Packet Tracer - Resolución de problemas de redes empresariales

Charlie Delgado Peralta 20211092

Objetivos

Parte 1: Verificar las tecnologías de switching

Parte 2: Verificar DHCP

Parte 3: Verificar Routing

Parte 4: Verificar las tecnologías WAN Parte

5. Verificar la conectividad

Situación

Esta actividad aplica una variedad de tecnologías que ha visto durante sus estudios de CCNA, incluido el routing IPv4, el routing IPv6, la seguridad de puertos, EtherChannel, DHCP y NAT. Su tarea consiste en revisar los requisitos, aislar y resolver cualquier problema, y después registrar los pasos que siguió para verificar los requisitos.

La compañía reemplazó los routers R1 y R3 para acomodar una conexión de fibra entre las ubicaciones. Las configuraciones de los routers anteriores con conexiones seriales se modificaron y aplicaron como configuración inicial. IPv6 se está probando en una pequeña parte de la red y debe verificarse.

Nota: Las contraseñas se han eliminado para facilitar la solución de problemas en este ejercicio. Se deben volver a aplicar las protecciones de contraseña típicas; sin embargo, la actividad no calificará esos elementos.

Tabla de asignación de direcciones

Dispositivo	Interfaz	IP Address / Prefix	Gateway predeterminado
R1	G0/0/1	192.168.10.1 /24	N/D
	S0/1/0	10.1.1.1 /30	N/D
	G0/0/0	10.3.3.1 /30	N/D
R2	G0/0	209.165.200.225 /27	N/D
		2001:db8:b:209: :1/64	
	G0/1	192.168.20.1 /30	N/D
		2001:db8:b:20: :1/64	
	S0/0/0	10.1.1.2 /30	N/D

	G0/1/0	10.2.2.1 /30 2001:db8:b: 10:2: :1/64	N/D
R3	G0/1,30	192.168.30.1 /24	N/D
	G0/1.40	192.168.40.1 /24	N/D
Dispositivo	**Interfaz**	**IP Address / Prefix**	**Gateway predeterminado**
	G0/1.50	192.168.50.1 /24 2001:db8:b:50: :1/64	N/D
	G0/1,99	No corresponde	No corresponde
	G0/1/0	10.3.3.2 /30	N/D
	G0/2/0	10.2.2.2 /30 2001:db8:b: 10:2: :2/64	N/D
S1	VLAN10	192.168.10.2 /24	192.168.10.1
S2	VLAN11	192.168.99.2 /24	N/D
S3	VLAN30	192.168.99.3 /24	No corresponde
S4	VLAN30	192.168.99.4 /24	N/D
PC1	NIC	IPv4 DHCP asignado	IPv4 DHCP asignado
PC2	NIC	IPv4 DHCP asignado	IPv4 DHCP asignado
PC3	NIC	IPv4 DHCP asignado	IPv4 DHCP asignado
PC4	NIC	IPv4 DHCP asignado 2001:db8:b:50: :10/64	IPv4 DHCP asignado fe80::3
Servidor TFTP	NIC	192.168.20.254 /24 2001:db8:b:20: :254/64	192.168.20.1 fe80::2

Instrucciones Parte 1: Verificar tecnologías de conmutación

a. La seguridad de puerto se configura para permitir sólo **el acceso** de PC1 **a la interfaz** de F0/3 S1. Todas las violaciones deben deshabilitar la interfaz.

Ejecute el comando en S1 para mostrar el estado actual de seguridad del puerto.

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

b. Introduzca el modo de configuración de interfaz para la interfaz F0/3 y configure la seguridad del puerto.

```
S1(config-if)# switchport port-security
```

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

c. Los dispositivos de la LAN en S1 deben estar en VLAN 10. Muestre las configuraciones actuales de VLAN.

¿Qué puertos están asignados actualmente a la VLAN 10?

F0/3, F0/4

d. PC1 debería recibir una dirección IP del router R1.

¿El PC tiene actualmente asignada una dirección IP?

No

e. Observe que la interfaz G0/1 en R1 no está en la misma VLAN que PC1. Cambie la interfaz G0/1 para que sea miembro de la VLAN 10 y configure portfast en la interfaz.

```
S1 (config-if) # int G0/1
S1(config-if)# switchport access vlan 10
S1(config-if)# spanning-tree portfast
```

f. Restablezca la dirección de interfaz en PC1 desde la GUI o mediante el símbolo del sistema y el comando **ipconfig /renew** . ¿PC1 tiene una dirección? Si no es así, vuelva a comprobar los pasos. Pruebe la conectividad al servidor TFTP. El ping debería realizarse correctamente.

g. La LAN conectada a R3 tenía un switch adicional agregado a la topología. El agregado de enlaces mediante EtherChannel se configura en **S2**, **S3**, y **S4**. Los enlaces EtherChannel deben establecerse en troncal. Los enlaces EtherChannel deben configurarse para formar un canal sin utilizar un protocolo de negociación. Ejecute el comando en cada switch para determinar si el canal funciona correctamente.

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

¿Hubo algún problema con EtherChannel?

S3 muestra Po1 como caído (SD)

h. Modifique S3 para incluir los puertos F0/1 y F0/2 como canal de puerto 1.

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

Verifique el estado del EtherChannel en S3. Debería estar estable ahora. Si no es así, verifique los pasos anteriores.

i. Verifique el estado del tronco en todos los switches.

```
S3# show int trunk
```

¿Hubo algún problema con la conexión troncal?

S2 está utilizando VLAN 1 como VLAN nativa en la interfaz de enlace G0/1.

j. Corrija los problemas del tronco en S2.

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

k. El árbol de expansión debe establecerse en PVST+ en **S2**, **S3**y **S4**. **S2** debe configurarse para que sea el puente raíz para todas las VLAN. Ejecute el comando para mostrar el estado del árbol de expansión en S2.

```
S2# show spanning-tree summary totals
Switch en modo pvst
Puente de ruta para:
```

l. El resultado del comando muestra que S2 no es el puente raíz para ninguna VLAN. Corrija el estado del árbol de expansión en S2.

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

m. Compruebe el estado del árbol de expansión en S2 para verificar los cambios.

```
S2# show spanning-tree summary totals
Switch en modo pvst
Puente raíz para: predeterminado V30 V40 V50 V50 Native
```

Parte 2: Verificar DHCP

- R1 es el servidor de DHCP para las LAN del R1.
- R3 es el servidor DHCP para todas las 3 LAN conectadas a R3.

a. Compruebe el direccionamiento de las PC.

¿Todos tienen direcciones correctas?

No, PC3 y PC4 tienen puertas de enlace incorrectas

b. Compruebe la configuración de DHCP en R3. Filtre la salida del comando **show run** para comenzar con la configuración DHCP.

```
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
```

¿Hay algún problema con las configuraciones DHCP?

La configuración del router predeterminado es incorrecta en LAN40 y LAN50.

c. Realice las correcciones necesarias y restablezca las direcciones IP en las PC. Compruebe la conectividad con todos los dispositivos.

¿Pudo hacer ping a todas las direcciones IPv4?

No

Parte 3: Verificar enrutamiento.

Compruebe que se hayan cumplido los siguientes requisitos. Si no es así, complete las configuraciones.

- Todos los routers están configurados con el ID 1 del proceso OSPF y actualizaciones de enrutamiento se deben enviar a través de las interfaces que no tienen routers conectados.
- R2 se configura con una ruta predeterminada que apunte a ISP y Redistribuya la ruta predeterminada.
- R2 se configura con una ruta predeterminada IPv6 completamente calificada que apunte a ISP y redistribuya la ruta predeterminada en el dominio OSPFv3.
- NAT se configura en R2 y no se permiten que direcciones sin traducir atraviesen Internet.

a. Verifique las tablas de routing de todos los routers.

```
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] a través de 10.2.2.1, 01:15:53, GigabiteThernet0/2/0
O 192.168.10.0 [110/649] a través de 10.3.3.1, 01:15:53, GigabiteThernet0/1/0
192.168.20.0 [110/2] a través de 10.2.2.1, 01:15:53, GigabiteThernet0/2/0 <output
omitted>
```

¿Todas las redes aparecen en todos los routers?

Todas las redes están en las tablas de routing. Sin embargo, la ruta predeterminada no se propaga a R1 y R3, por lo que solo hay conectividad al exterior desde R2.

b. Hacer ping al host externo desde R2.

¿El ping se realizó correctamente?

R2 debería poder hacer ping al host externo

c. Corrija la propagación de ruta predeterminada.

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

d. Compruebe las tablas de routing en R1 y R3 para asegurarse de que la ruta predeterminada esté presente.

e. Pruebe la conectividad IPv6 desde R2 a host externo y servidor TFTP. Los pings deberían ser correctos. Solucione problemas si no lo son.

f. Pruebe la conectividad IPv6 de R2 a PC4. Si el ping falla, asegúrese de comprobar que el direccionamiento IPv6 coincide con la Tabla de direccionamiento.

g. Pruebe la conectividad IPv6 desde R3 al host externo. Si el ping falla, compruebe las rutas IPv6 en R3. Asegúrese de validar la ruta predeterminada que se origina desde R2. Si la ruta no aparece, modifique la configuración OSPF IPv6 en R2.

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

h. Compruebe la conectividad desde R2 al host externo. El ping debería realizarse correctamente.

Parte 4: Verifique las tecnologías WAN

- El enlace serie entre R1 y R2 se utiliza como enlace de copia de seguridad en caso de falla y solo debe transportar tráfico si el enlace de fibra no está disponible.
- El enlace Ethernet entre R2 y R3 es una conexión de fibra.
- El enlace Ethernet entre R1 y R3 es una conexión de fibra y debe usarse para reenviar tráfico desde R1.

a. Eche un vistazo de cerca a la tabla de routing en R1.

¿Hay alguna ruta que use el enlace serial?

Sí. El tráfico de la red 192.168.20.0 y la ruta predeterminada utilizan S0/1/0 en lugar de G0/0/0.

Utilice el comando traceroute para verificar las rutas sospechosas.

```
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 mse
```

Observe que el tráfico se envía a través de la interfaz S0/1/0 en lugar de la interfaz G0/0/0.

b. Las configuraciones originales que provenían de las conexiones WAN serie anteriores se transfirieron a los nuevos dispositivos. Compare la interfaz G0/0/0 y la configuración de interfaz Serial0/1/0. Observe que ambos tienen un valor de coste OSPF establecido. Elimine la configuración de coste OSPF de la interfaz G0/0/0. También será necesario eliminar la configuración en el enlace en R3 que se conecta a R1.

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

c. Vuelva a emitir el comando traceroute desde R1 para verificar que la ruta ha cambiado.

d. El cambio se ha realizado para dirigir el tráfico a través del enlace más rápido, sin embargo, es necesario probar la ruta de copia de seguridad. Apague la interfaz G0/2/0 en R3 y pruebe la conectividad con el servidor TFTP y el host externo.

¿Fueron correctos los pings?

Se puede acceder al servidor TFTP; sin embargo, no se puede acceder al host externo.

e. R2 es necesario para realizar NAT para todas las redes internas. Compruebe las traducciones de NAT en R2.

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

f. Observe que la lista está vacía si solo ha intentado hacer ping desde R1. Intente realizar un ping desde R3 al host externo y vuelva a comprobar las traducciones de NAT en R2. Ejecute el comando para mostrar las estadísticas NAT actuales que también proporcionarán las interfaces involucradas en 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. Establezca la interfaz Serial 0/0/0 como una interfaz interna para traducir direcciones.

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

h. Pruebe la conectividad al host externo desde R1. El ping debería ser exitoso. Vuelva a habilitar la interfaz G0/2/0 en R3.

Parte 5: Verificar la conectividad

- Los dispositivos deben configurarse de acuerdo con la tabla de asignación de direcciones.
- Todos los dispositivos deben poder enviar un comando ping a todos los demás dispositivos de manera interna. Los equipos internos deberían poder hacer ping al host externo.
- PC4 debería poder hacer ping al servidor TFTP y al host externo mediante IPv6.