Packet Tracer - Troubleshoot Enterprise Network

Objectives

Part 1: Verify Switching Technologies

Part 2: Verify DHCP

Part 3: Verify Routing

Part 4: Verify WAN Technologies

Part 5: Verify Connectivity

Scenario

This activity uses a variety of technologies that you have encountered during your CCNA studies, including IPv4 routing, IPv6 routing, port security, EtherChannel, DHCP, and NAT. Your task is to review the requirements, isolate and resolve any problems, and then document the steps you took to verify the requirements.

The company replaced routers R1 and R3 to accommodate a fiber connection between the locations. Configurations from the previous routers with serial connections were modified and applied as a starting configuration. IPv6 is being tested on a small portion of the network and needs to be verified.

Note: Passwords have been removed for ease of troubleshooting in this exercise. The typical password protections should be reapplied; however, the activity will not grade those items.

Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/1	192.168.10.1 /24	N/A
R1	S0/1/0	10.1.1.1 /30	N/A
R1	G0/0/0	10.3.3.1 /30	N/A
R2	G0/0	209.165.200.225 /27	N/A
R2	G0/0	2001:db8:b:209::1/64	N/A
R2	G0/1	192.168.20.1 /30	N/A
R2	G0/1	2001:db8:b:20::1/64	N/A
R2	S0/0/0	10.1.1.2 /30	N/A
R2	G0/1/0	10.2.2.1 /30	N/A
R2	G0/1/0	2001:db8:b:10:2::1/64	N/A
R3	G0/1.30	192.168.30.1 /24	N/A
R3	G0/1.40	192.168.40.1 /24	N/A
R3	G0/1.50	192.168.50.1 /24	N/A
R3	G0/1.50	2001:db8:b:50::1/64	N/A

Device	Interface	IP Address / Prefix	Default Gateway
R3	G0/1.99	N/A	N/A
R3	G0/1/0	10.3.3.2 /30	N/A
R3	G0/2/0	10.2.2.2 /30	N/A
R3	G0/2/0	2001:db8:b:10:2::2/64	N/A
S1	VLAN10	192.168.10.2 /24	192.168.10.1
S2	VLAN11	192.168.99.2 /24	N/A
S3	VLAN30	192.168.99.3 /24	N/A
S4	VLAN30	192.168.99.4 /24	N/A
PC1	NIC	IPv4 DHCP assigned	IPv4 DHCP assigned
PC2	NIC	IPv4 DHCP assigned	IPv4 DHCP assigned
PC3	NIC	IPv4 DHCP assigned	IPv4 DHCP assigned
PC4	NIC	IPv4 DHCP assigned	IPv4 DHCP assigned
PC4	NIC	2001:db8:b:50::10/64	fe80::3
TFTP Server	NIC	192.168.20.254 /24	192.168.20.1
TFTP Server	NIC	2001:db8:b:20::254/64	fe80::2

Blank Line, No additional information

Instructions

Part 1: Verify Switching Technologies

Open configuration window

a. Port security is configured to only allow **PC1** to access **S1's** F0/3 interface. All violations should disable the interface.

Issue the command on S1 to display the current port security status.

```
S1# show port-security
```

b. Enter interface configuration mode for interface F0/3 and set up port security.

```
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
```

c. Devices in the LAN on S1 should be in VLAN 10. Display the current state of VLAN configuration.

Question:

What ports are currently assigned to VLAN 10?

F0/3, F0/4.

d. PC1 should be receiving an IP address from the router R1.

Question:

Does the PC currently have an IP address assigned?

No, there is simply an APIPA address.

e. Notice the G0/1 interface on R1 is not in the same VLAN as PC1. Change the G0/1 interface to be a member of VLAN 10 and set portfast on the interface.

```
S1(config-if)# int G0/1
```

```
S1(config-if)# switchport access vlan 10
S1(config-if)# spanning-tree portfast
```

f. Reset the interface address on PC1 from the GUI or by using the command prompt and the **ipconfig /renew** command. Does PC1 have an address? If not, recheck your steps. Test connectivity to the TFTP Server. The ping should be successful.

g. The LAN connected to R3 had an additional switch added to the topology. Link aggregation using EtherChannel is configured on **S2**, **S3**, and **S4**. The EtherChannel links should be set to trunk. The EtherChannel links should be set to form a channel without using a negotiation protocol. Issue the command on each switch to determine if the channel is working correctly.

```
S2# show etherchannel summary
<output omitted>
1      Po1(SU)           -      Fa0/1(P) Fa0/2(P)
2      Po2(SU)           -      Fa0/3(P) Fa0/4(P)
```

Question:

Were there any problems with EtherChannel?

S3 indicates Po1 is down (SD).

h. Modify S3 to include ports F0/1 and F0/2 as port channel 1.

```
S3(config)# interface range f0/1-2
S3(config-if-range)# channel-group 1 mode on
```

Check the status of the EtherChannel on S3. It should be stable now. If it is not, check the previous steps.

i. Verify the trunk status on all switches.

```
S3# show int trunk
```

Question:

Were there any issues with trunking?

On the connection G0/1 interface, S2 uses VLAN 1 as the Native VLAN.

j. Correct the trunk issues on S2.

```
S2(config)# int g0/1
S2(config-if)# switchport trunk native vlan 99
```

k. Spanning Tree should be set to PVST+ on **S2**, **S3**, and **S4**. **S2** should be configured to be the root bridge for all VLANs. Issue the command to display the spanning-tree status on S2.

```
S2# show spanning-tree summary totals
Switch is in pvst mode
Root bridge for:
```

l. The command output shows that S2 is not the root bridge for any VLANs. Correct the spanning-tree status on S2.

```
S2(config)# spanning-tree vlan 1-1005 root primary
```

m. Check the spanning-tree status on S2 to verify the changes.

```
S2# show spanning-tree summary totals
Switch is in pvst mode
Root bridge for: default V30 V40 V50 Native
```

Close configuration window

Part 2: Verify DHCP

- R1 is the DHCP server for the R1 LAN.
- R3 is the DHCP server for all 3 LANs attached to R3.

a. Check the addressing of the PCs.

Question:

Do they all have correct addressing?

No, PC3 and PC4 have incorrect gateways.

b. Check the DHCP settings on R3. Filter the output from the **show run** command to start with the DHCP configuration.

Open configuration window

```
R3# sh run | begin dhcp
ip dhcp excluded-address 192.168.30.1 192.168.30.9
ip dhcp excluded-address 192.168.40.1 192.168.40.9
ip dhcp excluded-address 192.168.50.1 192.168.50.9
!
ip dhcp pool LAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
ip dhcp pool LAN40
 network 192.168.40.0 255.255.255.0
 default-router 192.168.30.1
ip dhcp pool LAN50
 network 192.168.50.0 255.255.255.0
 default-router 192.168.30.1
```

Question:

Are there any issues with the DHCP configurations?

On LAN40 and LAN50, the router's default settings are invalid.

c. Make any necessary corrections and reset the IP addresses on the PCs. Check connectivity to all devices.

Question:

Were you able to ping all IPv4 addresses?

Internally, IPv4 connectivity for PCs 1, 2, 3, and 4 should be complete. The hosts are unable to ping outside. Part 3 will address this issue.

Close configuration window

Part 3: Verify Routing

Verify that the following requirements have been met. If not, complete the configurations.

- All routers are configured with OSPF process ID 1 and no routing updates should be sent across interfaces that do not have routers connected.
- R2 is configured with an IPv4 default route pointing to the ISP and redistributes the default route in the OSPFv2 domain.
- R2 is configured with a default IPv6 fully qualified default route point to the ISP and redistributes the default route in the OSPFv3 domain.
- NAT is configured on R2 and no untranslated addresses are permitted to cross the internet.

a. Check the routing tables on all routers.

Open configuration window

```
R3# show ip route ospf
<output omitted>
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.1.1.0 [110/649] via 10.2.2.1, 01:15:53, GigabitEthernet0/2/0
O    192.168.10.0 [110/649] via 10.3.3.1, 01:15:53, GigabitEthernet0/1/0
192.168.20.0 [110/2] via 10.2.2.1, 01:15:53, GigabitEthernet0/2/0
```

```
<output omitted>
```

Question:

Do all of the networks appear on all routers?

The routing tables include information on all networks. However, R1 and R3 are not receiving the default route, therefore R2 is the sole node with access to the outside.

b. Ping the Outside Host from R2.

Question:

Was the ping successful?

R2 must be capable of pinging the outside host.

c. Correct the default route propagation.

```
R2(config)# router ospf 1
R2(config-router)# default-information originate
```

d. Check the routing tables on R1 and R3 to make certain the default route is present.

e. Test IPv6 connectivity from R2 to Outside Host and TFTP Server. The pings should be successful. Troubleshoot if they are not.

f. Test IPv6 connectivity from R2 to PC4. If the ping fails be sure to check that the IPv6 addressing matches the Addressing Table.

g. Test IPv6 connectivity from R3 to Outside Host. If the ping fails, check the IPv6 routes on R3. Be sure to validate the default route originating from R2. If the route does not appear, modify the IPv6 OSPF configuration on R2.

```
R2(config)# ipv6 router ospf 1
R2(config-rtr)# default-information originate
```

h. Check connectivity from R2 to Outside Host. The ping should be successful.

Close configuration window

Part 4: Verify WAN Technologies

- The serial link between R1 and R2 is used as a backup link in case of failure and should only carry traffic if the fiber link is unavailable.
- The Ethernet link between R2 and R3 is a fiber connection.
- The Ethernet link between R1 and R3 is a fiber connection and should be used to forward traffic from R1.

Open configuration window

a. Take a close look at the routing table on R1.

Question:

Are there any routes using the serial link?

Yes. Instead of G0/0/0, traffic for the 192.168.20.0 network and the default route uses S0/1/0.

Use the traceroute command to verify any suspicious paths.

```
R1# traceroute 192.168.20.254
Type escape sequence to abort.
Tracing the route to 192.168.20.254

  1   10.1.1.2        1 msec    1 msec    1 msec
  2   192.168.20.254  1 msec    9 msec    0 msec
```

Notice the traffic is being sent via the S0/1/0 interface as opposed to the G0/0/0 interface.

b. The original configurations that came from the previous serial WAN connections were transferred to the new devices. Compare the G0/0/0 interface and Serial0/1/0 interface settings. Notice they both have an OSPF cost value set. Remove the OSPF cost setting from the G0/0/0 interface. It will also be necessary to remove the setting on the link on R3 that connects to R1.

```
R1(config)# int g0/0/0
R1(config-if)# no ip ospf cost 648
R3(config)# int g0/1/0
R3(config-if)# no ip ospf cost 648
```

c. Reissue the traceroute command from R1 to verify that the path has changed.

d. The change has been made to direct traffic over the faster link, however the backup route needs to be tested. Shut down the G0/2/0 interface on R3 and test connectivity to the TFTP Server and Outside Host.

Question:

Were the pings successful?

Outside Host cannot be reached, but the TFTP Server can. The absence of connectivity may have other explanations, which the students should consider. In this instance, the issue is that the Serial interface on R2's NAT setting is not set to inside.

e. R2 is required to perform NAT for all internal networks. Check the NAT translations on R2.

```
R2# show ip nat translations
```

f. Notice that the list is empty if you have only attempted to ping from R1. Attempt a ping from R3 to Outside Host and recheck the NAT translations on R2. Issue the command to display the current NAT statistics which will also provide the interfaces involved in NAT.

```
R2# show ip nat statistics
<output will vary>
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: GigabitEthernet0/1 , GigabitEthernet0/1/0
Hits: 17  Misses: 27
Expired translations: 17
Dynamic mappings:
```

g. Set the Serial 0/0/0 interface as an inside interface to translate addresses.

```
R2(config)# int s0/0/0
R2(config-if)# ip nat inside
```

h. Test connectivity to Outside Host from R1. The ping should now be successful. Re-enable the G0/2/0 interface on R3.

Close configuration window

Part 5: Verify Connectivity

- Devices should be configured according to the Addressing Table.
- Every device should be able to ping every other device internally. The internal PCs should be able to ping the Outside Host.
- PC4 should be able to ping the TFTP Server and the Outside Host using IPv6.

End of document