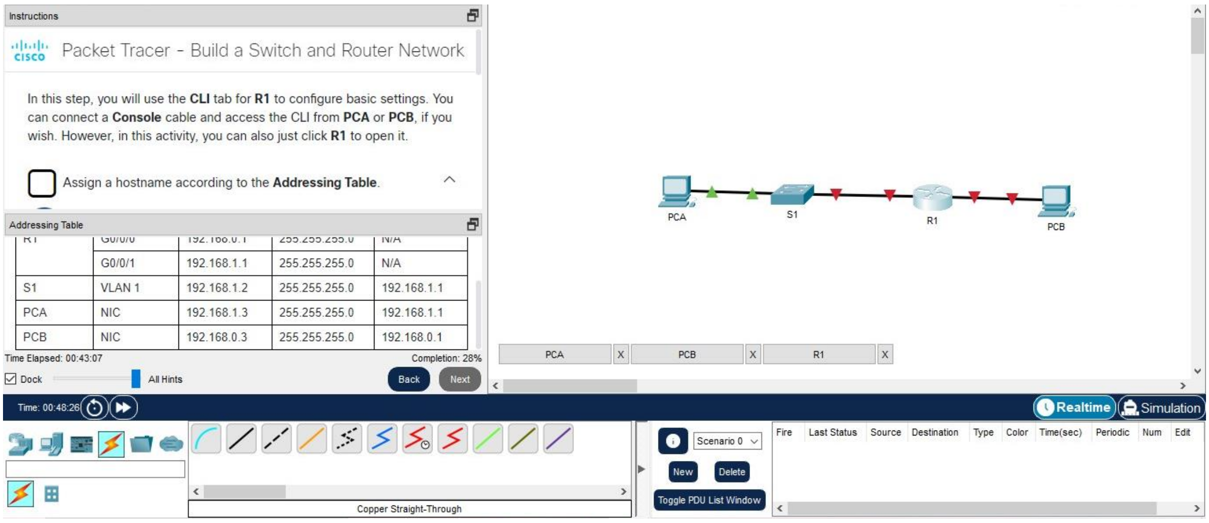
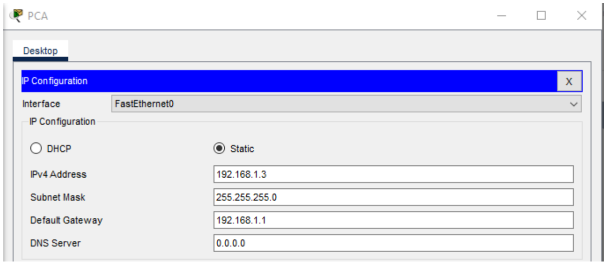
Packet tracer tutored activity build a switch and router network

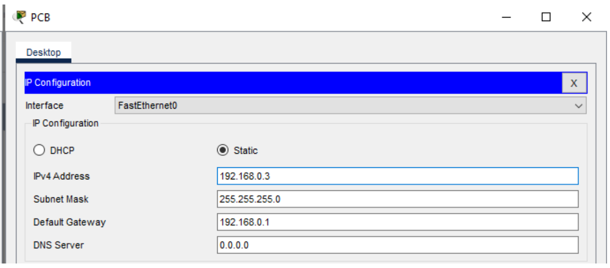
Part 1: Set Up Cable with Copper Straight-Throught



Part 2: Configure Devices and Verify Connectivity

Step 2: Set the IP Configuration





Step 2: Configure The Router R1

CLI

IOS Command Line Interface

```
Router>en
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd $ Authorized Users Only! $
R1(config)#banner motd $Authorized Access Only!$
R1(config)#interface g0/0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:acad::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

Copy Paste

```
R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

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

R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

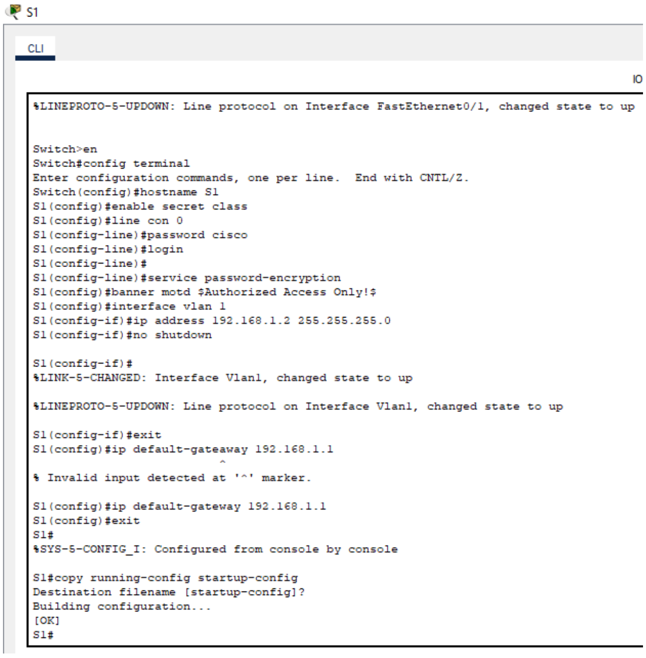
Copy Paste

Top

Step 3: Test connectivity between PCA and PCB

```
C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time<1ms TTL=127
Reply from 192.168.0.3: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

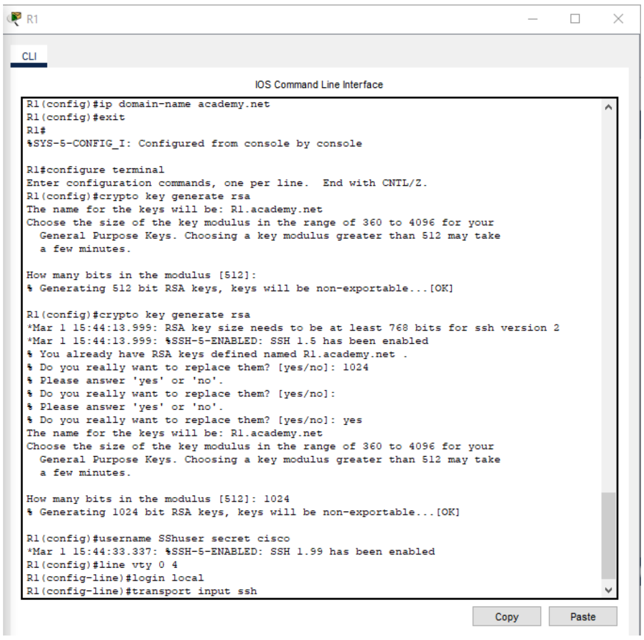
Step 4:Configure The S1




```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>en
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#
S1(config-line)#service password-encryption
S1(config)#banner motd $Authorized Access Only!$
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.2 255.255.255.0
S1(config-if)#no shutdown

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#exit
S1(config)#ip default-gateaway 192.168.1.1
                          ^
% Invalid input detected at '^' marker.

S1(config)#ip default-gateway 192.168.1.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

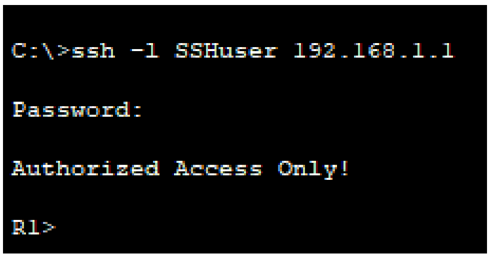
Pasrt 3: Secure remote access to R1

Step 1: CLI R1

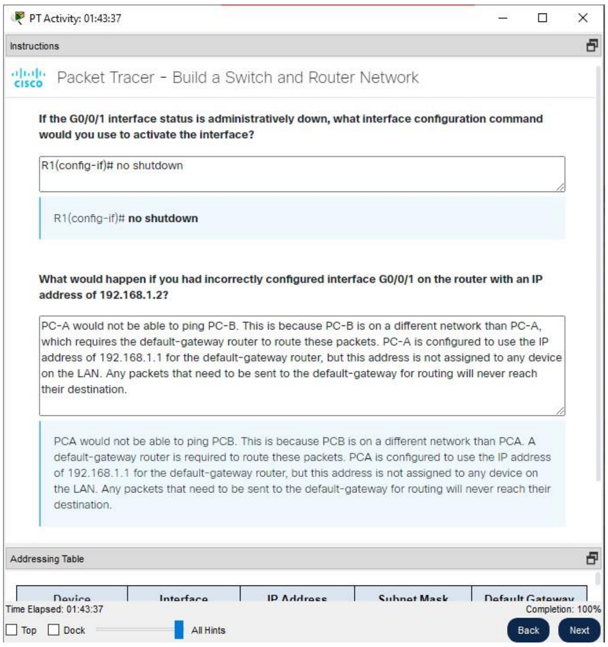


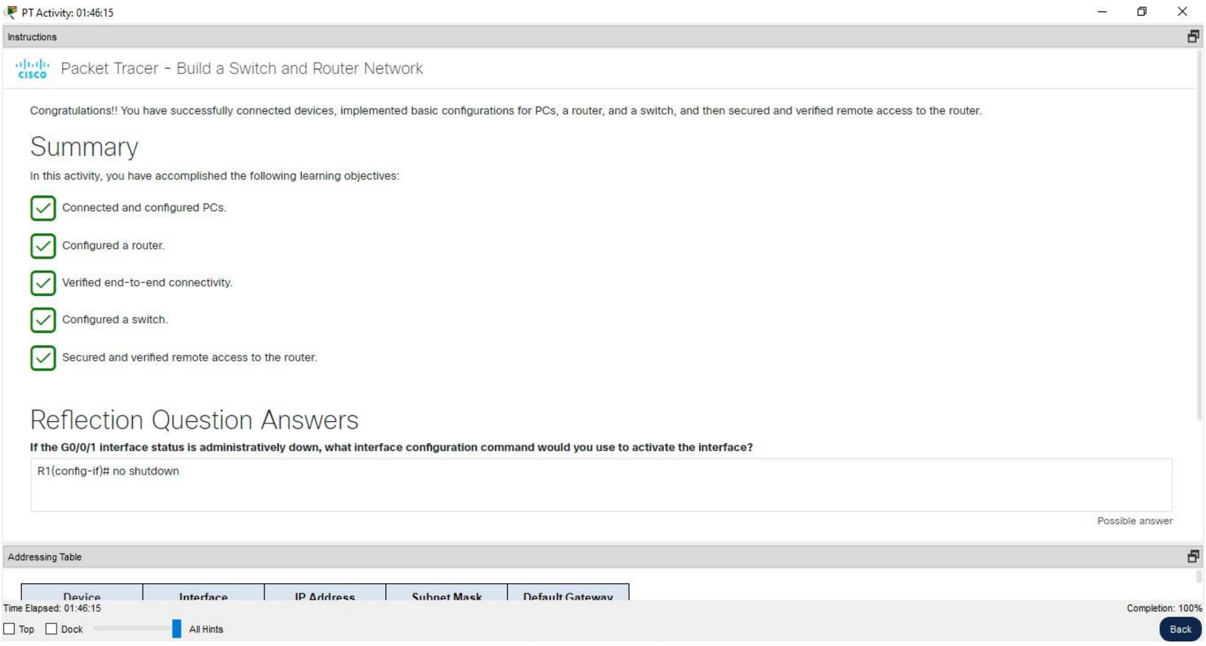

```
R1(config)#ip domain-name academy.net
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto key generate rsa
The name for the keys will be: R1.academy.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#crypto key generate rsa
*Mar 1 15:44:13.999: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 15:44:13.999: %SSH-5-ENABLED: SSH 1.5 has been enabled
% You already have RSA keys defined named R1.academy.net .
% Do you really want to replace them? [yes/no]: 1024
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]:
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: R1.academy.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#username SShuser secret cisco
*Mar 1 15:44:33.337: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
```

Step 2: Verify SSH remote access From PCA or PCB



```
C:\>ssh -l SSHuser 192.168.1.1

Password:

Authorized Access Only!

R1>
```


PT Activity: 01:43:37
Instructions
Packet Tracer - Build a Switch and Router Network
If the G0/0/1 interface status is administratively down, what interface configuration command would you use to activate the interface?
R1(config-if)# no shutdown
R1(config-if)# no shutdown
What would happen if you had incorrectly configured interface G0/0/1 on the router with an IP address of 192.168.1.2?
PC-A would not be able to ping PC-B. This is because PC-B is on a different network than PC-A, which requires the default-gateway router to route these packets. PC-A is configured to use the IP address of 192.168.1.1 for the default-gateway router, but this address is not assigned to any device on the LAN. Any packets that need to be sent to the default-gateway for routing will never reach their destination.
PCA would not be able to ping PCB. This is because PCB is on a different network than PCA. A default-gateway router is required to route these packets. PCA is configured to use the IP address of 192.168.1.1 for the default-gateway router, but this address is not assigned to any device on the LAN. Any packets that need to be sent to the default-gateway for routing will never reach their destination.
Addressing Table
Device
Interface
IP Address
Subnet Mask
Default Gateway
Time Elapsed: 01:43:37
Completion: 100%
Top
Dock
All Hints
Back
Next


PT Activity: 01:46:15
Instructions
Packet Tracer - Build a Switch and Router Network
Congratulations!! You have successfully connected devices, implemented basic configurations for PCs, a router, and a switch, and then secured and verified remote access to the router.
Summary
In this activity, you have accomplished the following learning objectives:
Connected and configured PCs.
Configured a router.
Verified end-to-end connectivity.
Configured a switch.
Secured and verified remote access to the router.
Reflection Question Answers
If the G0/0/1 interface status is administratively down, what interface configuration command would you use to activate the interface?
R1(config-if)# no shutdown
Possible answer
Addressing Table
Device
Interface
IP Address
Subnet Mask
Default Gateway
Time Elapsed: 01:46:15
Completion: 100%
Top
Dock
All Hints
Back

Packet Tracer - Troubleshoot Default Gateway Issues

Addressing Table

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.

Instructions

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.

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**	**Yes**
PC1 to S1	**No**	**IP address on PC1**	**Change PC1 IP address**	**Yes**
PC1 to R1	**No**	**IP address on PC1**	**Change PC1 IP address**	**Yes**
PC2 to S1	**Yes**			
PC2 to R1	**Yes**			
PC3 to PC4	**Yes**			
PC3 to S2	**No**	**IP on S2**	**Change IP for S2**	**Yes**
PC3 to R1	**Yes**			
PC4 to S2	**No**	**IP on S2**	**Change IP for S2**	**Yes**
PC4 to R1	**Yes**			

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.

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.

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.

Step 2: Verify that the problem is now resolved.

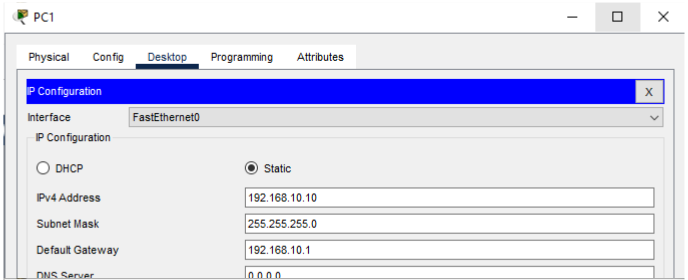
a. Verify your solution has solved the problem by performing the test you used to identify the problem. For example, can PC1 now ping PC2?

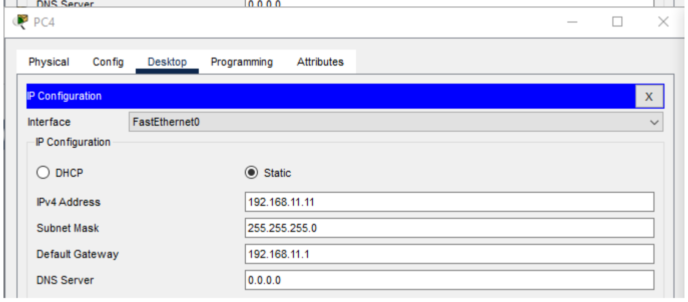
b. If the problem is resolved, indicate so in your documentation. For example, in the table above, a simple checkmark would suffice in the “Verified” column.

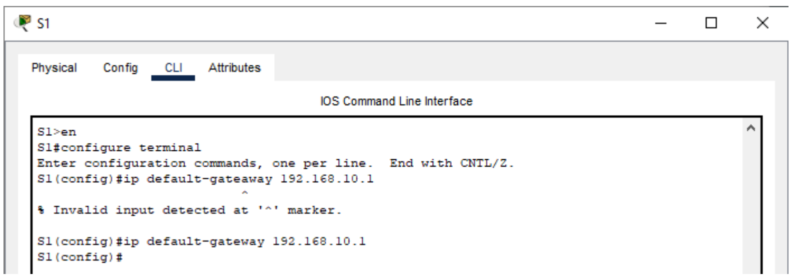
Step 3: Verify that all issues are resolved.

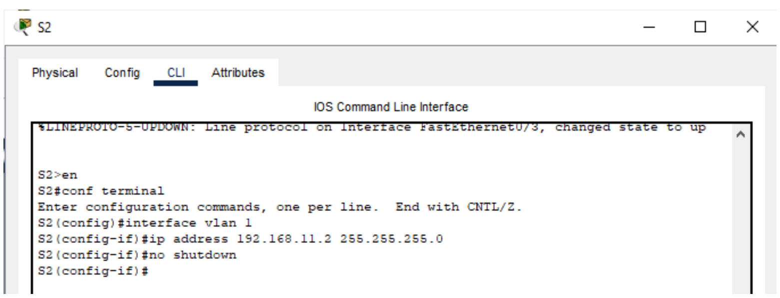
a. If you still have an outstanding issue with a solution that has not yet been implemented, return to Part 2, Step 1.

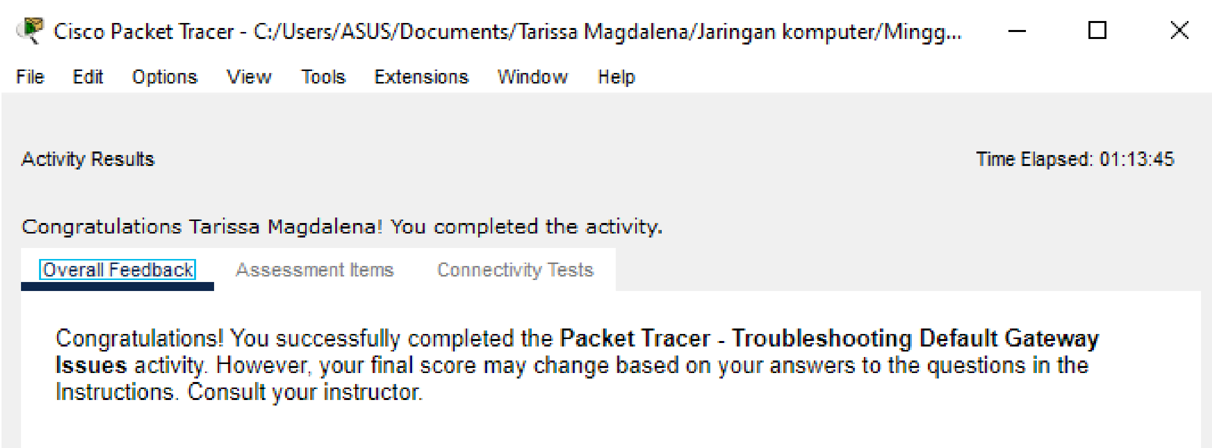
b. If all your current issues are resolved, have you also resolved any remote connectivity issues (such as can PC1 ping PC4)? If the answer is no, return to Part 1, Step 1c to test remote connectivity.


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.10.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.10.1

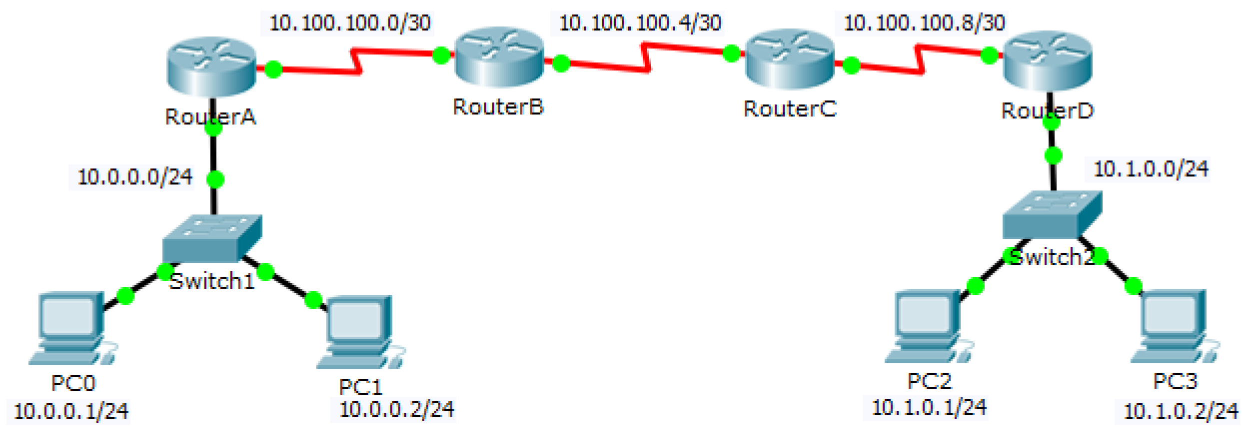

PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.11.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.11.1
DNS Server
0.0.0.0


S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1>en
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip default-gateaway 192.168.10.1
^
% Invalid input detected at '^' marker.
S1(config)#ip default-gateway 192.168.10.1
S1(config)#


S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
S2>en
S2#conf terminal
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)#


Cisco Packet Tracer - C:/Users/ASUS/Documents/Tarissa Magdalena/Jaringan komputer/Mingg...
File
Edit
Options
View
Tools
Extensions
Window
Help
Activity Results
Time Elapsed: 01:13:45
Congratulations Tarissa Magdalena! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Congratulations! You successfully completed the Packet Tracer - Troubleshooting Default Gateway Issues activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.

Packet Tracer - Testing Connectivity with Traceroute Topology



Objectives

Part 1: Test End-to-End Connectivity with the tracert Command

Part 2: Compare to the traceroute Command on a Router

Background

This activity is designed to help you troubleshoot network connectivity issues using commands to trace the route from source to destination. You are required to examine the output of **tracert** (the Windows command) and **traceroute** (the IOS command) as packets traverse the network and determine the cause of a network issue. After the issue is corrected, use the **tracert** and **traceroute** commands to verify the completion.

Part 1: Test End-to-End Connectivity with the tracert Command

Step 1: Send a ping from one end of the network to the other end.

Click **PC1** and open the **Command Prompt**. Ping **PC3** at **10.1.0.2**. What message is displayed as a result of the ping?

Answer: Destination host unreachable.

Step 2: Trace the route from PC1 to determine where in the path connectivity fails.

a. From the **Command Prompt** of **PC1**, enter the **tracert 10.1.0.2** command.

b. When you receive the **Request timed out** message, press **Ctrl**+**C**. What was the first IP address listed in the **tracert** output?

   Answer: 10.0.0.254

c. Observe the results of the **tracert** command. What is the last address reached with the **tracert** command?

   Answer: 10.100.100.6

Step 3: Correct the network problem.

a. Compare the last address reached with the **tracert** command with the network addresses listed on the topology. The furthest device from the host 10.0.0.2 with an address in the network range found is the point of failure. What devices have addresses configured for the network where the failure occurred?
Answer: Router B and Router C

b. Click **RouterC** and then the **CLI** tab. What is the status of the interfaces?

Answer: They appear to be up and active

c. Compare the IP addresses on the interfaces with the network addresses on the topology. Does there appear to be anything extraordinary?

Answer: The serial 0/0/0 interface has an incorrect IP address based on the topology.

d. Make the necessary changes to restore connectivity; however, do not change the subnets. What is solution?

Answer: Change the IP address on S 0/0/0 to 10.100.100.9/30

Step 4: Verify that end-to-end connectivity is established.

a. From the **PC1 Command Prompt**, enter the **tracert 10.1.0.2** command.

b. Observe the output from the **tracert** command. Was the command successful? Yes.

```
C:\>tracert 10.1.0.2

Tracing route to 10.1.0.2 over a maximum of 30 hops:

  1   0 ms      0 ms      1 ms      10.0.0.254
  2   0 ms      1 ms      0 ms      10.100.100.2
  3   1 ms      3 ms      3 ms      10.100.100.6
  4   11 ms     11 ms     2 ms      10.100.100.10
  5   *         4 ms      0 ms      10.1.0.2

Trace complete.

C:\>
```

Part 2: Compare to the traceroute Command on a Router

a. Click **RouterA** and then the **CLI** tab.

b. Enter the **traceroute 10.1.0.2** command. Did the command complete successfully?

Answer: Yes

```
RouterA>enable
RouterA#traceroute 10.1.0.2
Type escape sequence to abort.
Tracing the route to 10.1.0.2

  1   10.100.100.2    15 msec   1 msec    1 msec
  2   10.100.100.6    1 msec    2 msec    3 msec
  3   10.100.100.10   2 msec    2 msec    1 msec
  4   10.1.0.2        2 msec    3 msec    12 msec
RouterA#
```

c. Compare the output from the router **traceroute** command with the PC **tracert** command. What is noticeably different about the list of addresses returned?

   Answer: The router has one less IP address because it will be using RouterB as the next device along the path.

Part 3: Using Extended Traceroute

In addition to **traceroute,** Cisco IOS also includes extended traceroute. Extended traceroute allows the administrator to adjust minor traceroute operation parameters by asking simple questions.

As part of the verification process, use extended traceroute on **RouterA** to increase the number of ICMP packets traceroute sends to each hop.

Note: Windows **tracert** also allows the user to adjust a few aspects through the use of command line options.

a. Click **RouterA** and then the **CLI** tab.

b. Enter the **traceroute** and press **ENTER**. Notice that just the traceroute command should be entered.

c. Answer the questions asked by extended traceroute as follows. Extended **traceroute** should run right after the last question is answered.

```
Protocol [ip]: ip
Target IP address: 10.1.0.2
Source address: 10.100.100.1
Numeric display [n]: n
Timeout in seconds [3]: 3
Probe count [3]: 5
Minimum Time to Live [1]: 1
Maximum Time to Live [30]: 30
```

   Note: the value displayed in brackets is the default value and will be used by **traceroute** if no value is entered. Simply press **ENTER** to use the default value.

   How many questions were answered with non-default values? What was the new value?

   Answer: Probe count. The default value is 3 but the new value provided was 5

   How many ICMP packets were sent by **RouterA**?

   Answer: 5

   Note: Probe count specifies the number of ICMP packets sent to each hop by **traceroute**. A higher number of probes allows for a more accurate average round trip time for the packets.

d. Still on **RouterA**, run extended **traceroute** again but this time change the timeout value to 7 seconds.

What happened? How does the different timeout value affect **traceroute**?

Answer: The timeout parameter informs traceroute how long it should wait for a reply before declaring the hop unreachable. The default value is 3 seconds.

Can you think of a use for the timeout parameter?

Answer: if the path is too congested but still operational, it can be useful to change the timeout value to ensure traceroute waits long enough before declaring the hop unreachable.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Test End-to-End Connectivity with the **tracert** Command	Step 1	10	
	Step 2b	10	
	Step 2c	10	
	Step 3a	10	
	Step 3c	10	
	Step 3d	5	
	Step 3e	5	
	Step 4b	10	
	Part 1 Total	**80**	
Part 2: Compare to the **traceroute** Command on a Router	a	2	
	b	3	
	c	5	
	Part 2 Total	**10**	
Part 3: Extended Traceroute	a	2	
	b	3	
	c	2	
	d	3	
	Part 3 Total	**10**	
	Packet Tracer Score	**10**	
	Total Score	**100**	

