the cause of the connectivity issue between PC1 and PC2. The link lights are green and no configuration on S1 would cause traffic to not pass between PC1 and PC2. So the problem must be with PC1, PC2, or both.

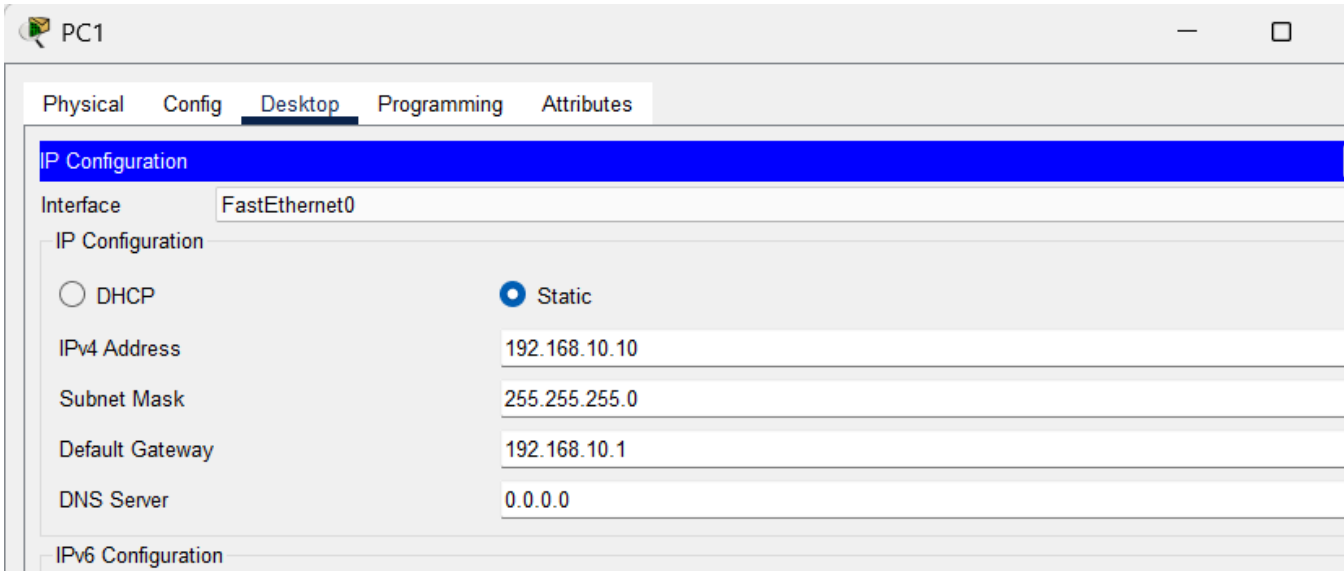
b. Verify the device addressing to ensure it matches the network documentation. For example, the IP address for PC1 is incorrect as verified with the **ipconfig** command.

c. Suggest a solution that you think will resolve the problem and document it. For example, change the IP address for PC1 to match the documentation.

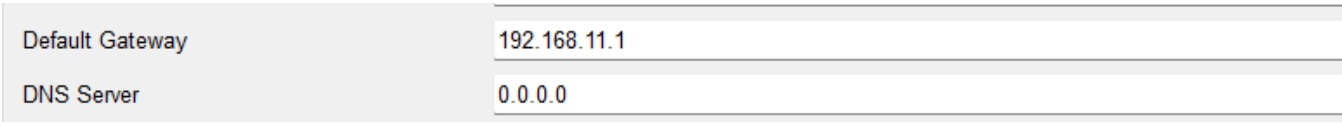
Note: Often there is more than one solution. However, it is a troubleshooting best practice to implement and verify one solution at a time. Implementing more than one solution could introduce additional issues in a more complex scenario.

Solution:

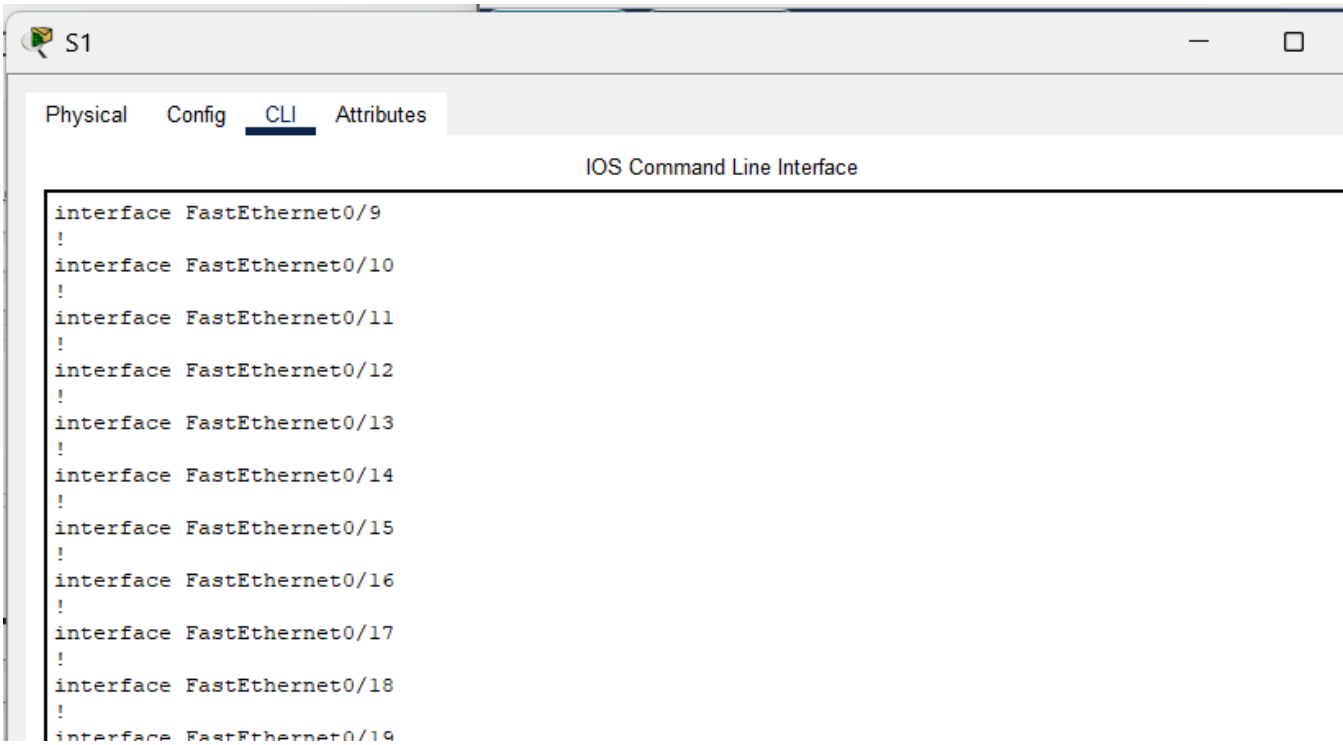
1. **IP address on PC1 is wrongly configured. But, fix it.**



2. **Default gateway in PC 4 is wrongly configured. Fix it.**



3. **S1 default gateway is not configured.**



4. **S2 IP address is not configured**

```
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.11.2 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#
```

Part 2: Implement, Verify, and Document Solutions

In Part 2 of this activity, you will implement the solutions you identified in Part 1. You will then verify the solution worked. You may need to return to Part 1 to finish isolating all the problems.

Step 1: Implement solutions to connectivity problems.

Refer to your documentation in Part 1. Choose the first issue and implement your suggested solution. For example, correct the IP address on PC1.

```
S1#
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway
% Incomplete command.
S1(config)#ip default-gateway?
default-gateway
S1(config)#ip default-gateway 192.168.10.1
S1(config)#ip default-gateway 192.168.10.1 ?
  <cr>
S1(config)#ip default-gateway 192.168.10.1
S1(config)#
```

Step 2: Verify that the problem is now resolved.

a. Verify your solution has solved the problem by performing the test you used to identify the problem. For example, can PC1 now ping PC2?

Yes

b. If the problem is resolved, indicate so in your documentation. For example, in the table above, a simple checkmark would suffice in the “Verified” column.

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.2: bytes=32 time<1ms TTL=254
Reply from 192.168.10.2: bytes=32 time<1ms TTL=254
Reply from 192.168.10.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 3: Verify that all issues are resolved.

a. If you still have an outstanding issue with a solution that has not yet been implemented, return to Part 2, Step 1.

b. If all your current issues are resolved, have you also resolved any remote connectivity issues (such as can PC1 ping PC4)? If the answer is no, return to Part 1, Step 1c to test remote connectivity.

```
C:\>ping 192.168.11.11

Pinging 192.168.11.11 with 32 bytes of data:

Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127
Reply from 192.168.11.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```