Experiment-12

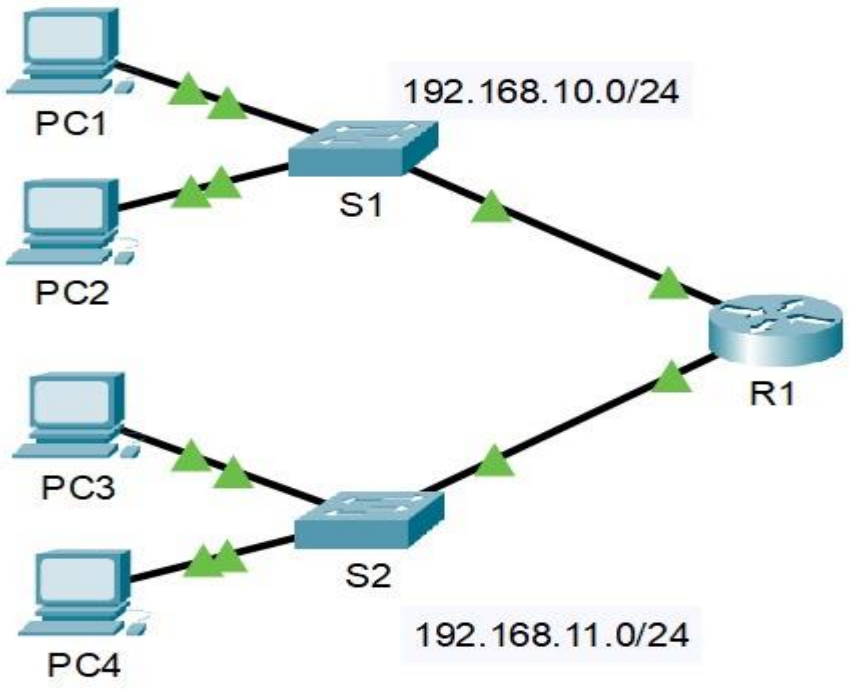
Aim-: To troubleshoot Default Gateway Issues.

Devices Used: Switches, Wires and Router.

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.

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	
S2	VLAN 1	192.168.11.2	255.255.255.0	
PC1	NIC	192.168.10.10	255.255.255.0	
PC2	NIC	192.168.10.11	255.255.255.0	
PC3	NIC	192.168.11.10	255.255.255.0	
PC4	NIC	192.168.11.11	255.255.255.0	

Procedure

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.

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.

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.

Results: Troubleshoot Default Gateway Issues has been done.

```
R1>enable
R1#show run
Building configuration...

Current configuration : 631 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO1941/K9 sn FTX1524742F
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
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
```

```
!
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
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

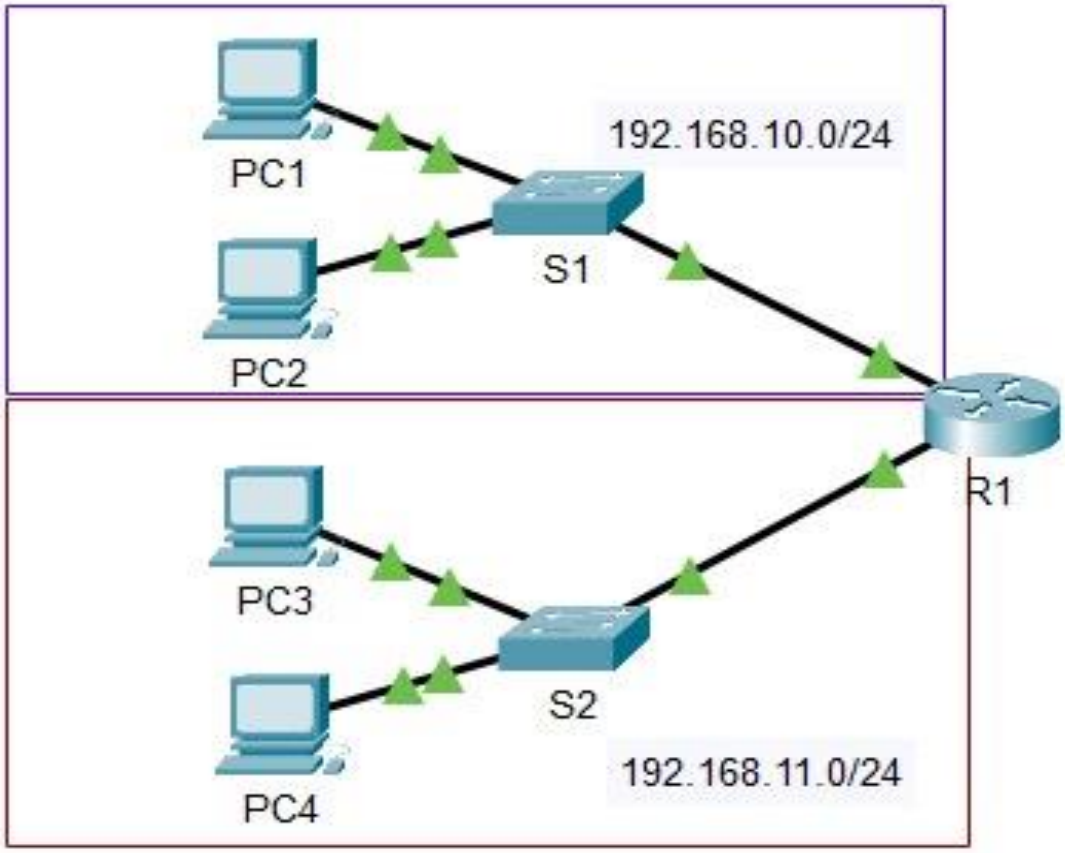
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.11.11

Pinging 192.168.11.11 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

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 = 1ms, Average = 0ms

C:\>
```

```
S1>enable
S1#show run
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
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.10.2 255.255.255.0
!
!
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


S1#
S1#
S1#
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip default-gateway 192.168.10.1
S1(config)#
```

```
S2>enable
S2#show run
Building configuration...

Current configuration : 1106 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
!
!
!
!
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
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
```

```
!
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 GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
!
ip default-gateway 192.168.11.1
!
!
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


S2#
S2#configure 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)#
```


192.168.10.0/24
PC1
PC2
S1
R1
PC3
S2
PC4
192.168.11.0/24