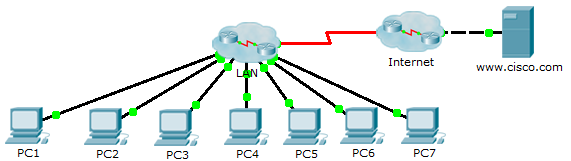
Packet Tracer – Troubleshooting Challenge - Using Documentation to Solve Issues (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

1. Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP Address | Subnet Mask | Default Gateway |
| PC1 | NIC | 10.2.15.10 | 255.255.255.0 | 10.2.15.1 |
| PC2 | NIC | 10.2.25.10 | 255.255.255.0 | 10.2.25.1 |
| PC3 | NIC | 10.2.35.10 | 255.255.255.0 | 10.2.35.1 |
| PC4 | NIC | 10.3.100.4 | 255.255.255.0 | 10.3.100.1 |
| PC5 | NIC | 10.3.100.5 | 255.255.255.0 | 10.3.100.1 |
| PC6 | NIC | 10.4.1.10 | 255.255.255.0 | 10.4.1.1 |
| PC7 | NIC | 10.5.1.10 | 255.255.255.0 | 10.5.1.1 |
| DNS Server | NIC | 10.1.100.2 | 255.255.255.0 | 10.1.100.1 |
| R1 | S0/0/0 | 10.1.0.4 | 255.255.255.248 | N/A |
| G0/0 | 10.4.1.1 | 255.255.255.0 | N/A |
| R2 | S0/0/0 | 10.1.0.3 | 255.255.255.248 | N/A |
| G0/0.100 | 10.3.100.1 | 255.255.255.0 | N/A |
| G0/0.105 | 10.3.105.1 | 255.255.255.0 | N/A |
| R3 | S0/0/0 | 10.1.0.2 | 255.255.255.248 | N/A |
| G0/0.5 | 10.2.5.1 | 255.255.255.0 | N/A |
| G0/0.15 | 10.2.15.1 | 255.255.255.0 | N/A |
| G0/0.25 | 10.2.25.1 | 255.255.255.0 | N/A |
| G0/0.35 | 10.2.35.1 | 255.255.255.0 | N/A |
| R4 | S0/0/0 | 10.1.0.5 | 255.255.255.248 | N/A |
| G0/0 | 10.5.1.1 | 255.255.255.0 | N/A |
| R5 | S0/0/0 | 10.1.0.1 | 255.255.255.248 | N/A |
| S0/0/1 | 209.165.201.2 | 255.255.255.252 | N/A |
| G0/0 | 10.1.100.1 | 255.255.255.0 | N/A |
| S1 | None | None | None | None |
| S2 | VLAN 105 | 10.3.105.21 | 255.255.255.0 | 10.3.105.1 |
| S3 | VLAN 105 | 10.3.105.22 | 255.255.255.0 | 10.3.105.1 |
| S4 | VLAN 5 | 10.2.5.21 | 255.255.255.0 | 10.2.5.1 |
| S5 | VLAN 5 | 10.2.5.23 | 255.255.255.0 | 10.2.5.1 |
| S6 | VLAN 5 | 10.2.5.22 | 255.255.255.0 | 10.2.5.1 |
| S7 | None | None | None | None |

1. Objectives

Part 1: Gather Documentation

Part 2: Test Connectivity

Part 3: Gather Data and Implement Solutions

Part 4: Test Connectivity

1. Scenario

This is Part II of a two-part activity. Part I is **Packet Tracer - Troubleshooting Challenge - Documenting the Network**, which you should have completed earlier in the chapter. In Part II, you will use your troubleshooting skills and documentation from Part I to solve connectivity issues between PCs.

1. Gather Documentation
   1. Retrieve network documentation.

To successfully complete this activity, you will need your documentation for the **Packet Tracer - Troubleshooting Challenge - Documenting the Network** activity you completed previously in this chapter. Locate that documentation now.

* 1. Documentation requirements.

The documentation you completed in the previous activity should have an accurate topology and addressing table. If necessary, update your documentation to reflect an accurate representation of a correct answer from the **Packet Tracer - Troubleshooting Challenge - Documenting the Network** activity. You may need to consult with your instructor.

**Instructor Note**: The student must have a complete and accurate picture of the answer network from the previous activity, **Packet Tracer - Troubleshooting Challenge - Documenting the Network**. You will need to either verify that the student’s previous work is correct or provide accurate documentation.

1. Test Connectivity
   1. Determine location of connectivity failure.

At the end of this activity, there should be full connectivity between PC to PC and PC to the www.cisco.pka server. However, right now you must determine where connectivity fails by pinging from:

• PCs to **www.cisco.pka** server

• PC to PC

• PC to default gateway

* 1. What pings were successful?

Document both the successful and failed pings.

None of the PCs can ping the www.cisco.pka server. PC1, PC2, and PC3 can ping each other. PC4 and PC5 can ping each other. All PCs can ping their respective default gateways.

1. Gather Data and Implement Solutions
   1. Choose a PC to begin gathering data.

Choose any PC and begin gathering data by testing connectivity to the default gateway. You can also use **traceroute** to see where connectivity fails.

* 1. Telnet to the default gateway and continue gathering data.
     1. If the PC you chose does not have connectivity to its default gateway, choose another PC to approach the problem from a different direction.
     2. After you have established connectivity through a default gateway, the login password is **cisco** and the privileged EXEC mode password is **class**.
  2. Use troubleshooting tools to verify the configuration.

At the default gateway router, use troubleshooting tools to verify the configuration with your own documentation. Remember to check switches in addition to the routers. Be sure to verify the following:

• Addressing information

• Interface activation

• Encapsulation

• Routing

• VLAN configuration

• Duplex or speed mismatches

* 1. Document network symptoms and possible solutions.

As you discover symptoms of the PC connectivity issue, add them to your documentation.

**Instructor Note**: The following is only one way the student might progress through this activity. The student can start from any PCs, except **www.cisco.pka**. For this sample answer, we started at **PC4**.

Problem 1: From **PC4**, you can access the default gateway, **R2**. Telnet to **R2** and verify the routing table. **R2** only has directly connected routes, so verify the current interface configuration using the **show protocols** or **show ip interface brief** command. Careful examination of the IP addresses will reveal that the S0/0/0 address is incorrect. It should be 10.1.0.3 instead of 10.1.100.3. The **show ip protocols** command reveals no problems with the EIGRP configuration on **R2**.

Solution 1: Configure the correct IP address for the S0/0/0 interface on **R2**.

Problem 2: After EIGRP converges on **R2**, use the **show ip route** command to gather further information about possible problems. **R2** has correct connected routes but only has two EIGRP routes. Missing routes include the four VLANs for **R3**, the **R1** LAN, and the **R4** LAN. Pinging **R3** is successful, so telnet to **R3**. Because **R2** is not receiving routes from **R3**, check the EIGRP configuration on **R3** with the **show ip protocols** command. **R3** is sending and receiving EIGRP updates and is advertising the correct network. However, automatic networks summarization is in effect. Therefore, **R3** is only sending the classful 10.0.0.0/8 network in EIGRP periodic updates.

Solution 2: Configure **R3** with the **no auto-summary** command.

Problem 3: Exit back to **R3** and check the routing table. Routes are missing for the **R1** and **R4** LANs. Test connectivity to **R1** and **R4** by ping the serial interfaces for those routers. Pings to **R1** fail but succeed to **R4**. Telnet to **R4**. On **R4**, display the routing table. **R4** has no EIGRP routes, so use **show ip protocols** command to verify EIGRP routing. The command generates no output under the Routing for Networks section, so EIGRP is either not configured correctly. Use **show run** command to check the EIGRP commands. EIGRP is missing the network command.

Solution 3: Configure **R4** with the EIGRP command, network 10.0.0.0.

Problem 4: After EIGRP converges, check the **R4** routing table. The **R1** LAN is still missing. Because the pings to **R1** fail, access **R1** from **PC6**. First, ping the default gateway address and then telnet into **R1**. Display the routing table. Notice that only the F0/0 network is in the routing table. Check the interface configuration with **show ip interface brief** command. The S0/0/0 interface is physically “up” but the data link layer is “down”. Investigate S0/0/0 with the **show interface** command. The encapsulation is set to PPP instead of Frame Relay.

Solution 4: Change the S0/0/0 interface encapsulation on R1 from PPP to Frame Relay with the **encapsulation frame-relay** command. All PCs should now be able to ping each other.

Problem 5: PCs still cannot ping the www.cisco.pka server. From any device, test connectivity and then telnet to **R5**. Investigate the interface status with the **show ip interface brief** command. The S0/0/1 interface is administratively down.

Solution 5: Activate the S0/0/1 interface on **R5** with the **no shutdown** command.

Problem 6: PCs still can’t ping the www.cisco.pka server. However, PCs can ping the DNS server. The problem is either with the **R5** configuration or the ISP configuration. Because you do not have access to the ISP router, check the configuration on **R5**. The **show run** command reveals that **R5** is using NAT. The configuration is missing the NAT statement that binds the NAT pool to the access list.

Solution 6: Configure **R5** with the **ip nat inside source list 1 pool LAN overload** command.

* 1. Make changes based on your solutions from the previous step.

1. Test Connectivity
   1. Test PC connectivity.
      1. All PCs should now be able to ping each other and the **www.cisco.pka** server. If you changed any IP configurations, create new pings because the prior pings use the old IP address.
      2. If there are still connectivity issues between PCs or PC to server, return to Part 3 and continue troubleshooting.
   2. Check results.

Your Packet Tracer score should be 70/70. If not, return to Part 2 and continue to troubleshoot and implement your suggested solutions. You will not be able to click **Check Results** and see which required components are not yet completed.

1. Suggested Scoring Rubric

|  |  |  |  |
| --- | --- | --- | --- |
| Activity Section | Question Location | Possible Points | Earned Points |
| Part 2: Test Connectivity | Step 2-a | 15 |  |
| **Part 2 Total** | | **15** |  |
| Part 3: Gather Data and Implement Solutions | Step 4-a | 15 |  |
| **Part 3 Total** | | **15** |  |
| **Packet Tracer Score** | | **70** |  |
| **Total Score** | | **100** |  |

1. Device Configs
2. Router R1

R1#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R1

enable secret class

spanning-tree mode pvst

interface Gig0/0

ip address 10.4.1.1 255.255.255.0

duplex auto

speed auto

interface Gig0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.1.0.4 255.255.255.248

encapsulation frame-relay

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

router eigrp 1

passive-interface Gig0/0

network 10.0.0.0

no auto-summary

ip classless

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

end

1. Router R2

R2#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R2

enable secret class

spanning-tree mode pvst

interface GigabitEthernet0/0

no ip address

duplex auto

speed auto

interface GigabitEthernet0/0.100

encapsulation dot1Q 100

ip address 10.3.100.1 255.255.255.0

interface GigabitEthernet0/0.105

encapsulation dot1Q 105 native

ip address 10.3.105.1 255.255.255.0

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.1.0.3 255.255.255.248

encapsulation frame-relay

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

router eigrp 1

network 10.0.0.0

no auto-summary

ip classless

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

end

1. Router R3

R3#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R3

enable secret class

spanning-tree mode pvst

interface Gig0/0

no ip address

duplex auto

speed auto

interface Gig0/0.5

encapsulation dot1Q 5 native

ip address 10.2.5.1 255.255.255.0

interface Gig0/0.15

encapsulation dot1Q 15

ip address 10.2.15.1 255.255.255.0

interface Gig0/0.25

encapsulation dot1Q 25

ip address 10.2.25.1 255.255.255.0

interface Gig0/0.35

encapsulation dot1Q 35

ip address 10.2.35.1 255.255.255.0

interface Gig0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.1.0.2 255.255.255.248

encapsulation frame-relay

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

router eigrp 1

network 10.0.0.0

no auto-summary

ip classless

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

end

1. Router R4

R4#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R4

enable secret class

spanning-tree mode pvst

interface Gig0/0

ip address 10.5.1.1 255.255.255.0

duplex auto

speed auto

interface Gig0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.1.0.5 255.255.255.248

encapsulation frame-relay

interface Serial0/0/1

no ip address

shutdown

interface Vlan1

no ip address

shutdown

router eigrp 1

passive-interface Gig0/0

network 10.0.0.0

no auto-summary

ip classless

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

end

1. Router R5

R5#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R5

enable secret class

spanning-tree mode pvst

interface Gig0/0

ip address 10.1.100.1 255.255.255.0

duplex auto

speed auto

interface Gig0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 10.1.0.1 255.255.255.248

encapsulation frame-relay

ip nat inside

interface Serial0/0/1

ip address 209.165.201.2 255.255.255.252

ip nat outside

no cdp enable

interface Vlan1

no ip address

shutdown

router eigrp 1

passive-interface Gig0/0

passive-interface Serial0/0/1

network 10.0.0.0

default-information originate

no auto-summary

ip nat pool LAN 209.165.202.128 209.165.202.159 netmask 255.255.255.224

ip nat inside source list 1 pool LAN overload

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0/0/1

access-list 1 permit 10.0.0.0 0.255.255.255

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

end

1. Router ISP

ISP#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname ISP

spanning-tree mode pvst

interface Gig0/0

ip address 209.165.200.225 255.255.255.252

duplex auto

speed auto

interface Gig0/1

no ip address

duplex auto

speed auto

shutdown

interface Serial0/0/0

ip address 209.165.201.1 255.255.255.252

clock rate 64000

interface Serial0/0/1

no ip address

interface Serial0/2/0

no ip address

interface Serial0/2/1

no ip address

interface Vlan1

no ip address

shutdown

ip classless

ip route 209.165.202.128 255.255.255.224 Serial0/0/0

no cdp run

line con 0

line aux 0

line vty 0 4

login

end

1. Switch S1

S1#sh run

hostname S1

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S2

S2#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S2

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

switchport trunk native vlan 105

switchport mode trunk

interface FastEthernet0/2

switchport trunk native vlan 105

switchport mode trunk

interface FastEthernet0/3

switchport trunk native vlan 105

switchport mode trunk

interface FastEthernet0/4

interface FastEthernet0/5

switchport access vlan 100

switchport mode access

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

interface Vlan105

ip address 10.3.105.21 255.255.255.0

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S3

S3#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S3

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

interface FastEthernet0/2

switchport trunk native vlan 105

switchport mode trunk

interface FastEthernet0/3

switchport trunk native vlan 105

switchport mode trunk

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

switchport access vlan 100

switchport mode access

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

interface Vlan105

ip address 10.3.105.22 255.255.255.0

ip default-gateway 10.3.1.1

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S4

S4#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S4

enable secret class

spanning-tree mode pvst

spanning-tree vlan 1,5,15,25,35 priority 4096

interface FastEthernet0/1

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/2

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/3

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/4

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/5

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

interface Vlan5

ip address 10.2.5.21 255.255.255.0

ip default-gateway 10.2.5.1

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S5

S5#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S5

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/2

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/3

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/4

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

interface Vlan5

ip address 10.2.5.23 255.255.255.0

ip default-gateway 10.2.5.1

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S6

S6#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S6

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/2

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/3

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/4

switchport trunk native vlan 5

switchport mode trunk

interface FastEthernet0/5

interface FastEthernet0/6

switchport access vlan 15

switchport mode access

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

switchport access vlan 25

switchport mode access

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

switchport access vlan 35

switchport mode access

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

interface Vlan5

ip address 10.2.5.22 255.255.255.0

ip default-gateway 10.2.5.1

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

end

1. Switch S7

S7#sh run

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname S7

enable secret class

spanning-tree mode pvst

interface FastEthernet0/1

interface FastEthernet0/2

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

interface FastEthernet0/6

interface FastEthernet0/7

interface FastEthernet0/8

interface FastEthernet0/9

interface FastEthernet0/10

interface FastEthernet0/11

interface FastEthernet0/12

interface FastEthernet0/13

interface FastEthernet0/14

interface FastEthernet0/15

interface FastEthernet0/16

interface FastEthernet0/17

interface FastEthernet0/18

interface FastEthernet0/19

interface FastEthernet0/20

interface FastEthernet0/21

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet1/1

interface GigabitEthernet1/2

interface Vlan1

no ip address

shutdown

line con 0

line vty 0 4

login

line vty 5 15

login

end